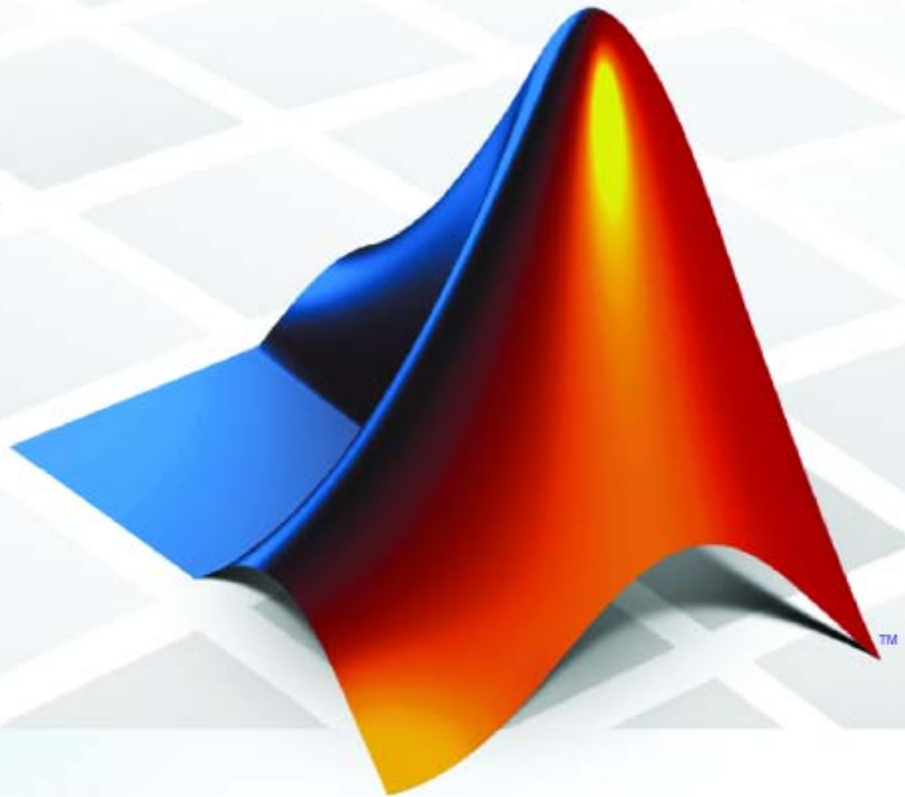


PolySpace[®] Products for C 7

User's Guide



How to Contact The MathWorks



www.mathworks.com Web
comp.soft-sys.matlab Newsgroup
www.mathworks.com/contact_TS.html Technical Support



suggest@mathworks.com Product enhancement suggestions
bugs@mathworks.com Bug reports
doc@mathworks.com Documentation error reports
service@mathworks.com Order status, license renewals, passcodes
info@mathworks.com Sales, pricing, and general information



508-647-7000 (Phone)



508-647-7001 (Fax)



The MathWorks, Inc.
3 Apple Hill Drive
Natick, MA 01760-2098

For contact information about worldwide offices, see the MathWorks Web site.

PolySpace® Products for C User's Guide

© COPYRIGHT 1999–2009 by The MathWorks, Inc.

The software described in this document is furnished under a license agreement. The software may be used or copied only under the terms of the license agreement. No part of this manual may be photocopied or reproduced in any form without prior written consent from The MathWorks, Inc.

FEDERAL ACQUISITION: This provision applies to all acquisitions of the Program and Documentation by, for, or through the federal government of the United States. By accepting delivery of the Program or Documentation, the government hereby agrees that this software or documentation qualifies as commercial computer software or commercial computer software documentation as such terms are used or defined in FAR 12.212, DFARS Part 227.72, and DFARS 252.227-7014. Accordingly, the terms and conditions of this Agreement and only those rights specified in this Agreement, shall pertain to and govern the use, modification, reproduction, release, performance, display, and disclosure of the Program and Documentation by the federal government (or other entity acquiring for or through the federal government) and shall supersede any conflicting contractual terms or conditions. If this License fails to meet the government's needs or is inconsistent in any respect with federal procurement law, the government agrees to return the Program and Documentation, unused, to The MathWorks, Inc.

Trademarks

MATLAB and Simulink are registered trademarks of The MathWorks, Inc. See www.mathworks.com/trademarks for a list of additional trademarks. Other product or brand names may be trademarks or registered trademarks of their respective holders.

Patents

The MathWorks products are protected by one or more U.S. patents. Please see www.mathworks.com/patents for more information.

Revision History

March 2008	Online Only	Revised for Version 5.1 (Release 2008a)
October 2008	Online Only	Revised for Version 6.0 (Release 2008b)
March 2009	Online Only	Revised for Version 7.0 (Release 2009a)
September 2009	Online Only	Revised for Version 7.1 (Release 2009b)

Introduction to PolySpace Products

1

Introduction to PolySpace Products	1-2
The Value of PolySpace Verification	1-2
How PolySpace Verification Works	1-4
Product Components	1-6
Installing PolySpace Products	1-6
Related Products	1-6
PolySpace Documentation	1-8
About this Guide	1-8
Related Documentation	1-8

How to Use PolySpace Software

2

PolySpace Verification and the Software Development Cycle	2-2
Software Quality and Productivity	2-2
Best Practices for Verification Workflow	2-3
Implementing a Process for PolySpace Verification ...	2-4
Overview of the PolySpace Process	2-4
Defining Quality Objectives	2-5
Defining a Verification Process to Meet Your Objectives ..	2-10
Applying Your Verification Process to Assess Code Quality	2-11
Improving Your Verification Process	2-11
Sample Workflows for PolySpace Verification	2-12
Overview of Verification Workflows	2-12
Software Developers – Standard Development Process ...	2-13
Software Developers – Rigorous Development Process ...	2-16

Quality Engineers – Code Acceptance Criteria	2-20
Quality Engineers – Certification/Qualification	2-23
Model-Based Design Users — Verifying Generated Code ..	2-25
Project Managers — Integrating PolySpace Verification with Configuration Management Tools	2-29

Setting Up a Verification Project

3

Creating a Project	3-2
What Is a Project?	3-2
Project Directories	3-3
Opening PolySpace Launcher	3-3
Specifying Default Directory	3-6
Creating New Projects	3-8
Opening Existing Projects	3-10
Specifying Source Files	3-10
Specifying Include Directories	3-13
Specifying Results Directory	3-15
Specifying Analysis Options	3-16
Configuring Text and XML Editors	3-17
Saving the Project	3-18
Specifying Options to Match Your Quality	
Objectives	3-19
Quality Objectives Overview	3-19
Choosing Contextual Verification Options	3-19
Choosing Strict or Permissive Verification Options	3-21
Choosing Coding Rules	3-23
Setting Up Project to Check Coding Rules	3-24
PolySpace MISRA Checker Overview	3-24
Checking Compliance with MISRA C Coding Rules	3-24
Creating a MISRA C Rules File	3-26
Excluding Files from the MISRA C Checking	3-28
Setting Up Project for Generic Target Processors	3-30
Project Model Files	3-30
Creating Project Model Files	3-31

Viewing Existing Generic Targets	3-31
Defining Generic Targets	3-32
Deleting a Generic Target	3-35
Common Generic Targets	3-35
Creating a Configuration File from a PolySpace Project Model File	3-36
Setting up Project to Automatically Test Orange	
Code	3-38
PolySpace Automatic Orange Tester	3-38
Enabling the Automatic Orange Tester	3-38

Emulating Your Runtime Environment

4

Setting Up a Target	4-2
Target/Compiler Overview	4-2
Specifying Target/Compilation Parameters	4-2
Predefined Target Processor Specifications (size of char, int, float, double...)	4-3
Generic Target Processors	4-5
Compiling Operating System Dependent Code (OS-target issues)	4-5
Address Alignment	4-9
Ignoring or Replacing Keywords Before Compilation	4-10
Verifying Code That Uses KEIL or IAR Dialects	4-13
How to Gather Compilation Options Efficiently	4-20
Verifying an Application Without a “Main”	4-22
Main Generator Overview	4-22
Automatically Generating a Main	4-23
Manually Generating a Main	4-23
Main Generator Assumptions	4-24
Applying Data Ranges to External Variables and Stub Functions (DRS)	4-26
Overview of Data Range Specifications (DRS)	4-26
Specifying Data Ranges	4-26
File Format	4-27

Variable Scope	4-29
Performing Efficient Module Testing with DRS	4-31
Reducing Oranges with DRS	4-32

Preparing Source Code for Verification

5

Stubbing	5-2
Stubbing Overview	5-2
Manual vs. Automatic Stubbing	5-2
Adding Precision Constraints Using Stubs	5-6
Default and Alternative Behavior for Stubbing (PURE and WORST)	5-7
Function Pointer Cases	5-10
Stubbing Functions with a Variable Argument Number ..	5-10
Finding Bugs in <code>_polyspace_stdstubs.c</code>	5-12
Preparing Code for Variables	5-14
Assigning Ranges to Variables/Assert?	5-14
Checking Properties on Global Variables at Any Point:	
Global assert	5-15
Modeling Variable Values External to my Application ...	5-15
How are Variables Initialized?	5-16
Verifying Code with Undefined or Undeclared Variables and Functions	5-18
Preparing Code for Built-in Functions	5-19
Preparing Multitasking Code	5-20
PolySpace Software Assumptions	5-20
Modelling Synchronous Tasks	5-21
Modelling Interruptions and Asynchronous	
Events/Tasks/Threads	5-23
Are Interruptions Maskable or Preemptive by Default? ...	5-25
Shared Variables	5-27
Mailboxes	5-30
Atomicity (Can an Instruction be Interrupted by Another)	5-33
Priorities	5-34

Verifying “Unsupported” Code	5-36
Ignoring Assembly Code	5-36
Dealing with Backward “goto” Statements	5-43
Types Promotion	5-45

Running a Verification

6

Types of Verification	6-2
Running Verifications on PolySpace Server	6-3
Starting Server Verification	6-3
What Happens When You Run Verification	6-4
Running Verification Unit-by-Unit	6-5
Managing Verification Jobs Using the PolySpace Queue Manager	6-7
Monitoring Progress of Server Verification	6-8
Viewing Verification Log File on Server	6-11
Stopping Server Verification Before It Completes	6-13
Removing Verification Jobs from Server Before They Run	6-14
Changing Order of Verification Jobs in Server Queue	6-15
Purging Server Queue	6-16
Changing Queue Manager Password	6-18
Sharing Server Verifications Between Users	6-18
Running Verifications on PolySpace Client	6-22
Starting Verification on Client	6-22
What Happens When You Run Verification	6-23
Monitoring the Progress of the Verification	6-24
Stopping Client Verification Before It Completes	6-25
Running Verifications from Command Line	6-27
Launching Verifications in Batch	6-27
Managing Verifications in Batch	6-27

Verification Process Failed Errors	7-2
Messages Described in This Section	7-2
Hardware Does Not Meet Requirements	7-2
You Did Not Specify the Location of Included Files	7-3
PolySpace Software Cannot Find the Server	7-4
Limit on Assignments and Function Calls	7-6
Compilation Errors	7-7
Overview	7-7
Configure a Text Editor	7-7
Examining the Compile Log	7-8
Messages Described in This Section	7-9
Syntax Error	7-9
Undeclared Identifier	7-10
No Such File or Directory	7-11
Errors Resulting from Unsupported Non-ANSI Keywords	
Such as @interrupt	7-12
Link Errors and Warnings	7-15
Overview	7-15
Function: Wrong Argument Type	7-16
Function: Wrong Argument Number	7-16
Variable: Wrong Type	7-17
Variable: Signed/Unsigned	7-17
Variable: Different Qualifier	7-18
Variable: Array Against Variable	7-18
Variable: Wrong Array Size	7-19
Missing Required Prototype for varargs	7-19
Stubbing Errors	7-21
Conflicts Between Standard Library Functions and	
PolySpace Stubs	7-21
_polyspace_stdstubs.c Compilation Errors	7-21
General Troubleshooting Approaches	7-23
Restart with the -I option	7-23
Include Files with Stubs to Replace Automatic Stubbing ..	7-24
Create a _polyspace_stdstubs.c File with Necessary	
Includes	7-25
Provide a .c file Containing a Prototype Function	7-26

Ignore _polyspace_stdstubs.c	7-27
Automatic Stub Creation Errors	7-28
Three Types of Error Messages	7-28
Function Pointer Error	7-28
Unknown Prototype Error	7-29
Parameter -entry-points Error	7-29
Viewing Error Information When Verification Stops ..	7-31
Verification Stopped Errors	7-31
Using the Log File	7-31
Log File Example	7-31
Reducing Verification Time	7-33
Factors Impacting Verification Time	7-33
Displaying Verification Status Information	7-34
Techniques for Improving Verification Performance	7-35
Turning Antivirus Software Off	7-38
Tuning PolySpace Parameters	7-38
Subdividing Code	7-39
Reducing Procedure Complexity	7-49
Reducing Task Complexity	7-50
Reducing Variable Complexity	7-50
Choosing Lower Precision	7-51
Obtaining Configuration Information	7-52
Removing Preliminary Results Files	7-54

Reviewing Verification Results

8

Before You Review PolySpace Results	8-2
Overview: Understanding PolySpace Results	8-2
Why Gray Follows Red and Green Follows Orange	8-3
The Message and What It Means	8-4
The C Explanation	8-5

Opening Verification Results	8-8
Downloading Results from Server to Client	8-8
Downloading Server Results to UNIX or Linux Clients ...	8-11
Downloading Results from Unit-by-Unit Verifications	8-12
Opening Verification Results	8-12
Exploring the Viewer Window	8-13
Selecting Viewer Mode	8-16
Setting Character Encoding Preferences	8-17
Reviewing Results in Assistant Mode	8-19
What Is Assistant Mode?	8-19
Switching to Assistant Mode	8-19
Selecting the Methodology and Criterion Level	8-20
Exploring Methodology for C	8-21
Defining a Custom Methodology	8-23
Reviewing Checks	8-24
Saving Review Comments	8-26
Reviewing Results in Expert Mode	8-27
What Is Expert Mode?	8-27
Switching to Expert Mode	8-27
Selecting a Check to Review	8-28
Displaying the Call Sequence for a Check	8-31
Displaying the Access Sequence for Variables	8-31
Tracking Review Progress	8-32
Making the Reviewed Column Visible	8-34
Filtering Checks	8-37
Types of Filters	8-37
Creating a Custom Filter	8-39
Saving Review Comments	8-40
Importing and Exporting Review Comments	8-41
Reusing Review Comments	8-41
Exporting Review Comments to Other Verification Results	8-41
Importing Review Comments from Previous Verifications	8-42
Generating Reports of Verification Results	8-44
PolySpace Report Generator Overview	8-44
Generating Verification Reports	8-45
Automatically Generating Verification Reports	8-46

Generating Excel Reports	8-47
Using PolySpace Results	8-51
Review Runtime Errors: Fix Red Errors	8-51
Red Checks Where Gray Checks were Expected	8-52
Using Range Information in the Viewer	8-54
Why Review Dead Code Checks	8-60
Reviewing Orange Checks	8-61
Integration Bug Tracking	8-62
How to Find Bugs in Unprotected Shared Data	8-63
Dataflow Verification	8-63
Data and Coding Rules	8-64
Potential Side Effect of a Red Error	8-64
Relationships Between Variables	8-65
Two Distinct Colors in a while/for Statement	8-67

Managing Orange Checks

9

Understanding Orange Checks	9-2
What is an Orange Check?	9-2
Sources of Orange Checks	9-6
Too Many Orange Checks?	9-9
Do I Have Too Many Orange Checks?	9-9
How to Manage Orange Checks	9-10
Reducing Orange Checks in Your Results	9-11
Overview: Reducing Orange Checks	9-11
Applying Coding Rules to Reduce Orange Checks	9-12
Considering Generated Code	9-17
Improving Verification Precision	9-17
Stubbing Parts of the Code Manually	9-24
Describing Multitasking Behavior Properly	9-27
Considering Contextual Verification	9-28
Reviewing Orange Checks	9-29
Overview: Reviewing Orange Checks	9-29
Defining Your Review Methodology	9-29

Performing Selective Orange Review	9-31
Importing Review Comments from Previous Verifications	9-33
Performing an Exhaustive Orange Review	9-34
Automatically Testing Orange Code	9-38
Automatic Orange Tester Overview	9-38
Before Using the Automatic Orange Tester	9-41
Launching the Automatic Orange Tester	9-43
Reviewing the Test Results	9-47
Refining Data Ranges	9-51
Saving and Reusing Your Configuration	9-55
Exporting Data Ranges for PolySpace Verification	9-56
Configuring Compiler Options	9-57
Technical Limitations	9-58

Day to Day Use

10

PolySpace In One Click Overview	10-2
Using PolySpace In One Click	10-3
PolySpace In One Click Workflow	10-3
Setting the Active Project	10-3
Launching Verification	10-5
Using the Taskbar Icon	10-8

MISRA Checker

11

PolySpace MISRA Checker Overview	11-2
Setting Up MISRA C Checking	11-4
Checking Compliance with MISRA C Coding Rules	11-4
Creating a MISRA C Rules File	11-5
Excluding Files from the MISRA C Checking	11-7

Configuring Text and XML Editors	11-8
Running a Verification with MISRA C Checking	11-10
Starting the Verification	11-10
Examining the MISRA C Log	11-11
Opening MISRA-C Report	11-12
Rules Supported	11-14
Language Extensions	11-15
Character Sets	11-15
Identifiers	11-15
Types	11-17
Constants	11-17
Declarations and Definitions	11-18
Initialization	11-20
Arithmetic Type Conversion	11-20
Pointer Type Conversion	11-24
Expressions	11-25
Control Statement Expressions	11-28
Control Flow	11-29
Switch Statements	11-31
Functions	11-32
Pointers and Arrays	11-33
Structures and Unions	11-33
Preprocessing Directives	11-34
Standard Libraries	11-37
runtime Failures	11-39
Rules Partially Supported	11-40
Environment	11-40
Language Extension	11-41
Declarations and Definitions	11-42
Expressions	11-43
Control Statement Expressions	11-44
Control Flow	11-46
Functions	11-47
Pointers and Arrays	11-47
Preprocessing Directives	11-48
Rules Not Checked	11-51
Environment	11-51
Language Extensions	11-52

Documentation	11-52
Types	11-53
Functions	11-54
Pointers and Arrays	11-54
Structures and Unions	11-55
Standard Libraries	11-55

Using PolySpace Software in the Eclipse IDE

12

Verifying Code in the Eclipse IDE	12-2
Creating an Eclipse Project	12-3
Setting Up PolySpace Verification with Eclipse Editor ...	12-4
Launching Verification from Eclipse Editor	12-5
Reviewing Verification Results from Eclipse Editor	12-5
Using the PolySpace Spooler	12-6

Glossary

Index

Introduction to PolySpace Products

- “Introduction to PolySpace Products” on page 1-2
- “PolySpace Documentation” on page 1-8

Introduction to PolySpace Products

In this section...
“The Value of PolySpace Verification” on page 1-2
“How PolySpace Verification Works” on page 1-4
“Product Components” on page 1-6
“Installing PolySpace Products” on page 1-6
“Related Products” on page 1-6

The Value of PolySpace Verification

PolySpace® products verify C, C++, and Ada code by detecting run-time errors before code is compiled and executed. PolySpace verification uses formal methods not only to detect errors, but to prove mathematically that certain classes of run-time errors do not exist.

PolySpace verification can help you to:

- “Ensure Software Reliability” on page 1-2
- “Decrease Development Time” on page 1-3
- “Improve the Development Process” on page 1-4

Ensure Software Reliability

PolySpace software ensures the reliability of your C applications by proving code correctness and identifying run-time errors. Using advanced verification techniques, PolySpace software performs an exhaustive verification of your source code.

Because PolySpace software verifies all possible executions of your code, it can identify code that:

- Never has an error
- Always has an error
- Is unreachable

- Might have an error

With this information, you can be confident that you know how much of your code is run-time error free, and you can improve the reliability of your code by fixing the errors.

You can also improve the quality of your code by using PolySpace verification software to check that your code complies with MISRA C® standards.¹

Decrease Development Time

PolySpace software reduces development time by automating the verification process and helping you to efficiently review verification results. You can use it at any point in the development process, but using it during early coding phases allows you to find errors when it is less costly to fix them.

You use PolySpace software to verify C source code before compile time. To verify the source code, you set up verification parameters in a project, run the verification, and review the results. This process takes significantly less time than using manual methods or using tools that require you to modify code or run test cases.

A graphical user interface helps you to efficiently review verification results. Results are color-coded:

- **Green** – Indicates code that never has an error.
- **Red** – Indicates code that always has an error.
- **Gray** – Indicates unreachable code.
- **Orange** – Indicates unproven code (code that might have an error).

The color-coding helps you to quickly identify errors. You will spend less time debugging because you can see the exact location of an error in the source code. After you fix errors, you can easily run the verification again.

1. MISRA and MISRA C are registered trademarks of MISRA Ltd., held on behalf of the MISRA Consortium.

Using PolySpace verification software helps you to use your time effectively. Because you know which parts of your code are error-free, you can focus on the code that has definite errors or might have errors.

Reviewing the code that might have errors (orange code) can be time-consuming, but PolySpace software helps you with the review process. You can use filters to focus on certain types of errors or you can allow the software to identify the code that you should review.

Improve the Development Process

PolySpace software makes it easy to share verification parameters and results, allowing the development team to work together to improve product reliability. Once verification parameters have been set up, developers can reuse them for other files in the same application.

PolySpace verification software supports code verification throughout the development process:

- An individual developer can find and fix run-time errors during the initial coding phase.
- Quality assurance can check overall reliability of an application.
- Managers can monitor application reliability by generating reports from the verification results.

How PolySpace Verification Works

PolySpace software uses *static verification* to prove the absence of runtime errors. Static verification derives the dynamic properties of a program without actually executing it. This differs significantly from other techniques, such as runtime debugging, in that the verification it provides is not based on a given test case or set of test cases. The dynamic properties obtained in the PolySpace verification are true for all executions of the software.

What is Static Verification

Static Verification is a broad term, and is applicable to any tool which derives dynamic properties of a program without actually executing it. However, most Static Verification tools only verify the complexity of the software, in a search for constructs which may be potentially dangerous. PolySpace verification

provides deep-level verification identifying almost all runtime errors and possible access conflicts on global shared data.

PolySpace verification works by approximating the software under verification, using safe and representative approximations of software operations and data.

For example, consider the following code:

```
for (i=0 ; i<1000 ; ++i)
{
    tab[i] = foo(i);
}
```

To check that the variable 'i' never overflows the range of 'tab' a traditional approach would be to enumerate each possible value of 'i'. One thousand checks would be needed.

Using the static verification approach, the variable 'i' is modelled by its variation domain. For instance the model of 'i' is that it belongs to the [0..999] static interval. (Depending on the complexity of the data, convex polyhedrons, integer lattices and more elaborated models are also used for this purpose).

Any approximation leads by definition to information loss. For instance, the information that 'i' is incremented by one every cycle in the loop is lost. However the important fact is that this information is not required to ensure that no range error will occur; it is only necessary to prove that the variation domain of 'i' is smaller than the range of 'tab'. Only one check is required to establish that - and hence the gain in efficiency compared to traditional approaches.

Static code verification has an exact solution but it is generally not practical, as it would in general require the enumeration of all possible test cases. As a result, approximation is required if a usable tool is to result.

Exhaustiveness

Nothing is lost in terms of exhaustiveness. The reason is that PolySpace verification works by performing upper approximations. In other words, the computed variation domain of any program variable is always a superset of its actual variation domain. The direct consequence is that no runtime error (RTE) item to be checked can be missed by PolySpace verification.

Product Components

The PolySpace products for verifying C code are combined with the PolySpace products for verifying C++ code. These products are:

- “PolySpace® Client for C/C++ Software” on page 1-6
- “PolySpace® Server for C/C++ Software” on page 1-6

PolySpace Client for C/C++ Software

PolySpace® Client™ for C/C++ software is the management and visualization tool of PolySpace products. You use it to submit jobs for execution by PolySpace Server, and to review verification results. The PolySpace client software includes the Viewer, DRS, MISRA C Checker, Report Generator, and Automatic Orange Tester features.

PolySpace client software is typically installed on developer workstations that will send verification jobs to the PolySpace server.

PolySpace Server for C/C++ Software

PolySpace® Server™ for C/C++ software is the computational engine of PolySpace products. You use it to run jobs posted by PolySpace clients, and to manage multiple servers and queues. The PolySpace Server software includes the Remote Launcher, Report Generator, DRS, and HTML Generator features.

PolySpace server software is typically installed on machines dedicated to PolySpace software that will receive verifications coming from PolySpace clients.

Installing PolySpace Products

For information on installing and licensing PolySpace products, refer to the *PolySpace Installation Guide*.

Related Products

- “PolySpace Products for Verifying C++ Code” on page 1-7
- “PolySpace Products for Verifying Ada Code” on page 1-7

- “PolySpace Products for Linking to Models” on page 1-7

PolySpace Products for Verifying C++ Code

For information about PolySpace products that verify C++ code, see the following:

<http://www.mathworks.com/products/polyspaceclientc/>

<http://www.mathworks.com/products/polyspaceserverc/>

PolySpace Products for Verifying Ada Code

For information about PolySpace products that verify Ada code, see the following:

<http://www.mathworks.com/products/polyspaceclientada/>

<http://www.mathworks.com/products/polyspaceserverada/>

PolySpace Products for Linking to Models

For information about PolySpace products that link to models, see the following:

<http://www.mathworks.com/products/polyspacemodelsl/>

<http://www.mathworks.com/products/polyspaceumlrh/>

PolySpace Documentation

In this section...
“About this Guide” on page 1-8
“Related Documentation” on page 1-8

About this Guide

This document describes how to use PolySpace software to verify C code, and provides detailed procedures for common tasks. It covers both PolySpace Client for C/C++ and PolySpace Server for C/C++ products.

This guide is intended for both novice and experienced users.

Related Documentation

In addition to this guide, the following related documents are shipped with the software:

- ***PolySpace Products for C Getting Started Guide*** – Provides a basic workflow and step-by-step procedures for verifying C code using PolySpace software, to help you quickly learn how to use the software.
- ***PolySpace Products for C Reference*** – Provides detailed descriptions of all PolySpace options, as well as all checks reported in the PolySpace results.
- ***PolySpace Installation Guide*** – Describes how to install and license PolySpace products.
- ***PolySpace Release Notes*** – Describes new features, bug fixes, and upgrade issues.

You can access these guides from the **Help** menu, or by clicking the Help icon in the PolySpace window.

To access the online documentation for PolySpace products, go to:

[/www.mathworks.com/access/helpdesk/help/toolbox/polyspace/polyspace.html](http://www.mathworks.com/access/helpdesk/help/toolbox/polyspace/polyspace.html)

The MathWorks Online

For additional information and support, see:

www.mathworks.com/products/polyspace

How to Use PolySpace Software

- “PolySpace Verification and the Software Development Cycle” on page 2-2
- “Implementing a Process for PolySpace Verification” on page 2-4
- “Sample Workflows for PolySpace Verification” on page 2-12

PolySpace Verification and the Software Development Cycle

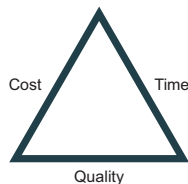
In this section...

“Software Quality and Productivity” on page 2-2

“Best Practices for Verification Workflow” on page 2-3

Software Quality and Productivity

The goal of most software development teams is to maximize both quality and productivity. However, when developing software, there are always three related variables: cost, quality, and time.



Changing the requirements for one of these variables always impacts the other two.

Generally, the criticality of your application determines the balance between these three variables – your quality model. With classical testing processes, development teams generally try to achieve their quality model by testing all modules in an application until each meets the required quality level. Unfortunately, this process often ends before quality objectives are met, because the available time or budget has been exhausted.

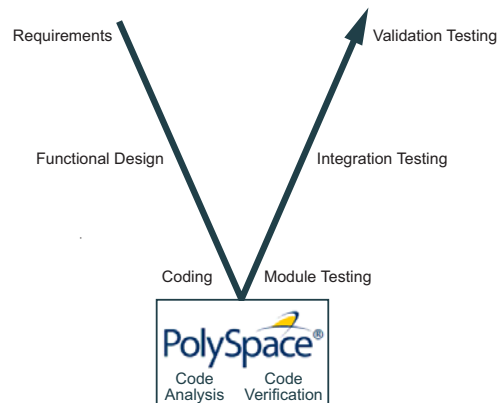
PolySpace verification allows a different process. PolySpace verification can support both productivity improvement and quality improvement at the same time, although there is always a balance between these goals.

To achieve maximum quality and productivity, however, you cannot simply perform code verification at the end of the development process. You must integrate verification into your development process, in a way that respects time and cost restrictions.

This chapter describes how to integrate PolySpace verification into your software development cycle. It explains both how to use PolySpace verification in your current development process, and how to change your process to get more out of verification.

Best Practices for Verification Workflow

PolySpace verification can be used throughout the software development cycle. However, to maximize both quality and productivity, the most efficient time to use it is early in the development cycle.



PolySpace Verification in the Development Cycle

Typically, verification is conducted in two stages. First, you verify code as it is written, to check coding rules and quickly identify any obvious defects. Once the code is stable, you verify it again before module/unit testing, with more stringent verification and review criteria.

Using verification at this stage of the development cycle improves both quality and productivity, because it allows you to find and manage defects soon after the code is written. This saves time because each developer is familiar with their own code, and can quickly determine why code cannot be proven safe. In addition, defects are cheaper to fix at this stage, since they can be addressed before the code is integrated into a larger system.

Implementing a Process for PolySpace Verification

In this section...
“Overview of the PolySpace Process” on page 2-4
“Defining Quality Objectives” on page 2-5
“Defining a Verification Process to Meet Your Objectives” on page 2-10
“Applying Your Verification Process to Assess Code Quality” on page 2-11
“Improving Your Verification Process” on page 2-11

Overview of the PolySpace Process

PolySpace verification cannot magically produce quality code at the end of the development process. Verification is a tool that helps you measure the quality of your code, identify issues, and ultimately achieve your own quality goals. To do this, however, you must integrate PolySpace verification into your development process.

To successfully implement polyspace verification within your development process, you must perform each of the following steps:

- 1** Define your quality objectives.
- 2** Define a process to match your quality objectives.
- 3** Apply the process to assess the quality of your code.
- 4** Improve the process.

Defining Quality Objectives

Before you can verify whether your code meets your quality goals, you must define those goals. Therefore, the first step in implementing a verification process is to define your quality objectives.

This process involves:

- “Choosing Robustness or Contextual Verification” on page 2-5
- “Choosing Coding Rules” on page 2-6
- “Choosing Strict or Permissive Verification Objectives” on page 2-7
- “Defining Software Quality Levels” on page 2-8

Choosing Robustness or Contextual Verification

Before using PolySpace products to verify your code, you must decide what type of software verification you want to perform. There are two approaches to code verification that result in slightly different workflows:

- **Robustness Verification** – Prove software works under all conditions.
- **Contextual Verification** – Prove software works under normal working conditions.

Note Some verification processes may incorporate both robustness and contextual verification. For example, developers may perform robustness verification on individual files early in the development cycle, while writing the code. Later, the team may perform contextual verification on larger software components.

Robustness Verification. Robustness verification proves that the software works under all conditions, including “abnormal” conditions for which it was not designed. This can be thought of as “worst case” verification.

By default, PolySpace software assumes you want to perform robustness verification. In a robustness verification, PolySpace software:

- Assumes function inputs are full range

- Initializes global variables to full range
- Automatically stubs missing functions

While this approach ensures that the software works under all conditions, it can lead to *orange checks* (unproven code) in your results. You must then manually inspect these orange checks in accordance with your software quality objectives.

Contextual Verification. Contextual verification proves that the software works under predefined working conditions. This limits the scope of the verification to specific variable ranges, and verifies the code within these ranges.

When performing contextual verification, you use PolySpace options to reduce the number of orange checks. For example, you can:

- Use Data Range Specifications (DRS) to specify the ranges for your variables, thereby limiting the verification to these cases. For more information, see “Applying Data Ranges to External Variables and Stub Functions (DRS)” on page 4-26.
- Create a detailed main program to model the call sequence, instead of using the default main generator. For more information, see “Verifying an Application Without a “Main”” on page 4-22.
- Provide manual stubs that emulate the behavior of missing functions, instead of using the default automatic stubs. For more information, see “Stubbing” on page 5-2.

Choosing Coding Rules

Coding rules are one of the most efficient means to improve both the quality of your code, and the quality of your verification results.

If your development team observes certain coding rules, the number of orange checks (unproven code) in your verification results will be reduced substantially. This means that there is less to review, and that the remaining checks are more likely to represent actual bugs. This can make the cost of bug detection much lower.

PolySpace software can check that your code complies with specified coding rules. Before starting code verification, you should consider implementing coding rules, and choose which rules to enforce.

For more information, see Chapter 11, “MISRA Checker”.

Choosing Strict or Permissive Verification Objectives

While defining the quality objectives for your application, you should determine which of these options you want to use.

Options that make verification more strict include:

- **-detect-unsigned-overflow** – Verification is more strict with overflowing computations on unsigned integers.
- **-no-def-init-glob** – Verification treats all global variables as non-initialized, therefore causing a red error if they are read before they are written to.
- **-wall** – Specifies that all C compliance warnings are written to the log file during compilation.

Options that make verification more permissive include:

- **-allow-ptr-arith-on-struct** – Enables navigation within a structure or union from one field to another.
- **-allow-negative-operand-in-shift** – Verification allows a shift operation on a negative number.
- **-ignore-constant-overflow** – Verification is permissive with overflowing computations on constants.
- **-allow-non-int-bitfields** – Allows you to define types of bitfields other than signed or unsigned int.
- **-allow-undef-variables** – Verification does not stop due to errors caused by undefined global variables.
- **-allow-unnamed-fields** – Verification does not stop due to errors caused by unnamed fields in structures.

- **-dialect** – Verification allows syntax associated with the IAR and Keil dialects.

For more information on these options, see “Option Descriptions” in the *PolySpace Products for C Reference*.

Defining Software Quality Levels

The software quality level you define determines which PolySpace options you use, and which results you must review.

You define the quality levels appropriate for your application, from level QL-1 (lowest) to level QL-4 (highest). Each quality level consists of a set of software quality criteria that represent a certain quality threshold. For example:

Software Quality Levels

Criteria	Software Quality Levels			
	QL1	QL2	QL3	QL4
Document static information	X	X	X	X
Enforce coding rules with direct impact on selectivity	X	X	X	X
Review all red checks	X	X	X	X
Review all gray checks	X	X	X	X
Review first criteria level for orange checks		X	X	X
Review second criteria level for orange checks			X	X
Enforce coding rules with indirect impact on selectivity			X	X
Perform dataflow analysis			X	X
Review third criteria level for orange checks				X

You define the quality criteria appropriate for your application. In the example above, the quality criteria include:

- **Static Information** – Includes information about the application architecture, the structure of each module, and all files. This information must be documented to ensure that your application is fully verified.
- **Coding rules** – PolySpace software can check that your code complies with specified coding rules. The section “Applying Coding Rules to Reduce Orange Checks” on page 9-12 defines two sets of coding rules – a first set with direct impact on the selectivity of the verification, and a second set with indirect impact on selectivity.
- **Red checks** – Represent errors that occur every time the code is executed.
- **Gray checks** – Represent unreachable code.
- **Orange checks** – Indicate unproven code, meaning a run-time error may occur. PolySpace software allows you to define three criteria levels for reviewing orange checks in the PolySpace Viewer. For more information, see “Reviewing Results in Assistant Mode” on page 8-19.
- **Dataflow analysis** – Identifies errors such as non-initialized variables and variables that are written but never read. This can include inspection of:
 - Application call tree
 - Read/write accesses to global variables
 - Shared variables and their associated concurrent access protection

Defining a Verification Process to Meet Your Objectives

Once you have defined your quality objectives, you must define a process that allows you to meet those objectives. Defining the process involves actions both within and outside PolySpace software.

These actions include:

- Setting standards for code development, such as coding rules.
- Setting PolySpace Analysis options to match your quality objectives. See “Creating a Project” on page 3-2.
- Setting review criteria in the PolySpace Viewer to ensure results are reviewed consistently. See “Defining a Custom Methodology” on page 8-23.

Applying Your Verification Process to Assess Code Quality

Once you have defined a process that meets your quality objectives, it is up to your development team to apply it consistently to all software components.

This process includes:

- 1** Launching PolySpace verification on each software component as it is written. See “Using PolySpace In One Click” on page 10-3.
- 2** Reviewing verification results consistently. See “Reviewing Results in Assistant Mode” on page 8-19.
- 3** Saving review comments for each component, so they are available for future review. See “Importing Review Comments from Previous Verifications” on page 9-33.
- 4** Performing additional verifications on each component, as defined by your quality objectives.

Improving Your Verification Process

Once you review initial verification results, you can assess both the overall quality of your code, and how well the process meets your requirements for software quality, development time, and cost restrictions.

Based on these factors, you may want to take actions to modify your process. These actions may include:

- Reassessing your quality objectives.
- Changing your development process to produce code that is easier to verify.
- Changing PolySpace analysis options to improve the precision of the verification.
- Changing PolySpace options to change how verification results are reported.

For more information, see Chapter 9, “Managing Orange Checks”.

Sample Workflows for PolySpace Verification

In this section...
“Overview of Verification Workflows” on page 2-12
“Software Developers – Standard Development Process” on page 2-13
“Software Developers – Rigorous Development Process” on page 2-16
“Quality Engineers – Code Acceptance Criteria” on page 2-20
“Quality Engineers – Certification/Qualification” on page 2-23
“Model-Based Design Users — Verifying Generated Code” on page 2-25
“Project Managers — Integrating PolySpace Verification with Configuration Management Tools” on page 2-29

Overview of Verification Workflows

PolySpace verification supports two objectives at the same time:

- Reducing the cost of testing and validation
- Improving software quality

You can use PolySpace verification in different ways depending on your development context and quality model. The primary difference being how you exploit verification results.

This section provides sample workflows that show how to use PolySpace verification in a variety of development contexts.

Software Developers – Standard Development Process

User Description

This workflow applies to software developers using a standard development process. Before implementing PolySpace verification, these users fit the following criteria:

- In Ada, no unit test tools or coverage tools are used – functional tests are performed just after coding.
- In C, either no coding rules are used, or rules are not followed consistently.

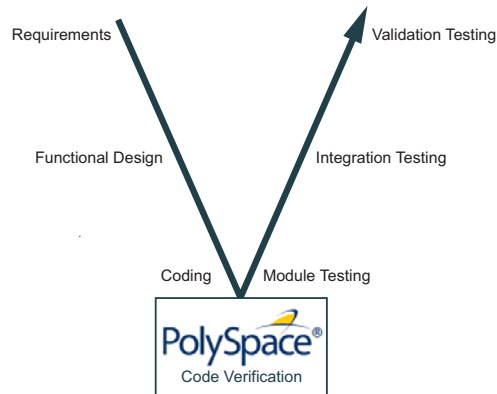
Quality Objectives

The main goal of PolySpace verification is to improve productivity while maintaining or improving software quality. Verification helps developers find and fix bugs more quickly than other processes. It also improves software quality by identifying bugs that otherwise might remain in the software.

In this process, the goal is not to completely prove the absence of errors. The goal is to deliver code of equal or better quality than other processes, while optimizing productivity to ensure a predictable time frame with minimal delays and costs.

Verification Workflow

This process involves file-by-file verification immediately after coding, and again just before functional testing.



The verification workflow consists of the following steps:

- 1 The project leader configures a PolySpace project to perform robustness verification, using default PolySpace options.

Note This means that verification uses the automatically generated “main” function. This main will call all unused procedures and functions with full range parameters.

- 2 Each developer performs file-by-file verification as they write code, and reviews verification results.
- 3 The developer fixes all **red** errors and examines **gray** code identified by the verification.
- 4 The developer repeats steps 2 and 3 as needed, while completing the code.
- 5 Once a developer considers a file complete, they perform a final verification.
- 6 The developer fixes any **red** errors, examines **gray** code, and performs a selective orange review.

Note The goal of the selective orange review is to find as many bugs as possible within a limited period of time.

Using this approach, it is possible that some bugs may remain in unchecked oranges. However, the verification process represents a significant improvement from the previous process.

Costs and Benefits

When using verification to detect bugs:

- **Red and gray checks** – The number of bugs found in red and gray checks varies, but approximately 40% of verifications reveal one or more red errors or bugs in gray code.
- **Orange checks** – The time required to find one bug varies from 5 minutes to 1 hour, and is typically around 30 minutes. This represents an average of two minutes per orange check review, and a total of 20 orange checks per package in Ada and 60 orange checks per file in C.

Disadvantages to this approach:

- **Setup time** – the time needed to set up your verification will be higher if you do not use coding rules. You may need to make modifications to the code before launching verification.

Software Developers – Rigorous Development Process

User Description

This workflow applies to software developers and test engineers working within development groups. These users are often developing software for embedded systems, and typically use coding rules.

These users typically want to find bugs early in the development cycle using a tool that is fast and iterative.

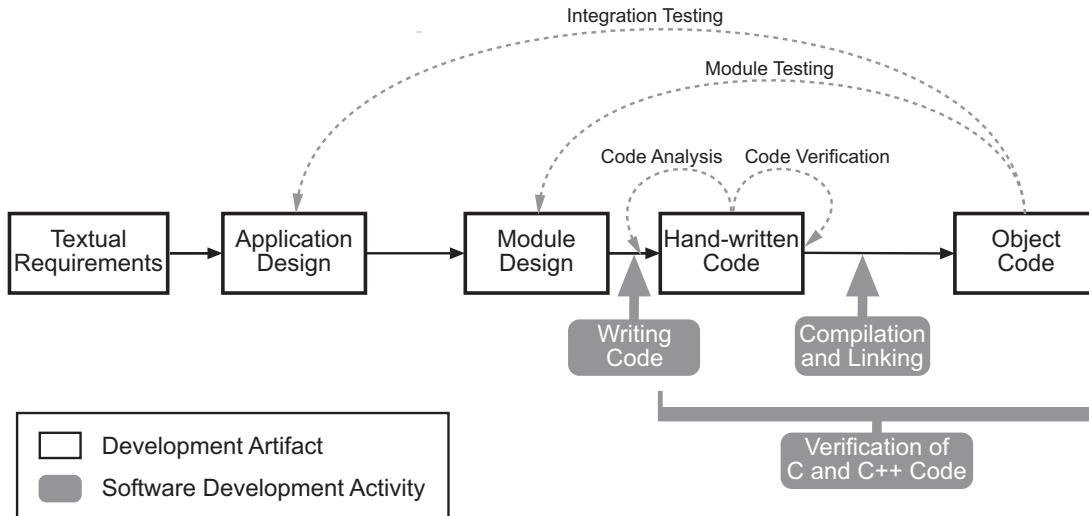
Quality Objectives

The goal of PolySpace verification is to improve software quality with equal or increased productivity.

Verification can prove the absence of runtime errors, while helping developers find and fix any bugs more quickly than other processes.

Verification Workflow

This process involves both code analysis and code verification during the coding phase, and thorough review of verification results before module testing. It may also involve integration analysis before integration testing.



Workflow for Code Verification

Note Solid arrows in the figure indicate the progression of software development activities.

The verification workflow consists of the following steps:

- 1 The project leader configures a PolySpace project to perform contextual verification. This involves:
 - Using Data Range Specifications (DRS) to define initialization ranges for input data. For example, if a variable “x” is read by functions in the file, and if x can be initialized to any value between 1 and 10, this information should be included in the DRS file.
 - Creates a “main” program to model call sequence, instead of using the automatically generated main.
 - Sets options to check the properties of some output variables. For example, if a variable “y” is returned by a function in the file and should always be returned with a value in the range 1 to 100, then PolySpace can flag instances where that range of values might be breached.

- 2 The project leader configures the project to check appropriate coding rules.
- 3 Each developer performs file-by-file verification as they write code, and reviews both coding rule violations and verification results.
- 4 The developer fixes any coding rule violations, fixes all **red** errors, examines **gray** code, and performs a selective orange review.
- 5 The developer repeats steps 2 and 3 as needed, while completing the code.
- 6 Once a developer considers a file complete, they perform a final verification.
- 7 The developer performs an exhaustive orange review on the remaining orange checks.

Note The goal of the exhaustive orange review is to examine all orange checks that were not reviewed as part of previous reviews. This is possible when using coding rules because the total number of orange checks is reduced, and the remaining orange checks are likely to reveal problems with the code.

Optionally, an additional verification can be performed during the integration phase. The purpose of this additional verification is to track integration bugs, and review:

- Red and gray integration checks;
- The remaining orange checks with a selective review: *Integration bug tracking*.

Costs and Benefits

With this approach, PolySpace verification typically provides the following benefits:

- 3–5 orange and 3 gray checks per file, yielding an average of 1 bug. Often, 2 of the orange checks represent the same bug, and another represent an anomaly.

- Typically, each file requires two verifications before it can be checked-in to the configuration management system.
- The average verification time is about 15 minutes.

Note If the development process includes data rules that determine the data flow design, the benefits might be greater. Using data rules reduces the potential of verification finding integration bugs.

If performing the optional verification to find integration bugs, you may see the following results. On a typical 50,000 line project:

- A selective orange review may reveal **one integration bug per hour** of code review.
- Selective orange review takes about 6 hours to complete. This is long enough to review orange checks throughout the whole application. This represents a step towards an exhaustive orange check review. However, spending more time is unlikely to be efficient, and will not guarantee that no bugs remain.
- An exhaustive orange review takes between 4 and 6 days, assuming that 50,000 lines of code contains approximately 400–800 orange checks.

Quality Engineers – Code Acceptance Criteria

User Description

This workflow applies to quality engineers who work outside of software development groups, and are responsible for independent verification of software quality and adherence to standards.

These users generally receive code late in the development cycle, and may even be verifying code that is written by outside suppliers or other external companies. They are concerned with not just detecting bugs, but measuring quality over time, and developing processes to measure, control, and improve product quality going forward.

Quality Objectives

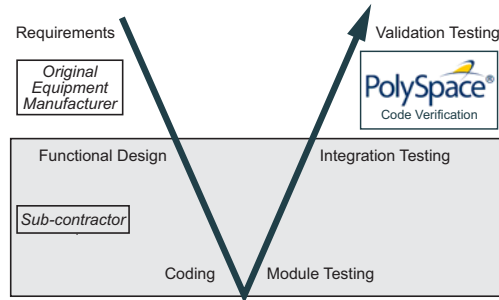
The main goal of PolySpace verification is to control and evaluate the safety of an application.

The criteria used to evaluate code can vary widely depending on the criticality of the application, from no red errors to exhaustive oranges review. Typically, these criteria become increasingly stringent as a project advances from early, to intermediate, and eventually to final delivery.

For more information on defining these criteria, see “Defining Software Quality Levels” on page 2-8.

Verification Workflow

This process usually involves both code analysis and code verification before validation phase, and thorough review of verification results based on defined quality objectives.



Note Verification is often performed multiple times, as multiple versions of the software are delivered.

The verification workflow consists of the following steps:

- 1** Quality engineering group defines clear quality objectives for the code to be written, including specific quality levels for each version of the code to be delivered (first, intermediate, or final delivery) For more information, see “Defining Quality Objectives” on page 2-5.
- 2** Development group writes code according to established standards.
- 3** Development group delivers software to the quality engineering group.
- 4** The project leader configures the PolySpace project to meet the defined quality objectives, as described in “Defining a Verification Process to Meet Your Objectives” on page 2-10.
- 5** Quality engineers perform verification on the code.
- 6** Quality engineers review all **red** errors, **gray** code, and the number of orange checks defined in the process.

Note The number of orange checks reviewed often depends on the version of software being tested (first, intermediate, or final delivery). This can be defined by quality level (see “Defining Software Quality Levels” on page 2-8).

- 7 Quality engineers create reports documenting the results of the verification, and communicate those results to the supplier.
- 8 Quality engineers repeat steps 5–7 for each version of the code delivered.

Costs and Benefits

The benefits of code verification at this stage are the same as with other verification processes, but the cost of correcting faults is higher, because verification takes place late in the development cycle.

It is possible to perform an exhaustive orange review at this stage, but the cost of doing so can be high. If you want to review all orange checks at this phase, it is important to use development and verification processes that minimize the number of orange checks. This includes:

- Developing code using strict coding and data rules.
- Providing accurate manual stubs for all unresolved function calls.
- Using DRS to provide accurate data ranges for all input variables.

Taking these steps will minimize the number of orange checks reported by the verification, and make it likely that any remaining orange checks represent true issues with the software.

Quality Engineers – Certification/Qualification

User Description

This workflow applies to quality engineers who work with applications requiring outside quality certification, such as IEC 61508 certification or DO-178B qualification.

These users generally receive code late in the development cycle, and must perform a set of activities to meet certification requirements.

Note For more information on using PolySpace products within an IEC 61508 certification environment, see the *IEC Certification Kit: Verification of C and C++ Code Using PolySpace Products*.

For more information on using PolySpace products within an DO-178B qualification environment, see the *DO Qualification Kit: PolySpace Client/Server for C/C++ Tool Qualification Plan*.

Quality Objectives

The main goal of PolySpace verification is to improve productivity by replacing other qualification activities.

In this context, software quality is already extremely high, so verification is not intended to improve quality. Instead, it is intended to reduce the cost of achieving such quality.

PolySpace verification can increase productivity by replacing existing activities, such as:

- Data and control flow verification
- Shared data conflict detection
- Robustness unit tests

These activities are often performed by hand, or with classical testing methods, which can be time consuming. PolySpace verification can complete

the same tasks more efficiently, bringing improved productivity and reducing the cost of the process.

Verification Workflow

The verification workflow consists of the following steps:

- 1** Developers write code using both coding and data rules.
- 2** The project leader configures the PolySpace project to meet the quality objectives of the certified process.
- 3** Quality engineers perform verification at the unit test stage.
- 4** Quality engineers review all **red** errors, **gray** code, and the number of orange checks defined in the certified process.
- 5** Quality engineers review verification results for data and control flow verification, and shared data detection.
- 6** Optionally, quality engineers perform an additional verification at the integration test phase.

Costs and Benefits

The replacement of these activities can lead to significant cost reductions. For example, the time spent on data and control flow verification can decrease from 3 months to 2 weeks.

Quality is also more consistent since the process is more automated. PolySpace tools are equally efficient on a Friday afternoon and on a Tuesday morning.

Model-Based Design Users – Verifying Generated Code

User Description

This workflow applies to users who have adopted model-based design to generate code for embedded application software.

These users generally use PolySpace software in combination with several other Mathworks products, including Simulink, Real-Time Workshop Embedded Coder, and Simulink Design Verifier. In many cases, these customers combine application components that are hand-written code with those created using generated code.

Quality Objectives

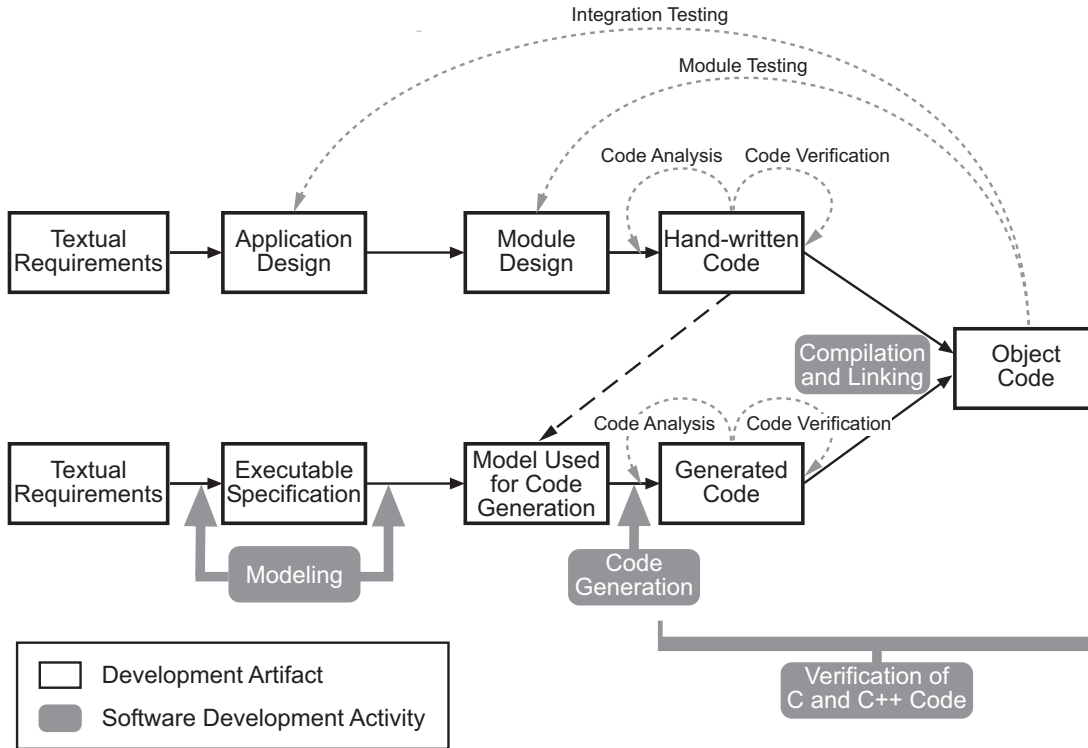
The goal of PolySpace verification is to improve the quality of the software by identifying implementation issues in the code, and ensuring the code is both semantically and logically correct.

PolySpace verification allows you to find run time errors:

- In hand-coded portions within the generated code
- In the model used for production code generation
- In the integration of hand-written and generated code

Verification Workflow

The workflow is different for hand-written code, generated code, and mixed code. PolySpace products can perform code verification as part of any of these workflows. The following figure shows a suggested verification workflow for hand-written and mixed code.



Workflow for Verification of Generated and Mixed Code

Note Solid arrows in the figure indicate the progression of software development activities.

The verification workflow consists of the following steps:

- 1** The project leader configures a PolySpace project to meet defined quality objectives.
- 2** Developers write hand-coded sections of the application.
- 3** Developers perform **PolySpace verification** on any hand-coded sections within the generated code, and review verification results according to the established quality objectives.
- 4** Developers create Simulink® model based on requirements.
- 5** Developers validate model to ensure it is logically correct (using tools such as Simulink Model Advisor, and the Simulink® Verification and Validation™ and Simulink® Design Verifier™ products).
- 6** Developers generate code from the model.
- 7** Developers perform **PolySpace verification** on the entire software component, including both hand-written and generated code.
- 8** Developers review verification results according to the established quality objectives.

Note The PolySpace Model Link™ SL product allows you to quickly track any issues identified by the verification back to the appropriate block in the Simulink model.

Costs and Benefits

PolySpace verification can identify errors in textual designs or executable models that are not identified by other methods. The following table shows how errors in textual designs or executable models can appear in the resulting code.

Examples of Common Run-Time Errors

Type of Error	Design or Model Errors	Code Errors
Arithmetic errors	<ul style="list-style-type: none">• Incorrect Scaling• Unknown calibrations• Untested data ranges	<ul style="list-style-type: none">• Overflows/Underflows• Division by zero• Square root of negative numbers
Memory corruption	<ul style="list-style-type: none">• Incorrect array specification in state machines• Incorrect legacy code (look-up tables)	<ul style="list-style-type: none">• Out of bound array indexes• Pointer arithmetic
Data truncation	<ul style="list-style-type: none">• Unexpected data flow	<ul style="list-style-type: none">• Overflows/Underflows• Wrap-around
Logic errors	<ul style="list-style-type: none">• Unreachable states• Incorrect Transitions	<ul style="list-style-type: none">• Non initialized data• Dead code

Project Managers – Integrating PolySpace Verification with Configuration Management Tools

User Description

This workflow applies to project managers responsible for establishing check-in criteria for code at different development stages.

Quality Objectives

The goal of PolySpace verification is to test that code meets established quality criteria before being checked in at each development stage.

Verification Workflow

The verification workflow consists of the following steps:

- 1** Project manager defines quality objectives, including individual quality levels for each stage of the development cycle.
- 2** Project leader configures a PolySpace project to meet quality objectives.
- 3** Developers run verification at the following stages:
 - **Daily check-in** — On the files currently under development. Compilation must complete without the permissive option.
 - **Pre-unit test check-in** — On the files currently under development.
 - **Pre-integration test check-in** — On the whole project, ensuring that compilation can complete without the permissive option. This stage differs from daily check-in because link errors are highlighted.
 - **Pre-build for integration test check-in** — On the whole project, with all multitasking aspects accounted for as appropriate.
 - **Pre-peer review check-in** — On the whole project, with all multitasking aspects accounted for as appropriate.
- 4** Developers review verification results for each check-in activity to ensure the code meets the appropriate quality level. For example, the transition criterion could be: “No bug found within 20 minutes of selective orange review”

Setting Up a Verification Project

- “Creating a Project” on page 3-2
- “Specifying Options to Match Your Quality Objectives” on page 3-19
- “Setting Up Project to Check Coding Rules” on page 3-24
- “Setting Up Project for Generic Target Processors” on page 3-30
- “Setting up Project to Automatically Test Orange Code” on page 3-38

Creating a Project

In this section...
“What Is a Project?” on page 3-2
“Project Directories” on page 3-3
“Opening PolySpace Launcher” on page 3-3
“Specifying Default Directory” on page 3-6
“Creating New Projects” on page 3-8
“Opening Existing Projects” on page 3-10
“Specifying Source Files” on page 3-10
“Specifying Include Directories” on page 3-13
“Specifying Results Directory” on page 3-15
“Specifying Analysis Options” on page 3-16
“Configuring Text and XML Editors” on page 3-17
“Saving the Project” on page 3-18

What Is a Project?

In PolySpace software, a project is a named set of parameters for a verification of your software project’s source files. You must have a project before you can run a PolySpace verification of your source code.

A project includes:

- The location of source files and include directories
- The location of a directory for verification results
- Analysis options

You can create your own project or use an existing project. You create and modify a project using the Launcher graphical user interface.

A project file has one of the following file types:

Project Type	File Extension	Description
Configuration	cfg	Required for running a verification. Does not include generic target processors.
PolySpace Project Model	ppm	For populating a project with analysis options, including generic target processors.
Desktop	dsk	In earlier versions of PolySpace software, for running a verification on a client computer.

Project Directories

Before you begin verifying your code with PolySpace software, you must know the location of your source files and include files. You must also know where you want to store the verification results.

To simplify the location of your files, you may want to create a project directory, and then in that directory, create separate directories for the source files, include files, and results. For example:

```
polyspace_project/
```

- sources
- includes
- results

Opening PolySpace Launcher

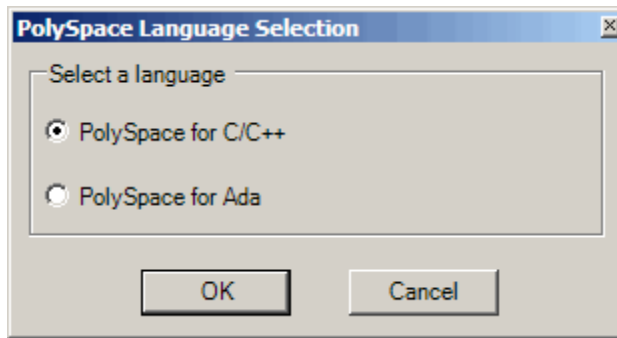
You use the PolySpace Launcher to create a project and start a verification.

To open the PolySpace Launcher:

- 1 Double-click the PolySpace Launcher icon.

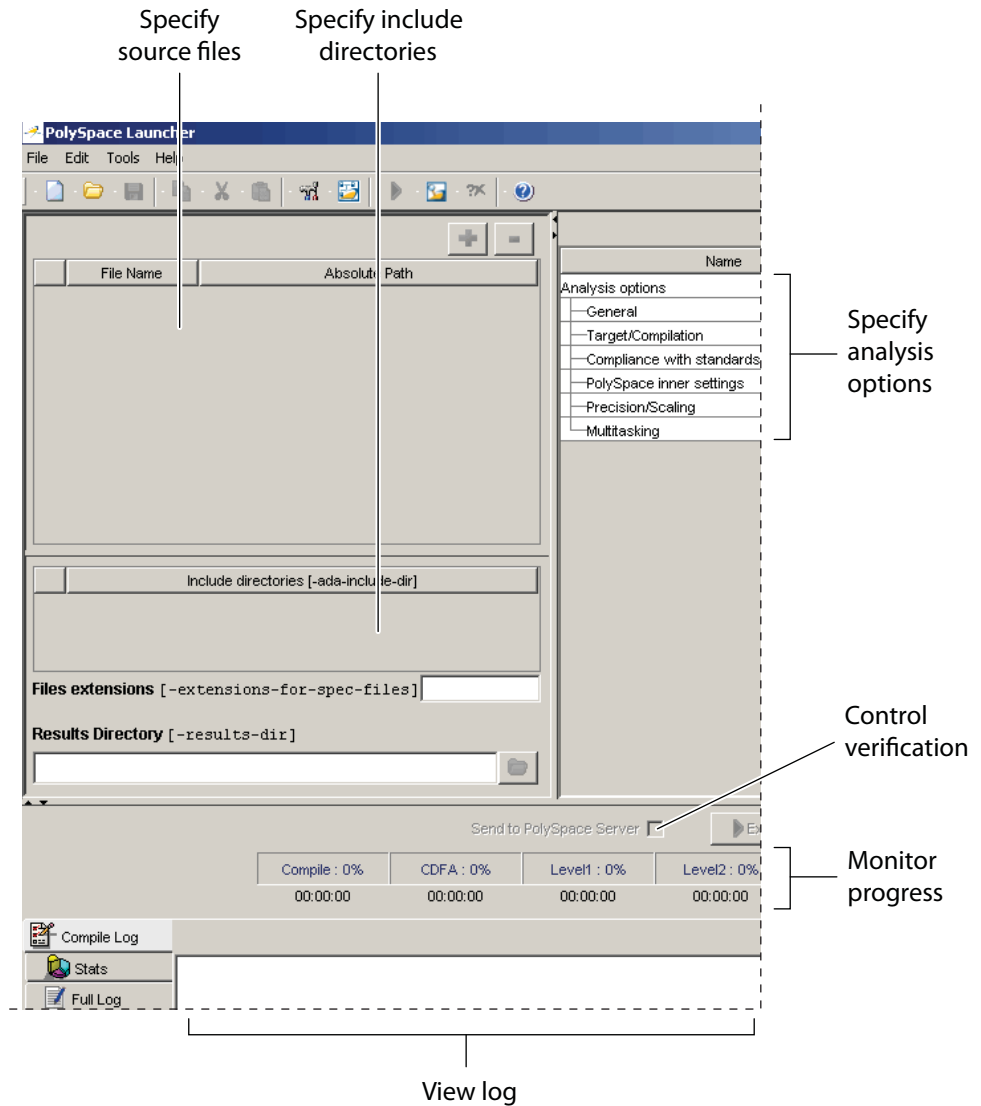


- 2** If you have both PolySpace Client for C/C++ and PolySpace Client for Ada products on your system, the **PolySpace Language Selection** dialog box will appear.



Select **PolySpace for C/C++**, then click **OK**.

The PolySpace Launcher window appears:



The Launcher window has three main sections.

Use this section...	For...
Upper-left	Specifying: <ul style="list-style-type: none">• Source files• Include directories• Results directory
Upper-right	Specifying analysis options
Lower	Controlling and monitoring a verification

You can resize or hide any of these sections. You learn more about the Launcher window later in this tutorial.

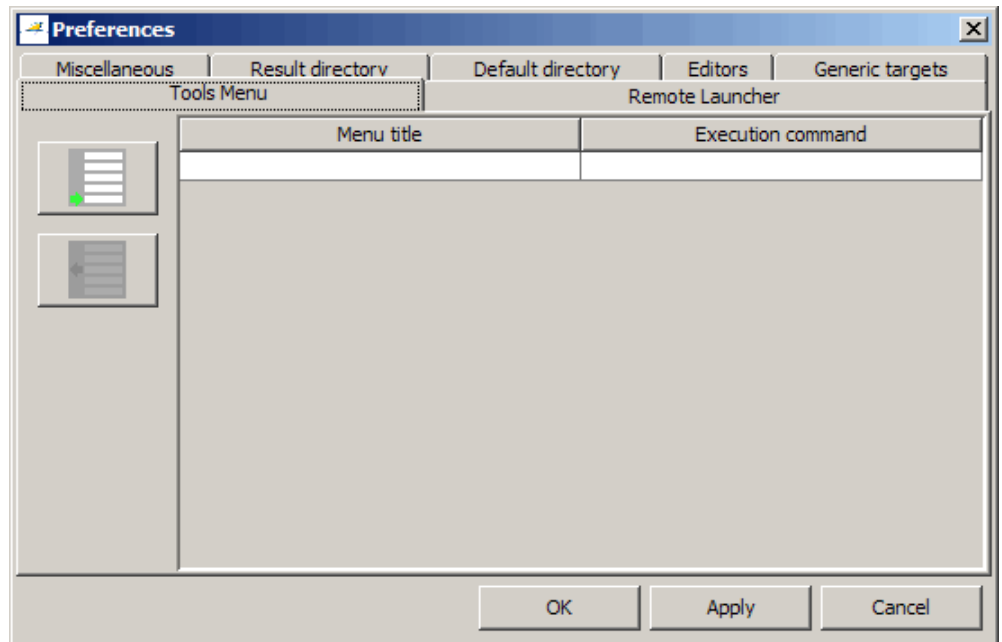
Specifying Default Directory

PolySpace software allows you to specify the default directory that appears in directory browsers in dialog boxes. If you do not change the default directory, the default directory is the installation directory. Changing the default directory to the project directory makes it easier for you to locate and specify source files and include directories in dialog boxes.

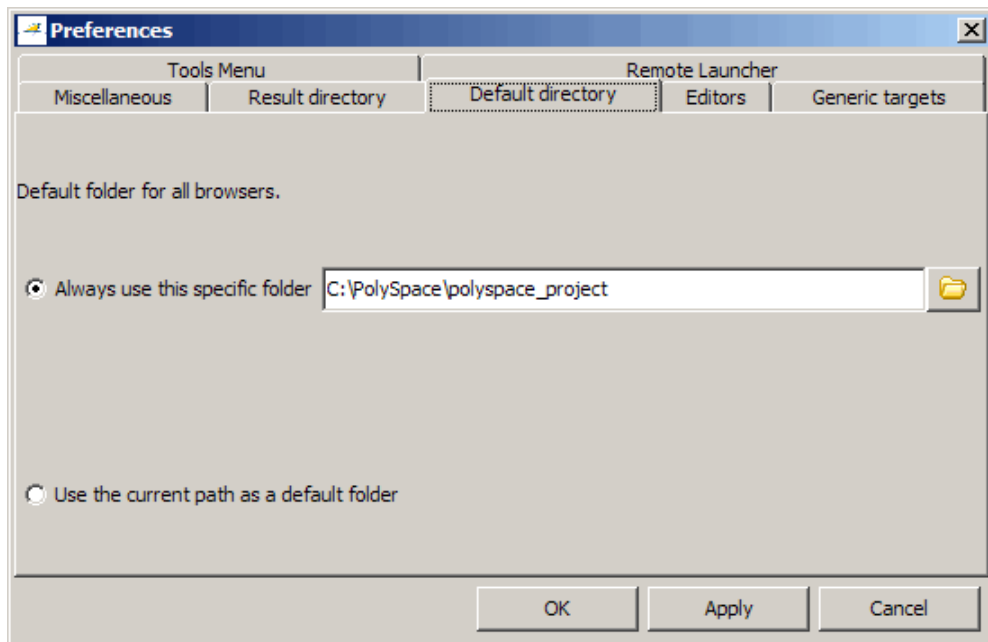
To change the default directory to the project directory:

- 1 Select **Edit > Preferences**.

The **Preferences** dialog box appears.



2 Select the **Default directory** tab.



3 Select **Always use this specific folder** if it is not already selected.

4 Enter or navigate to the project directory you want to use.

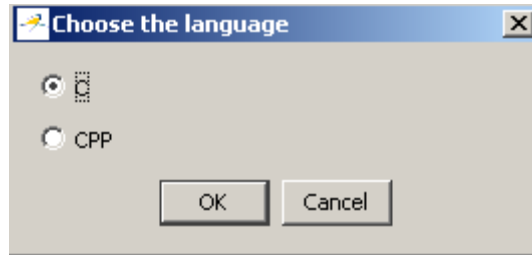
5 Click **OK** to apply the changes and close the dialog box.

Creating New Projects

To create a new project:

1 Select **File > New Project**.

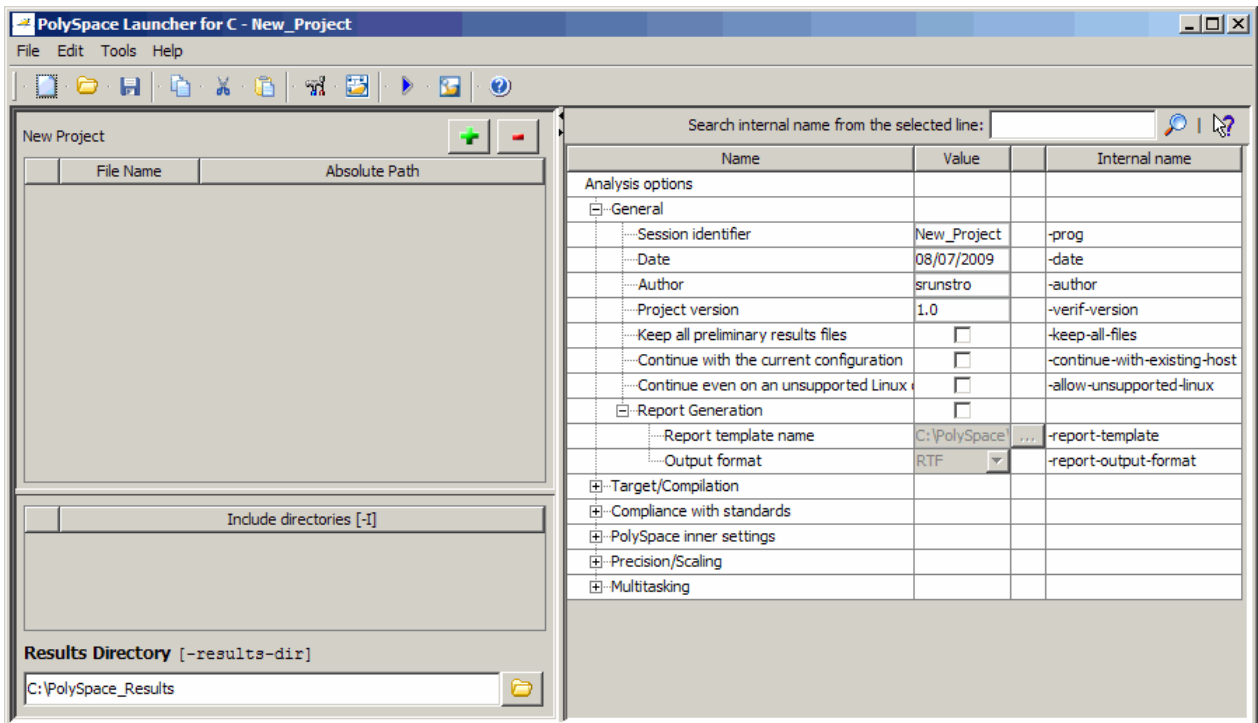
The **Choose the language** dialog box appears:



- 2 Select C, then click **OK**.

The default project name, `New_Project`, appears in the title bar.

In the **Analysis options** section, the **General** options node expands with default project identification information and options.



Opening Existing Projects

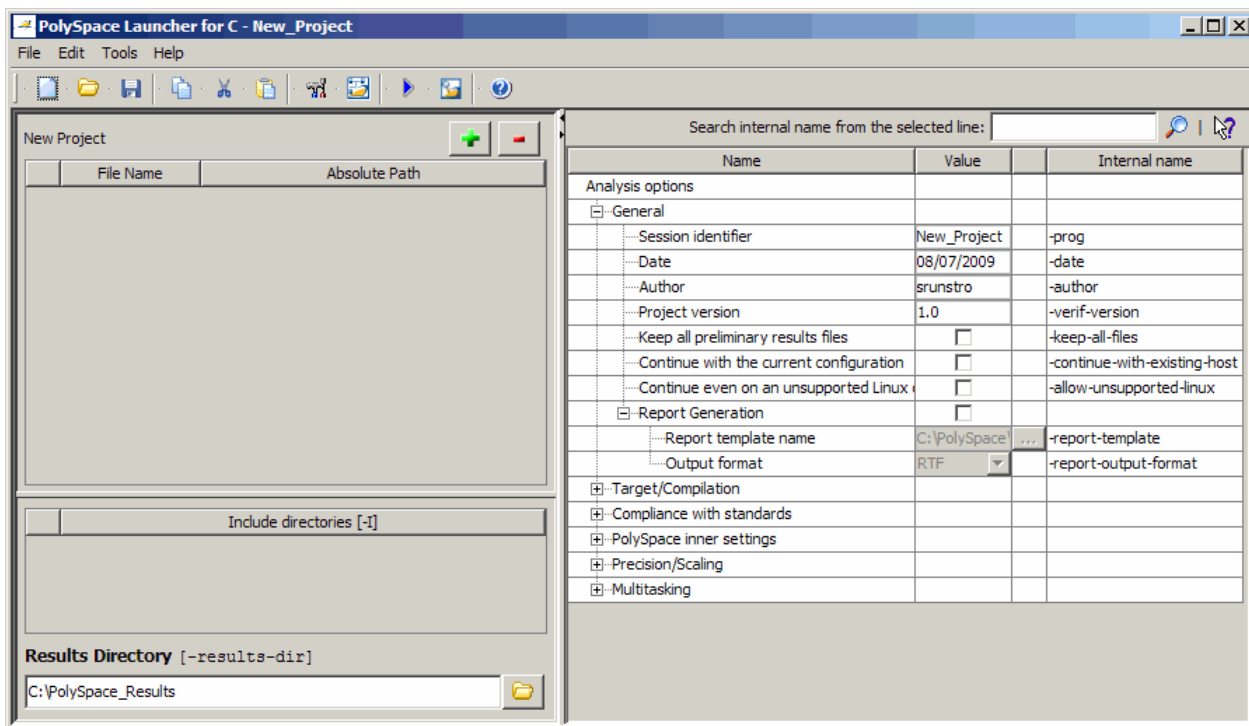
To open an existing project:

- 1 Select **File > Open Project**.

The **Please select a file** dialog box appears.

- 2 Select the project you want to open, then click **OK**.

The selected project opens in the Launcher.



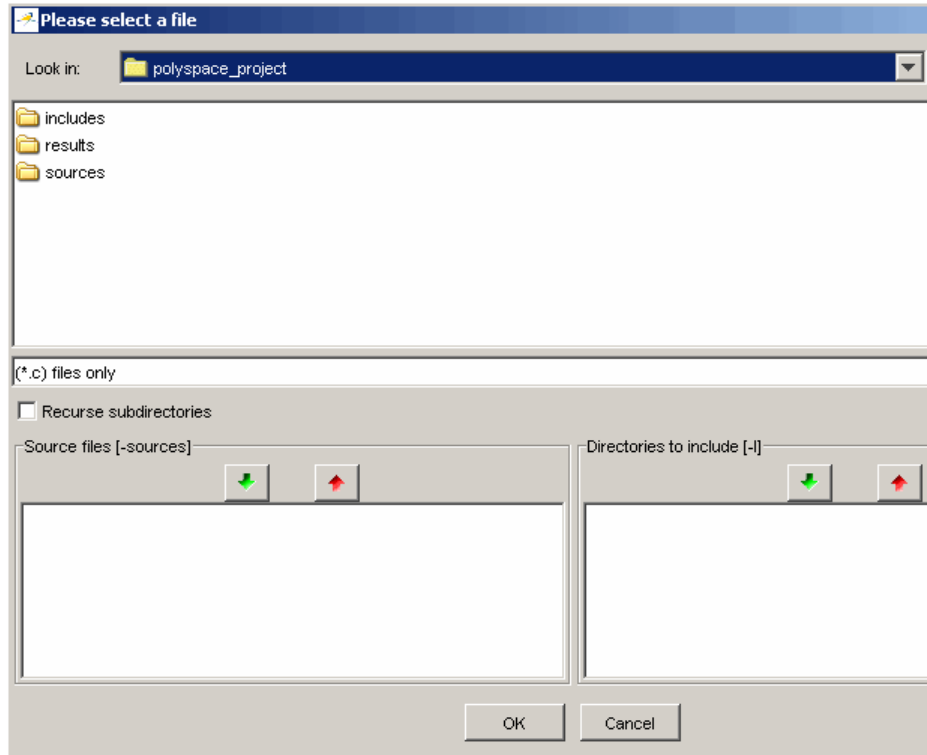
Specifying Source Files

To specify the source files for your project:

- 1 Click the green plus sign button in the upper right of the files section of the Launcher window.



The **Please select a file** dialog box appears.



- 2** In the **Look in** field, navigate to your project directory containing your source files.
- 3** Select the files you want to verify, then click the green down arrow button in the **Source files** section.

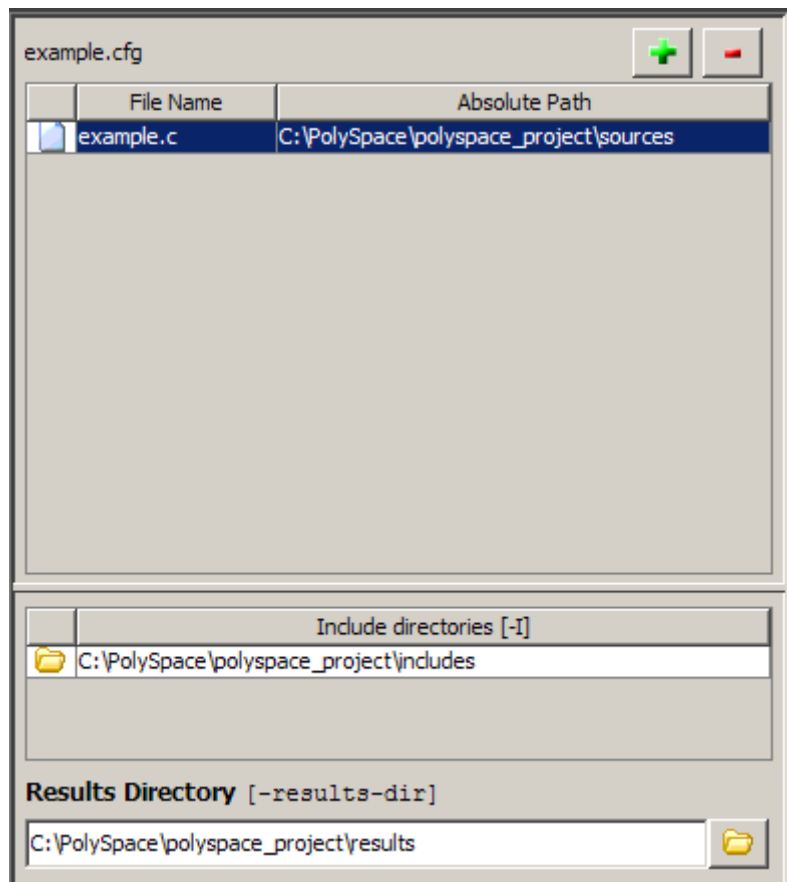


The path of each source files appear in the source files list.

Tip You can also drag directory and file names from an open directory directly to the source files list or include list.

- 4 Click **OK** to apply the changes and close the dialog box.

The source files you selected appear in the files section in the upper left of the Launcher window.



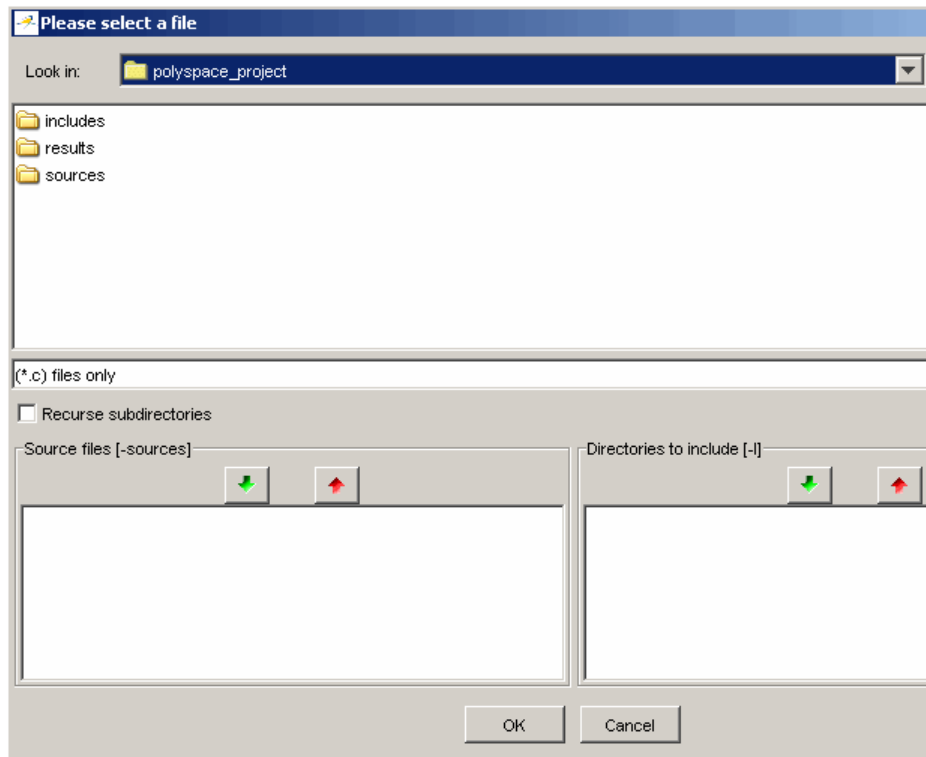
Specifying Include Directories

To specify the include directories for the project:

- 1 Click the green plus sign button in the upper right of the files section of the Launcher window.



The **Please select a file** dialog box appears.



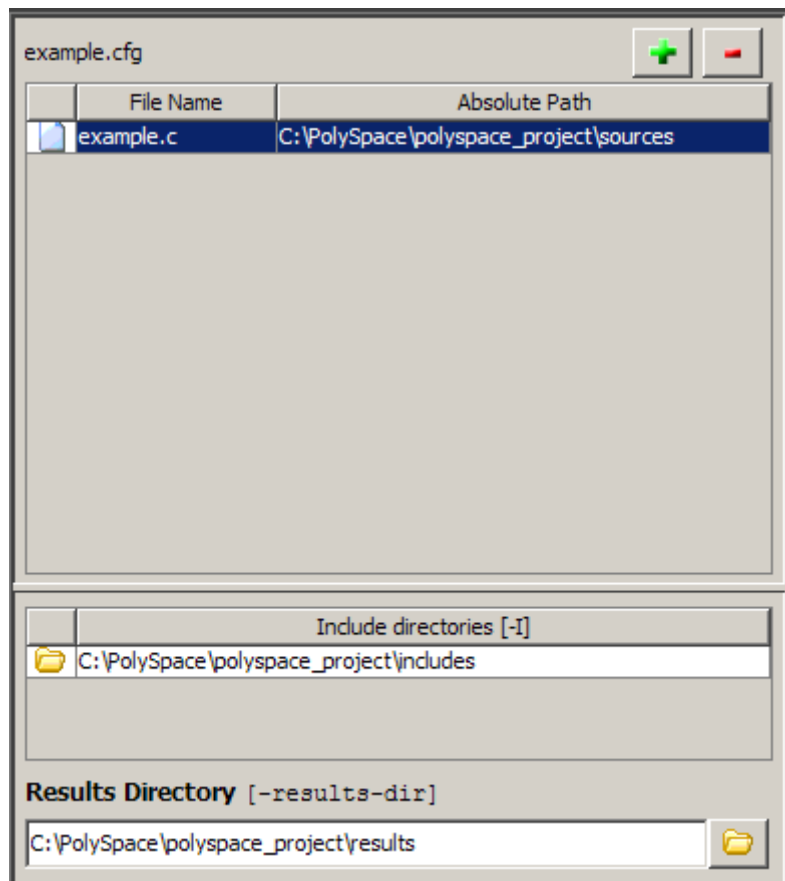
- 2 In the **Look in** field, navigate to your project directory.
- 3 Select the directory containing the include files for your project, then click the green down arrow button in the **Directories to include** section.



The path for each include directory appears in the source files list.

- 4 Click **OK** to apply the changes and close the dialog box.

The include directories you selected appear in the Include directories section on the left side of the Launcher window.

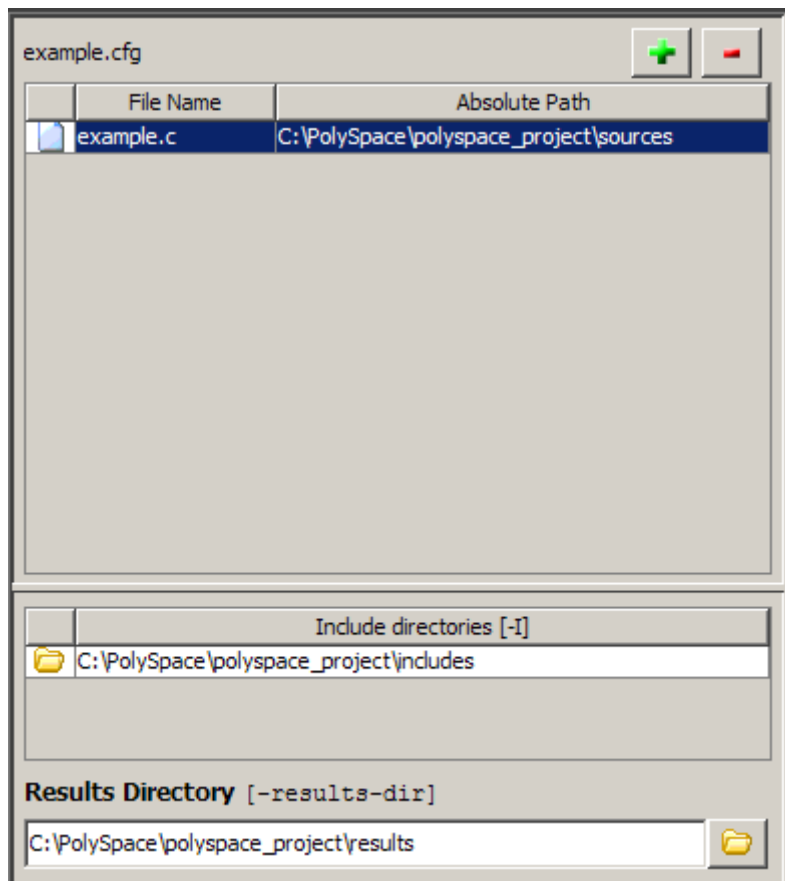


Specifying Results Directory

To specify the results directory for the project:

- 1 In the **Results Directory** section of the Launcher window, specify the full path of the directory that will contain your verification results. For example: `C:\polyspace_project\results`.

The files section of the Launcher window now looks like:



Specifying Analysis Options

The analysis options in the upper-right section of the Launcher window include identification information and parameters that PolySpace software uses during the verification process.

To specify General parameters for your project:

- 1** In the Analysis options section of the Launcher window, expand **General**.
- 2** The General options appear.

Search internal name from the selected line: <input type="text"/>			
Name	Value		Internal name
Analysis options			
[-] General			
... Session identifier	New_Project		-prog
... Date	08/07/2009		-date
... Author	username		-author
... Project version	1.0		-verif-version
... Keep all preliminary results files	<input type="checkbox"/>		-keep-all-files
... Continue with the current configuration	<input type="checkbox"/>		-continue-with-existing-host
... Continue even on an unsupported Linux	<input type="checkbox"/>		-allow-unsupported-linux
[-] Report Generation	<input type="checkbox"/>		
... Report template name	C:\PolySpace\...		-report-template
... Output format	RTF		-report-output-format
[+] Target/Compilation			
[+] Compliance with standards			
[+] PolySpace inner settings			
[+] Precision/Scaling			
[+] Multitasking			

- 3** Specify the appropriate general parameters for your project.

For detailed information about specific analysis options, see “Option Descriptions” in the *PolySpace Products or C Reference*.

Configuring Text and XML Editors

Before you running a verification you should configure your text and XML editors in the Launcher. Configuring text and XML editors allows you to view source files and MISRA® reports directly from the Launcher logs.

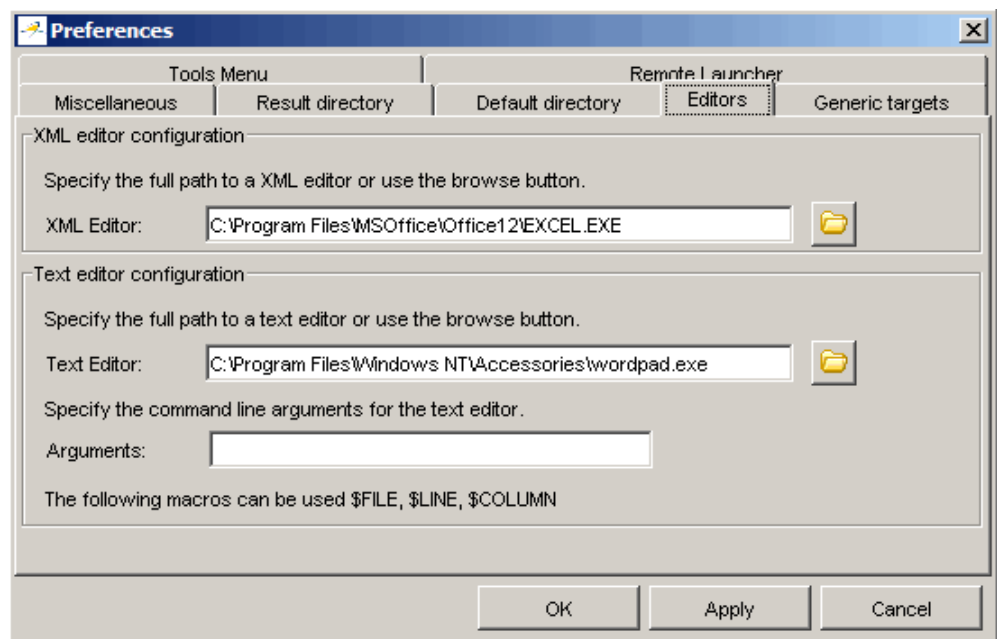
To configure your text and .XML editors:

- 1 Select **Edit > Preferences**.

The Preferences dialog box opens.

- 2 Select the **Editors** tab.

The Editors tab opens.



- 3 Specify an XML editor to use to view MISRA-C reports.

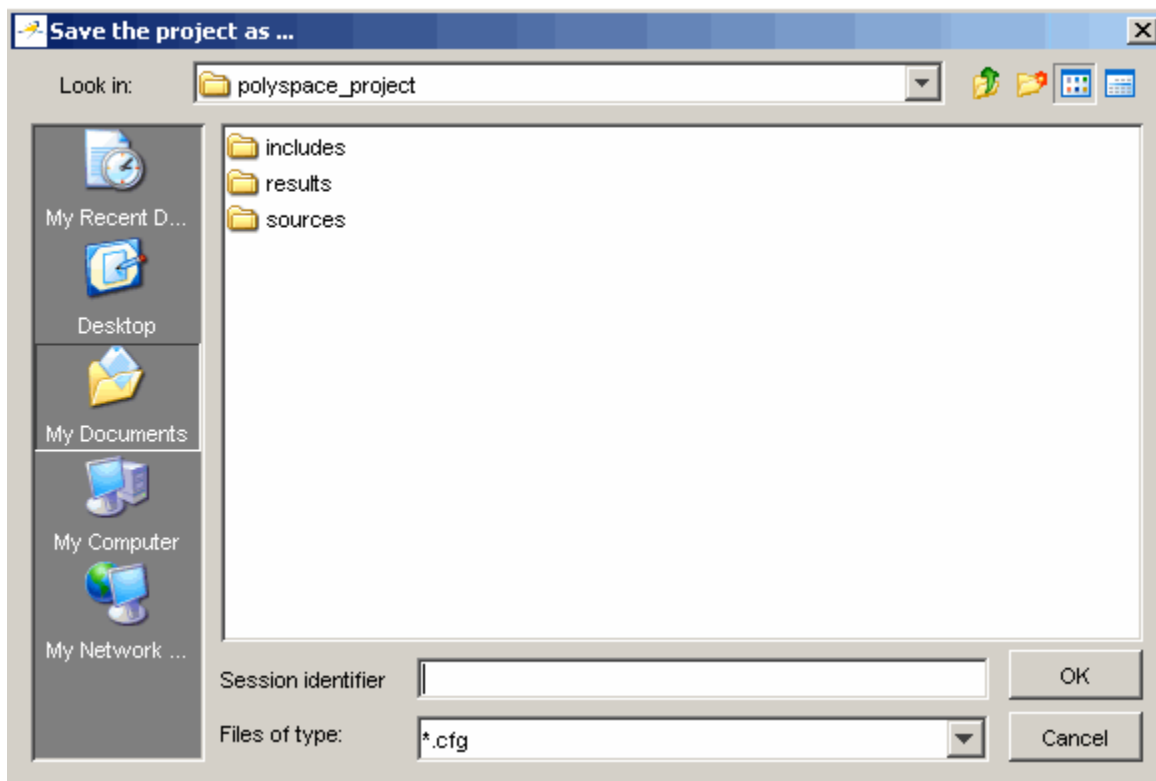
- 4 Specify a Text editor to use to view source files from the Launcher logs.

5 Click **OK**.

Saving the Project

To save the project:

1 Select **File > Save project**. The **Save the project as** dialog box appears.



2 In **Look in**, select your project directory.

3 In **Session identifier**, enter a name for your project.

4 Click **OK** to save the project and close the dialog box.

Specifying Options to Match Your Quality Objectives

While creating your project, you must configure analysis options to match your quality objectives.

This includes:

In this section...
“Quality Objectives Overview” on page 3-19
“Choosing Contextual Verification Options” on page 3-19
“Choosing Strict or Permissive Verification Options” on page 3-21
“Choosing Coding Rules” on page 3-23

Quality Objectives Overview

While creating your project, you must configure analysis options to match your quality objectives.

This includes choosing contextual verification options, coding rules, and options to set the strictness of the verification.

Note For information on defining the quality objectives for your project, see “Defining Quality Objectives” on page 2-5.

Choosing Contextual Verification Options

PolySpace software performs robustness verification by default. If you want to perform contextual verification, there are several options you can use to provide context for data ranges, function call sequence, and stubbing.

For more information on robustness and contextual verification, see “Choosing Robustness or Contextual Verification” on page 2-5.

To specify contextual verification for your project:

1 In the Analysis options section of the Launcher window, expand **PolySpace Inner Settings**.

2 Expand the **Generate a main** and **Stubbing** options.

Name	Value		Internal name
Analysis options			
+ General			
+ Target/Compilation			
+ Compliance with standards			
- PolySpace inner settings			
+ Run a verification unit by unit	<input type="checkbox"/>		-unit-by-unit
- Generate a main	<input checked="" type="checkbox"/>		-main-generator
... Write accesses to global variables	public	▼ ...	-main-generator-writes-variables
... Function calls	unused	▼ ...	-main-generator-calls
... Startup function to call			-function-called-before-main
- Stubbing			
... Variable range setup		...	-data-range-specifications
... Stub all functions	<input type="checkbox"/>		-permissive-stubber
... No automatic stubbing	<input type="checkbox"/>		-no-automatic-stubbing
+ Assumptions			
... Automatic Orange Tester	<input type="checkbox"/>		-prepare-automatic-tests
... Run verification in 32 or 64-bit mode	auto	▼	-machine-architecture
... Number of processes for multiple CPU	4		-max-processes
... Other options			
+ Precision/Scaling			

3 To set ranges on variables, use the following options:

- **Variable range setup (-data-range-specifications)** – Activates the DRS option, allowing you to set specific data ranges for a list of global variables.
- **Write accesses to global variables (-main-generator-writes-variables)** – Specifies how the generated main initializes global variables.

4 To specify function call sequence, use the following options:

- **Function calls (-main-generator-calls)** – Specifies how the generated main calls functions.
- **Startup function to call (-function-called-before-main)** – Specifies an initialization function called after initialization of global variables but before the main loop.

5 To control stubbing behavior, use the following options:

- **No automatic stubbing (-no-automatic-stubbing)** – Specifies that the software will not automatically stub functions. The software list the functions to be stubbed and stops the verification.
- **Stub all functions (-permissive-stubber)** – Specifies that the software stubs all functions, including those with function pointers as return type, or those with complex function pointers as parameters.

For more information on these options, see “Option Descriptions” in the *PolySpace Products for C Reference*.

Choosing Strict or Permissive Verification Options

PolySpace software provides several options that allow you to customize the strictness of the verification. You should set these options to match the quality objectives for your application.

To specify the strictness of your verification:

- 1** In the Analysis options section of the Launcher window, expand **Compliance with standards**.
- 2** Expand the **Strict** and **Permissive** options.

Name	Value	Internal name
Analysis options		
+ General		
+ Target/Compilation		
- Compliance with standards		
Code from DOS or Windows filesystem	<input checked="" type="checkbox"/>	-dos
+ Embedded assembler		
- Strict	<input type="checkbox"/>	-strict
Give all warnings	<input type="checkbox"/>	-Wall
- Permissive	<input type="checkbox"/>	-permissive
Allow non ANSI/ISO C-90 Standard types of bitfields	<input type="checkbox"/>	-allow-non-int-bitfield
Accept integral type conflicts	<input type="checkbox"/>	-permissive-link
Continue even with undefined global variables	<input type="checkbox"/>	-allow-undef-variables
Permits overflowing computations on constants	<input type="checkbox"/>	-ignore-constant-overflows
Allow un-named Unions/Structures	<input type="checkbox"/>	-allow-unnamed-fields
Do not check the sign of operand in left shifts	<input type="checkbox"/>	-allow-negative-operand-in-shift
+ Check MISRA-C:2004 rules	<input type="checkbox"/>	
+ Keil/IAR support	default ▾	-dialect
- PolySpace inner settings		

3 In addition, expand **PolySpace Inner Settings > Assumptions**.

4 Use the following options to make verification more strict:

- **Detect overflows on unsigned integers (-detect-unsigned-overflow)** – Verification is more strict with overflowing computations on unsigned integers.
- **Do not consider all global variables to be initialized (-no-def-init-glob)** – Verification treats all global variables as non-initialized, therefore causing a red error if they are read before they are written to.
- **Give all warnings (-wall)** – Specifies that all C compliance warnings are written to the log file during compilation.
- **Strict (-strict)** – Specifies strict verification mode, which is equivalent to using the -wall and -no-automatic-stubbing options simultaneously.

- 5 Use the following options to make verification more permissive:
- **Enable pointer arithmetic out of bounds of fields (-allow-ptr-arith-on-struct)** – Enables navigation within a structure or union from one field to another.
 - **Do not check the sign of operand in left shifts (-allow-negative-operand-in-shift)** – Verification allows a shift operation on a negative number.
 - **Permits overflowing computations on constants (-ignore-constant-overflow)** – Verification is permissive with overflowing computations on constants.
 - **Allow non ANSI/ISO C-90 Standard types in bitfields (-allow-non-int-bitfields)** – Allows you to define types of bitfields other than signed or unsigned int.
 - **Continue even with undefined global variables (-allow-undef-variables)** – Verification does not stop due to errors caused by undefined global variables.
 - **Allow un-named Unions/Structures (-allow-unnamed-fields)** – Verification does not stop due to errors caused by unnamed fields in structures.
 - **Kiel/IAR support (-dialect)** – Verification allows syntax associated with the IAR and Keil dialects.

For more information on these options, see “Option Descriptions” in the *PolySpace Products for C Reference*.

Choosing Coding Rules

PolySpace software can check that your code complies with specified coding rules. Before starting code verification, you should consider implementing coding rules, and choose which rules to enforce.

For more information, see “Setting Up Project to Check Coding Rules” on page 3-24.

Setting Up Project to Check Coding Rules

In this section...
“PolySpace MISRA Checker Overview” on page 3-24
“Checking Compliance with MISRA C Coding Rules” on page 3-24
“Creating a MISRA C Rules File” on page 3-26
“Excluding Files from the MISRA C Checking” on page 3-28

PolySpace MISRA Checker Overview

PolySpace software can check that C code complies with MISRA C 2004 standards.²

The MISRA checker enables PolySpace software to provide messages when MISRA C rules are not respected. Most messages are reported during the compile phase of a verification. The MISRA checker can check nearly all of the 141 MISRA C:2004 rules.

Note The PolySpace MISRA checker is based on MISRA C:2004 (<http://www.misra-c.com>).

Checking Compliance with MISRA C Coding Rules

To check MISRA C compliance, you set an option in your project before running a verification. PolySpace software finds the violations during the compile phase of a verification. When you have addressed all MISRA C violations, you run the verification again.

To set the MISRA C checking option:

- 1 In the Analysis options section of the Launcher window, expand **Compliance with standards**.

2. MISRA and MISRA C are registered trademarks of MISRA Ltd., held on behalf of the MISRA Consortium.

The Compliance with standards options appear.

- 2 Select the **Check MISRA-C:2004 rules** check box.
- 3 Expand the **Check MISRA-C:2004 rules** option.

Two options, **Rules configuration** and **Files and directories to ignore**, appear.

Name	Value		Internal name
Analysis options			
+ General			
+ Target/Compilation			
- Compliance with standards			
- Code from DOS or Windows filesystem	<input checked="" type="checkbox"/>		-dos
+ Embedded assembler			
+ Strict	<input type="checkbox"/>		-strict
+ Permissive	<input type="checkbox"/>		-permissive
- Check MISRA-C:2004 rules	<input checked="" type="checkbox"/>		
- Rules configuration		...	-misra2
- Files and directories to ignore		...	-includes-to-ignore
+ KeilMAR support	default	▼	-dialect
+ PolySpace inner settings			
+ Precision/Scaling			
+ Multitasking			

- 4 Specify which MISRA C rules to check and which, if any, files to exclude from the checking.


Note For more information on using the MISRA C checker, see Chapter 11, “MISRA Checker”.

Creating a MISRA C Rules File

You must have a rules file to run a verification with MISRA C checking.

Opening a New Rules File

To open a new rules file:

- 1 Click the button  to the right of the **Rules configuration** option.

A window for opening or creating a MISRA C rules file appears.

- 2 Select **File > New File**.

A table of rules appears.

Rules	Error	Warning	Off
MISRA C rules			
— Number of rules by mode :	7	1	134
+1 Environment			
+2 Language extensions			
+3 Documentation			
+4 Character sets			
+5 Identifiers			
+6 Types			
+7 Constants			
+8 Declarations and definitions			
+9 Initialisation			
+10 Arithmetic type conversions			
+11 Pointer type conversions			
+12 Expressions			
+13 Control statement expressions			
+14 Control flow			
+15 Switch statements			
-16 Functions			
—16.1 Functions shall not be defined with variable numbers of arguments.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
—16.2 Functions shall not call themselves, either directly or indirectly.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
—16.3 Identifiers shall be given for all of the parameters in a function prototype.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
—16.4 The identifiers used in the declaration and definition of a function shall match.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
—16.5 Functions with no parameters shall be declared with parameter type void.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
—16.6 The number of arguments passed to a function shall match the number in the function prototype.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
—16.7 A pointer parameter in a function prototype should be declared as pointer to const.	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
—16.8 All exit paths from a function with non-void return type shall have an explicit return statement.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
—16.9 A function identifier shall only be used with either a preceding &, or with a preceding *.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
—16.10 If a function returns error information, then that error information shall be checked.	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
-17 Pointer and arrays			
—17.1 Pointer arithmetic shall only be applied to pointers that address an array.	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
—17.2 Pointer subtraction shall only be applied to pointers that address elements of an array.	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
—17.3 >, >=, <, <= shall not be applied to pointer types except where they point to the same array.	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
—17.4 Array indexing shall be the only allowed form of pointer arithmetic.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
—17.5 The declaration of objects should contain no more than 2 levels of pointer indirection.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
—17.6 The address of an object with automatic storage shall not be assigned to a pointer.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
+18 Structures and unions			
+19 Preprocessing directives			
+20 Standard libraries			
+21 Run-time failures			

3 For each rule, you specify one of these states:

State	Causes the verification to...
Error	End after the compile phase when this rule is violated.
Warning	Display warning message and continue verification when this rule is violated.
Off	Skip checking of this rule.

Note The default state for most rules is **Warning**. The state for rules that have not yet been implemented is **Off**. Some rules always have state **Error** (you cannot change the state of these).

4 Click **OK** to save the rules and close the window.


The **Save as** dialog box opens.

5 In **File**, enter a name for the rules file.

6 Click **OK** to save the file and close the dialog box.

Excluding Files from the MISRA C Checking

You can exclude files from MISRA C checking. You might want to exclude some included files. To exclude `math.h` from the MISRA C checking of the project `example.cfg`:

1 Click the button  to the right of the **Files and directories to ignore** option.

2 Click the folder icon.



The **Select a file or directory to include** dialog box appears.

3 Select the files or directories (such as include files) you want to ignore.

4 Click **OK**.

The selected files appear in the list of files to ignore.

5 Click **OK** to close the dialog box.

Setting Up Project for Generic Target Processors

In this section...
“Project Model Files” on page 3-30
“Creating Project Model Files” on page 3-31
“Viewing Existing Generic Targets” on page 3-31
“Defining Generic Targets” on page 3-32
“Deleting a Generic Target ” on page 3-35
“Common Generic Targets” on page 3-35
“Creating a Configuration File from a PolySpace Project Model File” on page 3-36

Project Model Files

What Is a PolySpace Project Model File?

A PolySpace project model file is a project file that includes generic target processors. You can use this file to share project information with your development team.

Although you can populate a project with information, such as source files and project options, from a project model file, you cannot run a verification with a project model file. You must have a configuration file to run a verification.

Workflow for Using Project Model Files

A PolySpace project model file is a project file that includes generic target processors. A development team uses this file to share project information. The workflow is:

- 1** A team leader creates a project model file (.ppm). This file has the analysis options for the project, including generic targets.
- 2** The team leader distributes the .ppm file to the team.

- 3** A developer opens the `.ppm` file. From this file, PolySpace software populates the project parameters and the generic targets in the preferences.
- 4** The developer adds source files, include directories, and a results directory to the project and saves it as a configuration file (`.cfg`).
- 5** The developer launches a verification with the `.cfg` file.

Creating Project Model Files

You use the PolySpace Launcher to create a PolySpace project model file.

To create a project model file:

- 1** Select **File > New Project** to create a new project.
- 2** Define the generic target, as described in the following sections.
- 3** Select **File > Save project**.

The **Save the project as** dialog box appears.

- 4** Select ***.ppm** from the **Files of type** menu.
- 5** In **Session identifier**, enter a name for your project model file.
- 6** Click **OK** to save the file and close the dialog box.

Viewing Existing Generic Targets

Generic targets that you create are listed in the Preferences dialog box.

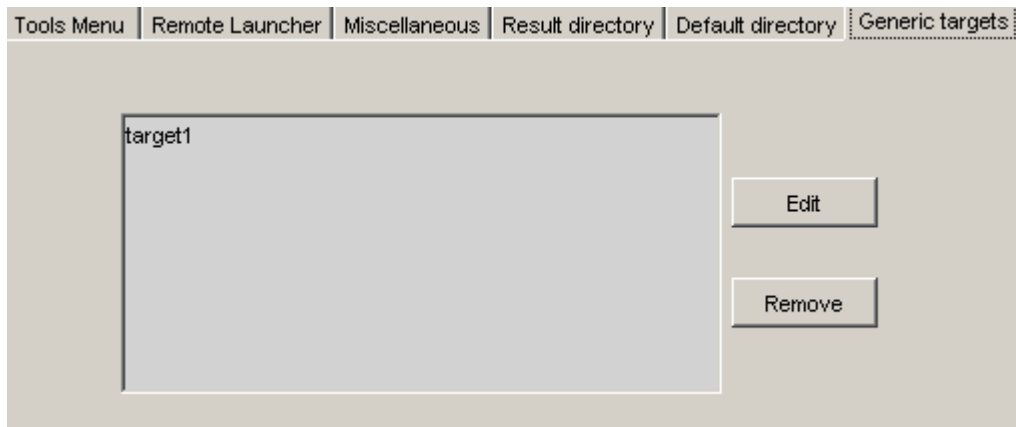
To view existing generic targets:

- 1** Select **Edit > Preferences**.

The **Preferences** dialog box appears.

- 2** Select the **Generic targets** tab.

Previously defined generic targets appear in the generic targets list.



3 Click **Cancel** to close the dialog box.

Defining Generic Targets

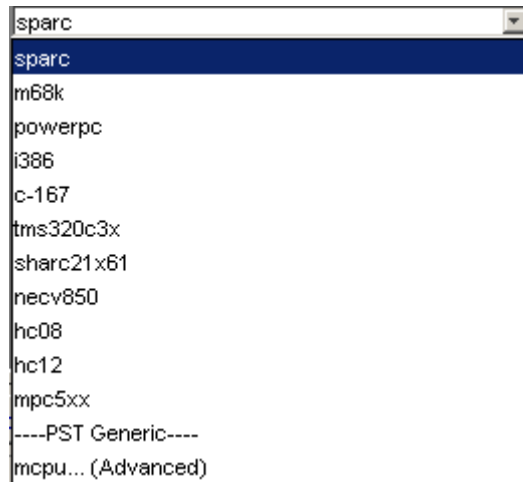
If your application is designed for a custom target processor, you can configure many basic characteristics of the target by selecting the PST Generic target, and specifying the characteristics of your processor.

To configure a generic target:

To define a generic target:

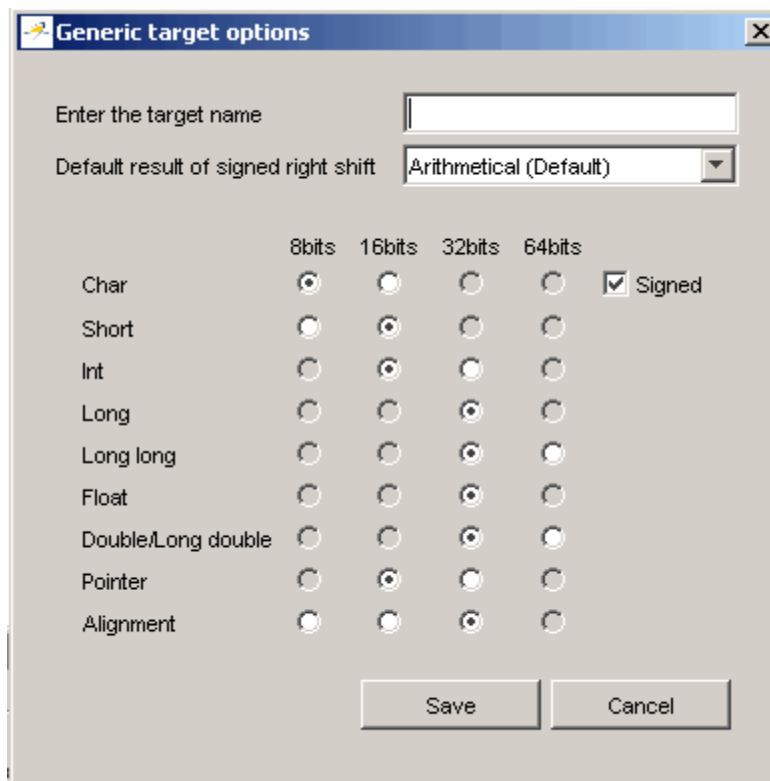
1 In **Analysis options**, expand **Target/Compilation**.

2 Click the down arrow to open the **Target processor type** menu.



3 Select **mcpu... (Advanced)**.

The **Generic target options** dialog box appears.



- 4** In **Enter the target name**, enter a name for your target.
- 5** Specify the appropriate parameters for your target, such as the size of basic types, and alignment with arrays and structures.

For example, when the alignment of basic types within an array or structure is always 8, it implies that the storage assigned to arrays and structures is strictly determined by the size of the individual data objects (without fields and end padding).

Note For more information, see “GENERIC ADVANCED TARGET OPTIONS” in the *PolySpace Products for C Reference*.

6 Click **Save** to save the generic target options and close the dialog box.

Deleting a Generic Target

Generic targets that you create are stored as a PolySpace software preference. Generic targets remain in your preferences until you delete them.

Note You cannot delete a generic target if it is the currently selected target processor type for the project.

To delete a generic target:

1 Select **Edit > Preferences**.

The **Preferences** dialog box appears.

2 Select the **Generic targets** tab.

3 Select the target you want to remove.

4 Click **Remove**.

5 Click **OK** to apply the change and close the dialog box.

Common Generic Targets

The following tables describe the characteristics of common generic targets.

ST7 (Hiware C compiler : HiCross for ST7)

ST7	char	short	int	long	long long	float	double	long double	ptr	char is	endian
size	8	16	16	32	32	32	32	32	16/32	unsigned	Big
alignment	8	16/8	16/8	32/16/8	32/16/8	32/16/8	32/16/8	32/16/8	32/16/8	N/A	N/A

ST9 (GNU C compiler : gcc9 for ST9)

ST9	char	short	int	long	long long	float	double	long double	ptr	char is	endian
size	8	16	16	32	32	32	64	64	16/64	unsigned	Big
alignment	8	8	8	8	8	8	8	8	8	N/A	N/A

Hitachi H8/300, H8/300L

Hitachi H8/300, H8/300L	char	short	int	long	long long	float	double	long double	ptr	char is	endian
size	8	16	16/32	32	64	32	654	64	16	unsigned	Big
alignment	8	16	16	16	16	16	16	16	16	N/A	N/A

Hitachi H8/300H, H8S, H8C, H8/Tiny

Hitachi H8/300H, H8S, H8C, H8/Tiny	char	short	int	long	long long	float	double	long double	ptr	char is	endian
size	8	16	16/32	32	64	32	64	64	32	unsigned	Big
alignment	8	16	32/16	32/16	32/16	32/16	32/16	32/16	32/16	N/A	N/A

Creating a Configuration File from a PolySpace Project Model File

To run a verification, you must have a configuration file, not just a project model file. However, you can create a configuration file from a project model file.

To create a configuration file from a project model file:

- 1 Open the project model file.

Note When opening files, you can select **Project Model (*.ppm) files** in the File of type section to view only project model files.

Opening the project model file populates the:

- Generic targets in the preferences
- Analysis options and other project information

- 2 Enter additional project information, such as the results directory and source files.

Note If you enter the results directory and source files in the project before you save it as a PolySpace project model file, then that information is saved in the file and appears in the project when you open the file.

- 3 Select **File > Save project**.

The **Save the project as** dialog box appears.

- 4 Enter a name for your configuration file.
- 5 Leave the default type as *.cfg.
- 6 Click **OK** to save the project and close the dialog box.

Setting up Project to Automatically Test Orange Code

In this section...
“PolySpace Automatic Orange Tester” on page 3-38
“Enabling the Automatic Orange Tester” on page 3-38

PolySpace Automatic Orange Tester

The PolySpace Automatic Orange Tester dynamically stresses unproven code (orange checks) to identify runtime errors, and provides information to help you identify the cause of these errors.

The Automatic Orange Tester complements the results review in the Viewer by automatically creating test cases for all input variables in orange code, and then dynamically testing the code to find actual runtime errors.

For more information, see “Automatically Testing Orange Code” on page 9-38.

Enabling the Automatic Orange Tester

Before you can use the Automatic Orange Tester, you must run a PolySpace verification with the `-prepare-automatic-tests` option enabled. This option generates the data necessary to perform dynamic tests in the Automatic Orange Tester.

To enable the automatic orange tester:

- 1** In the Analysis Options window, expand the **PolySpace inner settings** menu.
- 2** Select the **Automatic Orange Tester** check box.

Search internal name from the selected line:		
Name	Value	Internal name
Analysis options		
+ General		
+ Target/Compilation		
+ Compliance with standards		
- PolySpace inner settings		
+ Run a verification unit by unit	<input type="checkbox"/>	-unit-by-unit
+ Generate a main	<input checked="" type="checkbox"/>	-main-generator
+ Stubbing		
+ Assumptions		
Automatic Orange Tester	<input checked="" type="checkbox"/>	-prepare-automatic-tests
Run verification in 32 or 64-bit mode	auto	-machine-architecture
Number of processes for multiple CPU core systems	4	-max-processes
Other options		
+ Precision/Scaling		
+ Multitasking		

The `-prepare-automatic-tests` option is enabled.

For more information on using the Automatic Orange Tester, see “Automatically Testing Orange Code” on page 9-38.

Emulating Your Runtime Environment

- “Setting Up a Target” on page 4-2
- “Verifying an Application Without a “Main”” on page 4-22
- “Applying Data Ranges to External Variables and Stub Functions (DRS)” on page 4-26

Setting Up a Target

In this section...
“Target/Compiler Overview” on page 4-2
“Specifying Target/Compilation Parameters” on page 4-2
“Predefined Target Processor Specifications (size of char, int, float, double...)” on page 4-3
“Generic Target Processors” on page 4-5
“Compiling Operating System Dependent Code (OS-target issues)” on page 4-5
“Address Alignment” on page 4-9
“Ignoring or Replacing Keywords Before Compilation” on page 4-10
“Verifying Code That Uses KEIL or IAR Dialects” on page 4-13
“How to Gather Compilation Options Efficiently” on page 4-20

Target/Compiler Overview

Many applications are designed to run on specific target CPUs and operating systems. The type of CPU determines many data characteristics, such as data sizes and addressing. These factors can affect whether errors (such as overflows) will occur.

Since some run-time errors are dependent on the target CPU and operating system, you must specify the type of CPU and operating system used in the target environment before running a verification.

For detailed information on each Target/Compilation option, see “Target/Compiler Options” in the *PolySpace Products for C Reference*.

Specifying Target/Compilation Parameters

The Target/Compilation options in the Launcher allow you to specify the target processor and operating system for your application.

To specify target parameters for your project:

- 1 In the Analysis options section of the Launcher window, expand **Target/Compilation**.
- 2 The Target/Compilation options appear.

Name	Value		Internal name
Analysis options			
+ General			
- Target/Compilation			
Target processor type	sparc	...	-target
Operating system target for PolySpace stubs	Solaris		-OS-target
Defined Preprocessor Macros		...	-D
Undefined Preprocessor Macros		...	-U
Include		...	-include
Command/script to apply to preprocessed files		...	-post-preprocessing-command
Command/script to apply after the end of the code verification		...	-post-analysis-command
+ Compliance with standards			
+ PolySpace inner settings			
+ Precision/Scaling			
+ Multitasking			

- 3 Specify the appropriate parameters for your target CPU and operating system.

For detailed information on each Target/Compilation option, see “Target/Compiler Options” in the *PolySpace Products for C Reference*.

Predefined Target Processor Specifications (size of char, int, float, double...)

PolySpace software supports many commonly used processors, as listed in the table below. To specify one of the predefined processors, select it from the **Target processor type** drop-down list.

If your processor is not listed, you can specify a similar processor that shares the same characteristics.

Note The targets Motorola ST7, ST9, Hitachi H8/300, H8/300L, Hitachi H8/300H, H8S, H8C, H8/Tiny are described in the next section.

Target	char	short	int	long	long long	float	double	long double	ptr	char is	Endian	ptr diff type
sparc	8	16	32	32	64	32	64	128	32	signed	Big	int, long
i386	8	16	32	32	64	32	64	96	32	signed	Little	int, long
c-167	8	16	16	32	32	32	64	64	16	signed	Little	int
m68k / ColdFire ³	8	16	32	32	64	32	64	96	32	signed	Big	int, long
powerpc	8	16	32	32	64	32	64	128	32	unsigned	Big	int, long
tms320c3x	32	32	32	32	64	32	32	40 ⁴	32	signed	Little	int, long
sharc21x61	32	32	32	32	64	32	32 ⁵	64	32	signed	Little	int, long
NEC-V850	8	16	32	32	32	32	32	64	32	signed	Little	int
hc08 ⁶	8	16	16	32	32	32	32	32	16 ₇	unsigned	Big	int
hc12 ³	8	16	16	32	32	32	32	32	32 ₄	signed	Big	int
mpc5xx (#3)	8	16	32	32	64	32	32	32	32	signed	Big	int, long

If your target processor does not match the characteristics of any processor described above, contact The MathWorks technical support for advice.

3. The M68k family (68000, 68020, etc.) includes the “ColdFire” processor
4. All operations on long double values will be imprecise (that is, shown as orange).
5. On this target, a double may be 32 or 64 bits long. Only 32 bits double are supported.
6. Non ANSI C specified keywords and compiler implementation-dependent pragmas and interrupt facilities are not tokens into account by this support
7. all kinds of pointers (near or far pointer) have 2 bytes (hc08) or 4 bytes (hc12) of width physically.

Note The following table describes target processors that are not fully supported by PolySpace software, but for which you can still perform verification. In these cases, you should select the target processor listed in the “Nearest Processor” column. The characteristics that are not identical between the target processor and its equivalent are highlighted in red below. You should take these differences into account when reviewing verification results.

Target	char	short	int	long	long long	float	double	long double	ptr	char is	ptr diff type	Nearest target processor
tms470r1x	8	16	32	32	N/A	32	64	64 ⁸	32	signed	int, long	i386
tms320c2x	16	16	16	32	N/A	32	32	32	16	signed	int	Unsupported

Generic Target Processors

If your application is designed for a custom target processor, you can configure many basic characteristics of the target by selecting the PST Generic target, and specifying the characteristics of your processor.

For more information, see “Setting Up Project for Generic Target Processors” on page 3-30.

Compiling Operating System Dependent Code (OS-target issues)

This section describes the options required to compile and verify code designed to run on specific operating systems. It contains the following:

- “List of Predefined Compilation Flags” on page 4-6
- “My Target Application Runs on Linux” on page 4-8
- “My Target Application Runs on Solaris” on page 4-8
- “My Target Application Runs on Vxworks” on page 4-9

8. All operations on long double values will be imprecise (that is, shown as orange).

- “My Target Application Does Not Run on Linux, vxworks nor Solaris” on page 4-9

List of Predefined Compilation Flags

These flags concern predefined OS-target: no-predefined-OS, linux, vxworks, Solaris and visual (-OS-target option).

OS-target	Compilation flags	-include file and content
no-predefined-OS	-D __STDC__	
visual	-D __STDC__	-include <product_dir>/cininclude/pst-visual.h
vxworks	-D __STDC__ -DANSI_PROTOTYPES -DSTATIC= -DCONST=const -D __STDC__ -D __GNUC__=2 -Dunix -D __unix -D __unix__ -Dsparc -D __sparc -D __sparc__ -Dsun -D __sun -D __sun__ -D __svr4__ -D __SVR4	-include <product_dir>/cininclude/pst-vxworks.h

OS-target	Compilation flags	-include file and content
linux	-D __STDC__ -D __GNUC__=2 -D __GNUC_MINOR__=6 -D __GNUC__=2 -D __GNUC_MINOR__=6 -D __ELF__ -D unix -D __unix -D __unix__ -D linux -D __linux -D __linux__ -D i386 -D __i386 -D __i386__ -D i686 -D __i686 -D __i686__ -D pentiumpro -D __pentiumpro -D __pentiumpro__	<product_dir>/cinclude/pst-linux.h
Solaris	-D __STDC__ -D __GNUC__=2 -D __GNUC_MINOR__=8 -D __GNUC__=2 -D __GNUC_MINOR__=8 -D __GCC_NEW_VARARGS__ -D unix -D __unix -D __unix__ -D sparc -D __sparc -D __sparc__ -D sun -D __sun -D __sun__ -D svr4 -D __SVR4	No -include file mentioned

Note The use of the `OS-target` option is entirely equivalent to the following alternative approaches.

- Setting the same `-D` flags manually, or
 - Using the `-include` option on a copied and modified `pst-OS-target.h` file
-

My Target Application Runs on Linux

The minimum set of options is as follows:

```
polyspace-c \  
-OS-target Linux \  
-I /usr/local/PolySpace/CURRENT-VERSION/include/include-linux \  
-I /usr/local/PolySpace/CURRENT-VERSION/include/include-linux/next \  
...
```

where the PolySpace product has been installed in the directory `/usr/local/PolySpace/CURRENT-VERSION`.

If your target application runs on Linux® but you are launching your verification from Windows, the minimum set of options is as follows:

```
polyspace-c \  
-OS-target Linux \  
-I POLYSPACE_C\Verifier\include\include-linux \  
-I POLYSPACE_C\Verifier\include\include-linux\next \  
...
```

where the PolySpace product has been installed in the directory `POLYSPACE_C`.

My Target Application Runs on Solaris

If PolySpace software runs on a Linux machine:

```
polyspace-c \  
-OS-target Solaris \  
-I /your_path_to_solaris_include
```

If PolySpace runs on a Solaris™ machine:

```
polyspace-c \  
-OS-target Solaris \  
-I /usr/include
```

My Target Application Runs on Vxworks

If PolySpace runs on either a Solaris or a Linux machine:

```
polyspace-c \  
-OS-target vxworks \  
-I /your_path_to/Vxworks_include_directories
```

My Target Application Does Not Run on Linux, vxworks nor Solaris

If PolySpace runs on either a Solaris or a Linux machine:

```
polyspace-c \  
-OS-target no-predefined-OS \  
-I /your_path_to/MyTarget_include_directories
```

Address Alignment

PolySpace handles address alignment by calculating `sizeof` and alignments. This approach takes into account 3 constraints implied by the ANSI standard which guarantee that:

- that global `sizeof` and `offsetof` fields are optimum (i.e. as short as possible);
- the alignment of all addressable units is respected;
- global alignment is respected.

Consider the example:

```
struct foo {char a; int b;}
```

- Each field must be aligned; that is, the starting offset of a field must be a multiple of its own size⁹
- So in the example, `char a` begins at offset 0 and its size is 8 bits. `int b` cannot begin at 8 (the end of the previous field) because the starting offset must be a multiple of its own size (32 bits). Consequently, `int b` begins at offset=32. The size of the `struct foo` before global alignment is therefore 64 bits.
- The global alignment of a structure is the maximum of the individual alignments of each of its fields;
- In the example, `global_alignment = max (alignment char a, alignment int b) = max (8, 32) = 32`
- The size of a struct must be a multiple of its global alignment. In our case, `b` begins at 32 and is 32 long, and the size of the struct (64) is a multiple of the `global_alignment` (32), so `sizeof` is not adjusted.

Ignoring or Replacing Keywords Before Compilation

You can ignore noncompliant keywords such as “far” or 0x followed by an absolute address. The template provided in this section allows you to ignore these keywords.

To ignore keywords:

- 1 Save the following template in `c:\PolySpace\myTpl.pl`.
- 2 In the Target/Compilation options, select **Command/script to apply to preprocessed files**.
- 3 Select `myTpl.pl` using the browse button.

For more information, see `-post-preprocessing-command`.

Content of the myTpl.pl file

```
#!/usr/bin/perl  
  
#####
```

9. except in the cases of “double” and “long” on some targets.


```

# Post Processing template script
#
#####
# Usage from Launcher GUI:
#
# 1) Linux: /usr/bin/perl PostProcessingTemplate.pl
# 2) Solaris: /usr/local/bin/perl PostProcessingTemplate.pl
# 3) Windows: \Verifier\tools\perl\win32\bin\perl.exe <pathtoscript>\
PostProcessingTemplate.pl
#
#####

$version = 0.1;

$INFILE = STDIN;
$OUTFILE = STDOUT;

while (<$INFILE>)
{

    # Remove far keyword
    s/far//;

    # Remove "@ 0xFE1" address constructs
    s/\@s0x[A-F0-9]*//g;

    # Remove "@0xFE1" address constructs
    # s/\@0x[A-F0-9]*//g;

    # Remove "@ ((unsigned)&LATD*8)+2" type constructs
    s/\@s\(\(unsigned\)\&[A-Z0-9]+\*8\)\+\d//g;

    # Convert current line to lower case
    # $_ =~ tr/A-Z/a-z;

    # Print the current processed line
    print $OUTFILE $_;
}

```

Perl Regular Expression Summary

```
#####  
# Metacharacter What it matches  
#####  
# Single Characters  
# . Any character except newline  
# [a-z0-9] Any single character in the set  
# [^a-z0-9] Any character not in set  
# \d A digit same as  
# \D A non digit same as [^0-9]  
# \w An Alphanumeric (word) character  
# \W Non Alphanumeric (non-word) character  
#  
# Whitespace Characters  
# \s Whitespace character  
# \S Non-whitespace character  
# \n newline  
# \r return  
# \t tab  
# \f formfeed  
# \b backspace  
#  
# Anchored Characters  
# \B word boundary when no inside []  
# \B non-word boundary  
# ^ Matches to beginning of line  
# $ Matches to end of line  
#  
# Repeated Characters  
# x? 0 or 1 occurrence of x  
# x* 0 or more x's  
# x+ 1 or more x's  
# x{m,n} Matches at least m x's and no more than n x's  
# abc All of abc respectively  
# to|be|great One of "to", "be" or "great"  
#  
# Remembered Characters  
# (string) Used for back referencing see below  
# \1 or $1 First set of parentheses
```

```

# \2 or $2 First second of parentheses
# \3 or $3 First third of parentheses
#####
# Back referencing
#
# e.g. swap first two words around on a line
# red cat -> cat red
# s/(\w+) (\w+)/$2 $1/;
#
#####

```

Verifying Code That Uses KEIL or IAR Dialects

Typical embedded control applications frequently read and write port data, set timer registers and read input captures. To deal with this without using assembly language, some microprocessor compilers have specified special data types like `sfr` and `sbit`. Typical declarations are:

```

sfr A0 = 0x80;
sfr A1 = 0x81;
sfr ADCUP = 0xDE;
sbit EI = 0x80;

```

These declarations reside in header files such as `regxx.h` for the basic 80Cxxx micro processor. The definition of `sfr` in these header files customizes the compiler to the target processor.

When accessing a register or a port, using `sfr` data is then simple, but is not part of standard ANSI C:

```

int status,P0;

void main (void) {
    ADCUP = 0x08; /* Write data to register */
    A1 = 0xFF; /* Write data to Port */
    status = P0; /* Read data from Port */
    EI = 1; /* Set a bit (enable all interrupts) */
}

```

You can verify this type of code using the **Kiel/IAR support** option (`-dialect`). This option allows the software to support the Keil or IAR C

language extensions even if some structures, keywords, and syntax are not ANSI standard. The following tables summarize what is supported when verifying code that is associated with the keil or iar dialects.

The following table summarizes the supported keil C language extensions:

Example: -dialect keil -sfr-types sfr=8

Type/Language	Description	Example	Restrictions
Type bit	<ul style="list-style-type: none"> An expression to type bit gives values in range [0,1]. Converting an expression in the type, gives 1 if it is not equal to 0, else 0. This behavior is similar to c++ bool type. 	<pre>bit x = 0, y = 1, z = 2; assert(x == 0); assert(y == 1); assert(z == 1); assert(sizeof(bit) == sizeof(int));</pre>	pointers to bits and arrays of bits are not allowed
Type sfr	<ul style="list-style-type: none"> The -sfr-types option defines unsigned types name and size in bits. The behavior of a variable follows a variable of type integral. A variable which overlaps another one (in term of address) will be considered as volatile. 	<pre>sfr x = 0xf0; // declaration of variable x at address 0xF0 sfr16 y = 0x4EEF;</pre> <p>For this example, options need to be:</p> <pre>-dialect keil -sfr-types sfr=8, \ sfr16=16</pre>	sfr and sbit types are only allowed in declarations of external global variables.

Example: -dialect keil -sfr-types sfr=8 (Continued)

Type/Language	Description	Example	Restrictions
Type sbit	<ul style="list-style-type: none"> Each read/write access of a variable is replaced by an access of the corresponding sfr variable access. Only external global variables can be mapped with a sbit variable. Allowed expressions are integer variables, cells of array of int and struct/union integral fields. a variable can also be declared as extern bit in an another file. 	<pre>sfr x = 0xF0; sbit x1 = x ^ 1; // 1st bit of x sbit x2 = 0xF0 ^ 2; // 2nd bit of x sbit x3 = 0xF3; // 3rd bit of x sbit y0 = t[3] ^ 1; /* file1.c */ sbit x = P0 ^ 1; /* file2.c */ extern bit x; x = 1; // set the 1st bit of P0 to 1</pre>	
Absolute variable location	Allowed constants are integers, strings and identifiers.	<pre>int var _at_ 0xF0 int x @ 0xFE ; static const int y @ 0xA0 = 3;</pre>	Absolute variable locations are ignored (even if declared with a #pragma location).

Example: -dialect keil -sfr-types sfr=8 (Continued)

Type/Language	Description	Example	Restrictions
Interrupt functions	A warnings in the log file is displayed when an interrupt function has been found: "interrupt handler detected : <name>" or "task entry point detected : <name>"	<pre>void foo1 (void) interrupt XX = YY using 99 { } void foo2 (void) _ task_ 99 _priority_ 2 { }</pre>	Entry points and interrupts are not taken into account as -entry-points.
Keywords ignored	alien, bdata, far, idata, ebddata, huge, sdata, small, compact, large, reentrant. Defining -D __C51__, keywords large code, data, xdata, pdata and xhuge are ignored.		

The following table summarize the iar dialect:

Example: -dialect iar -sfr-types sfr=8

Type/Language	Description	Example	Restrictions
Type bit	<ul style="list-style-type: none"> An expression to type bit gives values in range [0,1]. Converting an expression in the type, gives 1 if it is not equal to 0, else 0. This behavior is similar to c++ bool type. If initialized with values 0 or 1, a variable of type bit is a simple variable (like a c++ bool). 	<pre>union { int v; struct { int z; } y; } s; void f(void) { bit y1 = s.y.z . 2; bit x4 = x.4; bit x5 = 0xF0 . 5; y1 = 1; // 2nd bit of s.y.z // is set to 1 };</pre>	pointers to bits and arrays of bits are not allowed

Example: -dialect iar -sfr-types sfr=8 (Continued)

Type/Language	Description	Example	Restrictions
	<ul style="list-style-type: none"> A variable of type bit is a register bit variable (mapped with a bit or a sfr type) 		
Type sfr	<ul style="list-style-type: none"> The -sfr-types option defines unsigned types name and size. The behavior of a variable follows a variable of type integral. A variable which overlaps another one (in term of address) will be considered as volatile. 	<pre>sfr x = 0xf0; // declaration of variable x at address 0xF0</pre>	sfr and sbit types are only allowed in declarations of external global variables.
Individual bit access	<ul style="list-style-type: none"> Individual bit can be accessed without using sbit/bit variables. Type is allowed for integer variables, cells of integer array, and struct/union integral fields. 	<pre>int x[3], y; x[2].2 = x[0].3 + y.1;</pre>	
Absolute variable location	Allowed constants are integers, strings and identifiers.	<pre>int var @ 0xF0; int xx @ 0xFE ; static const int y @0xA0 = 3;</pre>	Absolute variable locations are ignored (even if declared with a #pragma location).

Example: -dialect iar -sfr-types sfr=8 (Continued)

Type/Language	Description	Example	Restrictions
Interrupt functions	<ul style="list-style-type: none"> • A warning is displayed in the log file when an interrupt function has been found: "interrupt handler detected : funcname" • A monitor function is a function that disables interrupts while it is executing, and then restores the previous interrupt state at function exit. 	<pre>interrupt [1] \ using [99] void \ foo1(void) { ... }; monitor [3] void \ foo2(void) { ... };</pre>	Entry points and interrupts are not taken into account as -entry-points.
Keywords ignored	saddr, reentrant, reentrant_idata, non_banked, plm, bdata, idata, pdata, code, data, xdata, xhuge, interrupt, __interrupt and __intrinsic		
Unnamed struct/union	<ul style="list-style-type: none"> • Fields of unions/structs with no tag and no name can be accessed without naming their parent struct. • Option -allow-unnamed-fields need to be used to allow anonymous struct fields. • On a conflict between a field of an anonymous struct with other identifiers: 	<pre>union { int x; }; union { int y; struct { int z; }; } @ 0xF0;</pre>	

Example: -dialect iar -sfr-types sfr=8 (Continued)

Type/Language	Description	Example	Restrictions
	<ul style="list-style-type: none"> ▪ with a variable name, field name is hidden ▪ with a field of another anonymous struct at different scope, closer scope is chosen ▪ with a field of another anonymous struct at same scope: an error "anonymous struct field name <name> conflict" is displayed in the log file. 		
no_init attribute	<ul style="list-style-type: none"> • a global variable declared with this attribute is handled like an external variable. • It is handled like a type qualifier. 	<pre>no_init int x; no_init union { int y; } @ 0xFE;</pre>	#pragma no_init has no effect

The option `sfr-types` defines the size of a sfr type for the keil or iar dialect.

The syntax for an sfr element in the list is `type-name=typesize`.

For example:

```
sfr-types sfr=8,sfr16=16
```

defines two `sfr` types: `sfr` with a size of 8 bits, and `sfr16` with a size of 16-bits. A value type-name must be given only once. 8, 16 and 32 are the only supported values for `type-size`.

Note As soon as an `sfr` type is used in the code, you must specify its name and size, even if it is the keyword `sfr`.

Note Many IAR and Keil compilers currently exist that are associated to specific targets. It is difficult to maintain a complete list of those supported.

How to Gather Compilation Options Efficiently

The code is often tuned for the target (as discussed to “Verifying Code That Uses KEIL or IAR Dialects” on page 4-13). Rather than applying minor changes to the code, create a single `polyspace.h` file which will contain all target specific functions and options. The `-include` option can then be used to force the inclusion of the `polyspace.h` file in all source files under verification.

Where there are missing prototypes or conflicts in variable definition, writing the expected definition or prototype within such a header file will yield several advantages.

Direct benefits:

- The error detection is much faster since it will be detected during compilation rather than in the link or subsequent phases.
- The position of the error will be identified more precisely.
- There will be no need to modify original source files.

Indirect benefits:

- The file is automatically included as the very first file in all original `.c` files.
- The file can contain much more powerful macro definitions than simple `-D` options.

- The file is reusable for other projects developed under the same environment.

Example

This is an example of a file that can be used with the `-include` option.

```
// The file may include (say) a standard include file implicitly
// included by the cross compiler

#include <stdlib.h>
#include "another_file.h"

// Generic definitions, reusable from one project to another
#define far
#define at(x)

// A prototype may be positioned here to aid in the solution of
// a link phase conflict between
// declaration and definition. This will allow detection of the
// same error at compilation time instead of at link time.
// Leads to:
// - earlier detection
// - precise localisation of conflict at compilation time
void f(int);

// The same also applies to variables.
extern int x;

// Standard library stubs can be avoided,
// and OS standard prototypes redefined.

#define POLYSPACE_NO_STANDARD_STUBS // use this flag to prevent the
//automatic stubbing of std functions
#define __polyspace_no_sscanf
#define __polyspace_no_fgetc
void sscanf(int, char, char, char, char, char);
void fgetc(void);
```

Verifying an Application Without a “Main”

In this section...
“Main Generator Overview” on page 4-22
“Automatically Generating a Main” on page 4-23
“Manually Generating a Main” on page 4-23
“Main Generator Assumptions” on page 4-24

Main Generator Overview

When your application is a function library (API) or a single module, you must provide a main that calls each function because of the execution model used by PolySpace. You can either manually provide a main, or have PolySpace generate one for you automatically.

When you run a verification on PolySpace Client for C/C++ software, the main is always generated. When you run a verification on PolySpace Server for C/C++ software, you can choose automatically generate a main by selecting the **Generate a main** (-main-generator) option.

PolySpace Client for C/C++ Software Default Behavior

The PolySpace Client for C/C++ product automatically checks whether the code for verification contains a "main" or not.

- If a main exists in the set of files, the verification proceeds with that main.
- If a main does not exist, the tool generates a main. You can specify the options: -main-generator-writes-variables and -main-generator-calls.

PolySpace Server for C/C++ Software Default Behavior

By default, the PolySpace Server for C/C++ product stops verification if it does not find a main. This behavior can help isolate files missing from the verification.

However, you can specify that the PolySpace Server for C/C++ product automatically generate a main. The tool then generates a main with the assumption of verifying a library. You can specify the options `-main-generator-writes-variables` and `-main-generator-calls`.

Automatically Generating a Main

When you run a client verification, or a server verification using the **Generate a main** (`-main-generator`) option, the software automatically generates a main.

The generated main has three distinct default behaviors.

- It first initializes any variables identified by the option `-main-generator-writes-variables`. The default setting for this option is `public`.
- It then calls a function which could be considered an initialization function with the option `-function-called-before-main`.
- It then calls any functions identified by the option `-main-generator-calls`. The default setting for this option is `-main-generator-calls unused`.

For more information on the main generator, see “MAIN GENERATOR OPTIONS (`-main-generator`) for PolySpace Software”.

Manually Generating a Main

Manually generating a main is often preferable to an automatically generated main, because it allows you to provide a more accurate model of the calling sequence to be generated.

There are three steps involved in manually defining the main.

- 1** Identify the API functions and extract their declaration.
- 2** Create a main containing declarations of a volatile variable for each type that is mentioned in the function prototypes.
- 3** Create a loop with a volatile end condition.

- 4 Inside this loop, create a switch block with a volatile condition.
- 5 For each API function, create a case branch that calls the function using the volatile variable parameters you created.

Consider the following example. Suppose that the API functions are:

```
int func1(void *ptr, int x);
void func2(int x, int y);
```

You should create the following main:

```
void main()
{
    volatile int random; /* We need an integer variable as a function
    parameter */
    volatile void * volatile ptr; /* We need a void pointer as a function
    parameter */
    while (random) {
        switch (random) {
            case 1:
                random = func1(ptr, random); break; /* One API function call */
            default:
                func2(random, random); /* Another API function call */
        }
    }
}
```

Main Generator Assumptions

When using the automatic main generator to verify a specific function, the main objective is to find problems with the function itself. To do this, the generated main makes assumptions about parameters so that you can focus on runtime errors (red, grey and orange) related to the function itself.

The main generator makes assumptions about the arguments of called functions to reduce the number of orange checks in the results. Therefore, when you see an orange check in your results, it is likely due to the function itself, not the main.

However, green checks are computed with the same assumptions. Therefore, you should be cautious of green checks involving the main itself, especially when conducting unit-by-unit verification.

Applying Data Ranges to External Variables and Stub Functions (DRS)

In this section...
“Overview of Data Range Specifications (DRS)” on page 4-26
“Specifying Data Ranges” on page 4-26
“File Format” on page 4-27
“Variable Scope” on page 4-29
“Performing Efficient Module Testing with DRS” on page 4-31
“Reducing Oranges with DRS” on page 4-32

Overview of Data Range Specifications (DRS)

By default, PolySpace verification assumes that all data inputs are set to their full range. Therefore, nearly any operation on these inputs could produce an overflow. The Data Range Specifications (DRS) module allows you to set external constraints on global variables and stub function return values. This can substantially reduce the number of orange checks in the verification results.

Note You can only apply data ranges to variables with external linkages (see “Variable Scope” on page 4-29) and stubbed functions.

Specifying Data Ranges

You activate the DRS feature using the option **Variable range setup** (-data-range-specification).

To use the DRS feature:

- 1** Create a DRS file containing the list global variables (or functions) and their associated data ranges, as described in “File Format” on page 4-27.
- 2** In the Analysis options section of the Launcher window, select **PolySpace inner settings > Stubbing**.

- 3** In the **Variable range setup parameter**, select the DRS file that you want to use.

File Format

The DRS file contains a list of global variables and associated data ranges. The point during verification at which the range is applied to a variable is controlled by the mode keyword: `init`, `permanent`, or `globalassert`.

The DRS file must have the following format:

```
variable_name min_value max_value <init|permanent|globalassert>
function_name.return min_value max_value permanent
```

```
variable_name val_min val_max <init|permanent|globalassert>
```

- *variable_name* — The name of the global variable.
- *min_value* — The minimum value for the variable.
- *min_value* and *max_value* — The minimum and maximum values for the variable. You can use the keywords "min" and "max" to denote the minimum and maximum values of the variable type. For example, for the type long, min and max correspond to -2^{31} and $2^{31}-1$ respectively.
- `init` — The variable is assigned to the specified range only at initialization, and keeps it until first write.
- `permanent` — The variable is permanently assigned to the specified range. If the variable is assigned outside this range during the program, no warning is provided. Use the `globalassert` mode if you need a warning.
- `globalassert` — After each assignment, an assert check is performed, controlling the specified range. The assert check is also performed at global initialization.
- *function_name* — The name of the stub function.

Tips

- You can use the keywords "min" and "max" to denote the minimum and maximum values of the variable type. For example, for the type long, min and max correspond to -2^{31} and $2^{31}-1$ respectively.

- You can use hexadecimal values. For example, `x 0x12 0x100 init`.
- Supported column separators are tab, comma, space, or semi-column.
- To insert comments, use shell style “#”.
- Functions must be stubbed functions (no provided body).
- `permanent` is the only supported mode for functions.
- Function names may be C or C++ functions with blanks or commas. For example, `f(int, int)`.
- Function names can be specified in the short form (“f”) as long as no ambiguity exists.
- The function returns either an integral (including enum and bool) or floating point type. If the function returns an integral type and you specify the range as a floating point `[v0.x, v1.y]`, the software applies the integral interval `[(int)v0-1, (int)v1+1]`.

Example

In the following example, the global variables are named `x`, `y`, `z`, `w`, `array`, and `v`.

```
x 12 100 init      # x is defined between [12;100] at \  
                  initialisation  
y 0 10000 permanent # y is permanently defined between \  
                  [0,10000] even any possible assignment.  
z 0 1 globalassert # z is checked in the range [0;1] after \  
                  each assignment  
w min max permanent # w is volatile and full range on its \  
                  declaration type  
v 0 max globalassert # v is positive and checked after each \  
                  assignment.  
arrayOfInt -10 20 init # All cells are defined between [-10;20] \  
                  at initialisation  
s1.id 0 max init   # s1.id is defined between [0;2^31-1] at \  
                  initialisation.  
array.c2 min 1 init # All cells array[i].c2 are defined \  
                  between [-2^31;1] at initialisation  
car.speed 0 350 permanent # Speed of Struct car is permanently \  
                  defined between 0 and 350 Km/h
```

```
bar.return -100 100 permanent # function bar returns -100..100
```

Variable Scope

DRS supports variables with external linkages, const variables, and defined variables. In addition, extern variables are supported with the option `-allow-undef-variables`.

Static variables are not supported by DRS. The following table summarizes possible uses:

	init	permanent	globalassert	comments
Integer	Ok	Ok	Ok	char, short, int, enum, long and long long If you define a range in floating point form, rounding is applied.
Real	Ok	Ok	Ok	float, double and long double If you define a range in floating point form, rounding is applied.
Volatile	No effect	Ok	Full range	Only for int and real
Structure field	Ok	Ok	Ok	Only for int and real fields, including arrays or structures of int or real fields (see below)

	init	permanent	globalassert	comments
Structure field in array	Ok	No effect	No effect	Only when leaves are int or real. Moreover the syntax is the following: <array_name>. <field_name>
Array	Ok	Ok	Ok	Only for int and real fields, including structures or arrays of integer or real fields (see below)
Pointer	No effect	No effect	No effect	
Union field	No effect	No effect	No effect	
Complete structure	No effect	No effect	No effect	
Array cell	No effect	No effect	No effect	Example: array[0], array[10] ...
Stubbed function return	No effect	Ok	No effect	Stubbed function returning integral or floating point

Note Every variable (or function) and associated data range will be written in the log file at compilation time of a PolySpace verification. If PolySpace software does not support the variable, a warning message is displayed.

Note DRS can initialize arrays of structures, structures of arrays, etc., as long as the last field is explicit (structures of arrays of integers, for example).

However, DRS cannot initialize a structure itself — you can only initialize the fields. For example, "s.x 20 40 init" is valid, but "s 20 40 init" is not (because PolySpace cannot determine what fields to initialize).

Performing Efficient Module Testing with DRS

DRS allows you to perform efficient static testing of modules. This is accomplished by adding design level information missing in the source-code.

A module can be seen as a black box having the following characteristics:

- Input data are consumed
- Output data are produced
- Constant calibrations are used during black box execution influencing intermediate results and output data.

Using the DRS feature, you can define:

- The nominal range for input data
- The expected range for output data
- The generic specified range for calibrations

These definitions then allow PolySpace software to perform a single static verification that performs two simultaneous tasks:

- answering questions about robustness and reliability
- checking that the outputs are within the expected range, which is a result of applying black-box tests to a module

In this context, you assign DRS keywords according to the type of data (inputs, outputs, or calibrations).

Type of Data	DRS Mode	Effect on Results	Why?	Oranges	Selectivity
Inputs (entries)	permanent	Reduces the number of oranges, (compared with a standard PolySpace verification)	Input data that were full range are set to a smaller range.	↓	↑
Outputs	globalassert	Increases the number of oranges, (compared with a standard PolySpace verification)	More verification is introduced into the code, resulting in both more orange checks and more green checks.	↑	→
Calibration	init	Increases the number of oranges, (compared with a standard PolySpace verification)	Data that were constant are set to a wider range.	↑	↓

Reducing Oranges with DRS

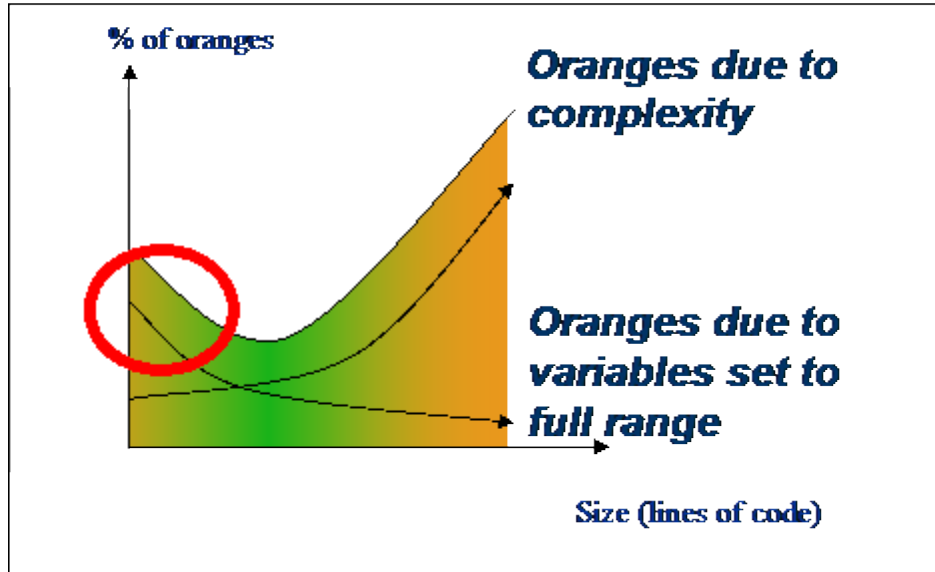
When performing robustness (worst case) verification, data inputs are always set to their full range. Therefore, every operation on these inputs, even a simple “one_input + 10” can produce an overflow, as the range of one_input varies between the min and the max of the type.

If you use DRS to restrict the range of “one-input” to the real functional constraints found in its specification, design document, or models, you can reduce the number of orange checks reported on the variable. For example, if you specify that “one-input” can vary between 0 and 10, PolySpace software will definitely know that:

- one_input + 100 will never overflow
- the results of this operation will always be between 100 and 110

This not only eliminates the local overflow orange, but also results in more accuracy in the data. This accuracy is then propagated through the rest of the code.

Using DRS removes the oranges located in the red circle below.



Why Is DRS Most Effective on Module Testing?

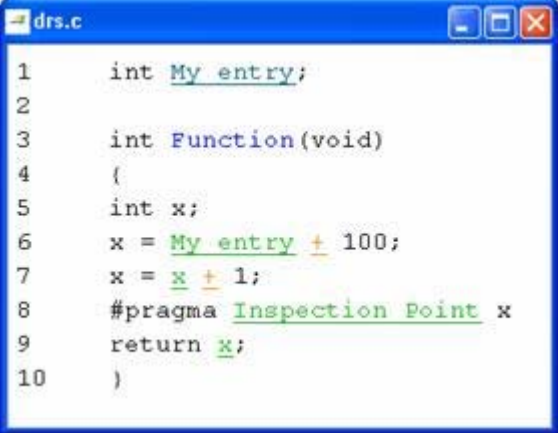
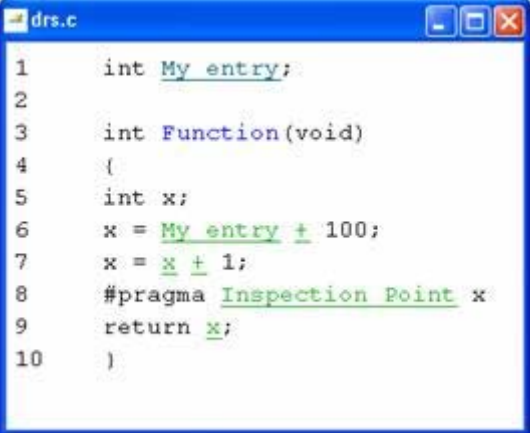
Removing oranges caused by full-range (worst-case) data can drastically reduce the total number of orange checks, especially when used on verifications of small files or modules. However, the number of orange checks caused by code complexity is not effected by DRS. For more information on oranges caused by code complexity, see “Subdividing Code” on page 7-39.

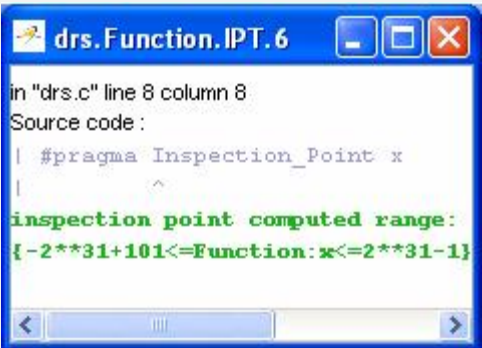
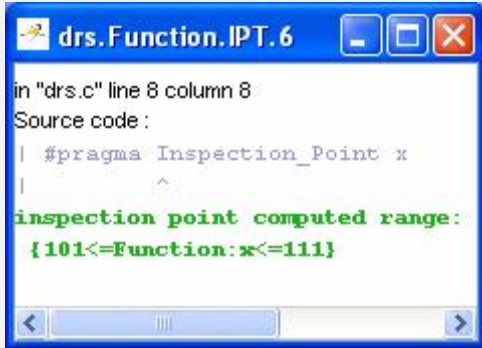
This section describes how DRS reduces oranges on files or modules only.

Example

The following example illustrates how DRS can reduce oranges. Suppose that in the real world, the input “My_entry” can vary between 0 and 10.

PolySpace verification produces the following results: one with DRS and one without.

Without DRS	With DRS – 2 Oranges Removed + Return Statement More Accurate
 <pre> 1 int My_entry; 2 3 int Function(void) 4 { 5 int x; 6 x = My_entry + 100; 7 x = x + 1; 8 #pragma Inspection Point x 9 return x; 10 } </pre>	 <pre> 1 int My_entry; 2 3 int Function(void) 4 { 5 int x; 6 x = My_entry + 100; 7 x = x + 1; 8 #pragma Inspection Point x 9 return x; 10 } </pre>
<ul style="list-style-type: none"> • With “<i>My_entry</i>“ being full range, the addition “+” is orange, • the result “x” is equal to all values between [min+100 max] • Due to previous computations, x+1 can here overflow too, making the addition “+”orange. 	<ul style="list-style-type: none"> • With “<i>My_entry</i>” being bounded to [0,10], the addition “+” is green • the result “x” is equal to [100,110] • Due to previous computations, x+1 can NOT overflow here, making the addition “+” green again.

Without DRS	With DRS – 2 Oranges Removed + Return Statement More Accurate
And the returned result is between [min+101 max]	And the returned result is between [101,111]
	

Preparing Source Code for Verification

- “Stubbing” on page 5-2
- “Preparing Code for Variables” on page 5-14
- “Preparing Code for Built-in Functions” on page 5-19
- “Preparing Multitasking Code” on page 5-20
- “Verifying “Unsupported” Code” on page 5-36

Stubbing

In this section...
“Stubbing Overview” on page 5-2
“Manual vs. Automatic Stubbing” on page 5-2
“Adding Precision Constraints Using Stubs” on page 5-6
“Default and Alternative Behavior for Stubbing (PURE and WORST)” on page 5-7
“Function Pointer Cases” on page 5-10
“Stubbing Functions with a Variable Argument Number” on page 5-10
“Finding Bugs in <code>_polyspace_stdstubs.c</code> ” on page 5-12

Stubbing Overview

A function stub is a small piece of code that emulates the behavior of a missing function.

Stubs do not need to model the details of the functions or procedures involved. They only need to represent the effect that the code might have on the remainder of the system.

Stubbing is useful because it allows you to verify code before all functions have been developed.

Manual vs. Automatic Stubbing

The approach you take to stubbing can have a significant influence on the speed and precision of your verification.

There are two types of stubs in PolySpace verification:

- **Automatic stubs** – When you attempt to verify code that calls an unknown function, the software automatically creates a stub function based on the function’s prototype (the function declaration). Automatic stubs generally do not provide insight into the behavior of the function.

- **Manual stubs** – You create these stub functions to emulate the behavior of the missing functions, and manually include them in the verification with the rest of the source code.

By default, PolySpace software automatically stubs functions. However, in some cases you may want to manually stub functions instead. For example, when:

- Automatic stubbing does not provide an adequate representation of the code it represents— both in regards to missing functions and assembly instructions.
- The entire code is to be provided, which may be the case when verifying a large piece of code. When the verification stops, it means the code is not complete.
- You want to improve the selectivity and speed of the verification.
- You want to gain precision by restricting return values generated by automatic stubs.
- You need to deal with a function that writes to global variables.

For Example:

```
void main(void)
{
    a=1;
    b=0;
    a_missing_function(&a, b);
    b = 1 / a;
}
```

Due to the reliance on the software's default stub, the division is shown with an orange warning because `a` is assumed to be anywhere in the full permissible integer range (including 0). If the function was commented out, then the division would be a green `"/`". A red `"/`" could only be achieved with a manual stub.

Note Automatically generated stubs do not deinitialize variables that are given as parameters.

Deciding which Stub Functions to Provide

In the following section, *procedure_to_stub* can represent either procedure or a sequence of assembly instructions which would be automatically stubbed in the absence of a manual stub. (Please refer to “Ignoring Assembly Code” on page 5-36).

Stubs do not need to model the details of the functions or procedures involved. They only need to represent the effect that the code might have on the remainder of the system.

Consider *procedure_to_stub*, If it represents:

- A timing constraint (such as a timer set/reset, a task activation, a delay, or a counter of ticks between two precise locations in the code) then you can stub it to an empty action (void *procedure*(void)). PolySpace needs no concept of timing since it takes into account all possible scheduling and interleaving of concurrent execution. There is therefore no need to stub functions that set or reset a timer. Simply declare the variable representing time as volatile.
- An I/O access: maybe to a hardware port, a sensor, a read/write of a file, a read of an EEPROM, or a write to a volatile variable. There is no need to stub a write access. If you wish to do so, simply stub a write access to an empty action (void *procedure*(void)). Stub read accesses to "read all possible values (volatile)".
- A write to a global variable. In this case, you may need to consider which procedures or functions write to it and why. Do not stub the concerned *procedure_to_stub* if:
 - The variable is volatile;
 - The variable is a task list. Such lists are accounted for by default because all tasks declared with the -task option are automatically modelled as though they have been started. Write a *procedure_to_stub* by hand if

- The variable is a regular variable read by other procedures or functions.
- A read from a global variable: If you want PolySpace to detect that it is a shared variable, you need to stub a read access. This is easily achieved by copying the value into a local variable.

In general, follow the Data Flow and remember that:

- PolySpace only cares about the C code which is provided;
- PolySpace need not be informed of timing constraints because all possible sequencing is taken into account;
- You can refer to execution hypotheses made by PolySpace for a complete list of constraints.

Example

The following example shows a header for a missing function (which might occur, for example, if the code is a subset of a project.) The missing function copies the value of the src parameter to dest so there would be a division by zero - a runtime error - at run time.

```
void main(void)
{
    a = 1;
    b = 0;
    a_missing_function(&a, b);
    b = 1 / a;
}
```

Due to the reliance on the software's default stub, the division is shown with an orange warning because a is assumed to be anywhere in the full permissible integer range (including 0). If the function was commented out, then the division would be a green "/". A red "/" could only be achieved with a manual stub.

Default Stubbing	Manual Stubbing	Function ignored
<pre>void main(void) { a = 1; b = 0; a_missing_function(&a, b); b = 1 / a; // orange division }</pre>	<pre>void a_missing_function (int *x, int y;) { *x = y; } void main(void) { a = 1; b = 0; a_missing_function(&a, b); b = 1 / a; // red division</pre>	<pre>void a_missing_function (int *x, int y;) { } void main(void) { a = 1; b = 0; a_missing_function(&a, b); b = 1 / a; // green division</pre>

Due to the reliance on the software's default stub, the assembly code is ignored and the division "/" is green. The red division "/" could only be achieved with a manual stub.

Summary

Stub manually to gain precision by restricting return values generated by automatic stubs; to deal with a function which writes to global variables.

Stub automatically in the knowledge that no runtime error will be ever introduced by automatic stubbing; to minimize preparation time.

Adding Precision Constraints Using Stubs

You can improve the selectivity of your verification by using stubs to indicate that some variables vary within functional ranges instead of the full range of the considered type.

You can apply this approach to:

- Parameters passed to functions.
- Variables that change from one execution to another (mostly globals).
Typically, this might include things like calibration data or mission specific

data. These variables might be read directly within the code, or read through an API of functions.

If a function returns an integer, default automatic stubbing assumes that it can take any value from the full type of an integer. This can lead to unproven code (orange checks) in your results. You can achieve more precise results by providing a manual stub that provides “outside” data that is representative of the data expected when the code is implemented.

There are a number of ways to model such data ranges within the code. The following table shows three possible approaches.

with volatile and assert	with assert and without volatile	without assert, without volatile, without "if"
<pre>#include <assert.h> int stub(void) { volatile int random; int tmp; tmp = random; assert(tmp>=1 && tmp<=10); return</pre>	<pre>#include <assert.h> extern int other_func(void); int stub(void) { int tmp; tmp= other_func(); assert(tmp>=1 && tmp<=10); return }</pre>	<pre>extern int other_func(void); int stub(void) { int tmp; do {tmp= other_func();} while (tmp<1 tmp>10); return tmp; }</pre>

There is no particular advantage to any of these approaches, except that the assertions in the first two can produce orange orange checks in your results.

Default and Alternative Behavior for Stubbing (PURE and WORST)

External functions are assumed to have no effect (read, write) on global variables. Any external function for which this assumption is not valid must be explicitly stubbed.

Consider the example `int f(char *)`;

When verifying this function, there are three options for automatic stubbing, as shown in the following table.

Approach	Worst Case Scenario in Stub
Default automatic stubbing	<pre>int f(char *x) { *x = rand(); return 0; }</pre>
pragma POLYSPACE_WORST	<pre>int f(char *x) { strcpy(x, "the quick brown fox, etc."); return &(x[2]); }</pre>
pragma POLYSPACE_PURE	<pre>int f(char *x) { return strlen(x); }</pre>

If the automatic stub does not accurately model the function using any of these approaches, you can use manual stubbing to achieve more precise results.

Stubbing Examples

The following table provides examples of the three stubbing approaches.

Initial Prototype	With pragma POLYSPACE_PURE	With pragma POLYSPACE_WORST	PolySpace default automatic stubbing
void f1(void);	Do nothing		

Initial Prototype	With pragma POLYSPACE_PURE	With pragma POLYSPACE_WORST	PolySpace default automatic stubbing
int f2 (int u);	Returns $[-2^{31}, 2^{31}-1]$	Returns $[-2^{31}, 2^{31}-1]$ and assumes the ability to write into (int *) u	Returns $[-2^{31}, 2^{31}-1]$
int f3 (int *u);			Assumes the ability to write into *u to any depth and returns $[-2^{31}, 2^{31}-1]$
int* f4 (int u);	Returns an absolute address (AA)	Returns AA or (int *) u and assumes the ability to write into (int *) u	Returns an absolute address
int* f5 (int *u);	Returns an absolute address	Returns $[-2^{31}, 2^{31}-1]$ and assumes the ability to write into *u, to any depth	Assumes the ability to write into *u, to any depth and returns an absolute address
void f6 (void (*ptr)(int), param2)	Does nothing	The function pointed to by ptr will be called with a full-range random value for the integer. Rules for param2 are as above.	
void f7 (void (*ptr)(param2)		Unless the option <code>-permissive-stubber</code> , is used, this function is not stubbed. The parameter (int *) associated with the function pointer is too complicated for PolySpace to stub it, and PolySpace stops. You must stub this function manually. Note If (*ptr) contains a pointer as a parameter, it won't be stubbed automatically and with <code>-permissive-stubber</code> , the function pointer ptr is called with random as a parameter.	

Function Pointer Cases

Function Prototype	Comments
<pre>int f(void (*ptr_ok)(int, char, float), other_type1 other_param1);</pre>	The -permissive-stubber option is not required.
<pre>int f(void (*ptr_ok)(int *, char, float), other_type1 other_param1);</pre>	The -permissive-stubber option is required because of the “int *” parameter of the function pointer passed as an argument
<pre>void _reg(int); int _seq(void *); unsigned char bar(void){ return 0; } void main(void){ unsigned char x=0; _reg(_seq(bar)); }</pre>	<p>Both functions “_reg” and “_seq” are automatically stubbed, but the call to the “bar” function is not exercised by the PolySpace software.</p> <p>The function that is a parameter is only called in stubbed functions if the stubbed function prototype contains a function pointer as parameter.</p> <p>Since here that is a “void *”, its not a function pointer</p>

Stubbing Functions with a Variable Argument Number

PolySpace is capable of stubbing most vararg functions. Nevertheless,

- This can generate imprecision in pointer verification;
- It causes a significant increase in complexity and hence in verification time.

There are three possible ways to deal with this.

- stub manually

- Add a `#pragma POLYSPACE_PURE "function_1"` on every varargs function that you know to be pure. This can reduce the complexity of pointer verification tenfold.

For example:

```
#pragma POLYSPACE_PURE f

void main(void) {
    int x = 0;
    f(&x);
    assert ( x == 0 ); // Green assertion,
                       //orange without use of #pragma POLYSPACE_PURE
}
```

- use `#define` to eliminate calls to functions. This is useful with functions like `printf` that generate complexity but are not useful for the verification, since they simply display a message.

For example:

```
#ifdef POLYSPACE
#define example_of_function(format, args...)
#else
void example_of_function(char * format, ...)
#endif
void main(void)
{
    int i = 3;
    example_of_function("test1 %d", i);
}
```

```
polyspace-c -D POLYSPACE
```

You can place this kind of line in any `.c` or `.h` file of the verification.

Note You should use `#define` only with functions that are pure.

Finding Bugs in `__polyspace_stdstubs.c`

By performing a selective orange review, you can sometimes find bugs in the `__polyspace_stdstubs.c` file. As for other oranges in the code, some are useless, others highlight real problems. How can we isolate the useful ones?

There are a number of practical ways to make it easy for the user to detect the useful oranges:

- Create the file using approaches with are sympathetic to PolySpace needs. This will yield up to 90% less useless oranges. For instance,
- Use functions that return random values instead of local volatile variables;
- Initialize char variables with a random char instead of a volatile int in order to reduce the number of overflow checks;
- Define an "APPLY_CONSTRAINT()" macro. Such a function will always create an orange check but it will be easy to filter.
- By checking oranges manually in the `__polyspace_stdstubs.c` file — many comments are included to explain where an orange is expected and why.

Collectively, these features turn the chore of separating out the useful orange warnings into a fast and painless activity.

The user should start by reading IDP checks.

Example

The orange check in `fgets()` is one such check.

```
for (i=0; i < length; i++) /* write in s up to n-1 char */
    s[i] = __polyspace_random_char();
    ^
IDP
```

This orange check is definitely a significant one. It means that PolySpace could not conclude that the buffer which is given as an argument to `fgets()` is always big enough to contain the specified character count. So, the severity of the problem highlighted depends on how the function is called in the application.

The check shouldn't generally be orange unless it is highlighting a real issue (unless `fgets()` is called very frequently. In that case, try using the `context-sensitivity` or `-inline` options).

Preparing Code for Variables

In this section...

“Assigning Ranges to Variables/Assert?” on page 5-14

“Checking Properties on Global Variables at Any Point: Global assert” on page 5-15

“Modeling Variable Values External to my Application” on page 5-15

“How are Variables Initialized?” on page 5-16

“Verifying Code with Undefined or Undeclared Variables and Functions” on page 5-18

Assigning Ranges to Variables/Assert?

Abstract

How can I use assert in PolySpace?

Explanation

Assert is a UNIX/linux/windows macro that aborts the program if the test performed inside the assertion proves to be false.

Assert failures are real RTEs because they lead to a processor halt. Because of this, PolySpace will produce checks for them. The behavior matches that exhibited during execution, because **all execution paths for unsatisfied conditions are truncated** (red and then gray). Thus it can be assumed that any verification performed downstream of the assert uses value ranges which satisfy the assert conditions.

Also refer to the use of volatile.

Solution

Assert can be used to constrain input variables to values within a particular range, for example:

```
#include <stdlib.h>
```



```

int random(void);

int return_between_bounds(int min, int max)
{
    int ret; // ret is not initialized
    ret = random(); // ret ~ [-2^31, 2^31-1]
    assert ((min<=ret) && (ret<=max));
    // assert is orange because the condition may or may not
    // be fulfilled
    // ret ~ [min, max] here because all execution paths that don't
    // meet the condition are stopped
    return ret;
}

```

Checking Properties on Global Variables at Any Point: Global assert

The global assert mechanism works by inserting a check on each write access to a global variable to ensure it is the range specified.

You enable this feature using DRS `globalassert` mode.

For more information, see “Applying Data Ranges to External Variables and Stub Functions (DRS)” on page 4-26.

Modeling Variable Values External to my Application

There are three main considerations.

- Usage of volatile variable;
- Express that the variable content can change at every new read access;
- Express that some variables are external to the application.

A volatile variable can be defined as a variable which does not respect following axiom:

"if I write a value V in the variable X, and if I read X's value before any other writing to X occurs, I will get V."

Thus the value of a volatile variable is "unknown". It can be any value that can be represented by a variable of its type, and that value can change at any time - even between 2 successive memory accesses.

A volatile variable is viewed as a "permanent random" by PolySpace because the value may have changed between one read access and the next.

Note Although the volatile characteristic of a variable is also commonly used by programmers to avoid compiler optimization, this characteristic has no consequence for PolySpace.

```
int return_random(void)
{
    volatile int random; // random ~ [-2^31, 2^31-1], although
                        // random is not initialized
    int y;
    y = 1 / random;    // division and init orange because
                        // random ~ [-2^31, 2^31-1]
    random = 100;
    y = 1 / random;    // division and init orange because
                        // random ~ [-2^31, 2^31-1]
    return random;    // random ~ [-2^31, 2^31-1]
}
```

How are Variables Initialized?

Consider external, volatile and absolute address variable in the following examples.

Extern

PolySpace works on the principle that a global or static extern variable could take any value within the range of its type.

```
extern int x;
void f(void)
int y;
y = 1 / x; // orange because x ~ [-2^31, 2^31-1]
y = 1 / x; // green because x ~ [-2^31 -1] U [1, 2^31-1]
```

Refer to “Before You Review PolySpace Results” on page 8-2 for more information on color propagation.

For extern structures containing fields of type “pointer to function”, this principle leads to red errors in the viewer. In this case, the resulting default behavior is that these pointers don’t point to any valid function. For results to be meaningful here, you may well need to define these variables explicitly.

Volatile

```
volatile int x; // x ~ [-2^31, 2^31-1], although x has not been
initialised
```

- if x is a global variable, the NIV is green
- if x is a local variable, the NIV is always orange

Absolute Addressing

The content of an absolute address is always considered to be potentially uninitialized (NIV orange):

```
int y;

void f1(void) {

#define X (* ((int *)0x20000))
  X = 100;
  y = 1 / X;    // NIV on X is orange
}

void f2(void) {
  int *p = (int *)0x20000;
  *p = 100;
  y = 1 / *p;  // NIV on *p is orange
}
```

Verifying Code with Undefined or Undeclared Variables and Functions

The definition and declaration of a variable are two different but related operations that are frequently confused.

Definition

- **for a function:** the body of the function has been written: `int f(void) { return 0; }`
- **for a variable:** a part of memory has been reserved for the variable: `int x;` or `extern int x=0;`

When a variable is not defined, you must specify the option **Continue even with undefined global variables** (`-allow-undef-variable`) before you start a verification. When you specify this option, PolySpace software considers the variable to be initialized, and to potentially have any value in its full range (see “How are Variables Initialized?” on page 5-16).

When a function is not defined, it is stubbed automatically.

Declaration

- **for a function:** the prototype: `int f(void);`
- **for an external variable:** `extern int x;`

A declaration provides information about the type of the function or variable. If the function or variable is used in a file where it has not been declared, a compilation error will result.

Preparing Code for Built-in Functions

PolySpace stubs all functions that are not defined within the verification. Polyspace provides an accurate stub for all the functions defined in the standard `libc`, taking into account functional aspect of the function.

All these functions are declared in the standard list of headers, and can be redefined using their own definitions by invalidating the associated set of functions:

- Using `D POLYSPACE_NO_STANDARD_STUBS` for all functions declared in Standard ANSI headers: `assert.h`, `ctype.h`, `errno.h`, `locale.h`, `math.h`, `setjmp.h` ('`setjmp`' and '`longjmp`' functions are partially implemented – see `<polyspace>/cinclude/__polyspace__stdstubs.c`), `signal.h` ('`signal`' and '`raise`' functions are partially implemented – see `<polyspace>/cinclude/__polyspace__stdstubs.c`), `stdio.h`, `stdarg.h`, `stdlib.h`, `string.h`, and `time.h`.
- Using `D POLYSPACE_STRICT_ANSI_STANDARD_STUBS` for functions only declared in `strings.h`, `unistd.h`, and `fcntl.h`.

Generally, these functions can be redefined and analyzed by PolySpace by invalidating the associated set of functions or only the specific function using `D __polyspace_no_<function name>`. For example, If you want to redefine the `fabs()` function, you need to add the `D __polyspace_no_fabs` directive and add the code of your own `fabs()` function in a PolySpace verification.

There are five exceptions to these rules The following functions which deal with memory allocation can not be redefined: `malloc()`, `calloc()`, `realloc()`, `valloc()`, `alloca()`, `__built_in_malloc()` and `__built_in_alloca()`.

Preparing Multitasking Code

In this section...
“PolySpace Software Assumptions” on page 5-20
“Modelling Synchronous Tasks” on page 5-21
“Modelling Interruptions and Asynchronous Events/Tasks/Threads” on page 5-23
“Are Interruptions Maskable or Preemptive by Default?” on page 5-25
“Shared Variables” on page 5-27
“Mailboxes” on page 5-30
“Atomicity (Can an Instruction be Interrupted by Another)” on page 5-33
“Priorities” on page 5-34

PolySpace Software Assumptions

This section describes the default behavior of the PolySpace software. If your code does not conform to these assumptions, you must make minor modifications to the code before starting verification.

The assumptions are as follows:

- The main procedure must terminate in order for entry-points (or tasks) to start.
- All tasks or entry-points start after the end of the main without any predefined basis regarding: the sequence, priority or preemption. If an entry-point is seen as dead code, it is because the main contains a red error and therefore does not terminate.
- PolySpace considers that there is no atomicity, nor timing constraints.
- Only entry points with `void any_name (void)` as prototype will be considered.

The MathWorks recommends that you read this entire section before applying the rules described below. Some rules are mandatory, and others allow you to gain selectivity.

Modelling Synchronous Tasks

In some circumstances, you must adapt your source code to allow synchronous tasks to be taken into account.

Suppose that an application has the following behavior:

- Once every 10 ms: `void tsk_10ms(void);`
- Once every 30 ms: ...
- Once every 50 ms

These tasks never interrupt each other. They include no infinite loops, and always return control to the calling context. For example:

```
void tsk_10ms(void)
{ do_things_and_exit();
  /* it's important it returns control*/
}
```

However, if you specify each entry-point at launch using the option:

```
polyspace-c -entry-points tsk_10ms,tsk_30ms,tsk_50ms
```

then the results are NOT valid, because each task is only called once.

To address this problem, you must specify that the tasks are purely sequential — that is, that they are functions to be called in a deterministic order. You can do this by writing a function to call each of the tasks in the correct sequence, and then declaring this new function as a single task entry point.

Solution 1

Write a function that calls the cyclic tasks in the right order: this is an **exact sequencer**. This sequencer is then specified at launch time as a single task entry point.

This solution:

- **is very precise;**
- requires knowledge of the exact sequence of events.

For example, the sequencer might be:

```
void one_sequential_C_function(void)
{
    while (1) {
        tsk_10ms();
        tsk_10ms();
        tsk_10ms();
        tsk_30ms ();
        tsk_10ms();
        tsk_10ms();
        tsk_50ms ();
    }
}
```

and the associated launching command:

```
polyspace-c -entry-points one_sequential_C_function
```

Solution 2

Make an **upper approximation sequencer**, taking into account every possible scheduling.

This solution:

- is less precise;
- **is quick to code**, especially for complicated scheduling

For example, the sequencer might be:

```
void upper_approx_C_sequencer(void)
{
    volatile int random;
    while (1) {
        if (random) tsk_10ms();
        if (random) tsk_30ms();
    }
}
```



```

        if (random) tsk_50ms();
        if (random) tsk_100ms();
        .....
    }
}

```

and the associated launching command:

```
polyspace-c -entry-points upper_approx_C_sequencer
```

Note If this is the only entry-point, then it can be added at the end of the main rather than specified as a task entry point.

Modelling Interruptions and Asynchronous Events/Tasks/Threads

You can adapt your source code to allow PolySpace software to consider both *asynchronous* tasks and *interruptions*. For example:

```

void interrupt isr_1(void)
{ ... }

```

Without such an adaptation, interrupt service routines will appear as gray (dead code) in the Viewer. The gray code indicates that this code is not executed and is not taken into account, and so all interruptions and tasks are ignored by PolySpace.

The standard execution model is such that the main is executed initially. Only if the main terminates and returns control (i.e. if it is not an infinite loop and has no red errors) will the entry points be started, with all potential starting sequences being modelled automatically. There are several different approaches which may be adopted to implement the required adaptations.

Solution 1: Where interrupts (ISRs) CANNOT preempt each other

If these 3 following conditions are fulfilled:

- the interrupt functions `it_1` and `it_2` (say) can never interrupt each other;

- each interrupt can be raised several times, at any time;
- they are returning functions, and not infinite loops.

Then these non preemptive interruptions may be grouped into a single function, and that function declared as a entry point.

```
void it_1(void);
void it_2(void);

void all_interruptions_and_events(void)
{ while (1) {
  if (random()) it_1();
  if (random()) it_2();
  ... }
}
```

The associated launching command would be:

```
polyspace-c -entry-points all_interruptions_and_events
```

Solution 2: Where interrupts CAN pre-empt each other

If two ISRs can be each be interrupted by the other, then:

- encapsulate each of them in a loop
- declare each loop as a entry point.

One way of approaching that is to replace the original file with a PolySpace version, as illustrated below.

```
original_file.c
void it_1(void)
{
  ... return;
}

void it_2(void)
{
  ... return;
}
```

```
void one_task(void)
{
    ... return;
}

polyspace.c
void polys_it_1(void)
{
    while (1)
    if (random())
        it_1();
}

void polys_it_2(void)
{
    while (1)
    if (random())
        it_2();
}

void polys_one_task(void)
{
    while (1)
    if (random())
        one_task();
}
```

The associated launching command would be

```
polyspace-c -entry-points polys_it_1,polys_it_2,polys_one_task
```

Are Interruptions Maskable or Preemptive by Default?

For user interruptions, no *implicit* critical section is defined: they all need to be written by hand.

Sometimes, an application which includes interrupts has a critical section written into its main entry point, but shared data is still flagged as unprotected.

This occurs because PolySpace does not distinguish between interrupt service routines and tasks. If you specify an interrupt to be a "-entry-point" entry point, it will have the same priority level as the other procedures declared as tasks ("-entry-points" option). So, because PolySpace makes an **upper approximation of all scheduling and all interleaving**, in this case that **includes the possibility that the ISR might be interrupted by any other task**. There are more paths modelled than could happen during execution, but this has no adverse effect on of the results obtained except that more scenarios are considered than could happen during "real life" execution - and the shared data is not seen as being protected.

To address this, the interrupt needs to be embedded in a specific procedure that uses the same critical section as the one used in the main task. Then, each time this function is called, the task will enter a critical section which will model the behavior of a nonmaskable interruption.

Original files

```
int shared_x ;

void my_main_task(void)
{
    // ...
    MASK_IT;
    shared_x = 12;
    UMASK_IT;
    // ...
}
int shared_x ;

void interrupt my_real_it(void)
{ /* which is by specification unmaskable */
    shared_x = 100;
}
```

Additional C files required by PolySpace:

```

extern void my_real_it(void); // declaration required

#define MASK_IT pst_mask_it()
#define UMASK_IT pst_unmask_it()

void pst_mask_it(void); // functions used to model the critical section
void pst_unmask_it(void); //

void other_task (void)
{
    MASK_IT;
    my_real_it();
    UMASK_IT;
}

```

The associated launch command:

```

polyspace-c \
-D interrupt= \
-entry-points my_main_task,other_task \
-critical-section-begin "pst_mask_it:table" \
-critical-section-end "pst_unmask_it:table"

```

Shared Variables

When PolySpace is launched without any options, all tasks are examined as though concurrent and with no assumptions about priorities, sequence order, or timing. Shared variables in this context will always be considered unprotected, and so will all be shown as orange in the variable dictionary.

The following explicit protection mechanisms can be used to protect the variables:

- critical section
- mutual exclusion

See details below:

- “Critical Sections” on page 5-28

- “Mutual Exclusion” on page 5-29
- “Semaphores” on page 5-30

Critical Sections

This is the most common protection mechanism found in applications, and is simple to represent in PolySpace:

- if one entry-point makes a call to a particular critical section, all other entry-points will be blocked on the "critical-section-begin" function call until the originating entry-point calls the "critical-section-end" function,
- this does not mean the code between two critical sections is atomic;
- it is a binary semaphore, so there is only one token per label (CS1 in the example below). Unlike many implementations of semaphores, it is not a decrementing counter that can keep track of a number of attempted accesses.

Consider the following example.

Original Code

```
void proc1(void)
{
    MASK_IT;
    x = 12; // X is protected
    y = 100;
    UMASK_IT;
}
void proc2(void)
{
    MASK_IT;
    x = 11; // X is protected
    UMASK_IT;
    y = 101; // Y is not protected
}
```

File Replacing the Original Include File

```
void begin_cs(void);
```

```
void end_cs(void);
#define MASK_IT begin_cs()
#define UMASK_IT end_cs()
```

Command line to launch PolySpace

```
polyspace-c \  
-entry-point proc1,proc2 \  
-critical-section-begin"begin_cs:label_1" \  
-critical-section-end"end_cs:label_1"
```

Mutual Exclusion

Mutual exclusion between tasks or interrupts can be implemented while preparing PolySpace for launching.

Suppose there are entry-points which never overlap each other, and that variables are shared by nature.

If entry-points are mutually exclusive, i.e. if they do not overlap in time, you may want PolySpace to take that into account. Consider the following example.

These entry points cannot overlap:

- t1 and t3
- t2, t3 and t4

These entry-points can overlap:

- t1 and t2
- t1 and t4

Before launching verification, the names of mutually exclusive entry-points are placed on a single line

```
polyspace-c -temporal-exclusion-file myExclusions.txt  
-entry-points t1,t2,t3,t4
```

The file `myExclusions.txt` is also required in the current directory. This will contain:

```
t1 t3
t2 t3 t4
```

Semaphores

Although it is possible to implement in `c`, it is not possible to take into account a semaphore system call in PolySpace. Nevertheless, Critical sections may be used to model the behavior.

Mailboxes

Suppose that an application has several tasks, some of which post messages in a mailbox while others read them asynchronously.

This communication mechanism is possible because the OS libraries provide send and receive procedures. It is likely that the source files will be unavailable because the procedures are part of the OS libraries, but the mechanism needs to be modelled if the verification is to be meaningful.

By default, PolySpace will automatically stub the missing OS send and receive procedures. Such a stub will exhibit the following behavior:

- for send (`char *buffer`, `int length`), the content of the buffer will be written only when the procedure is called;
- for receive (`char *buffer`, `int *length`), each element of the buffer will contain the full range of values appropriate to that data type.

This and other mechanisms are available, with different levels of precision.

Let PolySpace stub automatically

- quick and easy to code;
- **imprecise** because there is no direct connection between a mailbox sender and receiver. That means that even if the sender is only submitting data within a small range, the full data range appropriate for the type(s) will be for the receiver data.

Provide a **real mailbox** mechanism

- can be very costly (time consuming) to implement;
- can introduce errors in the stubs;
- provides little additional benefit when compared to the upper approximation solution

Provide an **upper approximation of the mailbox**

This models the mechanism such that new read from the mailbox reads **one** of the recently posted messages, but not necessarily the last one.

- quick and easy to code;
- **gives precise results;**

Consider the following detailed implementation of the upper approximation solution.

polyspace_mailboxes.h

```
typedef struct _r {
    int length;
    char content[100];
} MESSAGE;
extern MESSAGE mailbox;
void send(MESSAGE * msg);
void receive(MESSAGE *msg);
```

polyspace_mailboxes.c

```
#include "polyspace_mailboxes.h"

MESSAGE mailbox;

void send(MESSAGE * msg)
{
    volatile int test;
    if (test) mailbox = *msg;
    // a potential write to the mailbox
}

void receive(MESSAGE *msg)
{
    *msg = mailbox;
}
```

Original code

```
#include "polyspace_mailboxes.h"

void t1(void)
{
    MESSAGE msg_to_send;
    int i;
    for (i=0; i<100; i++)
        msg_to_send.content[i] = i;
    msg_to_send.length = 100;
    send(&msg_to_send);
}

void t2(void)
{
    MESSAGE msg_to_read;
    receive (&msg_to_read);
}
```

PolySpace then proceeds on the assumption that each new read from the mailbox reads a message, but not necessarily the last one.

The associated launching command is

```
polyspace-c -entry-points t1,t2
```

Atomicity (Can an Instruction be Interrupted by Another)

Atomic: In computer programming, atomic describes a unitary action or object that is essentially indivisible, unchangeable, whole, and irreducible

Atomicity: In a transaction involving two or more discrete pieces of information, either all of the pieces are committed or none are.

Instructional decomposition

In general terms, PolySpace does not take into account either CPU instruction decomposition or timing considerations.

It is assumed by PolySpace that instructions are never atomic except in the case of read and write instructions. PolySpace makes an **upper approximation of all scheduling and all interleaving**. There are more paths modelled than could happen during execution, but given that **all possible paths are always analyzed**, this has no adverse effect on of the results obtained.

Consider a 16 bit target that can manipulate a 32 bit type (an int, for example). In this case, the CPU needs at least two cycles to write to an integer.

Suppose that x is an integer in a multitasking system, with an initial value of 0x0000. Now suppose 0xFF55 is written it. If the operation was not atomic it could be interrupted by another instruction in the middle of the write operation.

- Task 1: Writes 0xFF55 to x.
- Task 2: Interrupts task 1. Depending on the timing, the value of x could be any of 0xFF00, 0x0055 or 0xFF55.

PolySpace considers write/read instructions atomic, so **task 2 can only read 0xFF55**, even if X is not protected (refer to “Shared Variables” on page 5-27).

Critical sections

In terms of critical sections, PolySpace does not model the concept of atomicity. A critical section only guarantees that once the function associated with `-critical-section-begin` has been called, any other function making use of the same label will be blocked. All other functions can still continue to run, even if somewhere else in another task a critical section has been started.

PolySpace's verification of Runtime Errors (RTEs) supposes that there was no conflict when writing the shared variables. Hence, even if a shared variable is not protected, the RTE verification is complete and correct.

More information is available in "Critical Sections" on page 5-28.

Priorities

Priorities are not taken into account by PolySpace as such. However, the timing implications of software execution are not relevant to the verification performed by PolySpace, which is usually the primary reason for implementing software task prioritization. In addition, priority inversion issues can mean that it would be dangerous to assume that priorities can protect shared variables. For that reason, PolySpace makes no such assumption.

In practice, while there is no facility to specify differing task priorities, all priorities **are** taken into account because the default behavior of the software assumes that:

- all task entry points (as defined with the option `-entry-points`) start potentially at the same time;
- they can interrupt each other in any order, no matter the sequence of instructions - and so all possible interruptions will be accounted for, in addition to some which can never occur in practice.

If you have two tasks `t1` and `t2` in which `t1` has higher priority than `t2`, simply use `polyspace-c -entry-points t1,t2` in the usual way.

- `t1` will be able to interrupt `t2` at any stage of `t2`, which models the behavior at execution time;

- t2 will be able to interrupt t1 at any stage of t1, which models a behavior which (ignoring priority inversion) would never take place during execution. PolySpace has made an **upper approximation of all scheduling and all interleaving**. There are more paths modelled than could happen during execution, but this has no adverse effect on of the results obtained.

Verifying “Unsupported” Code

In this section...
“Ignoring Assembly Code” on page 5-36
“Dealing with Backward “goto” Statements” on page 5-43
“Types Promotion” on page 5-45

Ignoring Assembly Code

You can ignore assembly code during verification using the **Discard assembly code** option (`-discard-asm`). Using this option can deal with many instances of assembly code within a C application, but it is not always a valid route to take.

Ignored assembly instructions will change the behavior of the code. For example, a write access to a shared variable can be written in assembly code. If this write access is ignored, the verification may produce inaccurate results.

In such cases, please refer to “Stubbing” on page 5-2, which applies to functions as well as to stubbed instructions.

PolySpace is designed for C code only. In most cases, the option `-discard-asm` combined with `-asm-begin` and `-asm-end` can be used to instruct PolySpace to discard a number of assembly code constructs:

- “Example: Ignore All Statements, the Rest of the Function Remains Unchanged” on page 5-37
- “Example: Automatic Stubbing” on page 5-39
- “Examples: Empty Body” on page 5-40
- “Example: #asm and #endasm Support” on page 5-41
- “Example: What to Do If `-discard-asm` Fails to Parse an `asm` Code Section” on page 5-42

Example: Ignore All Statements, the Rest of the Function Remains Unchanged

Discarding assembly code by using the `-discard-asm` is an acceptable approach where ignoring the assembly instructions will have no impact on the remainder of the function.

Also refer to the “Manual versus automatic stubbing”

```

int f(void)
{
    asm ("% reg val; mtmsr val;");
    asm ("\tmove.w #$2700,sr");
    asm ("\ttrap #7");
    asm(" stw r11,0(r3) ");
    assert (1); // is green
    return 1;
}

int other_ignored6(void)
{
#define A_MACRO(bus_controller_mode) \
    __asm__ volatile("nop"); \
    __asm__ volatile("nop"); \
    __asm__ volatile("nop"); \
    __asm__ volatile("nop"); \
    __asm__ volatile("nop"); \
    __asm__ volatile("nop")
    assert (1); // is green
    A_MACRO(x);
    assert (1); // is green
    return 1;
}

int pragma_ignored(void)
{
    #pragma asm
    SRST
    #pragma endasm
    assert (1); // is green
}

```

```
int other_ignored2(void)
{
    asm "% reg val; mtmsr val;";
    asm mtmsr val;
    assert (1); // is green
    asm ("px = pm(0,%2); \
        %0 = px1; \
        %1 = px2;"
        : "=d" (data_16), "=d" (data_32)
        : "y" ((UI_32 pm *)ram_address):
        "px");
    assert (1); // is green
}

int other_ignored1(void)
{
    __asm
    {MOV R8,R8
     MOV R8,R8
     MOV R8,R8
     MOV R8,R8
     MOV R8,R8}
    assert (1); // is green
}

int GNUC_include (void)
{
    extern int __P (char *__pattern, int __flags,
                  int (*__errfunc) (char *, int),
                  unsigned *__pglob) __asm__ ("glob64");
    __asm__ ("rorw $8, %w0" \
            : "=r" (__v) \
            : "0" ((guint16) (val)));
    __asm__ ("st g14,%0" : "=m" (*(AP)));
    __asm__(" \
            : "=r" (__t.c) \
            : "0" (((union { int i, j; } *) (AP))++)->i));
    assert (1); // is green
    return (int) 3 __asm__("% reg val");
}
```



```

}

int other_ignored3(void)
{
    __asm {ldab 0xffff,0;trapdis;};
    __asm {ldab 0xffff,1;trapdis;};
    assert (1); // is green
    __asm__ ("% reg val");
    __asm__ ("mtmsr val");
    assert (1); // is green
    return 2;
}

int other_ignored4(void)
{
    asm {
        port_in: /* byte = port_in(port); */
        mov EAX, 0
        mov EDX, 4[ESP]
        in AL, DX
        ret
        port_out: /* port_out(byte,port); */
        mov EDX, 8[ESP]
        mov EAX, 4[ESP]
        out DX, AL
        ret }
    assert (1); // is green
}

```

Example: Automatic Stubbing

When a function is preceded by `asm`, it will be stubbed automatically, even if a body is defined.

```
asm int m(int tt);
```

You must use the `-discard-asm` option.

Examples: Empty Body

Using the option `#pragma inline_asm(list of functions)` has the same effect.

You must use the `-discard-asm` option.

```
pragma inline_asm(ex1, ex2) // the 2 functions ex1 and ex2 will be
                             // stubbed, even if their body is defined

int ex1(void)
{
    % reg val;
    mtmsr val;
    return 3;    // is ignored
};

int ex2(void)
{
    % reg val;
    mtmsr val;
    assert (1); // is ignored
    return 3;
};

#pragma inline_asm(ex3) // the definition of ex3 is ignored

int ex3(void)
{
    % reg val;
    mtmsr val;    // is ignored
    return 3;
};

asm int h(int tt) // using the qualifier asm is equivalent
                 // to #pragma inline_asm
{
    % reg val;    // is ignored
    mtmsr val;    // is ignored
}
```

```

    return 3;    // is ignored
};

void f(void) {
    int x;

    x = ex1();    // ex1 is stubbed : x is full-range
    x = ex2();    // x is full-range
    x = ex3();    // x is full-range
    x = h(3);     // x is full-range
}

```

Also refer to “Stubbing” on page 5-2.

Example: #asm and #endasm Support

Using #asm and #endasm allows fragments of (typically) assembly code to be disregarded by PolySpace, regardless of whether or not you use the -discard-asm.

Consider the following example.

```

void test(void)
{
#asm
    mov _as:pe, reg
    jre _nop
#endasm
    int r;
    r=0;
    r++;
}

```

Explanation

By default, the usage of #asm and #endasm requires the usage of the -asm-begin and -asm-end options in the following way. The syntax to use this facility when launching PolySpace in batch mode is:

```
polyspace-c -asm-begin asm -asm-end endasm
```

Example: What to Do If `-discard-asm` Fails to Parse an asm Code Section

Occasionally, the `-discard-asm` option does not deal with a particular assembly code construction, particularly when the code fragment is compiler specific

Note You could also consider using the `-asm-begin` and `-asm-end` options instead of the following approach).

Consider this example.

```
1 int x=12;
2
3 void f(void)
4 {
5 #pragma will_be_ignored
6 x =0;
7 x= 1/x;      // no color is displayed
8             // not even C code
9 #pragma was_ignored
10 x++;
11 x=15;
12 }
13
14 void main (void)
15 {
16 int y;
17 f();
18 y = 1/x + 1 / (x-15); // Red ZDV, x is equal to 15
19
20 }
```

As shown in this example, any text or code placed between the two `#pragma` statements is ignored by the verification. This allows any unsupported construction to be ignored without changing the meaning of the original code. The options to enable this feature are accessible through the Graphical Interface PolySpace Launcher or in batch mode:

```
polyspace-c -asm-begin will_be_ignored -asm-end was_ignored
```

Dealing with Backward "goto" Statements

PolySpace is not designed to support backward "goto" statements. However, macros provide a solution in most cases. In general, verifications that includes backward "goto" statements stop at an early stage, and a message appears saying that backward "goto" statements are not supported.

Macros provided with the PolySpace software can work around this limitation **as long as the "goto" labels and jump instructions are in the same code block (and in the same scope).**

To insert these macros into the code:

- 1** Edit the C file containing the "goto" statements;
- 2** Add `#include pstgoto.h` at the beginning of the file (located in `<PolySpaceInstallDir>/cinclude`).
- 3** Go to the beginning of the block containing the "goto" statements.
- 4** Insert the `USE_1_GOTO(<tag>)` macro call after the variable declarations (local to the block).
- 5** Insert the `EXIT_1_GOTO(<tag>)` macro call before the end of this same block (take care with the closing bracket `}`).
- 6** Replace `"goto <tag>"` with `"GOTO(<tag>)"`.

For example, the following code would cause a verification to terminate:

```
{
/* local variable declarations */
int x; ...
/* Instructions */
...
label1:
...
goto label1
```

```
...  
}
```

You could address this problem as follows:

```
/* the pstgoto.h file is provided by PolySpace and its path */  
{  
/* local variable declarations */  
int x; ...  
USE_1_GOTO(label1);  
/* Instructions */  
...  
label1:  
...  
GOTO(label1);  
...  
EXIT_1_GOTO(label1);  
}
```

The code block may contain many instances of backward “goto” statements. Using matching `USE_n_GOTO()` and `EXIT_n_GOTO()` statements will address this (for example, `USE_2_GOTO()`, `USE_3_GOTO()`, etc.)

Note You must copy `pstgoto.h` from `<PolySpaceInstallDir>/cinclude`, and add it to the list of include directories (-I).

The code block may also use several different tags. You can use multiple “tag” parameters to address these situations. For example, use:

```
USE_n_GOTO (<tag 1>, <tag 2>, ..., <tag n>);  
EXIT_n_GOTO(<tag 1>, <tag 2>, ..., <tag n>);
```

Consider the following example:

Original Code	Modified Code for Verification
<pre> { . Reset: . { { if (X) goto Reset; } { if (Y) goto Reset; } } </pre>	<pre> { USE_1_GOTO(Reset); Reset: { { if (X) GOTO(Reset); } { if (Y) GOTO(Reset); } } EXIT_1_GOTO(Reset); </pre>

Types Promotion

- “Unsigned Integers Promoted to Signed Integers” on page 5-45
- “What are the Promotions Rules in Operators?” on page 5-46
- “Example” on page 5-47

Unsigned Integers Promoted to Signed Integers

It is important to understand the circumstances under which signed integers are promoted to unsigned.

For example, the execution of the following code would produce an assertion failure and a core dump.

```

#include <assert.h>
int f1(void) {
    int x = -2;

```

```
    unsigned int y = 5;
    assert(x <= y);
}
```

Implicit promotion explains this behavior. In this example, `x <= y` is implicitly:

```
((unsigned int) x) <= y /* implicit promotion since y is unsigned */
```

A negative cast into unsigned gives a large value. This value can never be `<= 5`, so the assertion can never hold true.

In this second example, consider the range of possible values for `x`:

```
void f2(void)
volatile int random;
unsigned int y = 7;
int x = random;
assert ( x >= -7 && x <= y );

assert (x>=0 && x<=7);
```

The first assertion is orange, it may cause an assert failure. However, given that the range of `x` after the first assertion is **not** `[-7 .. 7]`, but rather `[0 .. 7]`, the second assertion would hold true.

What are the Promotions Rules in Operators?

Knowledge of the rules applying to the standard operators of the C language will help you to analyze those orange and **red** checks which relate to overflows on type operations. Those rules are:

- Unary operators operate on the type of the operand;
- Shifts operate on the type of the left operand;
- Boolean operators operate on Booleans;
- Other binary operators operate on a common type. If the types of the 2 operands are different, they are promoted to the first common type which can represent both of them.

So:

- Be careful of constant types.
- Be careful when verifying any operation between variables of different types without an explicit cast.

Example

Consider the integral promotion aspect of the ANSI-C standard (see 6.2.1 in ISO/IEC 9899:1990). On arithmetic operators like +, -, *, % and /, an integral promotion is applied on both operands. From the PolySpace viewpoint, that can imply an OVFL or a UNFL orange check.

```

2 extern char random_char(void);
3 extern int random_int(void);
4
5 void main(void)
6 {
7   char c1 = random_char();
8   char c2 = random_char();
9   int i1 = random_int();
10  int i2 = random_int();
11
12  i1 = i1 + i2;    // A typical OVFL/UNFL on a + operator
13  c1 = c1 + c2;  // An OVFL/UNFL warning on the c1
14                // assignment [from int32 to int8]
15 }
```

Unlike the addition of two integers at line 12, an implicit promotion is used in the addition of the two chars at line 13. Consider this second “equivalence” example.

```

2 extern char random_char(void);
3
4 void main(void)
5 {
6   char c1 = random_char();
7   char c2 = random_char();
8
9   c1 = (char)((int)c1 + (int)c2); // Warning OVFL: due to
10                                // integral promotion
11 }
```

An orange check represents a warning of a potential overflow (OVFL), generated on the (char) cast [from int32 to int8]. A green check represents a verification that there is no possibility of any overflow (OVFL) on the +operator.

In general, integral promotion requires that the abstract machine should promote the type of each variable to the integral target size before realizing the arithmetic operation and subsequently adjusting the assignment type. See the equivalence example of a simple addition of two *char*(above).

Integral promotion respects the size hierarchy of basic types:

- *char* (*signed* or *not*) and *signed short* are promoted to *int*.
- *unsigned short* is promoted to *int* only if *int* can represent all the possible values of an *unsigned short*. If that is not the case (perhaps because of a 16-bit target, for example) then *unsigned short* is promoted to *unsigned int*.
- Other types like *(un)signed int*, *(un)signed long int* and *(un)signed long long int* promote themselves.

Running a Verification

- “Types of Verification” on page 6-2
- “Running Verifications on PolySpace Server” on page 6-3
- “Running Verifications on PolySpace Client” on page 6-22
- “Running Verifications from Command Line” on page 6-27

Types of Verification

You can run a verification on a server or a client.

Use...	For...
Server	<ul style="list-style-type: none">• Best performance• Large files (more than 800 lines of code including comments)• Multitasking
Client	<ul style="list-style-type: none">• An alternative to the server when the server is busy• Small files with no multitasking <hr/> <p>Note Verification on a client takes more time. You might not be able to use your client computer when a verification is running on it.</p> <hr/>

Running Verifications on PolySpace Server

In this section...

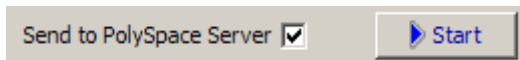
- “Starting Server Verification” on page 6-3
- “What Happens When You Run Verification” on page 6-4
- “Running Verification Unit-by-Unit” on page 6-5
- “Managing Verification Jobs Using the PolySpace Queue Manager” on page 6-7
- “Monitoring Progress of Server Verification” on page 6-8
- “Viewing Verification Log File on Server” on page 6-11
- “Stopping Server Verification Before It Completes” on page 6-13
- “Removing Verification Jobs from Server Before They Run” on page 6-14
- “Changing Order of Verification Jobs in Server Queue” on page 6-15
- “Purging Server Queue” on page 6-16
- “Changing Queue Manager Password” on page 6-18
- “Sharing Server Verifications Between Users” on page 6-18

Starting Server Verification

Most verification jobs run on the PolySpace server. Running verifications on a server provides optimal performance.

To start a verification that runs on a server:

- 1** Open the Launcher.
- 2** Open the project containing the files you want to verify. For more information, see Chapter 3, “Setting Up a Verification Project”.
- 3** Select the **Send to PolySpace Server** check box next to the **Start** button in the middle of the Launcher window.



Note If you select **Set this option to use the server mode by default in every new project** in the Remote Launcher pane of the preferences, the **Send to PolySpace Server** check box is selected by default when you create a new project.

4 Click **Start**.

The verification starts. For information on the verification process, see “What Happens When You Run Verification” on page 6-4.

Note If you see the message *Verification process failed*, click **OK** and go to “Verification Process Failed Errors” on page 7-2.

5 When you see the message *Verification process completed*, click **OK** to close the message dialog box.

6 For information on downloading and viewing your results, see “Opening Verification Results” on page 8-8.

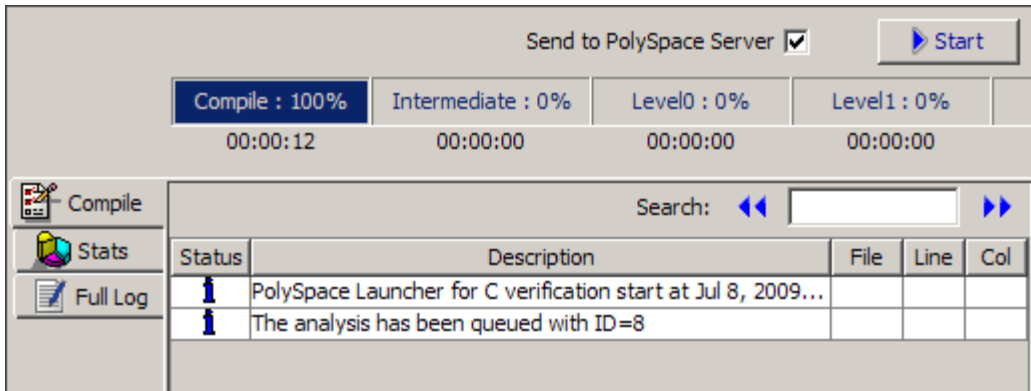
What Happens When You Run Verification

The verification has three main phases:

- 1 Checking syntax and semantics (the compile phase). Because PolySpace software is independent of any particular C compiler, it ensures that your code is portable, maintainable, and complies with ANSI® standards.
- 2 Generating a main if it does not find a main and the **Generate a Main** option is selected. For more information about generating a main, see “MAIN GENERATOR OPTIONS (-main-generator) for PolySpace Software” in the *PolySpace Products for C Reference*.
- 3 Analyzing the code for run-time errors and generating color-coded diagnostics.

The compile phase of the verification runs on the client. When the compile phase completes:

- A message dialog box tells you that the verification completed. This message means that the part of the verification that takes place on the client is complete. The rest of the verification runs on the server.
- A message in the log area tells you that the verification was transferred to the server and gives you the identification number (Analysis ID) for the verification. For the following verification, the identification number is 1.

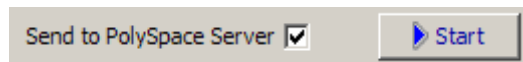


Running Verification Unit-by-Unit

When launching a server verification, you can create a separate verification jobs for each source file in the project. Each file is compiled, sent to the PolySpace Server, and verified individually. Verification results can then be viewed for the entire project, or for individual units.

To run a unit-by-unit verification:


- 1 In the Launcher, ensure that the **Send to PolySpace Server** check box is selected.



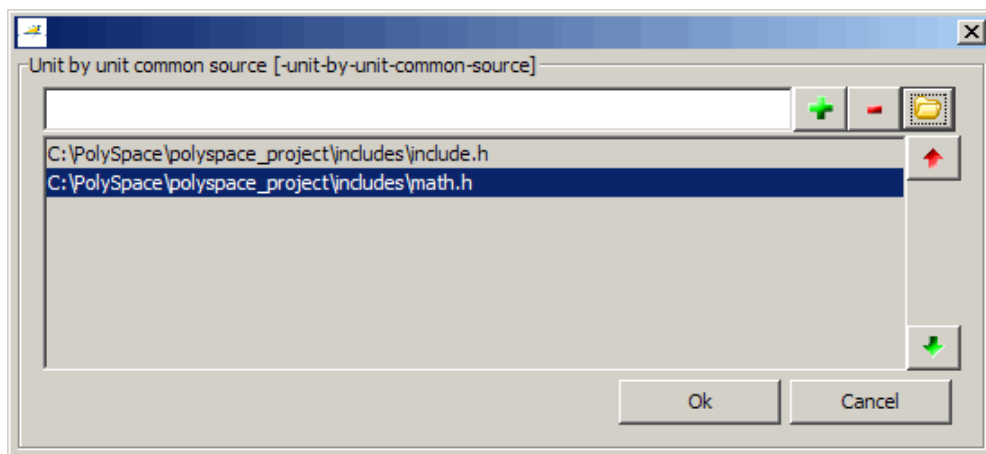
- 2 In the Analysis options, expand **PolySpace inner settings**.
- 3 Select the **Run a verification unit by unit** check box.

[-] PolySpace inner settings			
[-] Run a verification unit by unit	<input checked="" type="checkbox"/>		-unit-by-unit
Unit by unit common source	C:\PolySpace\poly	...	-unit-by-unit-common-source

4 Expand the **Run a verification unit by unit** item.

5 Click the button  to the right of the **Unit by unit common source** option.

The Unit by unit common source dialog box opens.



6 Click the folder icon .

The **Select a file to include** dialog box appears.

7 Select the common files to include with each unit verification.

These files are compiled once, and then linked to each unit before verification. Functions not included in this list are stubbed.

8 Click **Ok**.

9 Click **Start**.

Each file in the project is compiled, sent to the PolySpace Server, and verified individually as part of a verification group for the project.

Managing Verification Jobs Using the PolySpace Queue Manager

You manage all server verifications using the PolySpace Queue Manager (also called the PolySpace Spooler). The PolySpace Queue Manager allows you to move jobs within the queue, remove jobs, monitor the progress of individual verifications, and download results.

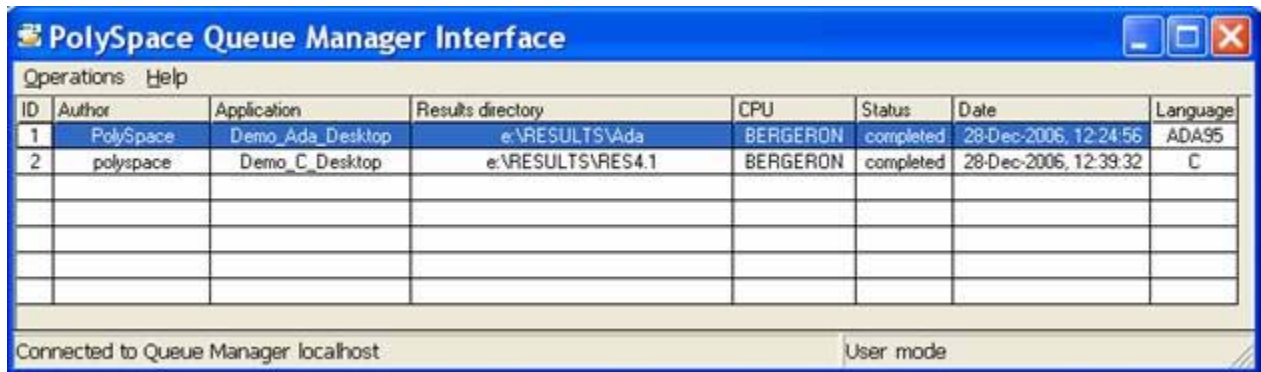
Note The PolySpace Queue Manager is not available on UNIX® or Linux systems. To manage server verifications on UNIX or Linux systems, you must use batch commands. For information on managing verification jobs from the command line, see “Managing Verifications in Batch” on page 6-27.

To manage verification jobs on the PolySpace Server:

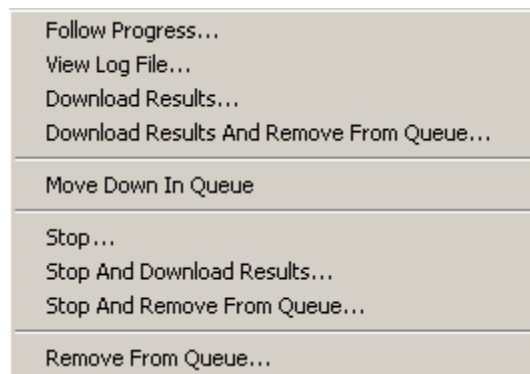
- 1 Double-click the **PolySpace Spooler** icon:




The **PolySpace Queue Manager Interface** opens.



- 2 Right-click any job in the queue to open the context menu for that verification.



- 3 Select the appropriate option from the context menu.

Tip You can also open the Polyspace Queue Manager Interface by clicking the PolySpace Queue Manager icon  in the PolySpace Launcher toolbar.

Monitoring Progress of Server Verification

You can view the log file of a server verification using the PolySpace Queue Manager.

To view a log file on the server:

- 1 Double-click the **PolySpace Spooler** icon:



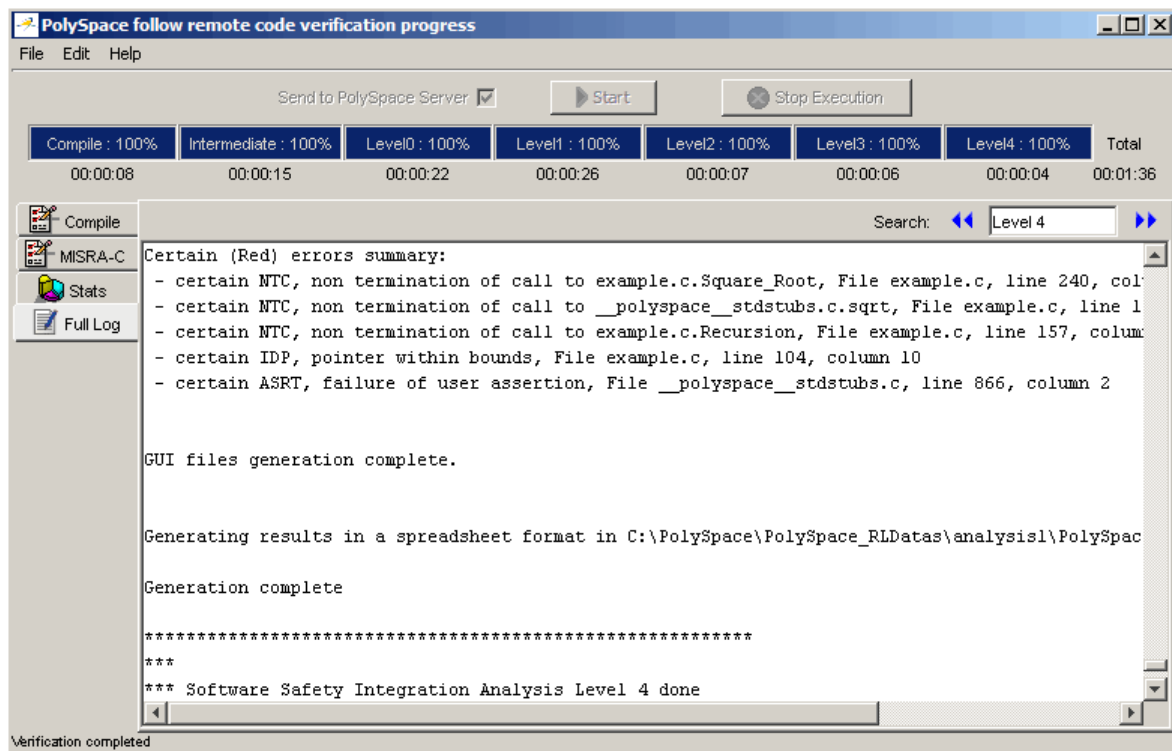
The **PolySpace Queue Manager Interface** opens.

PolySpace Queue Manager Interface							
Operations Help							
ID	Author	Application	Results directory	CPU	Status	Date	Language
1	your_name	Example_Project	C:\polyspace_project\results	anse	running	'008,	C

- 2 Right-click the job you want to monitor, and select **Follow Progress** from the context menu.

Note This option does not apply to unit-by-unit verification groups, only the individual jobs within a group.

A Launcher window labeled **PolySpace follow remote analysis progress for C** appears.



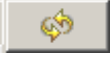
You can monitor the progress of the verification by watching the progress bar and viewing the logs at the bottom of the window. The word **processing** appears under the current phase. The progress bar highlights each completed phase and displays the amount of time for that phase.

The logs report additional information about the progress of the verification. The information appears in the log display area at the bottom of the window. The full log displays by default. It displays messages, errors, and statistics for all phases of the verification. You can search the full log by entering a search term in the **Search in the log** box and clicking the left arrows to search backward or the right arrows to search forward.

- 3 Click the **Compile Log** button to display compile phase messages and errors. You can search the log by entering search terms in the **Search in the log** box and clicking the left arrows to search backward or the right

arrows to search forward. Click on any message in the log to get details about the message.

- 4 Click the **Stats** button to display statistics, such as analysis options, stubbed functions, and the verification checks performed.

- 5 Click the refresh button  to update the stats log display as the verification progresses.

- 6 Select **File > Quit** to close the progress window.

When the verification completes, the status in the **PolySpace Queue Manager Interface** changes from running to completed.

PolySpace Queue Manager Interface							
Operations Help							
ID	Author	Application	Results directory	CPU	Status	Date	Language
1	your_name	Example_Project	C:\polyspace_project\results	ansel	completed	'008,	C

Viewing Verification Log File on Server

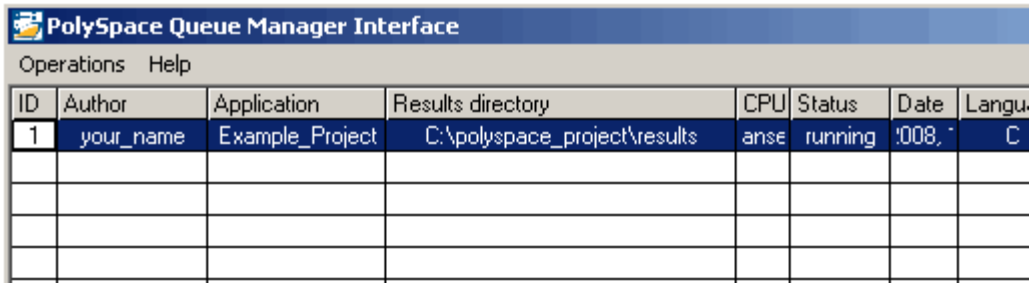
You can view the log file of a server verification using the PolySpace Queue Manager.

To view a log file on the server:

- 1 Double-click the **PolySpace Spooler** icon:



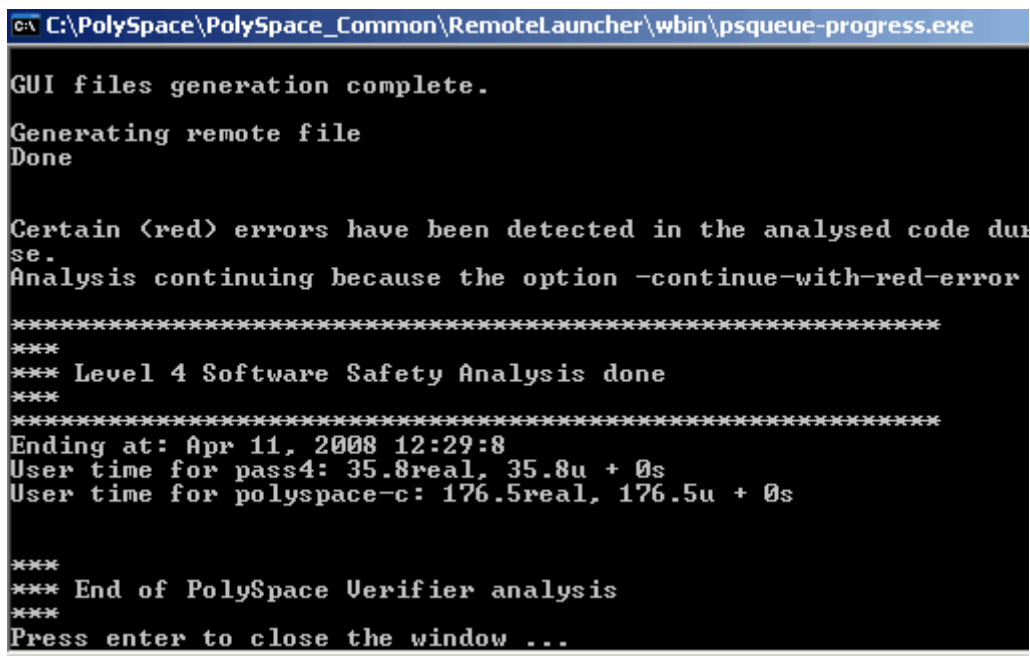
The **PolySpace Queue Manager Interface** opens.



PolySpace Queue Manager Interface							
Operations Help							
ID	Author	Application	Results directory	CPU	Status	Date	Language
1	your_name	Example_Project	C:\polyspace_project\results	anse	running	'008,	C

2 Right-click the job you want to monitor, and select **View log file**.

A window opens displaying the last one-hundred lines of the verification.



```

C:\PolySpace\PolySpace_Common\RemoteLauncher\wbin\psqueue-progress.exe
GUI files generation complete.
Generating remote file
Done

Certain (red) errors have been detected in the analysed code due to
se.
Analysis continuing because the option -continue-with-red-error
was used.

*****
***
*** Level 4 Software Safety Analysis done
***
*****
Ending at: Apr 11, 2008 12:29:8
User time for pass4: 35.8real, 35.8u + 0s
User time for polyspace-c: 176.5real, 176.5u + 0s

***
*** End of PolySpace Verifier analysis
***
Press enter to close the window ...
  
```

3 Press **Enter** to close the window.

Stopping Server Verification Before It Completes

You can stop a verification running on the server before it completes using the PolySpace Queue Manager. If you stop the verification, results will be incomplete, and if you start another verification, the verification starts over from the beginning.

To stop a server verification:

- 1 Double-click the **PolySpace Spooler** icon:



The **PolySpace Queue Manager Interface** opens.

PolySpace Queue Manager Interface							
Operations Help							
ID	Author	Application	Results directory	CPU	Status	Date	Language
1	your_name	Example_Project	C:\polyspace_project\results	anse	running	'008,	C

- 2 Right-click the job you want to monitor, and select one of the following options:

Right-click the job you want to monitor, and select one of the following options:

- **Stop** — Stops a unit-by-unit verification job without removing it. The status of the job changes from “running” to “aborted”. All jobs in the unit-by-unit verification group remain in the queue, and other jobs in the group will continue to run.
- **Stop and download results** — Stops the verification job immediately and downloads any preliminary results. The status of the verification

changes from “running” to “aborted”. The verification remains in the queue.

- **Stop and remove from queue** — Stops the verification immediately and removes it from the queue. If the job is part of a unit-by-unit verification group, the entire verification is removed, not just the individual job.

Removing Verification Jobs from Server Before They Run

If your job is in the server queue, but has not yet started running, you can remove it from the queue using the PolySpace Queue Manager.

Note If the job has started running, you must stop the verification before you can remove the job (see “Stopping Server Verification Before It Completes” on page 6-13). Once you have aborted a verification, you can remove it from the queue.

To remove a job from the server queue:

- 1 Double-click the **PolySpace Spooler** icon:



The **PolySpace Queue Manager Interface** opens.

PolySpace Queue Manager Interface							
Operations Help							
ID	Author	Application	Results directory	CPU	Status	Date	Language
1	your_name	Example_Project	C:\polyspace_project\results	anse	running	'008,	C

- 2 Right-click the job you want to remove, and select **Remove from queue**.

The job is removed from the queue.

Changing Order of Verification Jobs in Server Queue

You can change the priority of verification jobs in the server queue to determine the order in which the jobs run.

To move a job within the server queue:

- 1 Double-click the **PolySpace Spooler** icon:



The **PolySpace Queue Manager Interface** opens.

PolySpace Queue Manager Interface							
Operations Help							
ID	Author	Application	Results directory	CPU	Status	Date	Language
1	your_name	Example_Project	C:\polyspace_project\results	anse	running	'008,	C

- 2 Right-click the job you want to remove, and select **Move down in queue**.

The job is moved down in the queue.

- 3 Repeat this process to reorder the jobs as necessary.

Note You can move unit-by-unit verification groups in the queue, as well as individual jobs within a single unit-by-unit verification group. However, you can not move individual unit-by-unit verification jobs outside of the group.

Purging Server Queue

You can purge the server queue of all jobs, or completed and aborted jobs using the using the PolySpace Queue Manager.

Note You must have the queue manager password to purge the server queue.

To purge the server queue:

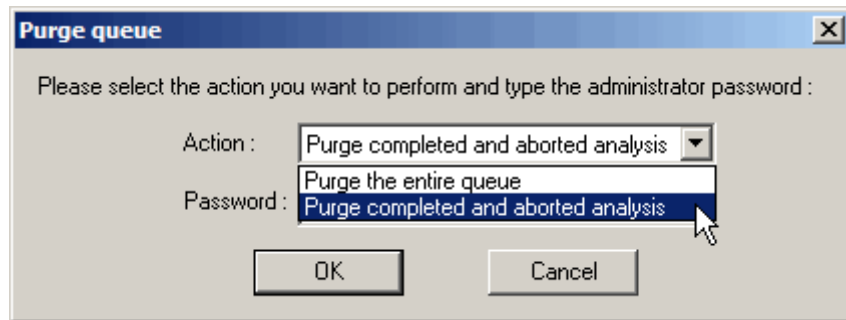
- 1 Double-click the **PolySpace Spooler** icon:



The **PolySpace Queue Manager Interface** opens.

PolySpace Queue Manager Interface							
Operations Help							
ID	Author	Application	Results directory	CPU	Status	Date	Language
1	your_name	Example_Project	C:\polyspace_project\results	anse	running	'008,	C

2 Select **Operations > Purge queue**. The Purge queue dialog box opens.



3 Select one of the following options:

- **Purge completed and aborted analysis** — Removes all completed and aborted jobs from the server queue.
- **Purge the entire queue** — Removes all jobs from the server queue.

Note For unit-by-unit verification jobs, no jobs are removed until the entire group has been verified.

4 Enter the Queue Manager **Password**.

5 Click **OK**.

The server queue is purged.

Changing Queue Manager Password

The Queue Manager has an administrator password to control access to advanced operations such as purging the server queue. You can set this password through the Queue Manager.

Note The default password is administrator.

To set the Queue Manager password:

- 1 Double-click the **PolySpace Spooler** icon:

The PolySpace Queue Manager Interface opens.

- 2 Select **Operations > Change Administrator Password**.

The Change Administrator Password dialog box opens.

- 3 Enter your old and new passwords, then click **OK**.

The password is changed.

Sharing Server Verifications Between Users

Security of Jobs in Server Queue

For security reasons, all verification jobs in the server queue are owned by the user who sent the verification from a specific account. Each verification has a unique encryption key, that is stored in a text file on the client system.

When you manage jobs in the server queue (download, kill, remove, etc.), the Queue Manager checks the public keys stored in this file to authenticate that the job belongs to you.

If the key does not exist, an error message appears: “key for verification <ID> not found”.

analysis-keys.txt File

The public part of the security key is stored in a file named `analysis-keys.txt` associated to a user account. This file is located in:

- **UNIX** — `/home/<username>/PolySpace`
- **Windows®** — `C:\Documents and Settings\<username>\Application Data\PolySpace`

The format of this ASCII file is as follows (tab-separated):

```
<id of launching> <server name of IP address> <public key>
```

where *<public key>* is a value in the range [0..F]

The fields in the file are tab-separated.

The file cannot contain blank lines.

Example:

```
1 m120 27CB36A9D656F0C3F84F959304ACF81BF229827C58BE1A15C8123786
2 m120 2860F820320CDD8317C51E4455E3D1A48DCE576F5C66BEEF391A9962
8 m120 2D51FF34D7B319121D221272585C7E79501FBCC8973CF287F6C12FCA
```

Sharing Verifications Between Accounts

To share a server verification with another user, you must provide the public key.

To share a verification with another user:

- 1 Find the line in your `analysis-keys.txt` file containing the *<ID>* for the job you want to share.
- 2 Add this line to the `analysis-keys.txt` file of the person who wants to share the file.

The second user can then download or manage the verification.

Magic Key to Share Verifications

A magic key allows you to share verifications without copying individual keys. This allows you to use the same key for all verifications launched from a single user account.

The format for a magic key is as follows:

```
0 <Server id> <your hexadecimal value>
```

When you add this key to your `verification-key.txt` file, all verification jobs you submit to the server queue use this key instead of a random one. All users who have this key in their `verification-key.txt` file can then download or manage your verification jobs.

Note This only works for verification jobs launched after you place the magic key in the file. If the verification was launched before the key was added, the normal key associated to the ID is used.

If `analysis-keys.txt` File is Lost or Corrupted

If your `analysis-keys.txt` file is corrupted or lost (removed by mistake) you cannot download your verification results. To access your verification results you must use administrator mode.

Note You must have the queue manager password to use Administrator Mode.

To use administrator mode:

- 1 Double-click the **PolySpace Spooler** icon:



The **PolySpace Queue Manager Interface** opens.

ID	Author	Application	Results directory	CPU	Status	Date	Language
1	your_name	Example_Project	C:\polyspace_project\results	anse	running	'008,	C

2 Select **Operations > Enter Administrator Mode**.

3 Enter the Queue Manager **Password**.

4 Click **OK**.

You can now manage all verification jobs in the server queue, including downloading results.

Running Verifications on PolySpace Client

In this section...
“Starting Verification on Client” on page 6-22
“What Happens When You Run Verification” on page 6-23
“Monitoring the Progress of the Verification” on page 6-24
“Stopping Client Verification Before It Completes” on page 6-25

Starting Verification on Client

For the best performance, run verifications on a server. If the server is busy or you want to verify a small file, you can run a verification on a client.

Note Because a verification on a client can process only a limited number of variable assignments and function calls, the source code should have no more than 800 lines of code.

If you launch a verification on C code containing more than 2,000 assignments and calls, the verification will stop and you will receive an error message.

To start a verification that runs on a client:

- 1 Open the Launcher.
- 2 Open the project containing the files you want to verify. For more information, see Chapter 3, “Setting Up a Verification Project”.
- 3 Ensure that the **Send to PolySpace Server** check box is not selected.
- 4 If you see a warning that multitasking is not available when you run a verification on the client, click **OK** to continue and close the message box. This warning only appears when you clear the **Send to PolySpace Server** check box.
- 5 Click the **Start** button.

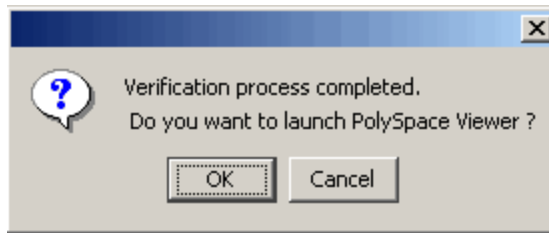


- 6 If you see a caution that PolySpace software will remove existing results from the results directory, click **Yes** to continue and close the message dialog box.

The progress bar and logs area of the Launcher window become active.

Note If you see the message `Verification process failed`, click **OK** and go to “Verification Process Failed Errors” on page 7-2.

- 7 When the verification completes, a message dialog box appears telling you that the verification is complete and asking if you want to open the Viewer.



- 8 Click **OK** to open your results in the Viewer.

For information on viewing your results, see “Opening Verification Results” on page 8-8.

What Happens When You Run Verification

The verification has three main phases:

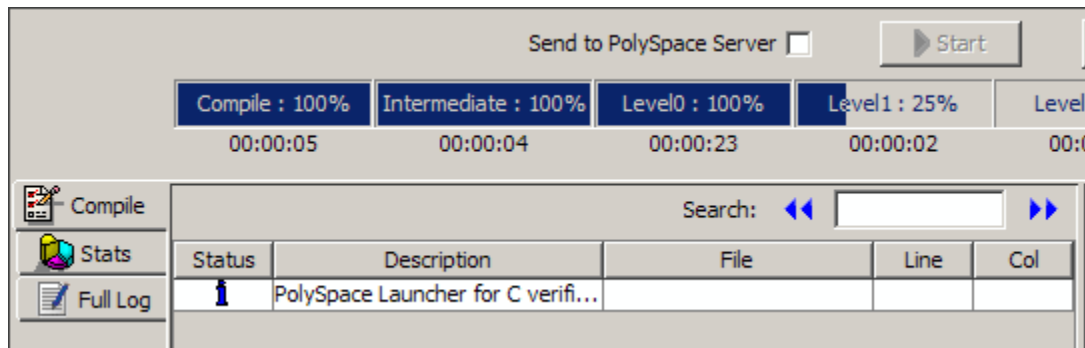
- 1 Checking syntax and semantics (the compile phase). Because PolySpace software is independent of any particular C compiler, it ensures that your code is portable, maintainable, and complies with ANSI standards.
- 2 Generating a main if it does not find a main and the **Generate a Main** option is selected. For more information about generating a main, see

“MAIN GENERATOR OPTIONS (-main-generator) for PolySpace Software” in the *PolySpace Products for C Reference*.

- 3 Analyzing the code for run-time errors and generating color-coded diagnostics.

Monitoring the Progress of the Verification

You can monitor the progress of the verification by watching the progress bar and viewing the logs at the bottom of the Launcher window.



The progress bar highlights the current phase in blue and displays the amount of time and completion percentage for that phase.


The logs report additional information about the progress of the verification. To view a log, click the button for that log. The information appears in the log display area at the bottom of the Launcher window.

To view the logs:

- 1 The compile log is displayed by default.

This log displays compile phase messages and errors. You can search the log by entering search terms in the **Search in the log** box and clicking the left arrows to search backward or the right arrows to search forward. Click on any message in the log to get details about the message.

- 2 Click the **Stats** button to display statistics, such as analysis options, stubbed functions, and the verification checks performed.

3 Click the refresh button  to update the stats log display as the verification progresses.

4 Click the **Full Log** button to display messages, errors, and statistics for all phases of the verification.

You can search the full log by entering a search term in the **Search in the log** box and clicking the left arrows to search backward or the right arrows to search forward.

Note Closing the Launcher window does *not* stop the verification. To resume display of the verification progress, open the Launcher window and open the project that you were verifying when you closed the Launcher window.

Stopping Client Verification Before It Completes

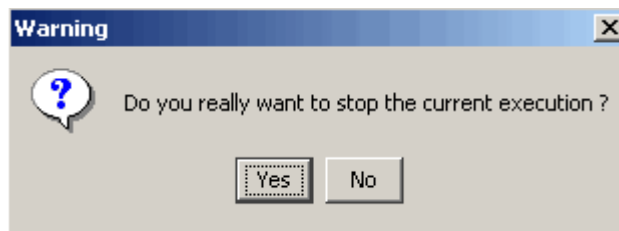
You can stop the verification before it completes. If you stop the verification, results will be incomplete, and if you start another verification, the verification starts over from the beginning.

To stop a verification:

1 Click the **Stop Execution** button.



A warning dialog box appears.



2 Click **Yes**.

The verification stops and the message **Verification process stopped** appears.

3 Click **OK** to close the **Message** dialog box.

Note Closing the Launcher window does *not* stop the verification. To resume display of the verification progress, open the Launcher window and open the project that you were verifying when you closed the Launcher window.

Running Verifications from Command Line

In this section...
“Launching Verifications in Batch” on page 6-27
“Managing Verifications in Batch” on page 6-27

Launching Verifications in Batch

A set of commands allow you to launch a verification in batch.

All these commands begin with the following prefixes:

- **Server verification** —
`<PolySpaceInstallDir>/Verifier/bin/polyspace-remote-c`
- **Client verification** —`polyspace-remote-desktop-c`

These commands are equivalent to commands with a prefix
`<PolySpaceInstallDir>/bin/polyspace-.`

For example, `polyspace-remote-desktop-c -server
[<hostname>:[<port>] | auto]` allows you to send a C client
verification remotely.

Note If your PolySpace server is running on Windows, the batch
commands are located in the `/wbin/` directory. For example,
`<PolySpaceInstallDir>/Verifier/wbin/polyspace-remote-c.exe`

Managing Verifications in Batch

In batch, a set of commands allow you to manage verification jobs in the
server queue.

On UNIX platforms, all these command begin with the prefix
`<PolySpaceCommonDir>/RemoteLauncher/bin/psqueue-.`

On Windows platforms, these commands begin with the prefix `<PolySpaceCommonDir>/RemoteLauncher/wbin/psqueue-:`

- `psqueue-download <id> <results dir>` — download an identified verification into a results directory. When downloading a unit-by-unit verification group, all the unit results are downloaded and a summary of the download status for each unit is displayed.
 - `[-f]` force download (without interactivity)
 - `-admin -p <password>` allows administrator to download results.
 - `[-server <name>[:port]]` selects a specific Queue Manager.
 - `[-v|version]` gives release number.
- `psqueue-kill <id>` — kill an identified verification. For unit-by-unit verification groups, you can stop the entire group, or individual jobs within the group. Stopping an individual job does not kill the entire group.
- `psqueue-purge all|ended` — remove all completed verifications from the queue. For unit-by-unit verification jobs, no jobs are removed until the entire group has been verified.
- `psqueue-dump` — gives the list of all verifications in the queue associated with the default Queue Manager. Unit-by-unit verification groups are shown using a tree structure.
- `psqueue-move-down <id>` — move down an identified verification in the Queue. Individual jobs can be moved within a unit-by-unit verification group, but not outside of the group.
- `psqueue-remove <id>` — remove an identified verification in the queue. You cannot remove a single job that is part of a unit-by-unit verification group, you can only remove the entire group.
- `psqueue-get-qm-server` — give the name of the default Queue Manager.
- `psqueue-progress <id>:` give progression of the currently identified and running verification. This command does not apply to unit-by-unit verification groups, only the individual jobs within a group.
 - `[-open-launcher]` display the log in the graphical user interface of launcher.
 - `[-full]` give full log file.

- `psqueue-set-password <password> <new password>` — change administrator password.
- `psqueue-check-config` — check the configuration of Queue Manager.
 - `[-check-licenses]` check for licenses only.
- `psqueue-upgrade` — Allow to upgrade a client side (see the PolySpace Installation Guide in the `<PolySpace Common Dir>/Docs` directory).
 - `[-list-versions]` give the list of available release to upgrade.
 - `[-install-version <version number> [-install-dir <directory>]] [-silent]` allow to install an upgrade in a given directory and in silent.

Note `<PolySpaceCommonDir>/bin/psqueue-<command> -h` gives information about all available options for each command.

Troubleshooting Verification Problems

- “Verification Process Failed Errors” on page 7-2
- “Compilation Errors” on page 7-7
- “Link Errors and Warnings” on page 7-15
- “Stubbing Errors” on page 7-21
- “Automatic Stub Creation Errors” on page 7-28
- “Viewing Error Information When Verification Stops” on page 7-31
- “Reducing Verification Time” on page 7-33
- “Obtaining Configuration Information” on page 7-52
- “Removing Preliminary Results Files” on page 7-54

Verification Process Failed Errors

In this section...
“Messages Described in This Section” on page 7-2
“Hardware Does Not Meet Requirements” on page 7-2
“You Did Not Specify the Location of Included Files” on page 7-3
“PolySpace Software Cannot Find the Server” on page 7-4
“Limit on Assignments and Function Calls” on page 7-6

Messages Described in This Section

If you see a message that includes `Verification process failed`, it indicates that PolySpace software could not perform the verification. The following sections present some possible reasons for a failed verification.

Message	See
Errors found when verifying host configuration	“Hardware Does Not Meet Requirements” on page 7-2
<code>include.h: No such file or directory(where include.h represents the included file)</code>	“You Did Not Specify the Location of Included Files” on page 7-3
<code>Error: Unknown host :</code>	“PolySpace Software Cannot Find the Server” on page 7-4
<code>License error: number-of assignments and function calls is too big for -unit mode</code>	“Limit on Assignments and Function Calls” on page 7-6

Hardware Does Not Meet Requirements

Message

In the verification log:

Errors found when verifying host configuration.

Cause

The verification fails if your computer does not have the minimal hardware requirements. For information about the hardware requirements, see www.mathworks.com/products/polyspaceclientc/requirements.html.

Solution

You can:

- Upgrade your computer to meet the minimal requirements.
- In the General section of the **Analysis** options, select **Continue with current configuration** and run the verification again.

You Did Not Specify the Location of Included Files**Message**

In the verification log (where `include.h` represents the included file):

```
include.h: No such file or directory
```

Cause

Either the files are missing or you did not specify the location of included files.

Solution

Do one of the following:

- Include the file in the directory.
- Specify the proper location of include files.

The MathWorks™ recommends that you create a project file to store include files, as described in “Creating a Project” on page 3-2.

PolySpace Software Cannot Find the Server

Message

Search in the verification log for:

Error: Unknown host :

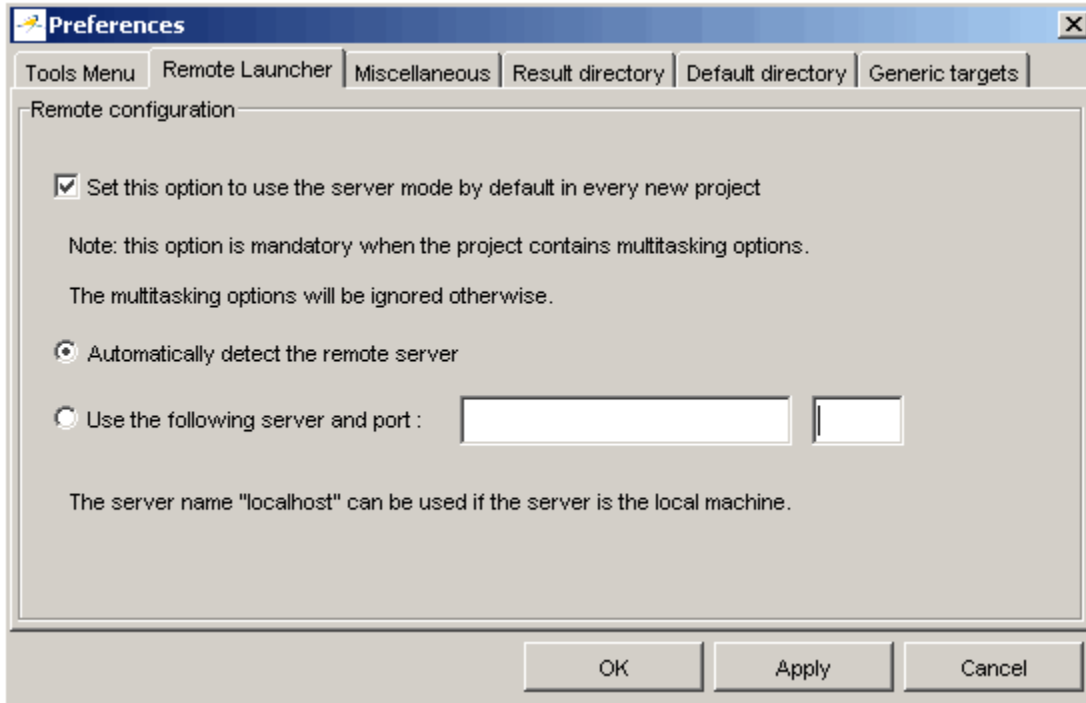
Cause

PolySpace software uses information in the preferences to locate the server. In this case, PolySpace software cannot find the server.

Solution

To find the server information in the preferences:

- 1 Select **Edit > Preferences**.
- 2 Select the **Remote Launcher** tab.



How you deal with this error depends on the selected remote configuration option.

Remote Configuration Option	Solution
Automatically detect the remote server	Specify the server by selecting Use the following server and port and providing the server name and port.
Use the following server and port	Confirm the server name and port number are accurate.

For information about setting up a server, see the *PolySpace Installation Guide*.

Limit on Assignments and Function Calls

Message

```
*****  
Beginning C to intermediate language translation  
*****  
C to intermediate language translation 1 (P_SP)  
...  
  
*** License error: number of assignments and function calls is  
too big for -unit mode (5534 v.s 2000).  
*** Aborting.
```

Cause

PolySpace Client for C/C++ software can only verify C code with up to 2,000 assignments and calls.

Solution

To verify code containing more than 2,000 assignments and calls, launch your verification on the PolySpace Server for C/C++.

Compilation Errors

In this section...

“Overview” on page 7-7

“Configure a Text Editor” on page 7-7

“Examining the Compile Log” on page 7-8

“Messages Described in This Section” on page 7-9

“Syntax Error” on page 7-9

“Undeclared Identifier” on page 7-10

“No Such File or Directory” on page 7-11

“Errors Resulting from Unsupported Non-ANSI Keywords Such as @interrupt” on page 7-12

Overview

You can use PolySpace software instead of your chosen compiler to make syntactical, semantic, and other static checks. PolySpace detects compilation errors during the standard compliance checking stage.

The compliance checking stage takes about the same amount of time to run as a compiler. Using PolySpace software early in development yields a number of benefits:

- Detection of link errors
- Detection of errors that only appear with two or more files
- Objective, automatic, and early control of development work (possibly to check code into a configuration management system)

Configure a Text Editor

Configure a text editor before you can open source files. See “Configuring Text and XML Editors” on page 3-17.

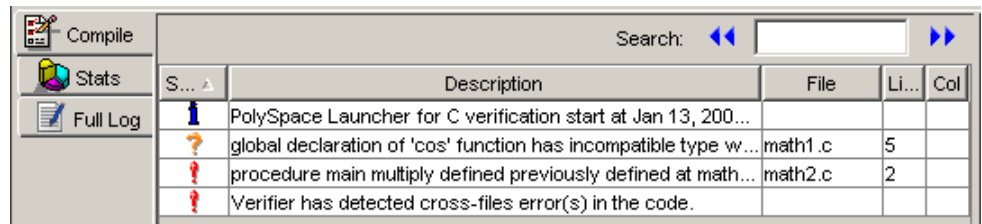
Examining the Compile Log

The compile log displays compile phase messages and errors. To search the log, enter search terms in the **Search in the log** box. Click the left arrows to search backward or the right arrows to search forward.

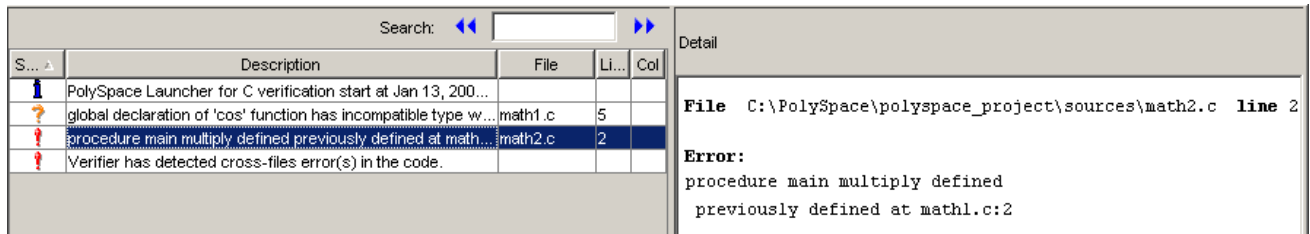
To examine errors in the compile log:

- 1 Click the **Compile** button in the log area of the Launcher window.





A list of compile phase messages appears in the log part of the window.





- 2 Select any of the messages to see message details, as well as the full path of the file containing the error.



- 3 To open the source file referenced by any message, right click the row for the message, then select Open Source File.

S... ▲	Description	File	Li...	Col
	PolySpace Launcher for C verification start at Jan 13, 200...			
	global declaration of 'cos' function has incompatible type w...	math1.c	5	
	procedure main multiply defined previously defined at math...	math2.c	2	
	Verifier has detected cross-files e			

 Open Source File
 Configure Editor

The file opens in your text editor.

4 Correct the error and run the verification again.

Messages Described in This Section

This section describes messages that include the following phrases:

Phrase Found in Message	See
syntax error	“Syntax Error” on page 7-9
undeclared identifier	“Undeclared Identifier” on page 7-10
No such file or directory	“No Such File or Directory” on page 7-11
Catastrophic error: could not open source file	“No Such File or Directory” on page 7-11

This section also describes error messages triggered by unsupported keywords. See “Errors Resulting from Unsupported Non-ANSI Keywords Such as @interrupt” on page 7-12.

This section includes sample code that triggers the example message.

Syntax Error

Message

```
Verifying compilation.c
compilation.c:3: syntax error; found `x' expecting `;'
```

Code Used

```
void main(void)
{
int far x;
x = 0;
x++;
}
```

Solution

The `far` keyword is unknown in ANSI C. This causes confusion at compilation time. Should `far` be a variable or a qualifier? The `int far x;` construction is illegal.

Possible corrections include:

- Remove `far` from the source code.
- Define `far` as a qualifier, such as `const` or `volatile`.
- Remove `far` artificially by specifying a compilation flag such as `-D far=` (with a space after the equal sign).

Note To specify `-D` compilation flags that are generic to the project, then for efficiency use the `-include` option. Refer to “How to Gather Compilation Options Efficiently” on page 4-20.

Undeclared Identifier

Message

```
Verifying compilation.c
compilation.c:3: undeclared identifier `x'
```

Code Used

```
void main(void)
{
  x = 0;
  x++;
}
```

Solution

The type is unknown, and therefore the compilation stops. Should `x` be a `float`, an `int`, or a `char`?

Some cross compilers define variables implicitly. Your code must declare variables verification. PolySpace software has no knowledge about implicit variables.

Similarly, some compilers interpret `__SP` as a reference to the stack pointer. Use the `-D` compilation flag.

Note To specify `-D` compilation flags that are generic to the project, then for efficiency use the `-include` option. Refer to “How to Gather Compilation Options Efficiently” on page 4-20.

No Such File or Directory

Messages

Here are examples of messages that include `No such file or directory` and `catastrophic error: could not open source file`:

```
compilation.c:1: one_file.h: No such file or directory
```

```
compilation.c:1: catastrophic error: could not open source file
"one_file.h" (where one_file.h is an include file)
```

Code Used

```
#include "one_file.h"
```

Solution

The `one_file.h` file is missing.

These files are essential for PolySpace software to complete the compilation, for

- Data coherency
- Automatic stubbing

Make sure that the PolySpace software can find the include folder that contains this file. Use the `-I` option in the launcher, as described in the “`-I` directory” reference page.

Errors Resulting from Unsupported Non-ANSI Keywords Such as `@interrupt`

Code that includes a non-ANSI keyword that PolySpace software does not support generates a compilation error. For example, keywords containing `@` as a first character cause a compilation error. But in this case, you cannot address the problem by using a compilation flag, nor with an `-include` file.

To address this problem, use the `-post-preprocessing` option.

When you use the `-post-preprocessing` option, write a script or command to replace the unsupported, non-ANSI keyword with a supported keyword. The command must process the standard output from preprocessing and produce its results in accordance with standard output.

The specified script file or command runs just after the preprocessing phase on each source file. The script executes on each preprocessed c file.

Note Preprocessed files have the extension `.ci`. All preprocessed files are contained in a single compressed file named `ci.zip`. This file is located in the results directory in one of the following locations:

- `<results>/ALL/SRC/MACROS/ci.zip`
 - `<results>/C-ALL/ci.zip`.
-

Caution Always preserve the number of lines in a preprocessed `.ci` file. Adding a line, or removing one, can result in unpredictable behavior, including changes to the location of checks and MACROS in the PolySpace viewer.

Here is an example of such a script file. Save the script in a file named `myscript.pl`.

```
#!/usr/bin/perl
bin STDOUT;

# Process every line from STDIN until EOF
while ($line = <STDIN>)
{
# Replace keyword titi with toto
$line =~ s/titi/toto/g;
# Remove @interrupt (replace with nothing)
$line =~ s/@interrupt/ /g;

# DONT DELTE: Print the current processed line to STDOUT
print $line;
}
```

to run the script on each preprocessed `c` file, use this command:

```
-post-preprocessing-command %POLYSPACE_C%\Verifier\tools\perl\win32\bin\perl.exe
<absolute path to myscript.pl>\myscript.pl
```

Note Because PolySpace software no longer includes Cygwin, all files must be executable by Windows. To support scripting, the PolySpace installation includes Perl. You can access Perl in

`%POLYSPACE_C%\Verifier\tools\perl\win32\bin\perl.exe.`

Link Errors and Warnings

In this section...

“Overview” on page 7-15
“Function: Wrong Argument Type” on page 7-16
“Function: Wrong Argument Number” on page 7-16
“Variable: Wrong Type” on page 7-17
“Variable: Signed/Unsigned” on page 7-17
“Variable: Different Qualifier” on page 7-18
“Variable: Array Against Variable” on page 7-18
“Variable: Wrong Array Size” on page 7-19
“Missing Required Prototype for varargs” on page 7-19

Overview

This section describes how to address some common types of link errors.

Link errors result from the checking that PolySpace performs for compliance with ANSI C standards. Link error messages can apply to functions, variables, and varargs.

The error message includes specific information that reflects the code that the PolySpace software is checking, such as the function name and type declaration.

Examining Preprocessed Code

Looking at the preprocessed code can help you to find link errors faster.

Preprocessed files have the extension `.ci`. All preprocessed files are contained in a single compressed file named `ci.zip`. This file is located in the results directory in one of the following locations:

- `<results>/ALL/SRC/MACROS/ci.zip`
- `<results>/C-ALL/ci.zip`.

Function: Wrong Argument Type

PolySpace Output

```
Verifying cross-files ANSI C compliance ...  
Error: global declaration of 'f' function has incompatible type with its definition  
      declared function type has 'arg 1' type incompatible with definition
```

```
int f(float y)          int f(int *y);  
{  
int r;                  void main(void)  
r=12;                   {  
}                        int r;  
                        r = f(&r);  
                        }  
                        }
```

Solution

The first parameter for the `f` function is either a float or a pointer to an integer. The global declaration must match the definition.

Function: Wrong Argument Number

PolySpace Output

```
Verifying cross-files ANSI C compliance ...  
Error: global declaration of 'f' function has incompatible type with its definition  
      declared function type has incompatible args. number with definition
```

```
int f(float y)          int f(int *y);  
{  
int r;                  void main(void)  
r=12;                   {  
}                        int r;  
                        r = f(&r);  
                        }  
                        }
```


Solution

These two functions have a different number of arguments. This mismatch in the number of arguments results in a nondeterministic execution.

Variable: Wrong Type

PolySpace Output

```
Verifying cross-files ANSI C compliance ...
Error: global declaration of 'x' variable has incompatible type with its definition
      declared 'float' (32) type incompatible with defined 'int' (32) type

extern float x                int x;
                               void main(void)
                               {}
```

Solution

Declare the `x` variable the same way in every file. If a variable `x` is an integer equal to 1, which is `0x0001`, what does this value mean when seen as a float? It could result in a NAN (Not A Number) during execution.

Variable: Signed/Unsigned

PolySpace Output

```
Verifying cross-files ANSI C compliance ...
Error: global declaration of 'x' variable has incompatible type with its definition
      declared 'unsigned' type incompatible with defined 'signed' type

extern unsigned char x;      char x;
                               void main(void)
                               {}
```

Solution

Consider the 8-bit binary value `10000010`. Given that a `char` is 8 bits, it is not clear whether it is 130 (unsigned), or maybe -126 (signed).

Variable: Different Qualifier

PolySpace Output

```
Verifying cross-files ANSI C compliance ...  
Warning: global declaration of 'x' variable has incompatible type with its definition  
declared 'non qualified' type incompatible with defined 'volatile' type  
'volatile' qualifier used
```

```
extern int x;          volatile int x;  
  
void main(void)  
{
```

Solution

PolySpace software flags the volatile qualifier, because that qualifier has major implications for the verification. Because it is not clear which statement is correct, the verification process generates a warning.

Variable: Array Against Variable

PolySpace Output

```
Verifying cross-files ANSI C compliance ...  
Error: global declaration of 'x' variable has incompatible type with its definition  
declared 'array' (384) type incompatible with defined 'int' (32) type
```

```
extern int x[12];     int x;  
  
void main(void)  
{  
  
}
```

Solution

The real allocated size for the x variable is one integer. Any function attempting to manipulate x[] corrupts memory.

Variable: Wrong Array Size

PolySpace Output

Verifying cross-files ANSI C compliance ...

Warning: global declaration of 'x' variable has incompatible type with its definition
declared array type has 'upper bound' 5 inferior to definition 'upper bound' 12

```
extern int x[12];          int x[5];

                           void main(void)
                           {
                           }
}
```

Solution

The real allocated size for the x variable is five integers. Any function attempting to manipulate x[] between x[5] and x[11] corrupts memory.

Missing Required Prototype for varargs

PolySpace Output

Verifying cross-files ANSI C compliance ...

Error: missing required prototype for varargs. procedure 'g'.

```
void g(int, ...);         void main(void)
                           {
                           }
void f(void)              g(4);
{                          }
g(12, abcde ,40)
}
```

Solution

Declare the prototype for g when main executes.

To eliminate this error, you can add the following line to main:

```
void g(int, ...)
```

Or, you can avoid modifying main by adding that same line in a new file and then when you launch the verification, use the option

```
include c:\PolySpace\new_file.h
```

where new_file.h is the new file that includes the line void g(int, ...).

Stubbing Errors

In this section...

“Conflicts Between Standard Library Functions and PolySpace Stubs” on page 7-21

“_polyspace_stdstubs.c Compilation Errors” on page 7-21

“General Troubleshooting Approaches” on page 7-23

“Restart with the -I option” on page 7-23

“Include Files with Stubs to Replace Automatic Stubbing” on page 7-24

“Create a _polyspace_stdstubs.c File with Necessary Includes” on page 7-25

“Provide a .c file Containing a Prototype Function” on page 7-26

“Ignore _polyspace_stdstubs.c” on page 7-27

Conflicts Between Standard Library Functions and PolySpace Stubs

A code set can compile successfully for a target, but during the `_polyspace_stdstubs.c` compilation phase for that same code, PolySpace software can generate an error message.

The error message highlights conflicts between:

- A standard library function that the application includes
- One of the standard stubs that PolySpace software uses in place of that function

For more information about errors generated during automatic stub creation, see “Automatic Stub Creation Errors” on page 7-28.

`_polyspace_stdstubs.c` Compilation Errors

Here are examples of the errors relating to stubbing standard library functions. The code uses standard library functions such as `sprintf` and `strcpy`, illustrating possible problems with these functions.

Example 1

```
C-STUBS/___polyspace__stdstubs.c:1117: string.h: No such file
or directory
```

```
Verifying C-STUBS/___polyspace__stdstubs.c
```

```
C-STUBS/___polyspace__stdstubs.c:1118: syntax error; found
'strlen' expecting `;'
```

```
C-STUBS/___polyspace__stdstubs.c:1120: syntax error; found `i'
expecting `;'
```

```
C-STUBS/___polyspace__stdstubs.c:1120: undeclared identifier `i'
```

Example 2

```
Verifying C-STUBS/___polyspace__stdstubs.c
```

```
Error: missing required prototype for varargs. procedure
'sprintf'.
```

Example 3

```
Verifying C-STUBS/___polyspace__stdstubs.c
```

```
C-STUBS/___polyspace__stdstubs.c:3027: missing parameter 4 type
```

```
C-STUBS/___polyspace__stdstubs.c:3027: syntax error; found `n'
expecting `)'
```

```
C-STUBS/___polyspace__stdstubs.c:3027: skipping `n'
```

```
C-STUBS/___polyspace__stdstubs.c:3037: undeclared identifier `n'
```

General Troubleshooting Approaches

You can use a range of techniques to address these error messages. These techniques reflect different balances for the verification between:

- Precision
- Amount of time preparing the code
- Execution time

Try any of the techniques in any order. Consider trying the simplest approaches first, and trying other techniques as necessary to achieve the balance of the trade-offs that you seek. Here are techniques, listed in order of estimated simplicity, from simplest to most thorough:

- “Restart with the `-I` option” on page 7-23
- “Include Files with Stubs to Replace Automatic Stubbing” on page 7-24
- “Create a `_polyspace_stdstubs.c` File with Necessary Includes” on page 7-25
 - Use when precision is important enough to justify extensive code preparation time
- “Provide a `.c` file Containing a Prototype Function” on page 7-26
 - Use when you do not want to invest much time for code preparation time
- “Ignore `_polyspace_stdstubs.c`” on page 7-27

If the problem remains after trying all these solutions, contact MathWorks™ support.

Restart with the `-I` option

Generally you can best address stubbing errors by restarting the verification. Include the header file containing the prototype and the required definitions, as used during compilation for the target.

The least invasive way of including the header file containing the prototype is to use the `-I` option.

Include Files with Stubs to Replace Automatic Stubbing

The PolySpace software provides a selection of files that contain stubs for most standard library functions. You can use those stubs in place of automatic stubbing.

For replacement of stubbing to work effectively, provide the correct include file for the function. In the following example, the standard library function is `strlen`. This example assumes that you have included `string.h`. Because the `string.h` file can differ between targets, there are no default include directories for PolySpace stub files.

If the compiler has implicit include files, manually specify those include files, as shown in this example.

```
(_polyspace_stdstubs.c located in <<results_dir>>/C-ALL/C-STUBS)

_polyspace_stdstubs.c
#if defined(_polyspace_strlen) || ... || defined(_polyspace_strtok)
#include <string.h>
size_t strlen(const char *s)
{
    size_t i=0;
    while (s[i] != 0)
        i++;
    return i;
}
#endif /* _polyspace_strlen */
```

If problems remain, try one of these solutions:

- “Create a `_polyspace_stdstubs.c` File with Necessary Includes” on page 7-25
- “Provide a `.c` file Containing a Prototype Function” on page 7-26
- “Ignore `_polyspace_stdstubs.c`” on page 7-27

Create a `_polyspace_stdstubs.c` File with Necessary Includes

- 1 Copy `<<results_dir>>/C-ALL/C-STUBS/_polyspace_stdstubs.c` to the source directory and rename it `polyspace_stubs.c`.

This file contains the whole list of stubbed functions, user functions, and standard library functions. For example:

```
#define _polyspace_strlen
#define a_user_function
```

- 2 Find the problem function in the file. For example:

```
#if defined(_polyspace_strlen) || ... || defined(_polyspace_strtok)
#include <string.h>
size_t strlen(const char *s)
{
    size_t i=0;
    while (s[i] != 0)
        i++;
    return i;
}
#endif /* __polyspace_strlen */
```

The verification requires you to include the `string.h` file that the application uses.

- 3 Do one of the following (The MathWorks recommends the first approach):

- Provide the `string.h` file that contains the real prototype and type definitions for the stubbed function.
- Extract the relevant part of that file for inclusion in the verification.

For example, for `strlen`:

```
string.h
// put it in the /homemade_include directory
typedef int size_t;
size_t strlen(const char *s);
```

- 4 Specify the path for the include files and relaunch PolySpace, using one of these commands:

```
polyspace-c -I /homemade_include
```

or

```
polyspace-c -I /our_target_include_path
```

Provide a .c file Containing a Prototype Function

- 1 Identify the function causing the problem (for example, `printf`).
- 2 If you cannot find a prototype for this function, provide a .c file containing the prototype for this function.
- 3 Restart the verification either with the PolySpace Launcher or from the command line.

You can find other `__polyspace_no_<function_name>` options in `__polyspace__stdstubs.c` files, such as:

```
__polyspace_no_vprintf  
__polyspace_no_vsprintf  
__polyspace_no_fprintf  
__polyspace_no_fscanf  
__polyspace_no_printf  
__polyspace_no_scanf  
__polyspace_no_sprintf  
__polyspace_no_sscanf  
__polyspace_no_fgetc  
__polyspace_no_fgets  
__polyspace_no_fputc  
__polyspace_no_fputs  
__polyspace_no_getc
```

Note If you are considering defining multiple project generic `-D` options, then using the `-include` option can provide a more efficient solution to this type of error. Refer to “How to Gather Compilation Options Efficiently” on page 4-20.

Ignore `_polyspace_stdstubs.c`

When all other troubleshooting approaches have failed, you can try ignoring `_polyspace_stdstubs.c`. To ignore `_polyspace_stdstubs.c`, but still see which standard library functions are in use:

1 Do one of the following:

- Deactivate all standard stubs using `-D POLYSPACE_NO_STANDARD_STUBS` option. For example:

```
polyspace-c -D POLYSPACE_NO_STANDARD_STUBS
```

- Deactivate all stubbed extensions to ANSI C standard by using `-D POLYSPACE_STRICT_ANSI_STANDARD_STUBS`. For example:

```
polyspace-c -D POLYSPACE_STRICT_ANSI_STANDARD_STUBS
```

This approach presents a list of functions PolySpace software tries to stub, as. It also lists the standard functions in use (most probably without any prototype), and generates the following type of message:

```
* Function strcpy may write to its arguments and may
return parts of them. Does not model pointer effects.
Returns an initialized value.
```

```
Fatal error: function 'strcpy' has unknown prototype
```

2 Add a proper include file in the C file that uses your standard library function. If you restart PolySpace with the same options, the default behavior results for these stubs for this particular function.

Consider the example `size_t strcpy(char *s, const char *i)` stubbed to

- Write anything in `*s`
- Return any possible `size_t`

Automatic Stub Creation Errors

In this section...
“Three Types of Error Messages” on page 7-28
“Function Pointer Error” on page 7-28
“Unknown Prototype Error” on page 7-29
“Parameter -entry-points Error” on page 7-29

Three Types of Error Messages

The PolySpace software generates three different types of error messages during the automatic creation of stubs.

For more information about stubbing errors, see “Stubbing Errors” on page 7-21.

Function Pointer Error

Message

```
Fatal error: function 'f' refers to a function pointer either  
much too complex or in a too-complex data-structure, or with  
unknown parameters.  
It cannot be stubbed automatically.
```

Solution

Consider a prototype `f` that contains a function pointer as a parameter.

If the function pointer prototype only contains scalars and/or floats, then the PolySpace software automatically stubs `f`.

For example, the verification process automatically stubs the following function:

```
int f()  
void (*ptr_ok)(int, char, float),
```

```
other_type1 other_param1);
```

If this function pointer prototype also contains pointers, you get the error message and have to stub the f function manually.

For example, stub the following function manually (unless you use the `-permissive-stubber` option):

```
int f()
void (*ptr_ok)(int *, char, float),
other_type1 other_param1);
```

Unknown Prototype Error

Message

```
Fatal error: function 'f' has unknown prototype
-----
Error message explanation:
- "function has wrong prototype" means that either the function
  has no prototype or its prototype is not ANSI compliant.
- "task is undefined" means that a function has been declared
  to be a task but has no known body
```

Solution

Provide an ANSI-compliant prototype.

Parameter -entry-points Error

Message

```
*** Verifier found an error in parameter -entry-points: task "w"
must be a userdef function
-----
---
--- Found some errors in launching command.          ---
--- Please consult rte-kernel -h to correct them    ---
--- and launch the verification again.              ---
```


Solution

A function or procedure declared to be an `-entry-point` cannot be an automatically stubbed function.

Viewing Error Information When Verification Stops

In this section...

“Verification Stopped Errors” on page 7-31

“Using the Log File” on page 7-31

“Log File Example” on page 7-31

Verification Stopped Errors

The verification log can indicate detection of an error in the previous phase, and that the verification has therefore stopped. This part of the verification process is the intermediate language verification.

Using the Log File

If PolySpace software provides no graphical result, it lists the errors and their locations at the end of the log file. To find them, scroll through the verification log file, starting at the end and working backwards.

Log File Example

This example only explains *where* to find the error list. See “Check Descriptions” for details about the error messages.

```
***** C to intermediate language translation 13.29 (P_SETUP) took  
0.000773real, 0.000773u + 0.0s
```

```
-----  
1 User Program Errors:  
* failure of correctness condition [non-initialized variable]  
"&" file intermediate.c line 5 column 0  
Please correct the program and restart the verifier.  
-----
```

```
***** C to intermediate language translation 13.30 (IL Partition)  
0 empty package(s) removed  
***** C to intermediate language translation 13.30 (IL Partition)
```

```
took 0.002252real, 0.002252u + 0.0s
**** C to intermediate language translation 13 (P_IL) took
1.069168real, 1.069168u + 0.0s
0 empty package(s) removed
**** C to intermediate language translation 14 (P_IPF)
96% init procedures removed
**** C to intermediate language translation 14 (P_IPF) took
0.002401real, 0.002401u + 0.0s
* terminating ../il-sources/a0.ads
* terminating ../il-sources/a0.adb
**** C to intermediate language translation 15 (P_TW)
**** C to intermediate language translation 15 (P_TW) took
0.003055real, 0.003055u + 0.0s
* assigns: 100% reduction
* asserts: 100% reduction
* total : 54% reduction
User time for command `iabc-c2if -input-file': 17 seconds on host
paris12

*****
***
*** C to intermediate language translation done
***

*****
Ending at: Oct 31, 2002 14:29:26
Certain (red) errors detected during previous phase.
You must correct them before continuing.
```


Reducing Verification Time

In this section...

- “Factors Impacting Verification Time” on page 7-33
- “Displaying Verification Status Information” on page 7-34
- “Techniques for Improving Verification Performance” on page 7-35
- “Turning Antivirus Software Off” on page 7-38
- “Tuning PolySpace Parameters” on page 7-38
- “Subdividing Code” on page 7-39
- “Reducing Procedure Complexity” on page 7-49
- “Reducing Task Complexity” on page 7-50
- “Reducing Variable Complexity” on page 7-50
- “Choosing Lower Precision” on page 7-51

Factors Impacting Verification Time

These factors affect how long it takes to run a verification:

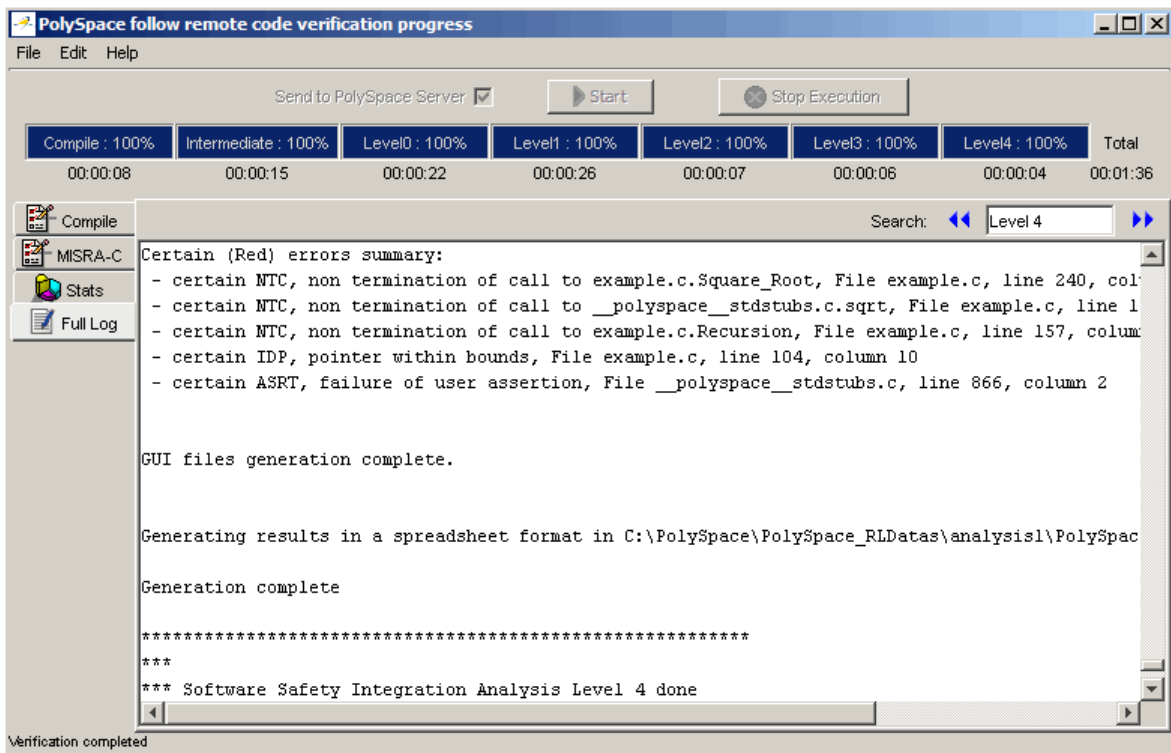
- The size of the code
- The number of global variables
- The nesting depth of the variables (the more nested they are, the longer it takes)
- The depth of the call tree of the application
- The intrinsic complexity of the code, particularly with regards to pointer manipulation

Because many factors impact verification time, there is no precise formula for calculating verification duration. Instead, PolySpace software provides graphical and textual output to indicate how the verification is progressing.

Displaying Verification Status Information

For *server* verifications, you can use the PolySpace Queue Manager to follow the progress of your verification. For more information, see “Monitoring Progress of Server Verification” on page 6-8.

For *client* verifications, you can monitor the progress of your verification using the progress bar and **Stats** log in the Launcher. For more information, see “Monitoring the Progress of the Verification” on page 6-24.



The progress bar highlights each completed phase and displays the amount of time for that phase. You can estimate the remaining verification time by extrapolating from this data, and considering the number of files and passes remaining.

Techniques for Improving Verification Performance

This chapter suggests methods to reduce the duration of a particular verification, with minimal compromise for the launch parameters or the precision of the results.

You can increase the size of a code sample for effective analysis by tuning the tool for that sample. Beyond that point, subdividing the code or choosing a lower precision level offers better results (-01, -00).

You can use several techniques to reduce the amount of time required for a verification, including

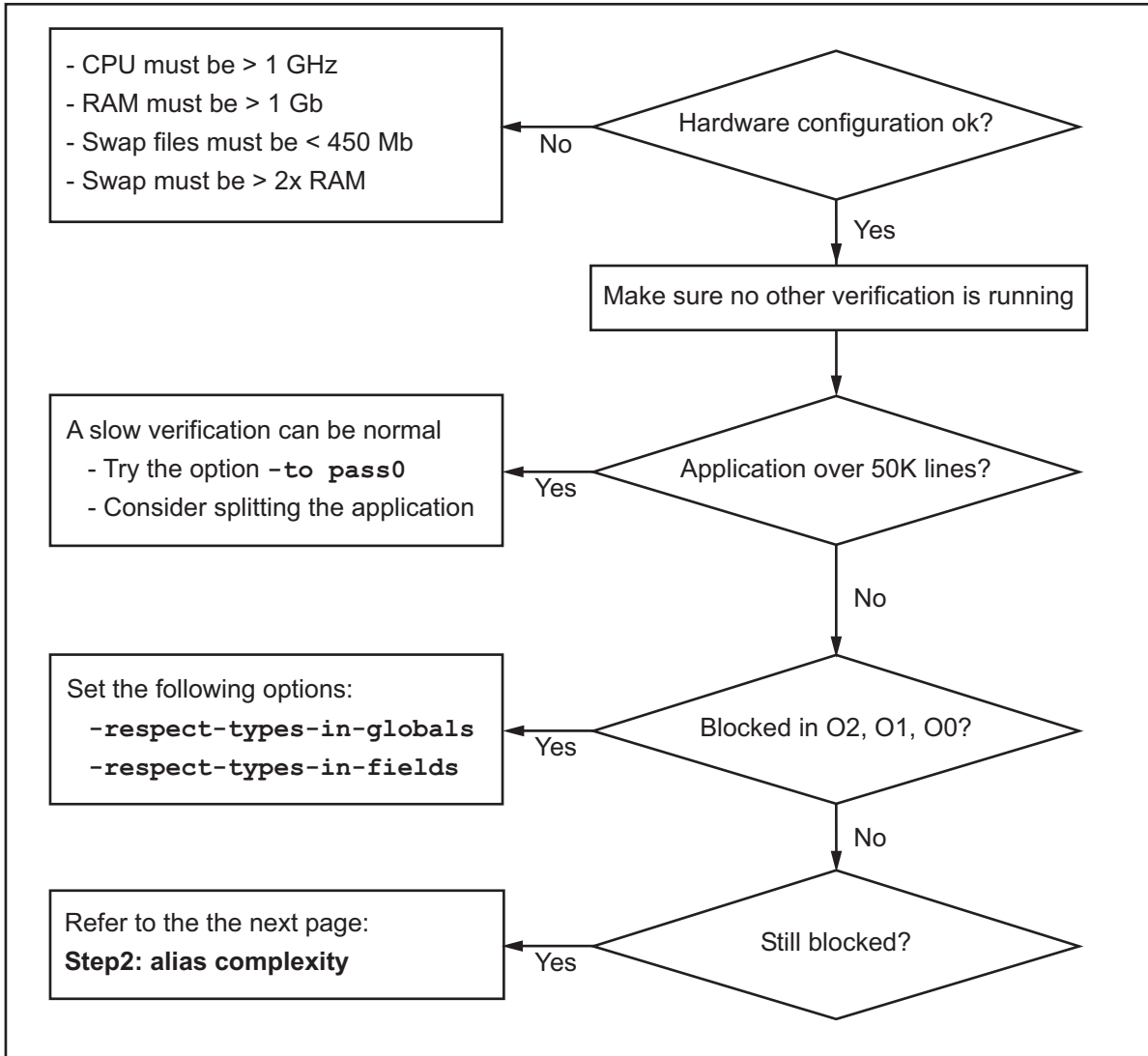
- “Turning Antivirus Software Off” on page 7-38
- “Tuning PolySpace Parameters” on page 7-38
- “Subdividing Code” on page 7-39
- “Reducing Procedure Complexity” on page 7-49
- “Reducing Task Complexity” on page 7-50
- “Reducing Variable Complexity” on page 7-50
- “Choosing Lower Precision” on page 7-51

You can combine these techniques. See the following performance tuning flow charts:

- “Standard Scaling Options Flow Chart” on page 7-36
- “Alias Complexity Flow Chart” on page 7-37

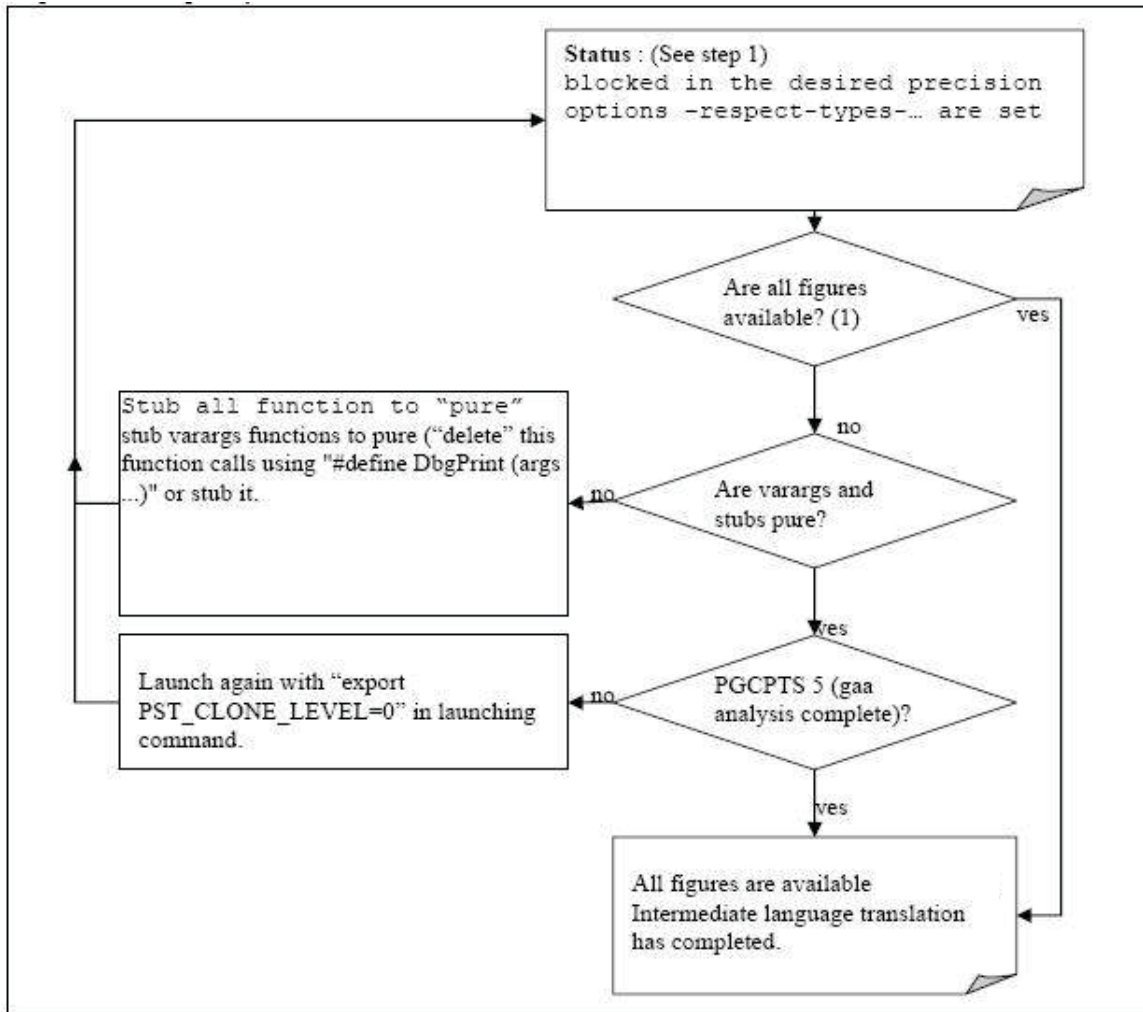
Standard Scaling Options Flow Chart

Step 1: standard scaling options



Alias Complexity Flow Chart

Step 2: alias complexity



Here is a typical set of statistics. You can find them for any application by using the `polyspace-stats` utility (available at MATLAB Central), at any point after the intermediate language translation completes.

```
Some stats on aliases use:
  Number of alias writes: 2672
  Number of must-alias writes: 0
  Number of alias reads: 0
  Number of invisibles: 60
  Number of global invisibles: 3808
Stats about alias writes:
  biggest sets of alias writes: Variable_1 (45), Variable_1 (32)
  procedures that write the biggest sets of aliases: procedure_f_1
(583), procedure_f_2 (369), procedure_f_3 (264)
```

You can reduce the pointers complexity by inlining the following functions :

```
procedure_g_1      procedure_g_2
procedure_g_3
```

In terms of reducing code complexity, The MathWorks recommends that you try the following techniques, in the order listed:

- “Reducing Procedure Complexity” on page 7-49
- “Reducing Task Complexity” on page 7-50
- “Reducing Variable Complexity” on page 7-50

After you use any of these techniques, restart the verification.

Turning Antivirus Software Off

Disabling or switching off any third-party antivirus software for the duration of a verification can reduce the verification time by up to 40%.

Tuning PolySpace Parameters

Impact of Parameter Settings

Compromise to balance the time required to perform a verification and the time required to review the results. Launching PolySpace verification with the following options reduces the time taken for verification. However, these parameter settings compromise the precision of the results. The less precise

the results of the verification, the more time you can spend reviewing the results.

Recommended Parameter Tuning

The MathWorks suggests that you use the parameters in the sequence listed. If the first suggestion does not increase the speed of verification sufficiently, then introduce the second, and so on.

- Switch from `-O2` to a lower precision;
- Set the `-respect-types-in-globals` and `-respect-types-in-fields` options;
- Set the `-k-limiting` option to 2, then 1, or 0;
- Manually stub missing functions which write into their arguments.
- If some code uses some large arrays, use the `-no-fold` option.

For example, an appropriate launching command is

```
polyspace-c -O0 -respect-types-in-globals -k-limiting 0
```

Subdividing Code

- “An Ideal Application Size” on page 7-39
- “Benefits of Subdividing Code” on page 7-40
- “Possible Issues with Subdividing Code” on page 7-40
- “Recommended Approach” on page 7-42
- “Selecting a Subset of Code” on page 7-43

An Ideal Application Size

People have used PolySpace software to analyze numerous applications with greater than 100,000 lines of code.

There always is a compromise between the time and resources required to analyze an application, and the resulting selectivity. The larger the project size, the broader the approximations PolySpace software makes. Broader

approximations produce more oranges. Large applications can require you to spend much more time analyzing the results and your application.

These approximations enable PolySpace software to extend the range of project sizes it can manage, to perform the verification further, and to solve traditionally incomputable problems. Balance the benefits derived from verifying a whole large application against the loss of precision that results.

Benefits of Subdividing Code

Subdividing a large application into smaller subsets of code provides several benefits. You:

- Quickly isolate a meaningful subset
- Keep all functional modules
- Can maintain a high precision level (for example, level O2)
- Reduce the number of orange items
- Get correct results are correct because you do not need to remove any thread affecting change shared data
- Reduce the code complexity considerably

Possible Issues with Subdividing Code

Subdividing code can lead to these problems:

- Orange checks can result from a lack of information regarding the relationship between modules, tasks, or variables.
- Orange checks can result from using too wide a range of values for stubbed functions.
- Some loss of precision; the verification consider all possible values for a variable.

When the Application is Incomplete. When the code consists of a small subset of a larger project, PolySpace software automatically stubs many procedures. PolySpace bases the stubbing on the specification or prototype of the missing functions. PolySpace verification assumes that all possible values for the parameter type are returnable.

Consider two 32-bit integers a and b , which are initialized with their full range due to missing functions. Here, $a*b$ causes an overflow, because a and b can be equal to 2^{31} . Precise stubbing can reduce the number of incidences of these data set issue **orange checks**.

Now consider a procedure f that modifies its input parameters a and b . f passes both parameters by reference. Suppose a can be from 0 through 10, and b any value between -10 and 10. In an automatically stubbed function, the combination $a=10$ and $b=10$ is possible, even if it is not possible with the real function. This situation introduces orange checks in a code snippet such as $1/(a*b - 100)$, where the division would be **orange**.

- So, even with precise stubbing, verification of a small section of code can introduce extra orange checks. However, the net effect from reducing the complexity is to reduce the total number of orange checks.
- With default stubbing, the increase in the number of orange checks as the result of this phenomenon tends to be more pronounced.

Considering the Effects of Application Code Size. PolySpace can make approximations when computing the possible values of the variables, at any point in the program. Such an approximation use a superset of the actual possible values.

For instance, in a relatively small application, PolySpace software can retain detailed information about the data at a particular point in the code. For example, the variable VAR can take the values $\{-2 ; 1 ; 2 ; 10 ; 15 ; 16 ; 17 ; 25\}$. If the code uses VAR to divide, the division is green (because 0 is not a possible value).

If the program is large, PolySpace software simplifies the internal data representation by using a less precise approximation, such as $[-2 ; 2] \cup \{10\} \cup [15 ; 17] \cup \{25\}$. Here, the same division appears as an orange check.

If the complexity of the internal data becomes even greater later in the verification, PolySpace can further simplify the VAR range to (say) $[-2 ; 20]$.

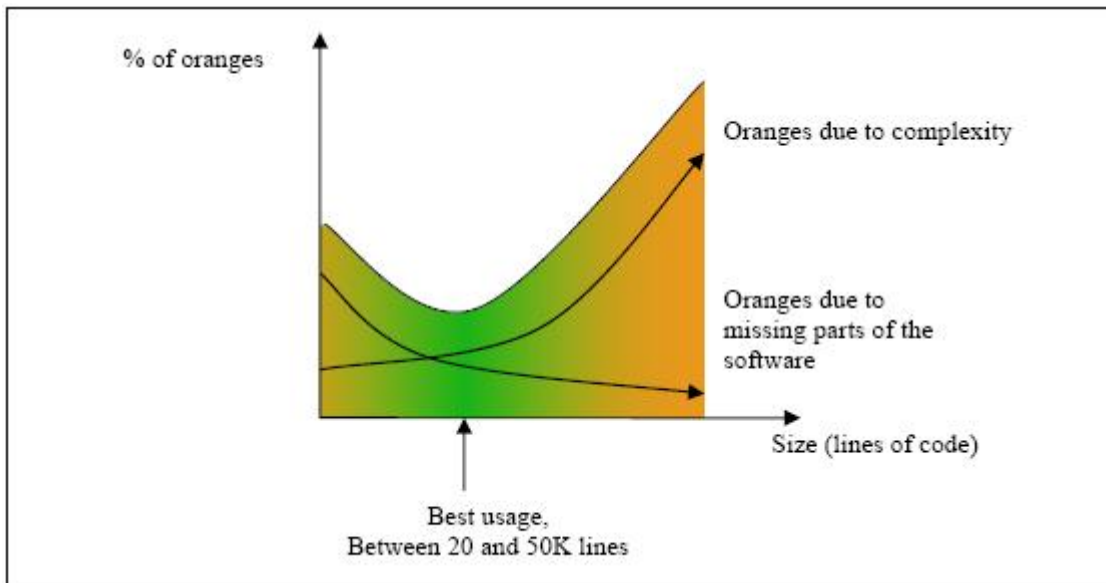
This phenomenon increases the number of orange warnings when the size of the program becomes large.

Recommended Approach

The MathWorks recommends that you begin with file-by-file verifications (when dealing with C language), package-by-package verifications (when dealing with Ada language), and class-by-class verifications (when dealing with C++ language).

The maximum application size is between 20,000 (for C++) and 50,000 lines of code (for C and Ada). For such applications of that size, approximations are not too significant. However, sometimes verification time is extensive.

Experience suggests that subdividing an application before verification normally has a beneficial impact on selectivity. The verification produces more red, green and gray checks, and fewer unproven Orange checks. This subdivision approach makes bug detection more efficient.



A compromise between selectivity and size

PolySpace verification is most effective when you use it as early as possible in the development process, before any other form of testing.

When you analyze a small module (for example, a file, piece of code, or package) using PolySpace software, focus on the **red** and **gray** checks. **Orange** unproven checks at this stage are interesting, because most of them deal with robustness of the application. The **Orange** checks change to **red**, **gray**, or **green** as the project progresses and you integrate more modules.

In the integration process, code can become so large (50,000 lines of code or more). This amount of code can cause the verification to take an unreasonable amount of time. You have two options:

- Stop using PolySpace verification at this stage (you have gained many benefits already).
- Analyze subsets of the code.

Selecting a Subset of Code

Subdividing a project for verification takes considerably less verification time for the sum of the parts than for the whole project considered in one pass. Consider data flow when you subdivide the code.

Consider two distinct concepts:

- **Function entry-points** — Function entry-points refer to the PolySpace execution model, because they start concurrently, without any assumption regarding sequence or priority. They represent the beginning of your call tree.
- **Data entry-points** — Regard lines in the code that acquire data as data entry points.

Example 1

```
int complete_treatment_based_on_x(int input)
{
    thousand of line of computation...
}
```

Example 2

```
void main(void)
{
```

```
int x;  
x = read_sensor();  
y = complete_treatment_based_on_x(x);  
}
```

Example 3

```
#define REGISTER_1 (*(int *)0x2002002)  
void main(void)  
{  
  x = REGISTER_1;  
  y = complete_treatment_based_on_x(x);  
}
```

In each case, the x variable is a data entry point and y is the consequence of such an entry point. y can be formatted data, due to a complex manipulation of x .

Because x is volatile, a probable consequence is that y contains all possible formatted data. You could remove the procedure `complete_treatment_based_on_x` completely, and let automatic stubbing work. The verification process considers y as potentially taking any value in the full range data (see “Stubbing” on page 5-2).

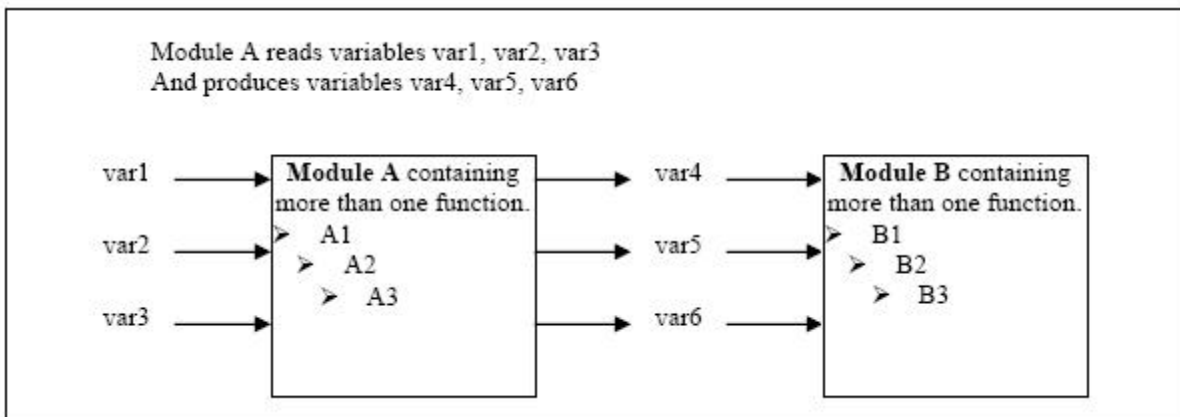
```
//removed definition of complete_treatment_based_on_x  
void main(void)  
{  
  x = ... // what ever  
  y = complete_treatment_based_on_x(x); // now stubbed!  
}
```

Typical Examples of Removable Components, According to the Logic of the Data. Here are some examples of removable components, based on the logic of the data:

- **Error management modules** often contain a large array of structures accessed through an API, but return only a Boolean value. Removing the API code and retaining the prototype causes the automatically generated stub to return a value in the range $[-2^{31}, 2^{31}-1]$, which includes 1 and 0. PolySpace considers the procedure able to return all possible answers, just like reality.

- **Buffer management for mailboxes coming from missing code** – Suppose an application reads a huge buffer of 1024 char. The application then uses the buffer to populate three small arrays of data, using a complicated algorithm before passing it to the main module. If the verification excludes the buffer, and initializes the arrays with random values instead, then the verification of the remaining code is just the same.
- Display modules

Subdivision According to Data Flow. Consider the following example.



In this application, variables 1, 2 and 3 can vary between the following ranges:

Var1	From 0 through 10
Var2	From 1 through 100
Var3	From -10 through 10

Module A consists of an algorithm which interpolates between var1 and var2. That algorithm uses var3 as an exponential factor, so when var1 is equal to 0, the result in var4 is also equal to 0.

As a result, var4, var5 and var6 have the following specifications:

Ranges	var4 var5 var6	Between -60 and 110 From 0 through 12 From 0 through 100
Properties	And a set of properties between variables	<ul style="list-style-type: none">• If var2 is equal to 0, than $\text{var4} > \text{var5} > 5$.• If var3 is greater than 4, than $\text{var4} < \text{var5} < 12$• ...

Subdivision in accordance with data flow allows you to analyze modules A and B separately.

- A uses variables 1, 2 and 3 initialized respectively to [0;10], [1;100] and [-10;10]
- B uses variables 4, 5 and 6 initialized respectively to [-60;110], [0;12] and [-10;10]

The consequences are:

- A slight loss of precision on the B module verification, because now PolySpace considers all combinations for variables 4, 5 and 6. It includes all possible combinations, even those combinations that the module A verification restricts.

For example, if the B module included the test

```
If var2 is equal to 0, than var4>var5>5
```

then the dead code on any subsequent else clause is undetected.

- An in-depth investigation of the code is not necessary to isolate a meaningful subset. It means that a logical split is possible for any application, in accordance with the logic of the data.
- The results remain valid, because there no requirement to remove (for example) a thread that changes shared data.
- The code is less complex.
- You can maintain the maximum precision level.

Typical examples of removable components:

- Error management modules. A function `has_an_error_already_occurred` can return TRUE or FALSE. Such a module can contain a large array of structures accessed through an API. Removing API code with the retention of the prototype results in the PolySpace verification producing a stub that returns $[-2^{31}, 2^{31}-1]$. That result clearly includes 1 and 0 (yes and no). The procedure `has_an_error_already_occurred` returns all possible answers, just like the code would at execution time.
- Buffer management for mailboxes coming from missing code. Suppose the code reads a large buffer of 1024 char and then collates the data into three small arrays of data, using a complicated algorithm. It then gives this data to a main module for treatment. For the verification, PolySpace can remove the buffer and initialize the arrays with random values.
- Display modules.

Subdivide According to Real-Time Characteristics. Another way of splitting an application is to isolate files which contain only a subset of tasks, and to analyze each subset separately.

If a verification initiates using only a few tasks, PolySpace loses information regarding the interaction between variables.

Suppose an application involves tasks T1 and T2, and variable x.

If T1 modifies x and reads it at a particular moment, then the values of x impact subsequent operations in T2.

For example, consider that T1 can write either 10 or 12 into x and that T2 can both write 15 into x and read the value of x. Two ways to achieve a sound standalone verification of T2 are:

- You could declare x as volatile to take into account all possible executions. Otherwise, x takes only its initial value or x variable remains constant, and verification of T2 is a subset of possible execution paths. You can get precise results, but it includes one scenario among all possible states for the variable x.

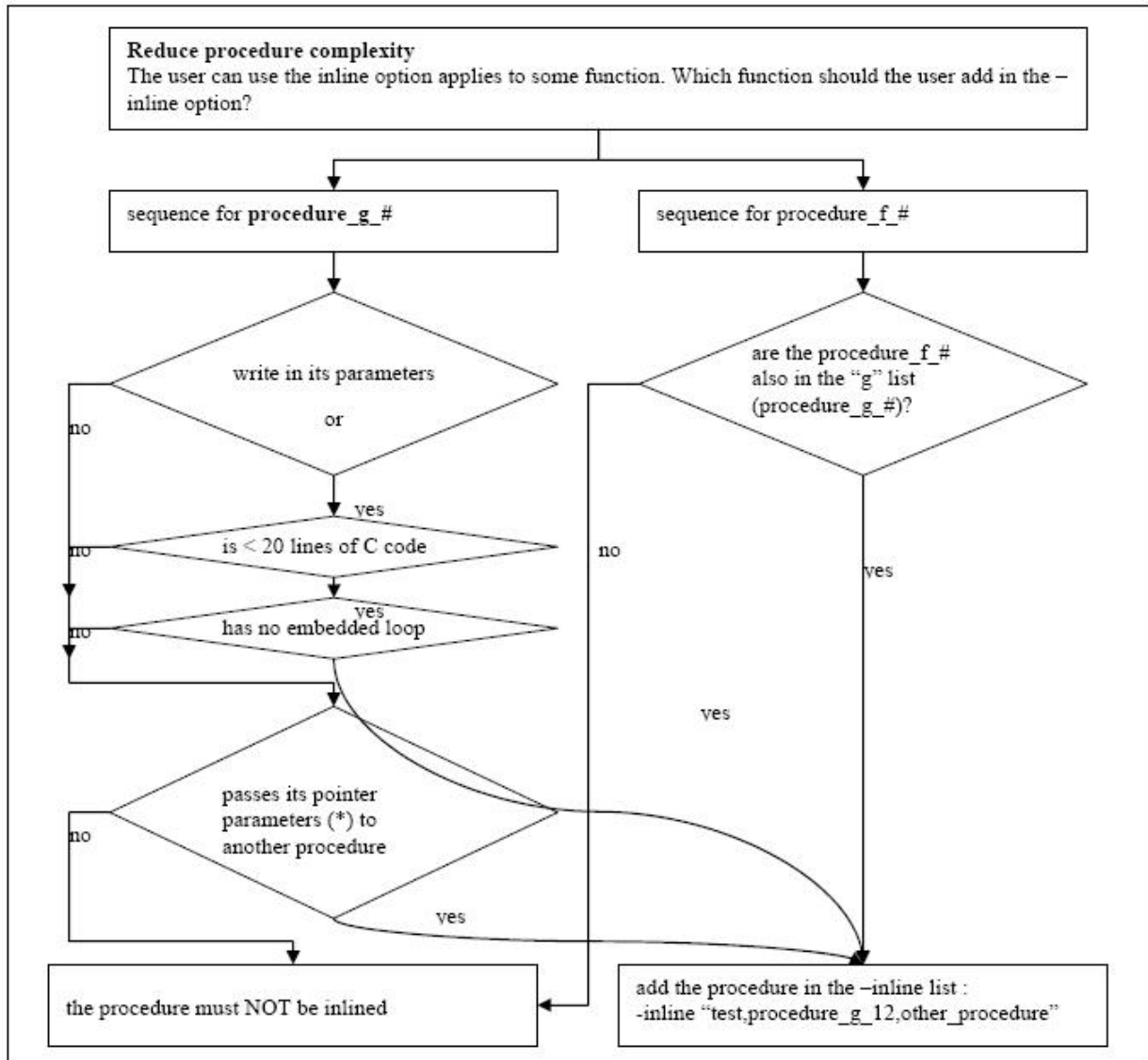
- You could initialize `x` to the whole possible range `[10;15]`, and then call the `T2` entry-point. This approach is accurate if `x` is calibration data.

Subdivide According to Files. This method is simple, but it can produce good results when you are trying to find red errors and bugs in gray code.

Simply extract a subset of files and perform a verification using one of these approaches:

- Use entry-points.
- Create a `main` that calls randomly all functions that the subset of the code does not call.

Reducing Procedure Complexity



For example, analyze whether a procedure pass its pointer parameters to another procedure?

YES	NO	NO
<pre>void f(int *p) { f2(p) }</pre>	<pre>void f(int q)</pre>	<pre>void f(int *r) { *r = 12 }</pre>

Reducing Task Complexity

If the code contains two or more tasks, and particularly if there are more than 10000 alias reads, set the `-lightweight-thread-model` option. This option reduces:

- Task complexity
- Verification time

There are some downsides:

- It causes more oranges and a slight loss of precision on reads of shared variables through pointers.
- The dictionary can omit some read/write accesses.

Reducing Variable Complexity

Variable Characteristic	Action
The types are complex.	Set the <code>-k-limiting [0-2]</code> option. Begin with 0. Go up to 1, or 2 in order to gain precision.
There are large arrays	Set the <code>-no-fold</code> option.

Choosing Lower Precision

The amount of simplification applied to the data representations depends on the required precision level (O0, O2), PolySpace software adjusts the level of simplification. For example:

- -O0 — shorter computation time
- -O2 — less orange warnings
- -O3 — less orange warnings and longer computation time. The MathWorks recommends using this option only for projects containing less than 1,000 lines of code.

Obtaining Configuration Information

The `polyspace-ver` command allows you to quickly gather information on your system configuration. You should use this information when entering support requests.

Configuration information includes:

- Hardware configuration
- Operating System
- PolySpace Licenses
- Specific version numbers for PolySpace products

To obtain your configuration information, enter the following command:

- **UNIX/Linux** — `<PolySpaceInstallDir>/Verifier/bin/polyspace-ver`
- **Windows** — `<PolySpaceInstallDir>/Verifier/wbin/polyspace-ver.exe`

The configuration information appears.

```

C:\WINNT\system32\cmd.exe
C:\PolySpace\PolySpaceForCandCPP_R2009b\Uerifier\wbin>polyspace-ver.exe
-----
Machine Hardware Configuration:
* Number of CPUs      : 1
* CPU frequency       : 2.211GHz
* CPU type            : i686
* Memory              : 1023MB
* Swap               : 2.40GB
* /tmp free space    : 169.44GB
-----

Machine Software Configuration:
Windows XP (Service Pack 3)
-----

PolySpace Licenses:
PolySpace_Client_C_CPP:
  License Number: DEMO
  Expiration date: 20-oct-2009

PolySpace_Server_C_CPP:
  License Number: DEMO
  Expiration date: 20-oct-2009

PolySpace_Model_Link_SL:
  License Number: DEMO
  Expiration date: 20-oct-2009
-----

PolySpace Versions:
PolySpace Version R2009b
* Kernel                CC-7.1.0.U1
* Viewer                IHME-R2009b-U9
* Launcher              IHML-R2009b-U9
* Remote Launcher      RL-R2009b-U6
* Visual Plugin        PUP6_0_1_5
* PolySpace In One Click POC-R2009b-U4
* MBD Plugin           MBD-R2009b-U4
* Automatic Orange Tester AOT-R2009b-U4

Remote Launcher configuration
* Compatibility version 3_12_2

Server :
PolySpace_Server_C_CPP.mathworks.com
-----

C:\PolySpace\PolySpaceForCandCPP_R2009b\Uerifier\wbin>

```

Note You can obtain the same configuration information by selecting **Help > About** in the Launcher.

Removing Preliminary Results Files

By default, the software automatically deletes preliminary results files when they are no longer needed by the verification. However, if you run a client verification using the option `keep-all-files`, preliminary results files are retained in the results directory. This allows you to restart the verification from any stage, but can leave unnecessary files in your results directory.

If you later decide that you no longer need these files, you can remove them.

To remove preliminary results files:

- 1** Open the project containing the results you want to delete In the Launcher.
- 2** Select **Tools > Clean Results**.

The preliminary results files are deleted.

Note To remove **all** verification results from your results directory (including the final results), select **Tools > Delete Results**.

Reviewing Verification Results

- “Before You Review PolySpace Results” on page 8-2
- “Opening Verification Results” on page 8-8
- “Reviewing Results in Assistant Mode” on page 8-19
- “Reviewing Results in Expert Mode” on page 8-27
- “Importing and Exporting Review Comments” on page 8-41
- “Generating Reports of Verification Results” on page 8-44
- “Using PolySpace Results” on page 8-51

Before You Review PolySpace Results

In this section...

“Overview: Understanding PolySpace Results” on page 8-2

“Why Gray Follows Red and Green Follows Orange” on page 8-3

“The Message and What It Means” on page 8-4

“The C Explanation” on page 8-5

Overview: Understanding PolySpace Results

PolySpace software presents verification results as colored entries in the source code. There are four main colors in the results:

- **Red** – Indicates code that always has an error (errors occur every time the code is executed).
- **Gray** – Indicates unreachable code (dead code).
- **Orange** – Indicates unproven code (code might have a run-time error).
- **Green** – Indicates code that never has a run-time error (safe code).

When you analyze these colors, remember these rules:

- An instruction is verified only if no run-time error is detected in the previous instruction.
- The verification assumes that each run-time error causes a “core dump.” The corresponding instruction is considered to have stopped, even if the actual run-time execution of the code might not stop. This means that red checks are always followed by gray checks, and orange checks only propagate the green parts through to subsequent checks.
- Focus on the verification message. Do not jump to false conclusions. You must understand the color of a check step by step, until you find the root cause of a problem.
- Determine the cause by examining the actual code. Do not focus on what the code is supposed to do.

Why Gray Follows Red and Green Follows Orange

Gray checks follow **red** checks, and **green** checks are propagated out of **orange** checks.

In the following example, consider why:

- The gray checks follow the **red** in the red function.
- There are **green** checks relating to the array.

```

void red(void)                extern int Read_An_Input(void);
{                               void propagate(void)
  int x;                       {
  x = 1 / x ;                 int X;
  x = x + 1;                 int y[100];
  }                           X = Read_An_Input();
                               y[X] = 0; // [array index within bounds]
                               y[X] = 0;
                               }

```

Consider each line of code for the red function:

- When PolySpace divides by X , X is not initialized. Therefore, the corresponding check (Non Initialized Variable) on X is red.
- As a result, PolySpace stops all possible execution paths because they all produce an RTE. Therefore, the subsequent instructions are gray (unreachable code).

Now, consider each line of code for the propagate function:

- X is assigned the return value of `Read_An_Input`. After this assignment, $X = [-2^{31}, 2^{31}-1]$.
- At the first array access, you might see an “out of bounds” error because X can equal -3 as well as 3 .
- Subsequently, all conditions leading to an RTE are truncated — they are no longer considered in the verification. On the following line, all executions in which $X = [-2^{31}, -1]$ and $[100, 2^{31}-1]$ are stopped.

- At the next instruction, $X = [0, 99]$.
- Therefore, at the second array access, the check is green because $X = [0, 99]$.

Summary

Green checks can be propagated out of orange checks.

The Message and What It Means

PolySpace software numbers checks to correspond to the code execution order.

Consider the instruction `x++;`

PolySpace first checks for a potential NIV (Non Initialized Variable) for `x`, and then checks the potential OVFL (overflow). This action mimics the actual execution sequence.

Understanding these sequences can help you understand the message presented by PolySpace, and what that message means.

Consider an orange NIV on `x` in the test:

```
if (x > 101);
```

You might conclude that the verification does not keep track of the value of `x`. However, consider the context in which the check is made:

```
extern int read_an_input(void);

void main(void)
{
  int x;
  if (read_an_input()) x = 100;
  if (x > 101) // [orange on the NIV : non initialised variable ]
    { x++; } // gray code
}
```

Explanation

You can see the category of each check by clicking it in the Viewer. When you examine an orange check, you see that any value of a variable that would that results in a run-time error (RTE) is not considered further. However, as this example NIV (Non Initialized Variable) shows, any value that does not cause an RTE is verified on subsequent lines.

The correct interpretation of this verification result is that if x is initialized, the only possible value for it is 100. Therefore, x can never be both initialized and greater than 101, so the rest of the code is gray. This conclusion may be different from what you first suspect.

Summary

In summary:

- " $x > 100$ " does **NOT** mean that PolySpace does not know anything about x .
- " $x > 100$ " **DOES** mean that PolySpace does not know whether X is initialized.

When you review results, remember:

- Focus on the PolySpace software message.
- Do not assume any conclusions.

The C Explanation

Verification results depend entirely on the code that you are verifying. When interpreting the results, do not consider:

- Any physical action from the environment in which the code operates.
- Any configuration that is not part of the verification.
- Any reason other than the code itself.

The only thing that the verification considers is the C code submitted to it.

Consider the following example, paying particular attention to the dead (gray) code following the "if" statement:

```

extern int read_an_input(void);

void main(void)
{
    int x;
    int y[100];
    x = read_an_input();
    y[x ] = 0; // [array index within bounds]
    y[x-1] = (1 / X) + X ;
    if (x == 0)
        y[x] = 1; // gray code on this line
}

```

You can see that:

- The line containing the access to the y array is unreachable.
- Therefore, the test to assess whether $x = 0$ is always false.
- **The initial conclusion is that "the test is always false."** You might conclude that this results from input data that is not equal to 0. However, Read_An_Input can be any value in the full integer range, so this is not the correct explanation.

Instead, consider the execution path leading to the gray code:

- The orange check on the array access ($y[x]$) truncates any execution path leading to a run-time error, meaning that subsequent lines deal with only $x = [0, 99]$.
- The orange check on the division also truncates all execution paths that lead to a run-time error, so all instances where $x = 0$ are also stopped. Therefore, for the code execution path after the orange division sign, $x = [1; 99]$.
- x is never equal to 0 **at this line**. The array access is green ($y(x - 1)$).

Summary

In this example, all the results are located in the same procedure. However, by using the call tree, you can follow the same process even if an orange check results from a procedure at the end of a long call sequence. Follow the "called

by" call tree, **and concentrate on explaining the issues by reference to the code alone.**

Opening Verification Results

In this section...

“Downloading Results from Server to Client” on page 8-8

“Downloading Server Results to UNIX or Linux Clients” on page 8-11

“Downloading Results from Unit-by-Unit Verifications” on page 8-12

“Opening Verification Results” on page 8-12

“Exploring the Viewer Window” on page 8-13

“Selecting Viewer Mode” on page 8-16

“Setting Character Encoding Preferences” on page 8-17

Downloading Results from Server to Client

When you run a verification on a PolySpace server, the PolySpace software stores the results on the PolySpace server. To view your results, download the results file from the server to the client.

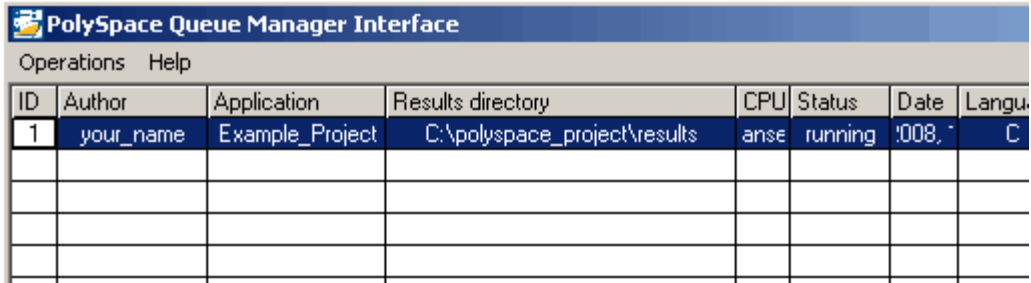
Note If you download results before the verification is complete, you get partial results and the verification continues.

To download verification results to your client system:

- 1 Double-click the **PolySpace Spooler** icon.



The **PolySpace Queue Manager Interface** opens.



The screenshot shows the PolySpace Queue Manager Interface. At the top, there is a title bar with the PolySpace logo and the text "PolySpace Queue Manager Interface". Below the title bar is a menu bar with "Operations" and "Help". The main area contains a table with the following columns: ID, Author, Application, Results directory, CPU, Status, Date, and Language. The first row of the table is highlighted in blue and contains the following data: ID: 1, Author: your_name, Application: Example_Project, Results directory: C:\polyspace_project\results, CPU: anse, Status: running, Date: '008, and Language: C. There are four empty rows below the first row.

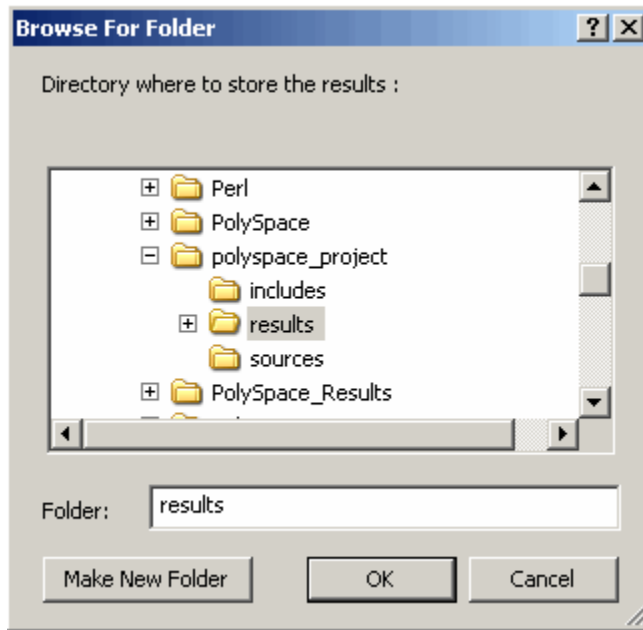
ID	Author	Application	Results directory	CPU	Status	Date	Language
1	your_name	Example_Project	C:\polyspace_project\results	anse	running	'008,	C

Note The PolySpace Queue Manager is not available on UNIX or Linux systems. If you are using the PolySpace Client for C/C++ on a UNIX or Linux system, you must use the `psqueue-download` command to download your results. For information, see “Downloading Server Results to UNIX or Linux Clients” on page 8-11.

- 2 Right-click the job that you want to view. From the context menu, select **Download Results** .

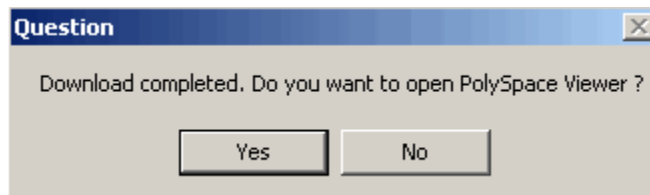
Note To remove the job from the queue after downloading your results, from the context menu, select **Download Results And Remove From Queue** .

The Browse For Folder dialog box opens.



- 3** Select the folder into which you want to download results.
- 4** Click **OK** to download the results and close the dialog box.

When the download is complete, a dialog box opens asking if you want to open the PolySpace Viewer.



- 5** Click **Yes** to open the results.

Once you download results, they remain on the client, and you can review them at any time using the PolySpace Viewer.

Downloading Server Results to UNIX or Linux Clients

If you are using PolySpace Client for on a UNIX or Linux system, the Queue Manager interface is not available. To download results from the PolySpace Server, you must use the `psqueue-download` command to download your results.

To download your results, enter the following command:

```
<PolySpaceCommonDir>/RemoteLauncher/bin/psqueue-download <id>  
<results dir>
```

The verification `<id>` is downloaded into the results directory `<results dir>`.

Note If you download results before the verification is complete, you get partial results and the verification continues.

Once you download results, they remain on the client, and you can review them at any time using the PolySpace Viewer.

The `psqueue-download` command has the following options:

- `[-f]` force download (without interactivity)
- `-admin -p <password>` allows administrator to download results.
- `[-server <name>[:port]]` selects a specific Queue Manager.
- `[-v|version]` gives release number.

Note When downloading a unit-by-unit verification group, all the unit results are downloaded and a summary of the download status for each unit is displayed.

For more information on managing verification jobs from the command line, see “Managing Verifications in Batch” on page 6-27.

Downloading Results from Unit-by-Unit Verifications

If you run a unit-by-unit verification, each source file is sent to PolySpace Server individually. The queue manager displays a job for the full verification group, as well as jobs for each unit (using a tree structure).

You can download and view verification results for the entire project, or for individual units.

To download the results from unit-by-unit verifications:

- To download results for an individual unit, right-click the job for that unit, then select **Download Results**.

The individual results are downloaded and can be viewed as any other verification results.

- To download results for a verification group, right-click the group job, then select **Download Results**.

The results for all unit verifications are downloaded, as well as an HTML summary of results for the entire verification group.

Opening Verification Results

Use the PolySpace Viewer to review the results of your verification.

Note You can also open the Viewer from the Launcher by clicking the Viewer icon in the Launcher toolbar with or without an open project.

To open the verification results:

- 1 Double-click the PolySpace Viewer icon.



- 2 Select **File > Open**.

3 In **Please select a file dialog box**, select the results file that you want to view.

4 Click **Open**.

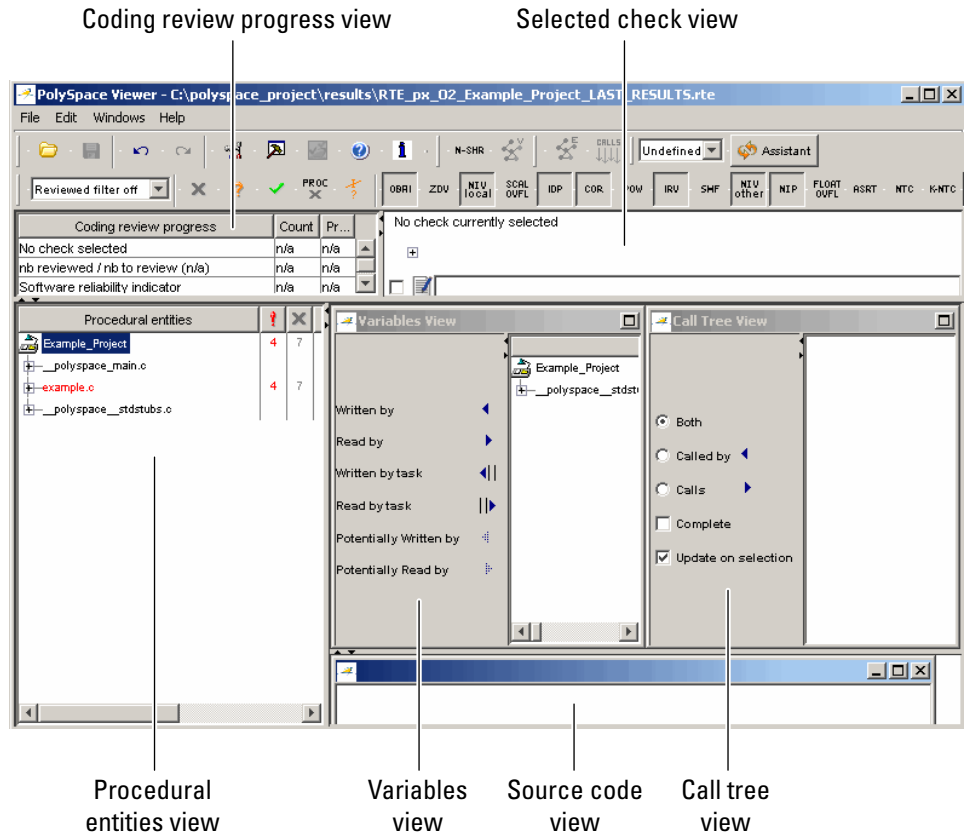
The results appear in the Viewer window.

Exploring the Viewer Window

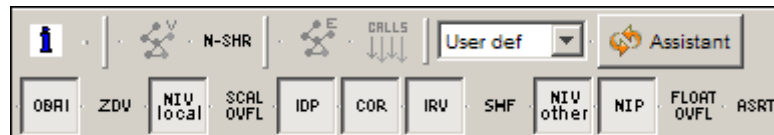
- “Overview” on page 8-13
- “Procedural Entities View” on page 8-15

Overview

The PolySpace Viewer looks like the following graphic.



The appearance of the Viewer toolbar depends on the Viewer mode. By default, you see the expert mode toolbar.



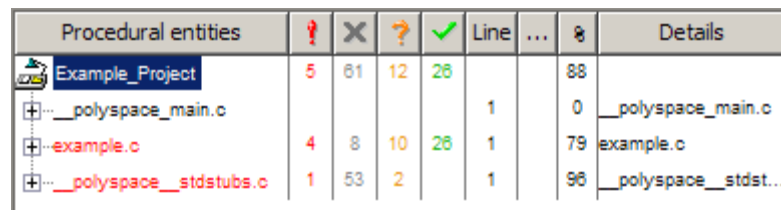
In both expert mode and assistant mode, the Viewer window has six sections below the toolbar. Each section provides a different view of the results. The following table describes these views.

This View...	Displays...
Procedural entities view (lower left)	List of the diagnostics (checks) for each file and function in the project
Source code view (lower right)	Source code for a selected check in the procedural entities view
Coding review progress view (upper left)	Statistics about the review progress for checks with the same type and category as the selected check
Selected check view (upper right)	Details about the selected check
Variables view	Information about global variables declared in the source code
Call tree view	Tree structure of function calls

You can resize or hide any of these sections.






Procedural Entities View


The procedural entities view, in the lower-left part of the Viewer window, displays a table with information about the diagnostics for each file in the project. The procedural entities view is also called the RTE (run-time error) view. The procedural entities view looks like the following graphic.



Procedural entities	!	X	?	✓	Line	...	%	Details
Example_Project	5	61	12	26			88	
+- __polyspace_main.c					1		0	__polyspace_main.c
+- example.c	4	8	10	26	1		79	example.c
+- __polyspace_stdstubs.c	1	53	2		1		96	__polyspace_stdst...

The file `example.c` is red because it has a run-time error. PolySpace software assigns to a file the color of the most severe error found in that file. The first column of the table is the procedural entity (the file or function). The following table describes some of the other columns in the procedural entities view.

Column Heading	Indicates
	Number of red checks (operations where an error always occurs)
	Number of gray checks (unreachable code)
	Number of orange checks (warnings for operations where an error might occur)
	Number of green checks (operations where an error never occurs)
	Selectivity of the verification (percentage of checks that are not orange) This is an indication of the level of proof.

Tip If you see three dots in place of a heading, , resize the column until you see the heading. Resize the procedural entities view to see additional columns.

Note You can select which columns appear in the procedural entities view by editing the preferences. To learn how to add a **Reviewed** column, see “Making the Reviewed Column Visible” on page 8-34.

What you select in the procedural entities view determines what you see in the other views. In the examples in this chapter, you learn how to use the views and how they interact.

Selecting Viewer Mode

You can review verification results in *expert* mode or *assistant* mode:

- In expert mode, you decide how you review the results.
- In assistant mode, PolySpace software guides you through the results.

You switch from one mode to the other by clicking the appropriate button in the Viewer toolbar.



Setting Character Encoding Preferences

If the source files that you want to verify are created on an operating system that uses different character encoding than your current system (for example, when viewing files containing Japanese characters), you receive an error message when you view the source file or run certain macros.

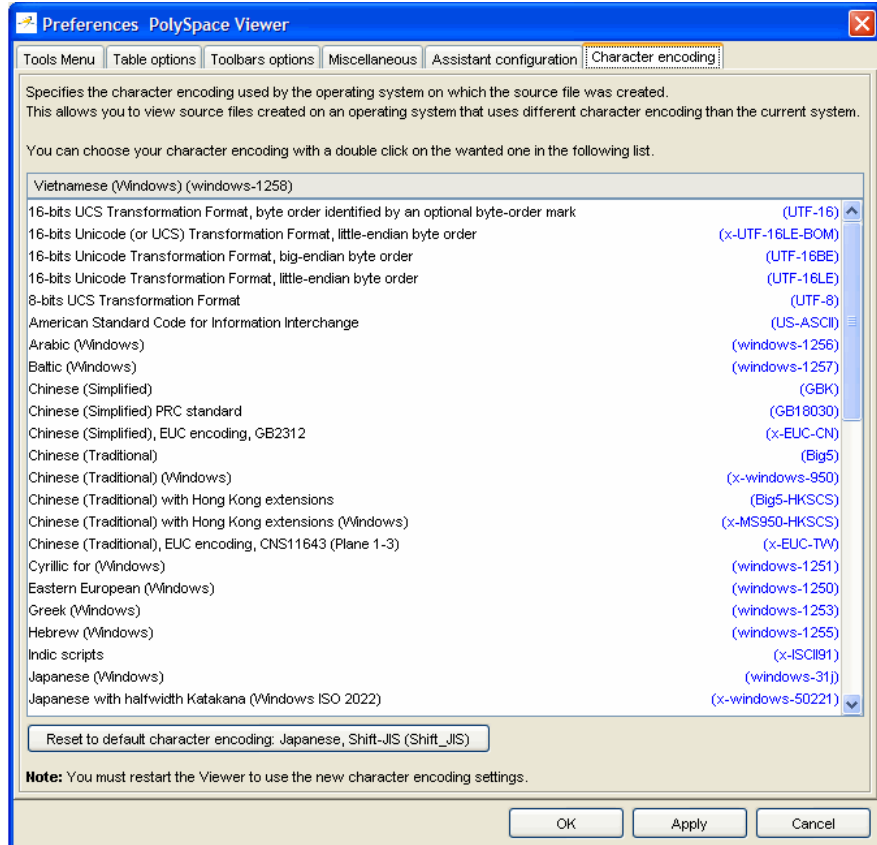
The **Character encoding** option allows you to view source files created on an operating system that uses different character encoding than your current system.

To set the character encoding for a source file:

- 1** In the Viewer, select **Edit > Preferences** .

The **Preferences PolySpace Viewer** dialog box opens.

- 2** Select the **Character encoding** tab.



- 3 Select the character encoding used by the operating system on which the source file was created.
- 4 Click **OK**.
- 5 Close and restart the Viewer to use the new character encoding settings.

Reviewing Results in Assistant Mode

In this section...

- “What Is Assistant Mode?” on page 8-19
- “Switching to Assistant Mode” on page 8-19
- “Selecting the Methodology and Criterion Level” on page 8-20
- “Exploring Methodology for C” on page 8-21
- “Defining a Custom Methodology” on page 8-23
- “Reviewing Checks” on page 8-24
- “Saving Review Comments” on page 8-26

What Is Assistant Mode?

In assistant mode, PolySpace software chooses the checks for you to review and the order in which you review them. PolySpace software presents checks in this order:

- 1 All red checks
- 2 All blocks of gray checks (the first check in each unreachable function)
- 3 Orange checks, according to the methodology and criterion level that you select

For more information about methodologies and criterion levels, see “Selecting the Methodology and Criterion Level” on page 8-20.

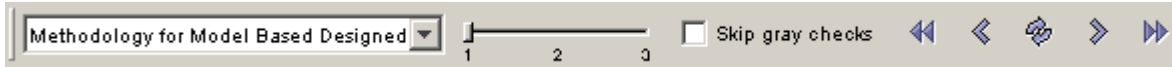
Switching to Assistant Mode

If the Viewer is in assistant mode, the mode toggle button is **Expert**. If the Viewer is in expert mode, the mode toggle button is **Assistant**. To switch from expert mode to assistant mode:

- Click the Viewer mode button



The Viewer window toolbar displays controls specific to assistant mode.



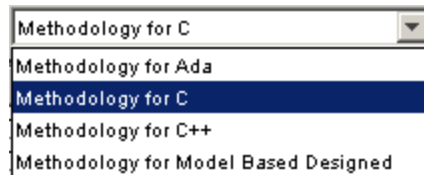
The controls for assistant mode include:

- A menu to select the review methodology for orange checks.
- A slider to select the criterion level within that methodology.
- A check box for omitting gray checks.
- Arrows for navigating through the reviews.

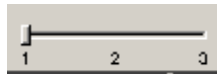
Selecting the Methodology and Criterion Level

A methodology is a named configuration set that defines the number of orange checks, by category, that you review in assistant mode. Each methodology has three criterion levels. Each level specifies the number of orange checks for a given category. The levels correspond to different development phases that have different review requirements. To select a methodology and level:

- 1 From the methodology menu, select **Methodology for C**.



- 2 Select the appropriate level on the level slider.



For the configuration Methodology for C, this table describes the three levels.

Level	Description
1	Fresh code

Level	Description
2	Unit tested code
3	Code Review

These three levels correspond to phases of the development process.

Exploring Methodology for C

A methodology defines the number of orange checks that you review in assistant mode. Each methodology has three criterion levels that specify increasing levels of review. These levels correspond to different development phases that have different review requirements.

Note You cannot change the parameters defined in the Methodology for C, but you can create your own custom methodologies.

To examine the configuration for **Methodology for C**:

- 1 Select **Edit > Preferences**.

The **Preferences PolySpace Viewer** dialog box opens.

- 2 Select the **Assistant configuration** tab.

You see the configuration for Methodology for C.

On the right side of the dialog box, a table shows the number of orange checks that you review for a given criterion and check category.

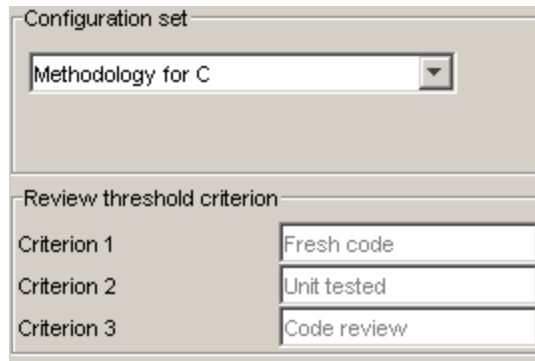
aneous Assistant configuration

Number of checks to review

	Criterion 1	Criterion 2	Criterion 3
Common			
ZDV	5	20	ALL
NIVL	10	50	ALL
S-OVFL	10	50	ALL
COR		10	10
POW	5	10	ALL
NIV		0	10
F-OVFL	5	10	20
ASRT		5	20
C & C++ only			
OBAI	10	20	ALL
SHF	5	10	ALL
IDP		10	20
NIP		10	20
C only			
IRV	5	20	ALL
C++ only			

For example, the table specifies that you review five orange ZDV checks when you select criterion 1. The number of checks increases as you move from criterion 1 to criterion 3, reflecting the changing review requirements as you move through the development process.

In the lower-left part of the dialog box, the section **Review threshold criterion** contains text that appears in the tooltip for the criterion slider on the Viewer toolbar (in assistant mode).



The table describes the criterion names for the configuration Methodology for C.

Criterion	Name in the Tooltip
1	Fresh code
2	Unit tested
3	Code Review

These names correspond to phases of the development process.

3 Click **OK** to close the dialog box.

Defining a Custom Methodology

A methodology defines the number of orange checks that you review in assistant mode. You cannot change the predefined methodologies, such as Methodology for C, but you can define your own methodology.

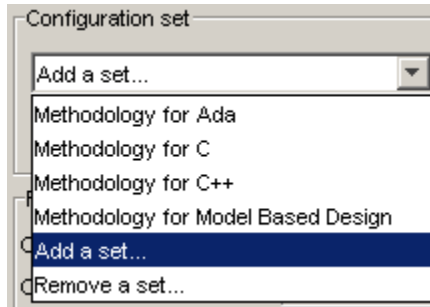
To define a custom methodology:

1 Select **Edit > Preferences**.

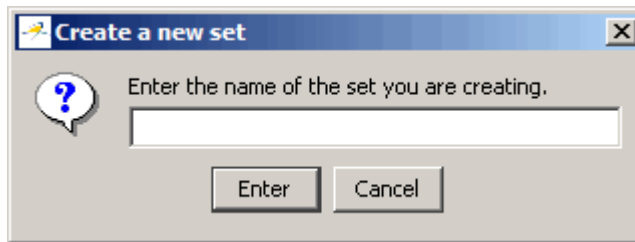
The **Preferences PolySpace Viewer** dialog box opens.

2 Select the **Assistant configuration** tab.

3 In the **Configuration set** drop-down menu, select **Add a set**.



The Create a new set dialog box opens.



- 4** Enter a name for the new configuration set, then click **Enter**.
- 5** Enter the number of checks to review for each type, and each criterion level.
- 6** Click **OK** to save the methodology and close the dialog box.

Reviewing Checks


In assistant mode, you review checks in the order in which PolySpace software presents them:

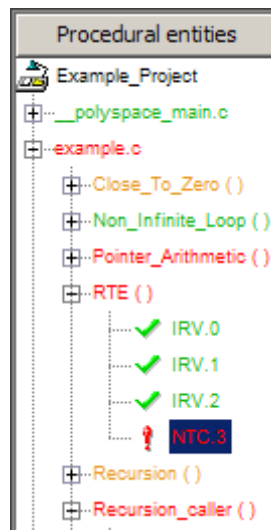
- 1** All reds.
- 2** All blocks of gray checks (the first check in each unreachable function).

Note You can omit gray checks. In the toolbar, select the **Skip gray checks** check box.

- 3** Orange checks, according to the methodology and criterion level that you select.

To navigate through these checks:

- 1** Click the forward arrow .
 - The procedural entities view (lower left), expands to show the current check.



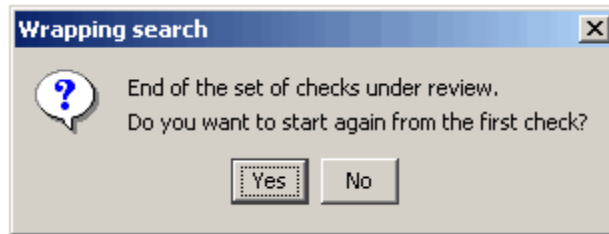
- The source code view (lower right) displays the source code for this check.
- The current check view (upper right) displays information about this check.

Note You can display the call sequence and track review progress. See “Reviewing Results in Expert Mode” on page 8-27.

- 2** Review the current check.

- 3 Continue to click the forward arrow until you have gone through all of the checks.

After the last check, a dialog box opens asking if you want to start again from the first check.



- 4 Click No.

Saving Review Comments

After you have reviewed your results, you can save your comments with the verification results. Saving your comments makes them available the next time you open the results file, allowing you to avoid reviewing the same check twice.

To save your review comments:

- 1 Select **File > Save Checks and Comments**.

Your comments are saved with the verification results.

Note Saving review comments also allows you to import those comments into subsequent verifications of the same module, allowing you to avoid reviewing the same check twice.

Reviewing Results in Expert Mode

In this section...

- “What Is Expert Mode?” on page 8-27
- “Switching to Expert Mode” on page 8-27
- “Selecting a Check to Review” on page 8-28
- “Displaying the Call Sequence for a Check” on page 8-31
- “Displaying the Access Sequence for Variables” on page 8-31
- “Tracking Review Progress” on page 8-32
- “Making the Reviewed Column Visible” on page 8-34
- “Filtering Checks” on page 8-37
- “Types of Filters” on page 8-37
- “Creating a Custom Filter” on page 8-39
- “Saving Review Comments” on page 8-40

What Is Expert Mode?

In expert mode, you can see all checks from the verification in the PolySpace Viewer. You decide which checks to review and in what order to review them.

Switching to Expert Mode

If the Viewer is in expert mode, the mode toggle button is **Assistant**. If the Viewer is in assistant mode, the mode toggle button is **Expert**. To switch from assistant to expert mode:

- Click the Viewer mode button:



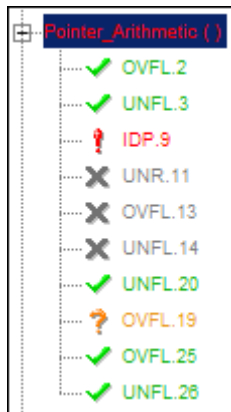
The Viewer window toolbar displays buttons and menus specific to expert mode.

Selecting a Check to Review

To review a check in expert mode:

- 1 In the procedural entities section of the window, expand any file containing checks.
- 2 Expand the procedure containing the check that you want to review.

You see a color-coded list of the checks:



Each item in the list of checks has an acronym that identifies the type of check and a number. For example, IDP.9, IDP stands for Illegal Dereferenced Pointer.

For more information about different types of checks, see “Check Descriptions” in the *PolySpace Products for C Reference*.

- 3 Click the check that you want to review.

The source code view displays the section of source code where this error occurs.

```
example.c
92     int i, *p = array;
93
94     for(i = 0; i < 100; i++)
95     {
96         *p = 0;
97         p++;
98     }
99
100    if(get_bus_status() > 0)
101    {
102        if(get_oil_pressure() > 0)
103        {
104            *p = 5; /* Out of bounds */
105        }
106        else
107        {
108            i++;
109        }
110    }
```

- 4 Place your cursor over any colored check in the code.

A tooltip provides ranges for variables, operands, function parameters, and return values.

```

92     int i, *p = array;
93
94     for(i = 0; i < 100; i++)
95     {
96         *p = 0;
97         p++;
98     }
99
100    if(get_bus_status() >= 0)
101        if(get_oil_pressure() >= 0)
102        {
103            {
104                *p = 5; /* Out of bounds */
105            }
106            else
107            {
108                i++;
109            }
110        }

```

returned value of get_bus_status (int 32): full-range [-2³¹ .. 2³¹-1]

5 In the code, click the red check.

You see a message box that describes the error.

in "example.c" line 104 column 10
Source code:

```


|         *p = 5; /* Out of bounds */
|         ^

```

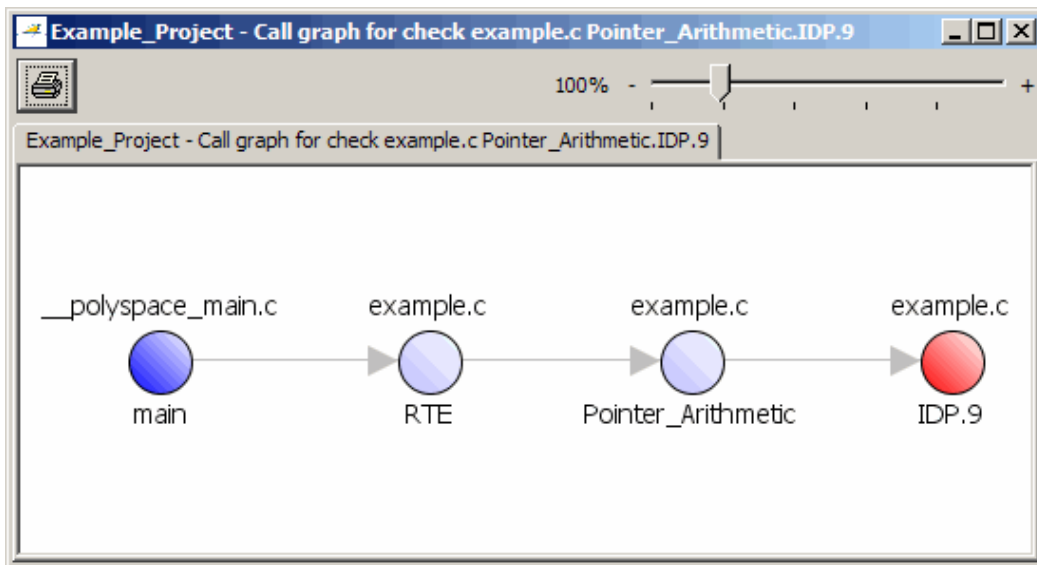
Error : pointer is outside its bounds

Displaying the Call Sequence for a Check

You can display the call sequence that leads to the code associated with a check. To see the call sequence for a check:

- 1 In the procedural entities window, expand the procedure containing the check that you want to review.
- 2 Select the check that you want to review.
- 3 In the toolbar, click the error call graph button. 

A window displays the call graph.



The call graph displays the code associated with the check.

Displaying the Access Sequence for Variables

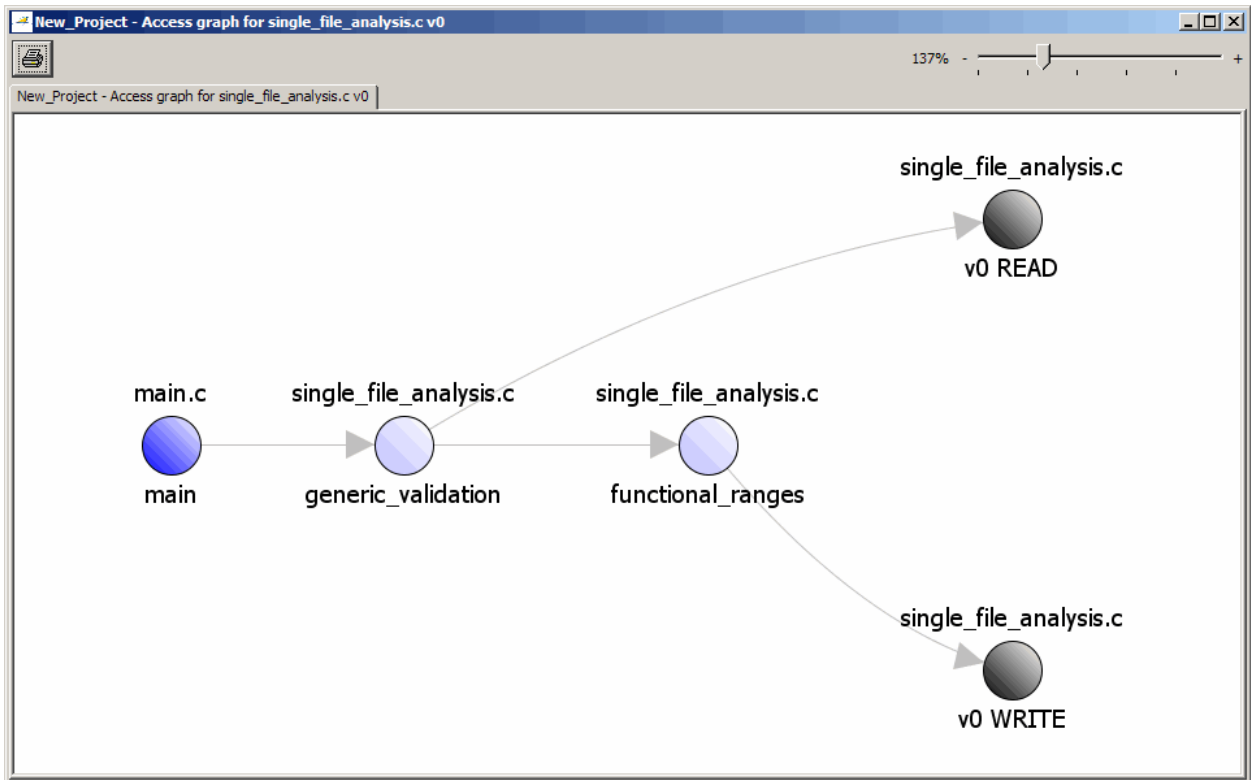
You can display the access sequence for any variable that is read or written in the code.

To see the access graph:

- 1 Select the Variables view.
- 2 Select the variable that you want to view.
- 3 In the toolbar, click the call graph button.



A window displays the access graph.



The access graph displays the read and write access for the variable.

Tracking Review Progress

You can keep track of the checks that you have reviewed by marking them. To mark that you have reviewed a check:

- 1 Expand the procedure containing the check that you want to review.
- 2 Click the check that you want to review.

In the upper-left part of the window, you see a table with statistics about the review progress for that category and severity of error.

Coding review progress	Count	Progress
num IDP reviewed / num IDP to review (Red)	0/1	0
num reviewed / num to review (Red)	0/5	0
Software reliability indicator	113/230	49

The **Count** column displays a ratio and the **Progress** column displays the equivalent percentage. The first row displays the ratio of reviewed checks to total checks that have the color and category of the current check. In this example, the first row displays the ratio of reviewed red IDP checks to total red IDP errors in the project.

The second row displays the ratio of reviewed checks to total checks that have the color of the current check. In this example, this is the ratio of red errors reviewed to total red errors in the project. The third row displays the ratio of the number of green checks to the total number of checks, providing an indicator of the reliability of the software.

In the upper-right part of the Viewer window, you see information about the current check.

```
example.c / Pointer_Arithmetic / line 104 / column 10
+      *p = 5; /* Out of bounds */
  FNO - Fix now
Error : pointer is outside its bounds
```

- 3 In the comment box, enter your comments.
- 4 Select the check box to indicate that you have reviewed this check.

The software updates the ratios of errors reviewed to total errors in the **Coding review progress** part of the window..

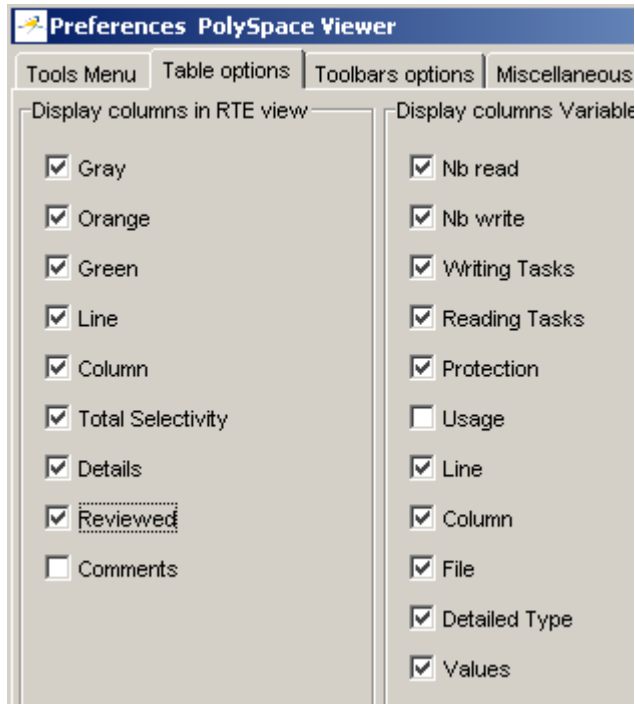
Coding review progress	Count	Progress
num IDP reviewed / num IDP to review (Red)	1/1	100
num reviewed / num to review (Red)	1/5	20
Software reliability indicator	113/230	49

Making the Reviewed Column Visible

You can change the PolySpace Viewer preferences so that the procedural entities part of the window displays a **Reviewed** column.

- 1 Select **Edit > Preferences**.
- 2 Select the **Table options** tab.
- 3 Under **Display columns in RTE view**, select the **Reviewed** check box.

Now the **Table options** tab looks like the following figure.



4 Click **OK** to apply the preference and close the dialog box.

In the **Procedural entities** view, you see a column of check boxes.

Procedural entities	!	X	?	✓	Line	...	#	Details	Reviewed
Example_Project	5	61	12	26			88		<input type="checkbox"/>
└─ __polyspace_main.c					1		0	__polyspace...	<input type="checkbox"/>
└─ example.c	4	8	10	26	1		79	example.c	<input type="checkbox"/>
└─ Close_To_Zero ()			6	3	37	12	33	example.c	<input type="checkbox"/>
└─ Non_Infinite_Loop ()				4	66	11	100	example.c	<input type="checkbox"/>
└─ Pointer_Arithmetic ()	1	3	1	5	89	12	90	example.c	<input type="checkbox"/>
└─ OVFL.2				✓	1	94	23	scalar variab...	<input type="checkbox"/>
└─ UNFL.3				✓	1	94	23	scalar variab...	<input type="checkbox"/>
└─ IDP.8	1			!			104	Error : pointe...	<input checked="" type="checkbox"/>
└─ UNR.11		1					107	unreachable ...	<input type="checkbox"/>
└─ OVFL.13		1					108	Unreachable...	<input type="checkbox"/>
└─ UNFL.14		1					108	Unreachable...	<input type="checkbox"/>
└─ UNFL.20				✓	1	114	19	scalar variab...	<input type="checkbox"/>
└─ OVFL.19			1				114	Warning : sc...	<input type="checkbox"/>
└─ OVFL.25				✓	1	118	12	scalar variab...	<input type="checkbox"/>
└─ UNFL.26				✓	1	118	12	scalar variab...	<input type="checkbox"/>

Tip If you do not see this column, resize **Procedural entities** so that you see the column. Resize the column to see the **Reviewed** label.

Note Selecting a check box in the **Reviewed** column automatically:

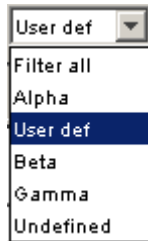
- Selects the check box for that check in the current check view (upper-right part of the window).
- Updates the counts in the coding review progress view (upper-left part of the window).

Filtering Checks

You can filter the checks that you see in the Viewer so that you can focus on certain types of checks. PolySpace software provides three predefined composite filters, a custom composite filter, and several individual filters.

The default filter is `User def`.

To filter checks, select a filter from the filter menu.



Types of Filters

There are three types of filters:

- “Individual Filters” on page 8-37
- “Composite Filters” on page 8-38
- “Custom Filters” on page 8-38

Individual Filters

You can use an individual filter to display or hide a given check category, such as IDP. When a filter is enabled, you do not see that check category. For example, when the IDP filter is enabled, you do not see IDP checks. When the filter is disabled, you see that check category. For example, when the IDP filter is disabled, you see IDP checks. You can also filter by check color. To enable or disable an individual filter, click the toggle button for that filter on the toolbar.

Tip The tooltip for a filter button indicates to you what filter the button is for and whether the filter is enabled or disabled.

Note When you filter a check category, you do see some red checks with that category.

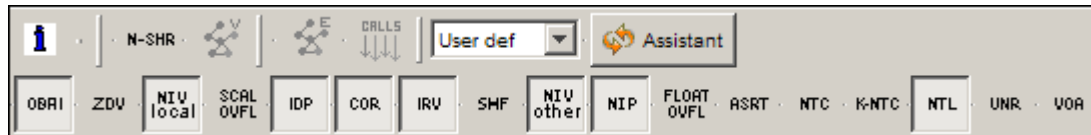
Composite Filters

Composite filters combine individual filters, allowing you to show or hide groups of checks.

Use This Filter...	To...
Alpha	Show all checks
Beta	Hide NIV, NIVL, NIP, Scalar OVFL, and Float OVFL checks
Gamma	Show red and gray checks
User def	Hide checks as defined in a custom filter that you can modify

Custom Filters

The custom filter is a composite filter that you define. It appears on the composite filter menu as `User def` and is the default composite filter. By default, the custom filter hides the `OBAI`, `NIV local`, `IDP`, `COR`, `IRV`, `NIV other`, `NIP`, and `NTL` checks, as shown in the following figure.



To modify the custom filter, see “Creating a Custom Filter” on page 8-39.

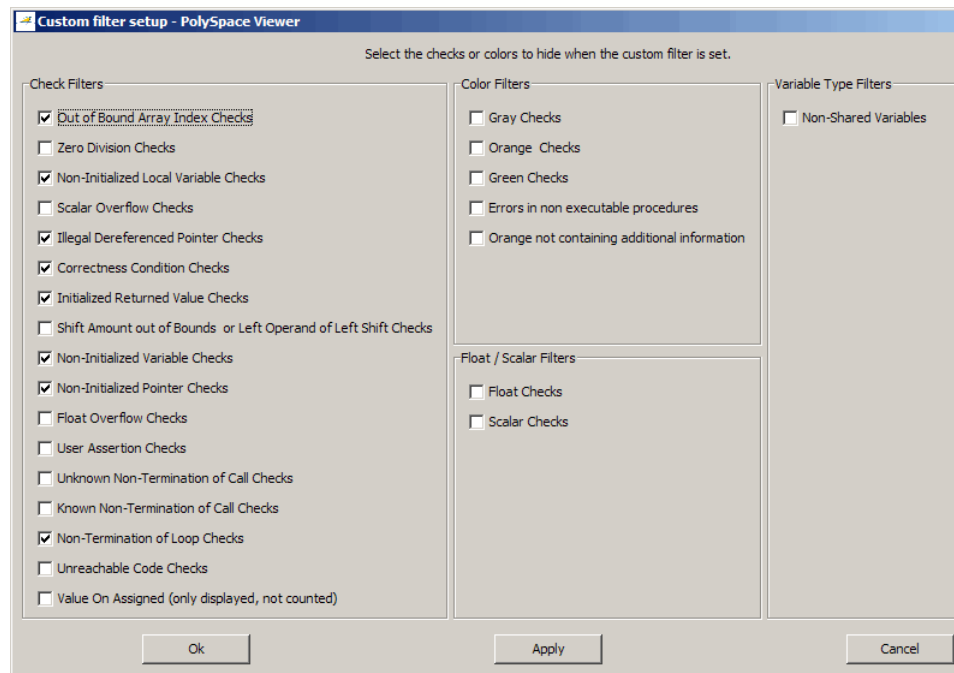
Creating a Custom Filter

The custom filter is a composite filter that you define. It appears on the composite filter menu as `User def`.

To modify the custom filter:

- 1 From the composite filters menu, select `User def`.
- 2 Select **Edit > Custom filters**.

The **Custom filter setup** dialog box opens.



- 3 Clear the filters for the checks that you want to display. For example, if you clear the **Out of Bound Array Index Checks** box, you see the OBAI checks.

Note You do not have to change any of the selections for this tutorial.

4 Select the filters for the checks that you do not want to display.

5 Click **OK** to apply the changes and close the dialog box.

PolySpace software saves the custom filter definition in the Viewer preferences.

Saving Review Comments

After you have reviewed your results, you can save your comments with the verification results. Saving your comments makes them available the next time you open the results file, allowing you to avoid reviewing the same check twice.

To save your review comments:

1 Select **File > Save Checks and Comments**.

Your comments are saved with the verification results.

Note Saving review comments also allows you to import those comments into subsequent verifications of the same module, allowing you to avoid reviewing the same check twice.

Importing and Exporting Review Comments

In this section...

“Reusing Review Comments” on page 8-41

“Exporting Review Comments to Other Verification Results” on page 8-41

“Importing Review Comments from Previous Verifications” on page 8-42

Reusing Review Comments

After you have reviewed verification results on a module, you can reuse your review comments with subsequent verifications of the same module. This allows you to avoid reviewing the same check twice, or to compare results over time.

The PolySpace Viewer allows you to either:

- Export review comments from the current results to another set of results.
- Import review comments from another set of results into the current results.

Note If the code has changed since the previous verification, the imported comments may not be applicable to your current results. For example, the justification for an orange check may no longer be relevant to the current code.

Exporting Review Comments to Other Verification Results

After you have reviewed verification results, you can export your review comments for use with other verifications of the same module, allowing you to avoid reviewing the same check twice.

Caution The comments you export replace any existing comments in the selected results.

To export review comments to other verification results:

- 1 Select **File > Export checks and comments**.
- 2 Navigate to the folder containing the other results file.
- 3 Select the results (.RTE) file, then click **Open**.

The review comments from the current results are exported into the selected results.

Note If the code has changed between the two verifications, the exported comments may not be applicable to the other results. For example, the justification for an orange check may no longer be relevant to the current code.

Importing Review Comments from Previous Verifications



If you have previously reviewed verification results for a module and saved your comments, you can import those comments into the current verification, allowing you to avoid reviewing the same check twice.

Caution The comments you import replace any existing comments in the current results.

To import review comments from a previous verification:

- 1 Open your most recent verification results in the Viewer.
- 2 Select **File > Import checks and comments**.
- 3 Navigate to the folder containing your previous results.
- 4 Select the results (.RTE) file, then click **Open**.

The review comments from the previous results are imported into the current results.

Once you import checks and comments, the **go to next check**  icon in assistant mode will skip any reviewed checks, allowing you to review only checks that you have not reviewed previously. If you want to view reviewed checks, click the **go to next reviewed check**  icon.

Note If the code has changed since the previous verification, the imported comments may not be applicable to your current results. For example, the justification for an orange check may no longer be relevant to the current code.

Generating Reports of Verification Results

In this section...
“PolySpace Report Generator Overview” on page 8-44
“Generating Verification Reports” on page 8-45
“Automatically Generating Verification Reports” on page 8-46
“Generating Excel Reports” on page 8-47

PolySpace Report Generator Overview

The PolySpace Report Generator allows you to generate reports about your verification results, using predefined report templates.

The PolySpace Report Generator provides the following report templates:

- **Coding Rules Report** – Provides information about compliance with MISRA-C Coding Rules, as well as PolySpace configuration settings for the verification.
- **Developer Report** – Provides information useful to developers, including summary results, detailed lists of red, orange, and gray checks, and PolySpace configuration settings for the verification.
- **Developer with Green Checks Report** – Provides the same content as the Developer Report, but also includes a detailed list of green checks.
- **Quality Report** – Provides information useful to quality engineers, including summary results, statistics about the code, graphs showing distributions of checks per file, and PolySpace configuration settings for the verification.

The PolySpace Report Generator allows you to generate verification reports in the following formats:

- HTML
- PDF
- RTF

- Microsoft® Word
- XML

Note Microsoft Word format is not available on UNIX platforms. RTF format is used instead.

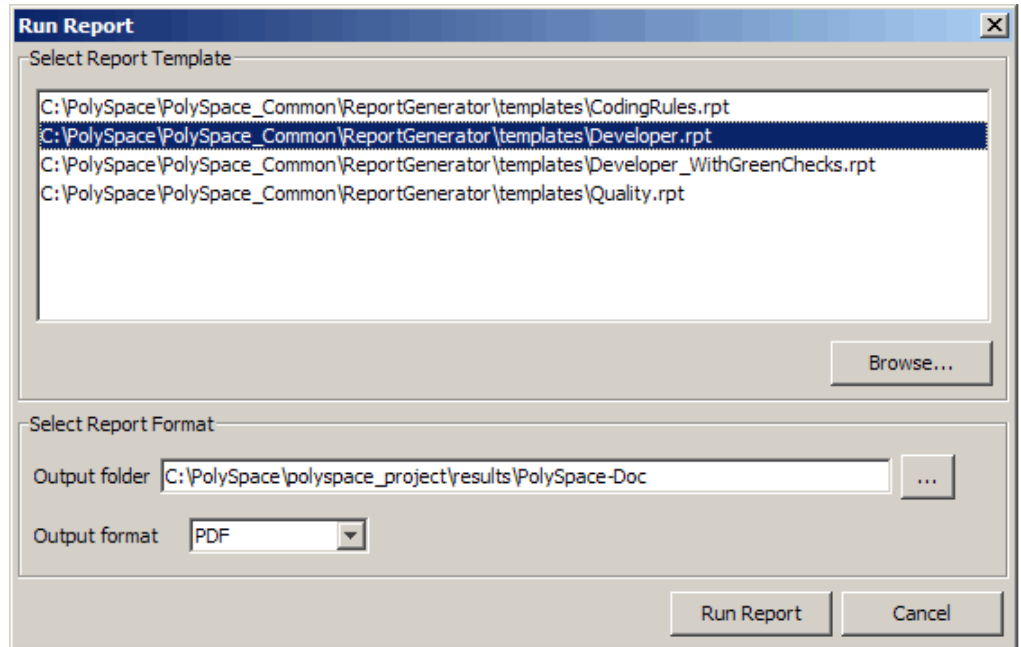
Generating Verification Reports

You can generate reports for any verification results using the PolySpace Report Generator.

To generate a verification report:

- 1** In the Viewer, open your verification results.
- 2** Select **Reports > Run Report**.

The Run Report dialog box opens.



- 3** In the Select Report Template section, select the type of report that you want to run.
- 4** Select the Output folder in which to save the report.
- 5** Select the Output format for the report.
- 6** Click **Run Report**.

The software creates the specified report.

Automatically Generating Verification Reports

You can specify that PolySpace software automatically generate reports for each verification using an option in the Launcher .

To automatically generate reports for each verification:

- 1** In the Launcher, open your project.

2 In the Analysis options section of the Launcher window, expand **General**.

You see the General options.

3 Select **Report Generation**.

4 Select the **Report template name**.

5 Select the **Output format** for the report.

6 Save your project.

Generating Excel Reports

You can also generate Microsoft Excel® reports of verification results.

Note Excel reports do not use the PolySpace Report Generator.

To generate an Excel report of your verification results:

1 In your results directory, navigate to the PolySpace-Doc folder. For example: `polyspace_project\results\PolySpace-Doc`.

The directory should have the following files:

```
Example_Project_Call_Tree.txt
Example_Project_RTE_View.txt
Example_Project_Variable_View.txt
Example_Project-NON-SCALAR-TABLE-APPENDIX.ps
PolySpace_Macros.xls
```

The first three files correspond to the call tree, RTE, and variable views in the PolySpace Viewer window.

2 Open the macros file `PolySpace_Macros.xls`.

You see a security warning dialog box.

3 Click **Enable Macros**.

A spreadsheet opens. The top part of the spreadsheet looks like the following figure.

The screenshot shows a spreadsheet interface with the following elements:

- Apply filters?**
 - No filters
 - Beta filters
- Generate checks by file?**
 - yes
 - no
- Two **Help** buttons flanking the central text.
- Central text: "Use this button to create the complete synthesis in one file. Select the RTE export view and a file in which to save results. If the other views are in the same directory as the RTE view then they will automatically be incorporated into the same file."
- A large red button labeled **Generate PolySpace Results Synthesis**.

- Specify the report options that you want, then click **Generate PolySpace Results Synthesis**.

The synthesis report combines the RTE, call tree, and variables views into one report.

The **Where is the PolySpace RTE View text file** dialog box opens.

- In **Look in**, navigate to the PolySpace-Doc folder in your results directory. For example: `polyspace_project\results\PolySpace-Doc`.
- Select `Project_RTE_View.txt`.
- Click **Open** to close the dialog box.

The **Where should I save the analysis file?** dialog box opens.

- Keep the default file name and file type.
- Click **Save** to close the dialog box and start the report generation.

Microsoft Excel opens with the spreadsheet that you generated. This spreadsheet has several worksheets.

Example_Project-Synthesis.xls	
A	
1	Call Graph of ll tree
2	
3	all tree
4	__polyspace_main.main
5	- > example.RTE
6	- > example.Close_To_Zero
7	> pst_stubs_0.random_float
8	> pst_stubs_0.random_float
9	> pst_stubs_0.random_int
10	> example.Non_Infinite_Loop
11	- > example.Pointer_Arithmetic
12	> pst_stubs_0.get_bus_status
13	> example.get_oil_pressure
14	> pst_stubs_0.get_bus_status
15	- > example.Recursion_caller
16	> pst_stubs_0.random_int
17	- > example.Recursion
18	** RecursiveCall to example.Recursion:
19	> pst_stubs_0.random_int
20	- > example.Recursion
21	Already displayed above
22	> pst_stubs_0.random_int
23	- > example.Square_Root
24	> pst_stubs_0.random_float
25	- > example.Square_Root_conv
26	> ?extern.cos
27	> ?extern.sqrt
28	- > example.Unreachable_Code
29	> pst_stubs_0.random_int
30	> pst_stubs_0.random_int

Application Call Tree / Shared Globals / Global Data Dictionary / Checks by file

- 10** Select the **Check Synthesis** tab to view the worksheet showing statistics by check category.

Example_Project-Synthesis.xls						
	A	B	C	D	E	F
1	RTE Statistics					
2	Check category	Check detail	R	O	Gy	Gr
3	OBAI	Out of Bounds Array Index	0	0	0	0
4	NIVL	Uninitialized Local Variable	0	1	2	32
5	IDP	Illegal Dereference of Pointer	1	1	0	7
6	NIP	Uninitialized Pointer	0	0	0	12
7	NIV	Uninitialized Variable	0	0	0	6
8	IRV	Initialized Value Returned	0	0	0	13
9	COR	Other Correctness Conditions	0	0	0	2
10	ASRT	User Assertion Failure	0	1	0	0
11	POW	Power Must Be Positive	0	0	0	0
12	ZDV	Division by Zero	0	1	0	4
13	SHF	Shift Amount Within Bounds	0	0	0	0
14	OVFL	Overflow	0	2	3	5
15	UNFL	Underflow	0	0	3	7
16	UOVFL	Underflow or Overflow	0	3	0	5
17	EXCP	Arithmetic Exceptions	0	0	0	0
18	NTC	Non Termination of Call	3	0	0	0
19	k-NTC	Known Non Termination of Call	0	0	0	0
20	NTL	Non Termination of Loop	0	0	0	0
21	UNR	Unreachable Code	0	0	1	0
22	UNP	Uncalled Procedure	0	0	0	0
23	IPT	Inspection Point	0	0	0	0
24	OTH	other checks	0	0	0	0
25	EXC	Exception handling	0	0	0	0
26	CCP	Control Flow	0	0	0	0

Using PolySpace Results

In this section...

“Review Runtime Errors: Fix Red Errors” on page 8-51

“Red Checks Where Gray Checks were Expected” on page 8-52

“Using Range Information in the Viewer” on page 8-54

“Why Review Dead Code Checks” on page 8-60

“Reviewing Orange Checks” on page 8-61

“Integration Bug Tracking” on page 8-62

“How to Find Bugs in Unprotected Shared Data” on page 8-63

“Dataflow Verification” on page 8-63

“Data and Coding Rules” on page 8-64

“Potential Side Effect of a Red Error” on page 8-64

“Relationships Between Variables” on page 8-65

“Two Distinct Colors in a while/for Statement” on page 8-67

Review Runtime Errors: Fix Red Errors

All Runtime Errors highlighted by PolySpace verification are determined by reference to the language standard, and are sometimes implementation dependant — that is, they may be acceptable for a particular compiler but unacceptable according to the language standard.

Consider an overflow on a type restricted from -128 to 127. The computation of $127+1$ cannot be 128, but depending on the environment a “wrap around” might be performed to give a result of -128.

This result is mathematically incorrect, and could have serious consequences if, for example, the computation represents the altitude of a plane.

By default, PolySpace verification does not make assumptions about the way you use a variable. Any deviation from the recommendations of the language standard is treated as a red error, and must therefore be corrected.

PolySpace verification identifies two kinds of red checks:

- Red errors which are compiler-dependant in a specific way. A PolySpace option may be used to allow particular compiler specific behavior . An example of a PolySpace option to permit compiler specific behavior is the option to force “IN/OUT” ADA function parameters to be initialized. Examples in C include options to deal with constant overflows, shift operation on negative values, and so on.
- You must fix all other red errors. They are bugs.

Most of the bugs you find are easy to correct once the software identifies them. PolySpace verification identifies bugs regardless of their consequence, or how difficult they may be to correct.

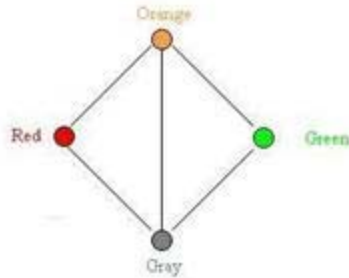
Red Checks Where Gray Checks were Expected

By default, PolySpace continues verification when it finds a red error. This is used to deal with two primary circumstances:

- A red error appears in code which was expected to be dead code.
- A red error appears which was expected, but the verification is required to continue.

PolySpace performs an upper approximation of variables. Consequently, it may be true that PolySpace verifies a particular branch of code as though it was accessible, despite the fact that it could never be reached during “real life” execution. In the example below, there is an attempt to compare elements in an array, and PolySpace is not able to conclude that the branch was unreachable. PolySpace may conclude that an error is present in a line of code, even when that code cannot be reached.

Consider the figure below.



As a result of imprecision, each color shown can be approximated by a color immediately above it in the grid. It is clear that green or red checks can be approximated by orange ones, but the approximation of gray checks is less obvious.

During PolySpace verification, data values possible at execution time are represented by supersets including those values - and possibly more besides.

Gray code represents a situation where no valid data values exist. Imprecision means that such situation can be approximated

- by an empty superset;
- by a nonempty super set, members of which may generate checks of any color.

And hence PolySpace cannot be guaranteed to find all dead code in a verification.

However, there is no problem in having gray checks approximated by red ones. Where a red error is encountered, all instructions which follow it in the relevant branch of execution are aborted as usual. At execution time, it is also true that those instructions would not be executed.

Consider the following example:

```
if (condition) then action_producing_a_red;
```

After the "if" statement, the only way execution can continue is if the condition is false; otherwise a **red check** would be produced. Therefore, after this branch the condition is always false. For that reason, the code verification continues, even with a specific error. Remember that this propagates values throughout your application. None of the execution paths leading to a run-time error will continue after the error and if the **red check** is a real problem rather than an approximation of a gray check, then the verification will not be representative of how the code will behave when the red error has been addressed.

It is applicable on the current example:

```
1 int a[] = { 1,2,3,4,5,7,8,9,10 };
2 void main(void)
3 {
4   int x=0;
5   int tmp;
6   if (a[5] > a[6])
7     tmp = 1 /x; // RED ERROR [scalar division by zero] in gray code
8 }
```

Using Range Information in the Viewer

- “Viewing Range Information” on page 8-54
- “Interpreting Range Information” on page 8-55
- “Diagnosing Errors with Range Information” on page 8-57

Viewing Range Information

You can see range information associated with variables and operators within the source code view. Place your cursor over an operator or variable. A tooltip message displays the range information, if it is available.

Note The displayed range information represents a superset of dynamic values, which the software computes using static methods.

If a line of code is entirely the same color, selecting (clicking) the line opens the Expanded Source Code window. Place your cursor over the required operator or variable in this window to view range information. In addition, you can select the line in the Expanded Source Code window to display error or warning messages (along with range information) in the selected check view.

In the source code view, if a line of code contains different colored checks, then selecting a check displays the error or warning message along with range information in the selected check view.

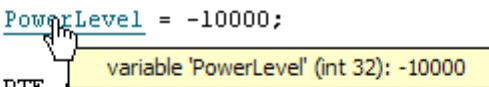
Interpreting Range Information

The software uses the following syntax to display range information of variables:

```
name (data_type) : [min1 .. max1] or [min2 .. max2] or [min3 .. max3] or exact value
```

In the following example,

```
30  {
31  int temp;
32  PowerLevel = -10000;
33
34  RTE
35
```

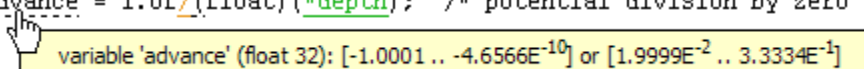


A screenshot of a code editor showing a tooltip for the variable 'PowerLevel'. The tooltip is a yellow box with a black border, containing the text 'variable 'PowerLevel' (int 32): -10000'. A mouse cursor is pointing at the variable name in the code.

the tooltip message indicates the variable `PowerLevel` is a 32-bit integer with the value `-10000`.

In the next example,

```
140
141  *depth = *depth + 1;
142  advance = 1.0f/(float)(*depth); /* potential division by zero */
143
144
```



A screenshot of a code editor showing a tooltip for the variable 'advance'. The tooltip is a yellow box with a black border, containing the text 'variable 'advance' (float 32): [-1.0001 .. -4.6566E-10] or [1.9999E-2 .. 3.3334E-1]'. A mouse cursor is pointing at the variable name in the code.

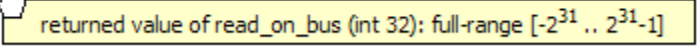
the tooltip message indicates that the variable `advance` is a 32-bit float that lies between either `-1.0001` and `-4.6566E-10` or `1.9999E-2` and `3.3334E-1`

The tooltip message also indicates whether the variable occupies the full range:

```

37
38     temp = read_on_bus();
39     switch(temp)
40         {

```



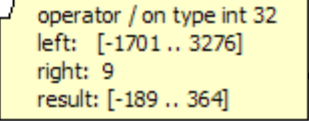
The tooltip message indicates that the returned value of the function `read_on_bus` is a 32-bit integer that occupies the full range of the data type, -2147483648 to 2147483647.

With operators, the software displays associated information. Consider the following example:

```

50
51     static s32 new_speed(s32 in, s8 ex_speed, u8 c_speed)
52     {
53         return (in * 9 + ((s32)ex_speed + (s32)c_speed) / 2 );
54     }
55
56     static char re
57     {

```



The tooltip message for the division operator `/` indicates that the:

- Operation is performed on 32-bit integers
- Dividend (left) is a value between -1701 and 3276
- Divisor (right) is an exact value, 9
- Quotient (result) lies between -189 and 364

Note You can run a `pass0` (Software Safety Analysis level 0) verification to produce results quickly. See “-from verification-phase” and “-to verification-phase” in the *PolySpace Products for C Reference Guide*. However, with a `pass0` verification, the software generates range information that is either a constant or full-range for the data type of the expression.

Diagnosing Errors with Range Information

You can use range information to diagnose errors. Consider the function `reset_temperature()` in the following example:

8 Reviewing Verification Results

The screenshot displays the PolySpace Viewer interface for a project named "Demo_C". The window title is "PolySpace Viewer - C:\CC-R2009b-v1\Examples\Demo_C\RTe_px_02_Demo_C_LAST_RESULTS.rte".

Coding review progress table:

Coding review progress	Count	Pr...
No check selected	n/a	n/a
num reviewed / num to review (n/a)	n/a	n/a
Software reliability indicator	n/a	n/a

Procedural entities view:

Entity	Line
Demo_C	9	111	327
example.c	4	11	12
initialisations.c	3	1	54
main.c	2	6	3
single_file_analysis.c	2	4	8
-init_globals ()			
-all_values_s16 ()	2	5	25
-all_values_s32 ()	2	5	24
-all_values_u16 ()	2	5	26
-functional_ranges ()	6	37	12
-IRV.0	1	40	7
-IRV.1	1	43	7
-IRV.2	1	44	7
-IRV.3	1	45	11
-IRV.4	1	46	7
-IRV.5	1	48	7
-generic_validation ()	1	4	2
-new_speed ()	11	51	11
-reset_temperature ()	1	5	58
-OBAI.0	1	60	12
-NIVL.1	1	60	13
-OVFL.2	1	60	13
-UNFL.3	1	60	13
-OVFL.4	1	60	18
-UNFL.5	1	60	18
-unused_fonction ()	137	11	0
tasks1.c	4	37	1
tasks2.c	2	20	1
_polyspace_stdsubs.c	1	87	2

Variables View:

Variables	Nb read	Nb write
initialisations.arr	3	2
initialisations.current_data	2	2
initialisations.first_paiload	0	3
initialisations.second_paiload	0	1
initialisations.tab	2	3
single_file_analysis.output_v1	0	2
single_file_analysis.output_v6	1	3
single_file_analysis.output_v7	3	2
single_file_analysis.saved_values	0	2
single_file_analysis.v0	1	2
single_file_analysis.v1	3	2

Source code view (single_file_analysis.c):

```
53     return (in / 9 + ((s32)ex_speed + (s32)c_speed) / 2 );
54 }
55 Error : arr;
56 static char reset_temperature(u8 in v3)
57 {
58     int array[255-(54 * BIN v3)];
59
60     return array[in v3-255] = 0;
61 }
62
63
64 s8 generic_validation(s8 extrapolated_speed, u8 computed_speed)
65 {
66     /*****
```

Clicking the red check, OBAI.0 in the **Procedural entities** view or [on line 60 in the source code view, displays an error message and range information in the selected check view:


```

single_file_analysis.c / reset_temperature / line 60 / column 12
+      return array[in_v3-255] = 0;
Error : array index is outside its bounds : [0..38]
array size: [0..38]
array index: [-255 .. -39]

```

The error message shows that the array size lies between 0 and 38 elements, but the array index is negative, lying between -255 and -39 .

Placing the cursor over `in_v3` in the source code view shows the following:

```

57  {
58  int array[255-(54 * BIN_v3)];
59
60  return array[in_v3-255] = 0;
61  }
62
63
64  s8 generic_val:          ted_speed)
65  {
66  /*****
67  *

```

variable 'in_v3' (unsigned int 8): [0 .. 216]
conversion from unsigned int 8 to unsigned int 32
right: [0 .. 216]
result: [0 .. 216]
conversion from unsigned int 32 to int 32
right: [0 .. 216]
result: [0 .. 216]

Although `in_v3` is green (as a local variable), it is in the range 0 - 216. This results in a negative index range. Moving the cursor to the beginning of the function reveals the cause of the red check: the input argument is between 0 and 216:

```

55
56  static char reset_temperature(u8 in_v3)
57  {
58  int array[255-(54 * BIN_v3)];
59
60  return array[in_v3-255] = 0;
61  }
62

```

parameter in_v3 (unsigned int 8): [0 .. 216]

Why Review Dead Code Checks

- “Functional Bugs in Gray Code” on page 8-60
- “Structural Coverage” on page 8-61

Functional Bugs in Gray Code

PolySpace verification finds different types of dead code. Common examples include:

- Defensive code which is never reached.
- Dead code due to a particular configuration.
- Libraries which are not used to their full extent in a particular context.
- Dead code resulting from bugs in the source code.

The causes of dead code listed in the following examples are taken from critical applications of embedded software by PolySpace verification.

- A lack of parenthesis and operand priorities in the testing clause can change the meaning significantly.
- Consider a line of code such as:

```
IF NOT a AND b OR c AND d
```

Now consider how misplaced parentheses might influence how that line behaves:

```
IF NOT (a AND b OR c AND d)
```

```
IF (NOT (a) AND b) OR (c AND d))
```

```
IF NOT (a AND (b OR c) AND d)
```

- The test of variable inside a branch where the conditions are never met
- An unreachable “else” clause where the wrong variable is tested in the “if” statement
- A variable that should be local to the file but instead is local to the function
- Wrong variable prototyping leading to a comparison which is always false (say)

As is the case for red errors, the consequences of dead code and how much time you must spend on it is unpredictable. For example, it can be:

- A one-week effort of functional testing on target, trying to build a scenario going into that branch.
- A three-minute code review discovering the bug.

Again, as for red errors, PolySpace does not measure the impact of dead code.

The tool provides a list of dead code. A short code review enables you to place each entry from that list into one of the five categories from the beginning of this chapter. Doing so identifies known dead code and uncovers real bugs.

Using PolySpace shows that at least 30% of gray code reveals real bugs.

Structural Coverage

PolySpace software always performs upper approximations of all possible executions. Therefore, if a line of code is shown in green, there is a possibility that it is a dead portion of code. Because PolySpace verification makes an upper approximation, it does not conclude that the code is dead, but it could conclude that no run-time error is found.

PolySpace verification finds around 80% of dead code that the developer finds by doing structural coverage.

Use PolySpace verification as a productivity aid in dead code detection. It detects dead code which might take days of effort to find by any other means.

Reviewing Orange Checks

Orange checks indicate *unproven code*. This means that the code can neither be proven safe, nor can it be proven to contain a runtime error.

The number of orange checks you review is determined by several factors, including:

- The stage of the development process
- Your quality objectives

There are also actions you can take to reduce the number of orange checks in your results.

For information on managing orange checks in your results, see Chapter 9, “Managing Orange Checks”.

Integration Bug Tracking

By default, you can achieve integration bug tracking by applying the selective orange methodology to integrated code. Each error category reveals integration bugs, depending on the coding rules that you choose for the project.

For instance, consider a function that receives two unbounded integers. The presence of an overflow can be checked only at integration phase because at unit phase the first mathematical operation reveals an orange check.

Consider these two circumstances:

- When you carry out integration bug tracking in isolation, a selective orange review highlights most integration bugs. A PolySpace verification is performed integrating tasks.
- When you carry out integration bug tracking together with an exhaustive orange review at unit phase, a PolySpace verification is performed on one or more files.

In this second case, an exhaustive orange review already has been performed, file by file. Therefore, at integration phase, assess **only checks that have turned from green to another color** .

For instance, if a function takes a structure as an input parameter, the standard hypothesis made at unit level is that the structure is well initialized. This consequentially displays a green NIV check at the first read access to a field. But this might not be true at integration time, where this check can turn orange if any context does not initialize these fields.

These orange checks reveal integration bugs.

How to Find Bugs in Unprotected Shared Data

Based on the list of entry points in a multi-task application, PolySpace verification identifies a list of shared data and provides some information about each entry:

- The data type.
- A list of read and write access to the data through functions and entry points.
- The type of any implemented protection against concurrent access.

A shared data item is a global data item that is read from or written to by two or more tasks. It is unprotected from concurrent access when one task can access it while another task is in the process of doing so. Consider all the possible situations:

- A scenario which would lead to such a conflict for a particular variable; then a bug exists and you must provide protection.
- No such scenarios; then one of the following explanations may apply:
 - The compilation environment guarantees an atomic read/write access on variables of type less than 1 or, 2 bytes. Therefore, all conflicts concerning a particular variable type still guarantee the integrity of the variables content. Be careful when you port the code.
 - The variable is protected by a critical section or a mutual temporal exclusion. You may want to include this information in the PolySpace launching parameters and reverify.

Consider checking whether variables are modified when they are supposed to be constant. Use the variables dictionary.

Dataflow Verification

Data flow verification is often performed within certification processes — typically in the avionic, aerospace, or transport markets.

This activity makes use of two features of PolySpace results, which are available any time after the Control and Data Flow verification phase:

- Call tree computation
- Dictionary containing read/write access to global variables. (You can also use this to build a database listing for each procedure, for its parameters, and for its variables.)

PolySpace software can help you to build these results by extracting information from both the call tree and the dictionary.

Data and Coding Rules

Data rules are design rules which dictate how modules and files interact with each other.

Consider global variables. It is not always apparent which global variables are produced by a given file, or which global variables are used by that file. The excessive use of global variables can lead to design problems, such as:

- File APIs (or functions accessible from outside the file) with no procedure parameters.
- The requirement for a formal list of variables which are produced and used, as well as the theoretical ranges they can take as input and output values.

Potential Side Effect of a Red Error

When the software finds a red error, you can continue the verification but proceed with caution. Consider this piece of code:

```
int *global_ptr;
int variable_it_points_to;

void big_red(void)
{
  int r;
  int my_zero = 0;
  if (condition==1)
    r = 1 / my_zero; // red ZDV
  ...
}

void other_function(void)
{
  if (condition==1)
    *global_ptr = 12;
}
```

```
... // hundreds of lines  
global_ptr = &variable_it_points_to;  
other_function();  
}
```

PolySpace works by propagating data sets representing ranges of possible values throughout the call tree, and throughout the functions in that call tree. Sometimes, PolySpace internally subdivides the functions for verification, and the propagation of the data ranges need several iterations (or integration levels) to be complete. You can observe that effect by examining the color of the checks upon completion of each of those levels.

- PolySpace detects gray code which exists due to a terminal RTE which is not be flagged in red until a subsequent integration level.
- PolySpace flags an **NTC** in red with the content in gray. This red NTC is the result of an imprecision; it should be gray.

Suppose that an NTC is hard to understand at a given integration level (level 4):

- If other **red checks** exist at level 4, fix them and restart the verification
- Otherwise, look through the results from each previous level to see whether you can locate other red errors. If so, fix them and restart the verification

Relationships Between Variables

Abstract

A red error can hide a bug which occurred on previous lines.

```

%% file1.c %%
1 void f(int);
2 int read_an_input(void);
3
4 int main(void)
5 {
6   int x,old_x;
7
8   x = read_an_input();
9   old_x = x;
10
11  if (x<0 || x>10)
12    return 0;
13
14  f(x);

```

```

%% file2.c %%
1 #include <math.h>
2
3 void f(int a)
4 {
5   int tmp;
6   tmp = sqrt(0-a);
7 }

```

Explanation 1

- ```

15
16 x = 1 / old_x; // division is red
17
18

```
- When `old_x` is assigned to `x` (file 1, line 9), PolySpace retains the following information:
    - `x` and `old_x` are equivalent to the full range of an integer:  $[-2^{31}; 2^{31}-1]$ .
    - `x` and `old_x` are equal.
  - After the `if` clause (file 1, line 11), `X` is equivalent to  $[0; 10]$ . Because `x` and `old_x` are equal, **`old_x` is equivalent to  $[0;10]$  as well**. Otherwise the return statement is executed.
  - When `X` is passed to "f" (file 1, line 14), the only possible conclusion for `sqrt` is that `x=0`. All other values lead to a run-time exception (file 2, line 6) `tmp = sqrt(0 a);`.
  - A red error occurs (file 1, line 16) because `x` and `old_x` are equal, therefore `old_x = 0`.



## Explanation 2

- Suppose that PolySpace **exits** immediately when encountering a run-time error. Introduce a print statement that writes to the standard output after the "f" procedure is called (file 1, line 14), to show the current value of `x` and `old_x`.
- The only way the program can reach the print statement is when `X = 0`. So, if `X=0`, `old_x` must also have been assigned to 0, which makes the division **red**.

## Summary

PolySpace builds relationships between variables and propagates the consequence of these relationships backwards and forwards.

## Two Distinct Colors in a while/for Statement

Inside the condition of a loop, a check might be **green** then **red**.

Consider the following example.

```

1 void main(void)
2 {
3 int tab[2] = { 1, 2 };
4 int index = 0;
5 while (tab[index]) { index--; }
 // the colour of "array index within bounds" is
 // first green
 // then red
6 }
```

In the Viewer, if you click the `tab` variable (line 5), you see:

```

Error : array index is outside its bounds : [0..1]
array index is within bounds : [0..1]
local variable is initialized (type: int 32)
Unreachable check : not initialized local variable error (type: int 32)
```

Now, visualize the C loop transformed into a label and a goto

```
if (not(tab[index]) goto end;
// first location of the check is green
loop_begin:
 index = index-1;
if (tab[index]) goto loop_begin;
// second location of the check is red
end:
```

In the example, the second color represents the second pass through the loop, and you should investigate.

# Managing Orange Checks

---

- “Understanding Orange Checks” on page 9-2
- “Too Many Orange Checks?” on page 9-9
- “Reducing Orange Checks in Your Results” on page 9-11
- “Reviewing Orange Checks” on page 9-29
- “Automatically Testing Orange Code” on page 9-38

## Understanding Orange Checks

### In this section...

“What is an Orange Check?” on page 9-2

“Sources of Orange Checks” on page 9-6

### What is an Orange Check?

Orange checks indicate *unproven code*. This means that the code can neither be proven safe, nor can it be proven to contain a runtime error.

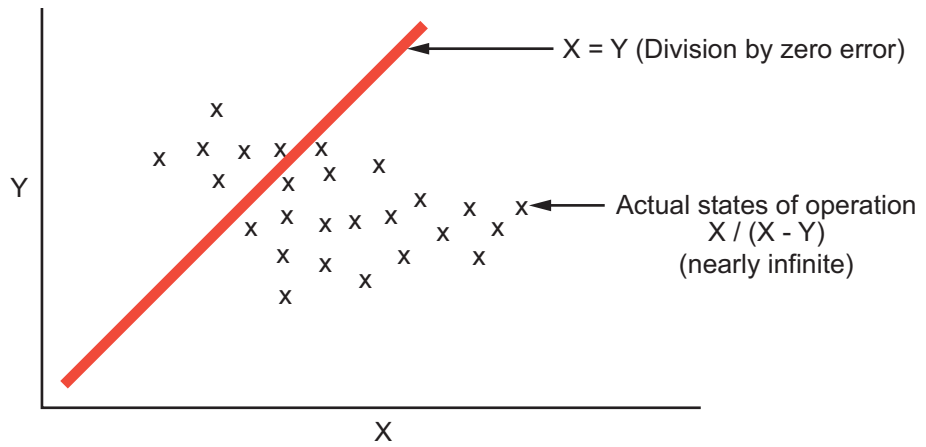
PolySpace verification does not try to find bugs, it attempts to prove the absence or existence of run time errors. Therefore, all code starts out as unproven prior to verification. The verification then attempts to prove that the code is either correct (green), is certain to fail (red), or is unreachable (gray). Any remaining code stays unproven (orange).

Code often remains unproven in situations where some paths fail while others succeed. For example, consider the following instruction:

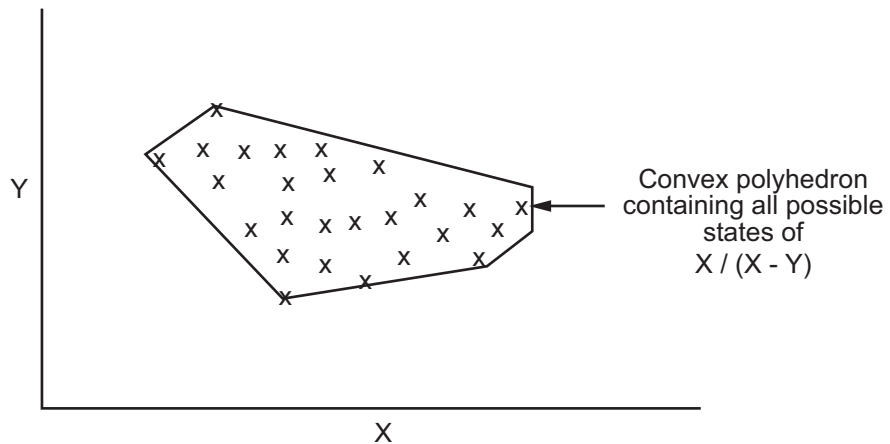
```
X = 1 / (X - Y);
```

Does a division-by-zero error occur?

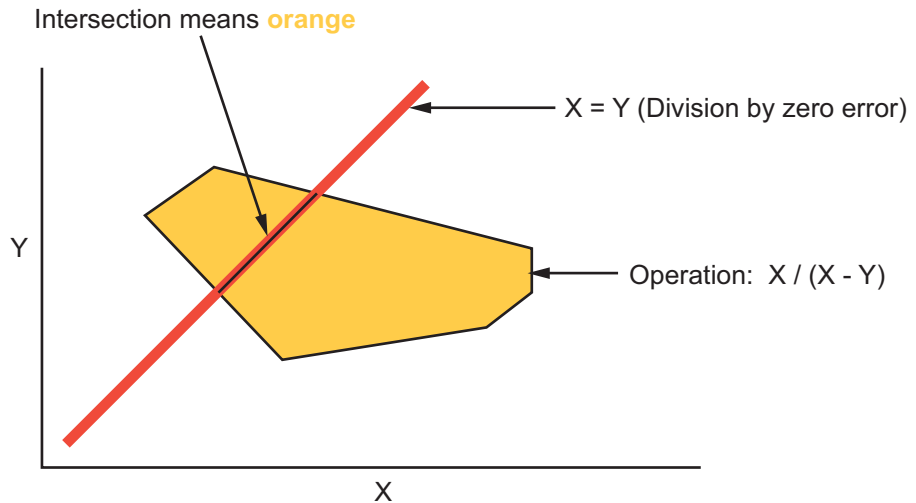
The answer clearly depends on the values of  $X$  and  $Y$ . However, there are an almost infinite number of possible values. Creating test cases for all possible values is not practical.



Although it is not possible to test every value for each variable, the target computer and programming language provide limits on the possible values of the variables. PolySpace verification uses these limits to compute a *cloud of points* (upper-bounded convex polyhedron) that contains all possible states for the variables.

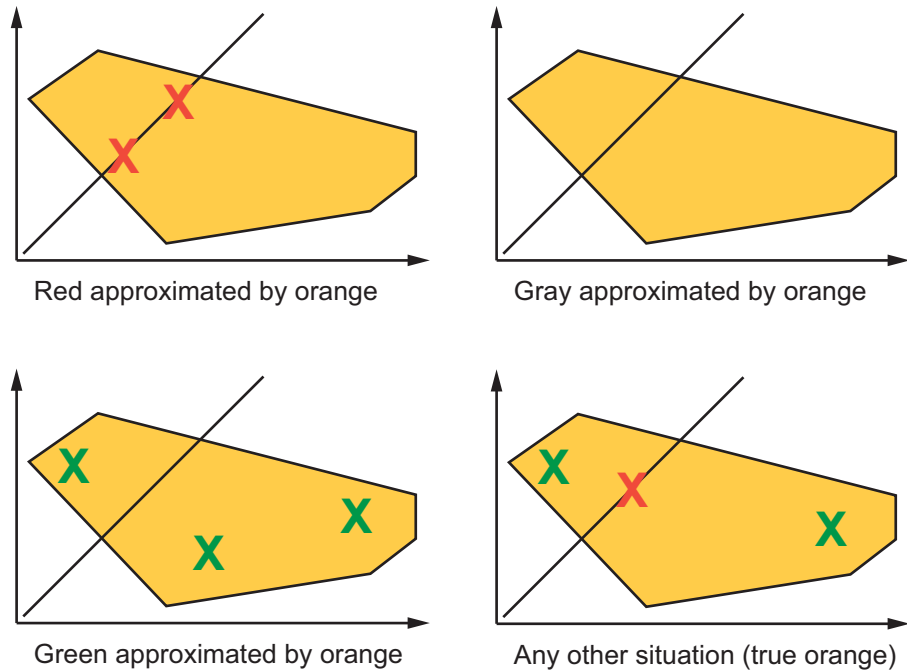


PolySpace verification then compares the data set represented by this polyhedron to the error zone. If the two data sets intersect, the check is orange.



**Graphical Representation of an Orange Check**

A true orange check represents a situation where some paths fail while others succeed. However, because the data set used in the verification is an approximation of actual values, an orange check may actually represent a check of any other color, as shown below.



PolySpace reports an orange check any time the two data sets intersect, regardless of the actual values. Therefore, you may find orange checks that represent bugs, while other orange checks represent code that is safe.

You can resolve some of these orange checks by increasing the precision of your verification, or by adding execution context, but often you must review the results to determine the source of an orange check.

### Sources of Orange Checks

Orange checks can be caused by any of the following:

- Potential bug
- Inconclusive check
- Data set issue
- Basic imprecision

Bugs can be revealed by any of these categories except for basic imprecision.

### Potential Bug

An orange check can reveal code which will fail under some circumstances. These types of orange checks often represent real bugs.

For example, consider a function `Recursion()`:

- `Recursion()` takes a parameter, increments it, then divides by it.
- This sequence of actions loops through an indirect recursive call to `Recursion_recurse()`.

If the initial value passed to `Recursion()` is negative, then the recursive loop will at some point attempt a division by zero. Therefore, the division operation causes an orange ZDV.

### Inconclusive Verification

An orange check can be caused by situations in which the verification is unable to conclude whether a problem exists.

In some code, it is impossible to conclude whether an error exists without additional information.

For example, consider a variable `X`, and two concurrent tasks `T1` and `T2`.

- `X` is initialized to 0.
- `T1` assigns the value 12 to `X`.



- T2 divides a local variable by  $X$ .
- A division by zero error is possible because T1 can be started before or after T2, so the division causes an orange ZDV.

The verification cannot determine if an error will occur unless you define the call sequence.

Most inconclusive orange checks take some time to investigate. An inconclusive orange check often results from complex code structure. Sometimes, such situations take an hour or more to understand. You may want to recode to ensure there is no risk, depending on the criticality of the function and the required speed of execution.

### **Data Set Issue**

An orange check can result from a theoretical set of data that cannot actually occur.

PolySpace verification uses an *upper approximation* of the data set, meaning that it considers all combinations of input data rather than any particular combination. Therefore, an orange check may result from a combination of input values that is not possible at execution time.

For example, consider three variables  $X$ ,  $Y$ , and  $Z$ :

- Each of these variables is defined as being between 1 and 1,000.
- The code computes  $X*Y*Z$  on a 16-bit data type.
- The result can potentially overflow, so it causes an orange OVFL.

When developing the code, you may know that the three variables cannot all take the value 1,000 at the same time, but this information is not available to the verification. Therefore, the multiplication is orange.

When an orange check is caused by a data set issue, it is usually possible to identify the cause quickly. After identifying a data set issue, you may want to comment the code to flag the warning, or modify the code to take the constraints into account.

### Basic Imprecision

An orange check can be caused by imprecise approximation of the data set used for verification.

For example, consider a variable  $X$ :

- Before the function call,  $X$  is defined as having the following values: -5, -3, 8, or any value in range  $[10 \dots 20]$ . This means that 0 has been excluded from the set of possible values for  $X$ .
- However, due to optimization at low precision levels (-00), the verification approximates  $X$  in the range  $[-5 \dots 20]$ , instead of the previous set of values.
- Therefore, calling the function  $x = 1/x$  causes an orange ZDV.

PolySpace verification is unable to prove the absence of a run-time error in this case.

In cases of basic imprecision, you may be able to resolve orange checks by increasing the precision level. If this does not resolve the orange check, verification cannot help directly. You need to review the code to determine if there is an actual problem.

For more information, see and “Approximations Used During Verification” in the *PolySpace Products for C Reference*.

## Too Many Orange Checks?

| In this section...                              |
|-------------------------------------------------|
| “Do I Have Too Many Orange Checks?” on page 9-9 |
| “How to Manage Orange Checks” on page 9-10      |

### Do I Have Too Many Orange Checks?

If the goal of code verification is to prove the absence of run time errors, you may be concerned by the number of orange checks (unproven code) in your results.

In reality, asking “Do I have too many orange checks?” is not the right question. There is not an ideal number of orange checks that applies for all applications, not even zero. Whether you have too many orange checks depends on:

- **Development Stage** – Early in the development cycle, when verifying the first version of a software component, a developer may want to focus exclusively on finding red errors, and not consider orange checks. As development of the same component progresses, however, the developer may want to focus more on orange checks.
- **Application Requirements** – There are actions you can take during coding to produce more provable code. However, writing provable code often involves compromises with code size, code speed, and portability. Depending on the requirements of your application, you may decide to optimize code size, for example, at the expense of more orange checks.
- **Quality Goals** – PolySpace software can help you meet quality goals, but it cannot define those goals for you. Before you verify code, you must define quality goals for your application. These goals should be based on the criticality of the application, as well as time and cost constraints.

It is these factors that ultimately determine how many orange checks are acceptable in your results, and what you should do with the orange checks that remain.

Thus, a more appropriate question is “How do I manage orange checks?”

This question leads to two main activities:

- Reducing the number of orange checks
- Working with orange checks

### **How to Manage Orange Checks**

PolySpace verification cannot magically produce quality code at the end of the development process. Verification is a tool that helps you measure the quality of your code, identify issues, and ultimately achieve the quality goals you define. To do this, however, you must integrate PolySpace verification into your development process.

Similarly, you cannot successfully manage orange checks simply by using PolySpace options. To manage orange checks effectively, you must take actions while coding, when setting up your verification project, and while reviewing verification results.

To successfully manage orange checks, perform each of the following steps:

- 1** Define your quality objectives to set overall goals for application quality. See “Defining Quality Objectives” on page 2-5.
- 2** Set PolySpace analysis options to match your quality objectives. See “Specifying Options to Match Your Quality Objectives” on page 3-19.
- 3** Define a process to reduce orange checks. See “Reducing Orange Checks in Your Results” on page 9-11.
- 4** Apply the process to work with remaining orange checks. See “Reviewing Orange Checks” on page 9-29.

## Reducing Orange Checks in Your Results

### In this section...

“Overview: Reducing Orange Checks” on page 9-11

“Applying Coding Rules to Reduce Orange Checks” on page 9-12

“Considering Generated Code” on page 9-17

“Improving Verification Precision” on page 9-17

“Stubbing Parts of the Code Manually” on page 9-24

“Describing Multitasking Behavior Properly” on page 9-27

“Considering Contextual Verification” on page 9-28

### Overview: Reducing Orange Checks

There are several actions you can take to reduce the number of orange checks in your results.

However, it is important to understand that while some actions increase the quality of your code, others simply change the number of orange checks reported by the verification, without improving code quality.

Actions that reduce orange checks and improve the quality of your code:

- **Apply coding rules** – Coding rules are the most efficient means to reduce oranges, and can also improve the quality of your code.
- **Move to generated code** – Generated code can reduce orange checks and eliminate certain types of coding errors.

Actions that reduce orange checks through increased verification precision:

- **Set precision options** – There are several PolySpace options that can increase the precision of your verification, at the cost of increased verification time.
- **Implement manual stubbing** – Manual stubs that accurately emulate the behavior of missing functions can increase the precision of the verification.

- **Specify multitasking behavior** – Accurately defining call sequences and other multitasking behavior can increase the precision of the verification.

Options that reduce orange checks but do not improve code quality or the precision of the verification:

- **Create empty stubs** – Providing empty stubs for missing functions can reduce the number of orange checks in your results, but does not improve the quality of the code.
- **Constrain data ranges** – You can use data range specifications (DRS) to limit the scope of a verification to specific variable ranges, instead of considering all possible values. This reduces the number of orange checks, but does not improve the quality of the code. Therefore, DRS should be used specifically to perform contextual verification, not simply to reduce orange checks.

Each of these actions have trade-offs, either in development time, verification time, or the risk of errors. Therefore, before taking any of these actions, it is important to define your quality objectives, as described in Chapter 2.

It is your quality objectives that determine how many orange checks are acceptable in your results, what actions you should take to reduce the number of orange checks, and what you should do with any orange checks that remain.

### **Applying Coding Rules to Reduce Orange Checks**

The number of orange checks in your results depends strongly on the coding style used in the project. Applying coding rules can both reduce the number of orange checks in your verification results, and improve the quality of your code. Coding rules are the most efficient way to reduce orange checks.

PolySpace software allows you to check MISRA C coding rules during verification. If your code complies with the first subset of MISRA rules (coding rules with a direct impact on selectivity), the total number of orange checks will decrease substantially, and the percentage of orange checks representing real bugs will increase.

In addition, some code constructions are known to produce orange checks. If your design avoids these constructions, you will see fewer orange checks in

your verification results. The second subset of MISRA rules (coding rules with an indirect impact on selectivity), checks for these constructions.

The following coding rules are recommended to reduce oranges:

- “Set of Coding Rules with a Direct Impact on Selectivity” on page 9-13
- “Set of Coding Rules with an Indirect Impact on Selectivity” on page 9-15

For more information on checking MISRA C coding rules, see Chapter 11, “MISRA Checker”.

### Set of Coding Rules with a Direct Impact on Selectivity

The following set of coding rules will typically improve the selectivity of your verification results.

| Rule #      | Description                                                                                                                                                      |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MISRA 8.11  | The <i>static</i> storage class specifier shall be used in definitions and declarations of objects and functions that have internal linkage                      |
| MISRA 8.12  | When an array is declared with external linkage, its size shall be stated explicitly or defined implicitly by initialization                                     |
| MISRA 11.2  | Conversion shall not be performed between a pointer to an object and any type other than an integral type, another pointer to a object type or a pointer to void |
| MISRA 11.3  | A cast should not be performed between a pointer type and an integral type                                                                                       |
| MISRA 12.12 | The underlying bit representations of floating-point values shall not be used                                                                                    |
| MISRA 13.3  | Floating-point expressions shall not be tested for equality or inequality                                                                                        |

| Rule #     | Description                                                                                                                                  |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| MISRA 13.4 | The controlling expression of a <i>for</i> statement shall not contain any objects of floating type                                          |
| MISRA 13.5 | The three expressions of a <i>for</i> statement shall be concerned only with loop control                                                    |
| MISRA 14.4 | The <i>goto</i> statement shall not be used.                                                                                                 |
| MISRA 14.7 | A function shall have a single point of exit at the end of the function                                                                      |
| MISRA 16.1 | Functions shall not be defined with variable numbers of arguments                                                                            |
| MISRA 16.2 | Functions shall not call themselves, either directly or indirectly                                                                           |
| MISRA 16.7 | A pointer parameter in a function prototype should be declared as pointer to const if the pointer is not used to modify the addressed object |
| MISRA 17.3 | >, >=, <, <= shall not be applied to pointer types except where they point to the same array                                                 |
| MISRA 17.4 | Array indexing shall be the only allowed form of pointer arithmetic                                                                          |
| MISRA 17.5 | The declaration of objects should contain no more than 2 levels of pointer indirection                                                       |
| MISRA 17.6 | The address of an object with automatic storage shall not be assigned to an object that may persist after the object has ceased to exist.    |
| MISRA 18.3 | An area of memory shall not be reused for unrelated purposes.                                                                                |
| MISRA 18.4 | Unions shall not be used                                                                                                                     |
| MISRA 20.4 | Dynamic heap memory allocation shall not be used.                                                                                            |

---

**Note** MISRA rules 16.7, 17.3 and 18.3 are not checked.

---



## Set of Coding Rules with an Indirect Impact on Selectivity

Good design practices generally lead to less code complexity, which can improve the selectivity of your verification results. The following set of coding rules help address design issues that can impact selectivity.

| Rule #     | Description                                                                                                                                                       |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MISRA 5.1  | Identifiers (internal and external) shall not rely on the significance of more than 31 characters                                                                 |
| MISRA 6.3  | <i>typedefs</i> that indicate size and signedness should be used in place of the basic types                                                                      |
| MISRA 8.7  | Objects shall be defined at block scope if they are only accessed from within a single function                                                                   |
| MISRA 9.2  | Braces shall be used to indicate and match the structure in the nonzero initialization of arrays and structures                                                   |
| MISRA 9.3  | In an enumerator list, the = construct shall not be used to explicitly initialize members other than the first, unless all items are explicitly initialized       |
| MISRA 10.3 | The value of a complex expression of integer type may only be cast to a type that is narrower and of the same signedness as the underlying type of the expression |
| MISRA 10.5 | Bitwise operations shall not be performed on signed integer types                                                                                                 |
| MISRA 11.1 | Conversion shall not be performed between a pointer to a function and any type other than an integral type                                                        |
| MISRA 11.5 | Type casting from any type to or from pointers shall not be used                                                                                                  |
| MISRA 12.1 | Limited dependence should be placed on C's operator precedence rules in expressions                                                                               |
| MISRA 12.2 | The value of an expression shall be the same under any order of evaluation that the standard permits                                                              |
| MISRA 12.4 | The right hand operand of a logical && or    operator shall not contain side effects                                                                              |

| Rule #      | Description                                                                                                                                                                              |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MISRA 12.5  | The operands of a logical && or    shall be primary-expressions                                                                                                                          |
| MISRA 12.6  | Operands of logical operators (&&,    and !) should be effectively Boolean. Expression that are effectively Boolean should not be used as operands to operators other than (&&,    or !) |
| MISRA 12.9  | The unary minus operator shall not be applied to an expression whose underlying type is unsigned                                                                                         |
| MISRA 12.10 | The comma operator shall not be used                                                                                                                                                     |
| MISRA 13.1  | Assignment operators shall not be used in expressions that yield Boolean values                                                                                                          |
| MISRA 13.2  | Tests of a value against zero should be made explicit, unless the operand is effectively Boolean                                                                                         |
| MISRA 13.6  | Numeric variables being used within a “for” loop for iteration counting should not be modified in the body of the loop                                                                   |
| MISRA 14.8  | The statement forming the body of a <i>switch</i> , <i>while</i> , <i>do while</i> or <i>for</i> statement shall be a compound statement                                                 |
| MISRA 14.10 | All <i>if else if</i> constructs should contain a final <i>else</i> clause                                                                                                               |
| MISRA 15.3  | The final clause of a <i>switch</i> statement shall be the <i>default</i> clause                                                                                                         |
| MISRA 16.3  | Identifiers shall be given for all of the parameters in a function prototype declaration                                                                                                 |
| MISRA 16.8  | All exit paths from a function with non-void return type shall have an explicit return statement with an expression                                                                      |
| MISRA 16.9  | A function identifier shall only be used with either a preceding &, or with a parenthesized parameter list, which may be empty                                                           |
| MISRA 19.4  | C macros shall only expand to a braced initializer, a constant, a parenthesized expression, a type qualifier, a storage class specifier, or a do-while-zero construct                    |

| Rule #      | Description                                                                                                                                                   |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MISRA 19.9  | Arguments to a function-like macro shall not contain tokens that look like preprocessing directives                                                           |
| MISRA 19.10 | In the definition of a function-like macro each instance of a parameter shall be enclosed in parentheses unless it is used as the operand of # or ##          |
| MISRA 19.11 | All macro identifiers in preprocessor directives shall be defined before use, except in #ifdef and #ifndef preprocessor directives and the defined() operator |
| MISRA 19.12 | There shall be at most one occurrence of the # or ## preprocessor operators in a single macro definition.                                                     |
| MISRA 20.3  | The validity of values passed to library functions shall be checked.                                                                                          |

---

**Note** MISRA rule 20.3 is not checked by PolySpace software.

---

## Considering Generated Code

Moving to generated code can reduce the number of orange checks in your results, and improve the overall quality of your software.

Generated code has a well-defined set of coding rules, and eliminates certain types of coding errors by construction. This results in higher ratio of green checks in your verification results.

The PolySpace Model Link SL, PolySpace Model Link TL, and PolySpace UML Link™ RH products allow you to integrate PolySpace verification into a generated code workflow.

For more information, see the *PolySpace Model Link Products User's Guide*.

## Improving Verification Precision

Improving the precision of a verification can reduce the number of orange checks in your results, although it does not affect the quality of the code itself.

There are a number of PolySpace options that affect the precision of the verification. The trade off for this improved precision is increased verification time.

The following sections describe how to improve the precision of your verification:

- “Balancing Precision and Verification Time” on page 9-18
- “Setting the Analysis Precision Level” on page 9-19
- “Setting Software Safety Analysis Level” on page 9-21
- “Other Options that Can Improve Precision” on page 9-22

### **Balancing Precision and Verification Time**

When performing code verification, you must find the right balance between precision and verification time. Consider the two following extremes:

- If a verification runs in one minute but contains only orange checks, the verification is not useful because each check must be reviewed manually.
- If a verification contains no orange checks (only gray, red, and green), but takes six months to run, the verification is not useful because of the time spent waiting for the results.

Higher precision yields more proven code (red, green, and gray), but takes longer to complete. The goal is therefore to get the most precise results in the time available. Factors that influence this compromise include the time available for verification, the time available to review results, and the stage in the development cycle.

For example, consider the following scenarios:

- **Unit testing** – Before going to lunch, a developer starts a verification. After returning from lunch the developer will review verification results for one hour.
- **Integration testing** – Before going home, a developer starts a verification. The developer will spend the next morning reviewing verification results.

- **Validation testing** – Before leaving the office on Friday evening, a developer starts a verification. The developer will spend the following week reviewing verification results.

Each of these scenarios require the developer to use PolySpace software in different ways. Generally, the first verification should use the lowest precision mode, while subsequent verifications increase the precision level.

---

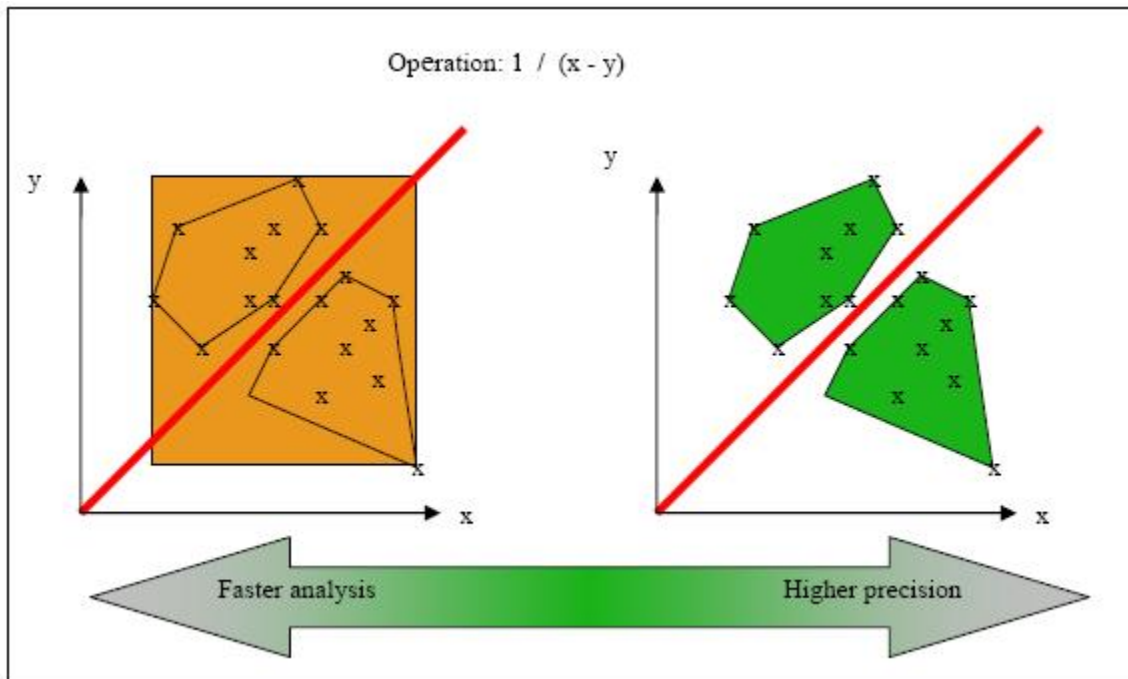
**Note** It is possible that a verification never ends. In this case, you may need to split the application.

---

### **Setting the Analysis Precision Level**

The analysis **Precision Level** specifies the mathematical algorithm used to compute the cloud of points (polyhedron) containing all possible states for the variables.

Although changing the precision level does not affect the quality of your code, orange checks caused by low precision become green when verified with higher precision.



### Affect of Precision Rate on Orange Checks

To set the precision level:

- 1 In the Analysis options section of the Launcher window, select **Precision/Scaling > Precision**.
- 2 Select the -00, -01, -02 or -03 precision level the Precision Level drop-down list.

For more information, see “-O(0-3)” in the *PolySpace Products for C Reference*.

---

**Note** You can select specific precision levels for individual modules in the verification.

---

## Setting Software Safety Analysis Level

The Software Safety Analysis level of your verification specifies how many times the abstract interpretation algorithm passes through your code. The deeper the verification goes, the more precise it is.

There are 5 Software Safety Analysis levels (pass0 to pass4). By default, verification proceeds to pass4, although it can go further if required. Each iteration results in a deeper level of propagation of calling and called context.

To set the Software Safety Analysis level:

- 1 In the Analysis options section of the Launcher window, select **Precision/Scaling > Precision**.
- 2 Select the appropriate level in the **To end of** drop-down list.

For more information, see “-to verification-phase” in the *PolySpace Products for C Reference*.

---

**Note** The Software Safety Analysis level applies to the entire application. You cannot select specific levels for individual modules in the verification.

---

### Example: Orange Checks and Software Safety Analysis Level

The following example shows how orange checks are resolved as verification proceeds through Software Safety Analysis levels 0 and 1.

| Safety Analysis Level 0                                                                                                                                  | Safety Analysis Level 1                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>#include &lt;stdlib.h&gt;  void ratio (float x, float *y) {   *y=(abs(x-*y))/(x+*y); }  void level1 (float x,              float y, float *t)</pre> | <pre>#include &lt;stdlib.h&gt;  void ratio (float x, float *y) {   *y=(abs(x-*y))/(x+*y); }  void level1 (float x,              float y, float *t)</pre> |

| Safety Analysis Level 0                                                                                                                                                                                                                             | Safety Analysis Level 1                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> { float v;   v = y;   ratio (x, &amp;y);   *t = 1.0/(v - 2.0 * x); }  float level2(float v) {   float t;   t = v;   level1(0.0, 1.0, &amp;t);   return t; }  void main(void) {   float r,d;   d= level2(1.0);   r = 1.0 / (2.0 - d); } </pre> | <pre> { float v;   v = y;   ratio (x, &amp;y);   *t = 1.0/(v - 2.0 * x); }  float level2(float v) {   float t;   t = v;   level1(0.0, 1.0, &amp;t);   return t; }  void main(void) {   float r,d;   d= level2(1.0);   r = 1.0 / (2.0 - d); } </pre> |

In this example, division by an input parameter of a function produces an orange during Level 0 verification, but turns to green during level 1. The verification gains more accurate knowledge of  $x$  as the value is propagated deeper.

### Other Options that Can Improve Precision

The following options can also improve verification precision:

- “Improve precision of interprocedural analysis” on page 9-23
- “Sensitivity context” on page 9-23
- “Inline” on page 9-23



---

**Note** Changing these options does not affect the quality of the code itself. Improved precision can reduce the number of orange checks, but will increase verification time.

---

**Improve precision of interprocedural analysis.** This option causes the verification to propagate information within procedures earlier than usual. This improves the precision within each Software Safety Analysis level, meaning that some orange checks are resolved in level 1 instead of later levels.

However, using this option increases verification time exponentially. In some cases this could cause a level 1 verification to take longer than a level 4 verification.

For more information, see “-path-sensitivity-delta number” in the *PolySpace Products for C Reference*.

**Sensitivity context.** This option splits each check within a procedure into sub-checks, depending on the context of a call. This improves precision for discrete calls to the procedure. For example, if a check is red for one call to the procedure and green for another, both colors will be revealed.

For more information, see “-context-sensitivity "proc1[,proc2[,...]]” in the *PolySpace Products for C Reference*.

**Inline.** This option creates clones of a each specified procedure for each call to it. This reduces the number of aliases in a procedure, and can improve precision in some situations.

However, using this option can duplicate large amounts of code, leading to increased verification time and other scaling problems.

For more information, see “-inline "proc1[,proc2[,...]]” in the *PolySpace Products for C Reference*.

### Stubbing Parts of the Code Manually

Manually stubbing parts of your code can reduce the number of orange checks in your results. However, manual stubbing generally does not improve the quality of your code, it only changes the results.

Stubs do not need to model the details of the functions or procedures involved. They only need to represent the effect that the code might have on the remainder of the system.

If a function is supposed to return an integer, the default automatic stubbing will stub it on the assumption that it can potentially take any value from the full type of an integer.

The following sections describe how to reduce orange checks using manual stubbing:

- “Manual vs. Automatic Stubbing” on page 9-24
- “Emulating Function Behavior with Manual Stubs” on page 9-25
- “Reducing Orange Checks with Empty Stubs” on page 9-26

### Manual vs. Automatic Stubbing

There are two types of stubs in PolySpace verification:

- **Automatic stubs** – The software automatically creates stubs for unknown functions based on the function’s prototype (the function declaration). Automatic stubs do not provide insight into the behavior of the function, but are very conservative, ensuring that the function does not cause any runtime errors.
- **Manual stubs** – You create these stub functions to emulate the behavior of the missing functions, and manually include them in the verification with the rest of the source code. Manual stubs can better emulate missing functions, or they can be empty.

By default, PolySpace software automatically stubs functions. However, because automatic stubs are conservative, they can lead to more orange checks in your results.

## Stubbing Example

The following example shows the effect of automatic stubbing.

```
void main(void)
{
 a=1;
 b=0;
 a_missing_function(&a, b);
 b = 1 / a;
}
```

Due to automatic stubbing, the verification assumes that *a* can be any integer, including 0. This produces an orange check on the division.

If you provide an empty manual stub for the function, the division would be green. This reduces the number of orange checks in the result, but does not improve the quality of the code itself. The function could still potentially cause an error.

However, if you provide a detailed manual stub that accurately emulates the behavior of the function, the division could be any color, including red.

## Emulating Function Behavior with Manual Stubs

You can improve both the speed and selectivity of your verification by providing manual stubs that accurately emulate the behavior of missing functions. The trade-off is time spent writing the stubs.

Manual stubs do not need to model the details of the functions or procedures involved. They only need to represent the effect that the code might have on the remainder of the system.

### Example

This example shows a header for a missing function (which may occur when the verified code is an incomplete subset of a project).

```
int a,b;
int *ptr;
void a_missing_function(int *dest, int src);
```

```
/* should copy src into dest */
void main(void)
{
 a = 1;
 b = 0;
 a_missing_function(&a, b);
 b = 1 / a;
}
```

The missing function copies the value of the `src` parameter to `dest`, so there is a division by zero error.

However, automatic stubbing always shows an orange check, because `a` is assumed to have any value in the full integer range. Only an accurate manual stub can reveal the true **red** error.

Using manual stubs to accurately model constraints in primitives and outside functions propagates more precision throughout the application, resulting in fewer orange checks.

### Reducing Orange Checks with Empty Stubs

Providing empty manual stubs can reduce the number of orange checks in your results, but it does not make your code more reliable.

For example, consider the following code:

```
void write_or_not1(int *x);

void write_or_not2(int *x);
{ //empty manual stub
}

void orange(void)
{
 int x = 12;
 int y;

 write_or_not1(&x);
 y = y / x; //Orange ZDV due to automatic stub
```

```
 }

void green(void)
{
 int x = 12;
 int y;

 write_or_not2(&x);
 y = y / x; // Green due to empty stub
}
```

The code for the two functions is identical, but the automatic stub produces an orange check, while the empty stub produces a green.

While the empty stub reduces the number of orange checks in your results, you must take additional steps to ensure the actual function does not result in a runtime error.

## Describing Multitasking Behavior Properly

The asynchronous characteristics of your application can have a direct impact on the number of orange checks. Properly describing characteristics such as implicit task declarations, mutual exclusion, and critical sections can reduce the number of orange checks in your results.

For example, consider a variable  $X$ , and two concurrent tasks T1 and T2.

- $X$  is initialized to 0.
- T1 assigns the value 12 to  $X$ .
- T2 divides a local variable by  $X$ .
- A division by zero error is possible because T1 can be started before or after T2, so the division causes an orange ZDV.

The verification cannot determine if an error will occur without knowing the call sequence. Modelling the task differently could turn this orange check green or red.

Refer to “*Preparing Multitasking Code*” on page 5-20 for information on tasking facilities, including:

- Shared variable protection:
  - Critical sections,
  - Mutual exclusion,
  - Tasks synchronization,
- Tasking:
  - Threads, interruptions,
  - Synchronous/asynchronous events,
  - Real-time OS.

### Considering Contextual Verification

By default, PolySpace software performs *robustness verification*, proving that the software works under all conditions. Robustness verification assumes that all data inputs are set to their full range. Therefore, nearly any operation on these inputs could produce an overflow.

PolySpace software also allows you to perform *contextual verification*, proving that the software works under normal working conditions. When performing contextual verification, you use the data range specifications (DRS) module to set external constraints on global variables and stub function return values, and the code is verified within these ranges.

Contextual verification can substantially reduce the number of orange checks in your verification results, but it does not improve the quality of your code.

---

**Note** DRS should be used specifically to perform contextual verification, it is not simply a means to reduce oranges.

---

For more information, see “Applying Data Ranges to External Variables and Stub Functions (DRS)” on page 4-26.

## Reviewing Orange Checks

| In this section...                                                   |
|----------------------------------------------------------------------|
| “Overview: Reviewing Orange Checks” on page 9-29                     |
| “Defining Your Review Methodology” on page 9-29                      |
| “Performing Selective Orange Review” on page 9-31                    |
| “Importing Review Comments from Previous Verifications” on page 9-33 |
| “Performing an Exhaustive Orange Review” on page 9-34                |

### Overview: Reviewing Orange Checks

After you define a process that matches your quality objectives, you do not have too many orange checks. You have the correct number of orange checks for your quality model.

At this point, the goal is not to eliminate orange checks, it is to work efficiently with them.

Working efficiently with orange checks involves:

- Defining a review methodology to work consistently with orange checks
- Reviewing orange checks efficiently
- Importing comments to avoid duplicating review effort
- Dynamically testing orange checks

### Defining Your Review Methodology

Before reviewing verification results, you should configure a methodology for your project. The methodology defines both the type and number of orange checks you need to review to meet three criteria levels.

| Number of checks to review |             |             |             |
|----------------------------|-------------|-------------|-------------|
|                            | Criterion 1 | Criterion 2 | Criterion 3 |
| <b>Common</b>              |             |             |             |
| ZDV                        | 5           | 20          | ALL         |
| NIVL                       | 10          | 50          | ALL         |
| S-OVFL                     | 10          | 50          | ALL         |
| COR                        | 0           | 10          | 10          |
| NIV                        | 0           | 0           | 10          |
| F-OVFL                     | 5           | 10          | 20          |
| ASRT                       | 0           | 5           | 20          |
| <b>C &amp; C++ only</b>    |             |             |             |
| OBAI                       | 10          | 20          | ALL         |
| SHF                        | 5           | 10          | ALL         |
| IDP                        | 0           | 10          | 20          |
| NIP                        | 0           | 10          | 20          |
| <b>C only</b>              |             |             |             |
| IRV                        | 5           | 20          | ALL         |

### Sample Review Methodology

The criteria levels displayed in the methodology represent quality levels you defined as part of the quality objectives for your project.

---

**Note** For information on setting the quality levels for your project, see Chapter 2.

---

After you configure a methodology, each developer uses it to review verification results. This ensures that all users apply the same standards when reviewing orange checks in each stage of the development cycle.

For more information on defining a methodology, see “Selecting the Methodology and Criterion Level” on page 8-20.



## Performing Selective Orange Review

Once you have defined a methodology for your project, you can use assistant mode to perform a *selective orange review*.

The number and type of orange checks you review is determined by your methodology and the quality level you are trying to achieve. As a project progresses, the quality level (and number of orange checks to review) generally increases.

For example, you may perform a level 1 review in the early stages of development, when trying to improve the quality of freshly written code. Later, you may perform a level 2 review as part of unit testing.

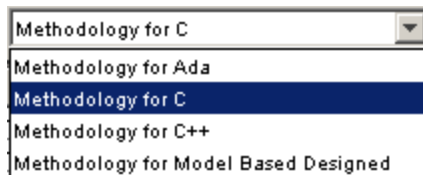
In general, the goal of a selective orange review is to find the maximum number of bugs in a short period of time. Many orange checks take only a few seconds to understand. Therefore, to maximize the number of bugs you can identify, you should focus on those checks you can understand quickly, spending no more than 5 minutes on each check. Checks that take longer to understand are left for later analysis.

To perform a selective orange review:

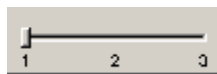
- 1 Click the **Assistant** button in the Viewer to select assistant mode.


The Viewer window toolbar displays the assistant mode controls.

- 2 Select the methodology for your project from the methodology menu.



- 3 Select the appropriate quality level for your review using the level slider.



- 4 Navigate through the checks by clicking the forward arrow .
- 5 Perform a quick code review on each orange check, spending no more than 5 minutes on each.

Your goal is to quickly identify whether the orange check is a:

- **potential bug** – code which will fail under some circumstances.
- **inconclusive check** – a check that requires additional information to resolve, such as the call sequence.
- **data set issue** – a theoretical set of data that cannot actually occur.

See “Sources of Orange Checks” on page 9-6 for more information on each of these causes.

---

**Note** If an orange check is too complicated to explain quickly, it may be an inconclusive check caused by complex code structure, or the result of basic imprecision (approximation of the data set used for verification). These types of checks often take a substantial amount of time to understand.

---

- 6 If you cannot identify a cause within 5 minutes, move on to the next check.

---

**Note** Your goal is to find the maximum number of bugs in a short period of time. Therefore, you want to identify the source of as many orange checks as possible, while leaving more complex situations for future analysis.

---

- 7 Once you understand the cause of an orange check, select the check box to indicate that you have reviewed the check.

```
example.c / Recursion / line 142 / column 15
+ advance = 1.0f/(float)(*depth); /* potential division by zero */
[checked] [comment icon] NAI - depth cannot be negative
Warning : float division by zero may occur
operator / on type float 32
left: 1.0
right: [-2.1475E+9 .. -2.9999] or [-2.0001 .. -9.9999E-1] or 0.0 or [2.9999]
```

- 8** Enter a comment for the reviewed check in the text box, indicating the results of your review.

For example, you can use acronyms to classify the checks being reviewed:

- **FNO** – Bug to be Fixed NOW
- **FNR** – Bug to be Fixed in Next Release
- **MQI** – Minor Quality Issue.
- **RBI** – RoBustness Issue
- **DFC** – DeFensive Code
- **NAI** – Not An Issue

- 9** Continue to click the forward arrow until you have reviewed all of the checks identified by the assistant.

- 10** Select **File > Save checks and comments** to save your review comments.

## Importing Review Comments from Previous Verifications



Once you have reviewed verification results for a module and saved your comments, you can import those comments into subsequent verifications of the same module, allowing you to avoid reviewing the same check twice.

To import review comments from a previous verification:

- 1** Open your most recent verification results in the Viewer.

- 2 Select **File > Import checks and comments**.
- 3 Navigate to the folder containing your previous results.
- 4 Select the results (.RTE) file, then click **Open**.

The review comments from the previous results are imported into the current results.

Once you import checks and comments, the **go to next check**  icon in assistant mode will skip any reviewed checks, allowing you to review only checks that you have not reviewed previously. If you want to view reviewed checks, click the **go to next reviewed check**  icon.

---

**Note** If the code has changed since the previous verification, the imported comments may not be applicable to your current results. For example, the justification for an orange check may no longer be relevant to the current code.

---

### Performing an Exhaustive Orange Review

Up to 80% of orange checks can be resolved using multiple iterations of the process described in “Performing Selective Orange Review” on page 9-31. However, for extremely critical applications, you may want to resolve all orange checks. Exhaustive orange review is the process for resolving the remaining orange checks.

An exhaustive orange review is generally conducted later in the development process, during the unit testing or integration testing phase. The purpose of an exhaustive orange review is to analyze any orange checks that were not resolved during previous selective orange reviews, to identify potential bugs in those orange checks.

You must balance the time and cost of performing an exhaustive orange review against the potential cost of leaving a bug in the code. Depending on your quality objectives, you may or may not want to perform an exhaustive orange review.

## Cost of Exhaustive Orange Review

During an exhaustive orange review, each orange check takes an average of 5 minutes to review. This means that 400 orange checks require about four days of code review, and 3,000 orange checks require about 25 days.

However, if you have already completed several iterations of selective orange review, the remaining orange checks are likely to be more complex than average, increasing the average time required to resolve them.

## Exhaustive Orange Review Methodology

Performing an exhaustive orange review involves reviewing each orange check individually. As with selective orange review, your goal is to identify whether the orange check is a:

- **potential bug** – code which will fail under some circumstances.
- **inconclusive check** – a check that requires additional information to resolve, such as the call sequence.
- **data set issue** – a theoretical set of data that cannot actually occur.
- **Basic imprecision** – checks caused by imprecise approximation of the data set used for verification.

---

**Note** See “Sources of Orange Checks” on page 9-6 for more information on each of these causes.

---

Although you must review each check individually, there are some general guidelines to follow.

- 1 Start your review with the modules that have the highest selectivity in your application.

If the verification finds only one or two orange checks in a module or function, these checks are probably not caused by either inconclusive verification or basic imprecision. Therefore, it is more likely that these orange checks contain actual bugs. In general, these types of orange checks can also be resolved more quickly.

- 2 Next, examine files that contain a large percentage of orange checks compared to the rest of the application. These files may highlight design issues.

Often, when you examine modules containing the most orange checks, those checks will prove inconclusive. If the verification is unable to draw a conclusion, it often means the code is very complex, which can mean low robustness and quality. See “Inconclusive Verification and Code Complexity” on page 9-36.

- 3 For all files you review, spend the first 10 minutes identifying checks that you can quickly categorize (such as potential bugs and data set issues), similar to what you do in a selective orange review.

Even after performing a selective orange review, a significant number of checks can be resolved quickly. These checks are more likely than average to reflect actual bugs.

- 4 Spend the next 40 minutes of each hour tracking more complex bugs.

If an orange check is too complicated to explain quickly, it may be an inconclusive check caused by complex code structure, or the result of basic imprecision (approximation of the data set used for verification). These types of checks often take a substantial amount of time to understand. See “Resolving Orange Checks Caused by Basic Imprecision” on page 9-37.

- 5 Depending on the results of your review, correct the code or comment it to identify the source of the orange check.

### **Inconclusive Verification and Code Complexity**

The most interesting type of inconclusive check occurs when verification reveals that the code is too complicated. In these cases, most orange checks in a file are related, and careful analysis identifies a single cause — perhaps a function or a variable modified many times. These situations often focus on functions or variables that have caused problems earlier in the development cycle.

For example, consider a variable *Computed\_Speed*.

- *Computed\_Speed* is first copied into a signed integer (between  $-2^{31}$  and  $2^{31}-1$ ).
- *Computed\_Speed* is then copied into an unsigned integer (between 0 and  $2^{31}-1$ ).
- *Computed\_Speed* is next copied into a signed integer again.
- Finally, *Computed\_Speed* is added to another variable.

The verification reports 20 orange overflows (OVFL).

This scenario does not cause a real bug, but the development team may know that this variable caused trouble during development and earlier testing phases. PolySpace verification also identified a problem, suggesting that the code is poorly designed.

### **Resolving Orange Checks Caused by Basic Imprecision**

On rare occasions, a module may contain many orange checks caused by imprecise approximation of the data set used for verification. These checks are usually local to functions, so their impact on the project as a whole is limited.

In cases of basic imprecision, you may be able to resolve orange checks by increasing the precision level. If this does not resolve the orange check, however, verification cannot help directly.

In these cases, PolySpace software can only assist you through the call tree and dictionary. The code needs to be reviewed using alternate means. These alternate means may include:

- Additional unit tests
- Code review with the developer
- Checking an interpolation algorithm in a function
- Checking calibration data

For more information on basic imprecision, see “Sources of Orange Checks” on page 9-6.

## Automatically Testing Orange Code

| In this section...                                              |
|-----------------------------------------------------------------|
| “Automatic Orange Tester Overview” on page 9-38                 |
| “Before Using the Automatic Orange Tester” on page 9-41         |
| “Launching the Automatic Orange Tester” on page 9-43            |
| “Reviewing the Test Results” on page 9-47                       |
| “Refining Data Ranges” on page 9-51                             |
| “Saving and Reusing Your Configuration” on page 9-55            |
| “Exporting Data Ranges for PolySpace Verification” on page 9-56 |
| “Configuring Compiler Options” on page 9-57                     |
| “Technical Limitations” on page 9-58                            |

### Automatic Orange Tester Overview

The PolySpace Automatic Orange Tester dynamically stresses unproven code (orange checks) to identify runtime errors, and provides information to help you identify the cause of these errors.

The Automatic Orange Tester complements results review in the Viewer. Manually performing an exhaustive orange review can be time consuming. The Automatic Orange Tester saves time by automatically creating test cases for all input variables in orange code, and then dynamically testing the code to find actual runtime errors.

The Automatic Orange Tester also provides detailed information on why each test-case failed, including the actual values that caused the error. You can use this information to quickly identify the cause of the error, and determine if there is an actual bug in the code.

---

**Note** To run the Automatic Orange Tester on Linux or Unix systems, you must have a 32-bit C compiler.

---



**PolySpace Automatic Orange Tester - \_testgen.tgf**

File Options Help

| Variable Name             | Type    | Values   | Advanced |
|---------------------------|---------|----------|----------|
| External Scope            |         |          |          |
| Function: random_float    |         |          |          |
| return                    | float32 | min..max | Advanced |
| Function: random_int      |         |          |          |
| return                    | int32   | min..max | Advanced |
| Function: get_bus_status  |         |          |          |
| return                    | int32   | min..max | Advanced |
| Function: read_bus_status |         |          |          |
| return                    | int32   | min..max | Advanced |

**Test Campaign Configuration**

Number of tests:

Number of iterations for loops:

Per test timeout (in second):

**Test Campaign Results**

Completed tests: **1000**

No PolySpace run-time errors detected: **176**

Total failed: **824**

Number of checks/Tests with errors: **15/824**

Timeout: **0**

Stopped tests: **0**

Test Completed Time Remaining: 00:00:00 100%

| Results | File                   | Line | Column | Error                     | # Testcases Failed |
|---------|------------------------|------|--------|---------------------------|--------------------|
| Log     | initialisations.c      | 47   | 6      | IDP (Illegal Derefer...   | 237                |
|         | initialisations.c      | 89   | 7      | NIVL (Non Initialised ... | 127                |
|         | example.c              | 26   | 2      | ASRT (User Assertio...    | 38                 |
|         | example.c              | 43   | 12     | OVFL (Float Overflow)     | 29                 |
|         | single_file_analysis.c | 25   | 137    | ASRT (User Assertio...    | 82                 |
|         | single_file_analysis.c | 26   | 137    | ASRT (User Assertio...    | 130                |
|         | example.c              | 104  | 10     | IDP (Illegal Derefer...   | 39                 |
|         | example.c              | 43   | 12     | UNFL (Float Underflow)    | 29                 |
|         | example.c              | 49   | 16     | OVFL (Float Overflow)     | 21                 |

### PolySpace® Automatic Orange Tester

---

**Note** The version of the product used to verify the source code must be the same as the one used for analysis in the Automatic Orange Tester. If you open verification results created with an older version of the product in the Automatic Orange Tester, you may get a compilation error.

To avoid this problem, re-launch the code verification with the current version of the product.

---

## How the Automatic Orange Tester Works

PolySpace verification mathematically analyzes the operations in the code to derive its dynamic properties without actually executing it (see “What is Static Verification” on page 1-4). While this verification can identify almost all runtime errors, some operations cannot be proved either true or false because the input values are unknown. These are reported as Orange checks in the Viewer (see “What is an Orange Check?” on page 9-2).

The Automatic Orange Tester takes the PolySpace verification results, and generates *instrumented code* around orange checks so the code can be run. It then generates test cases based on the input variables, and dynamically tests the code for runtime errors.

This dynamic testing approach allows the Automatic Orange Tester to separate actual runtime errors from theoretical problems. You can then focus on these errors to determine if an orange check is identifying an actual bug.

## Limitations of Dynamic Testing

Because the Automatic Orange Tester uses a finite number of test cases to analyze the code, there is no guarantee that it will identify a problem in any individual test campaign. It is therefore possible that a particular variable value causes an error, but that value was never tested.

Similarly, since the Automatic Orange Tester builds test cases each time you run it, there is not guarantee that it will produce the same results with each test campaign.

You can specify the number of tests to run in each test campaign. Running more tests increases the chances of finding a runtime error, but also takes more time to complete.

## Before Using the Automatic Orange Tester

Before you can use the Automatic Orange Tester, you must run a PolySpace verification with the `-prepare-automatic-tests` option enabled. This option generates the data necessary to perform dynamic tests in the Automatic Orange Tester.

To run the verification:

- 1 Open the PolySpace Launcher for C.
- 2 Load the project Demo\_C-without-MISRA-checker.cfg.
- 3 In the Analysis Options window, expand the **PolySpace inner settings** menu.
- 4 Select the **Automatic Orange Tester** check box.

The screenshot shows a window titled 'Search internal name from the selected line:' with a search bar and icons for search and help. Below is a table with three columns: 'Name', 'Value', and 'Internal name'. The 'PolySpace inner settings' section is expanded, and the 'Automatic Orange Tester' option is checked.

| Name                                              | Value                               | Internal name                   |
|---------------------------------------------------|-------------------------------------|---------------------------------|
| Analysis options                                  |                                     |                                 |
| + General                                         |                                     |                                 |
| + Target/Compilation                              |                                     |                                 |
| + Compliance with standards                       |                                     |                                 |
| - PolySpace inner settings                        |                                     |                                 |
| + Run a verification unit by unit                 | <input type="checkbox"/>            | -unit-by-unit                   |
| + Generate a main                                 | <input checked="" type="checkbox"/> | -main-generator                 |
| + Stubbing                                        |                                     |                                 |
| + Assumptions                                     |                                     |                                 |
| <b>Automatic Orange Tester</b>                    | <input checked="" type="checkbox"/> | <b>-prepare-automatic-tests</b> |
| Run verification in 32 or 64-bit mode             | auto                                | -machine-architecture           |
| Number of processes for multiple CPU core systems | 4                                   | -max-processes                  |
| Other options                                     |                                     |                                 |
| + Precision/Scaling                               |                                     |                                 |
| + Multitasking                                    |                                     |                                 |

The `-prepare-automatic-tests` option is enabled.

- 5 Deselect **Send to PolySpace Server**.
- 6 Click **Start**.

The PolySpace verification starts. During the compilation phase, the software generates the data necessary to perform dynamic tests. The PolySpace verification then continues as usual.

When the verification process completes, the software asks if you want to launch PolySpace Viewer.

**7** Click **OK** to launch the viewer.

## **Launching the Automatic Orange Tester**

Once the PolySpace verification is complete, you can use the Automatic Orange Tester to perform dynamic tests of the unproven (orange) code.

To perform dynamic tests with the Automatic Orange Tester:

**1** Open your results in the PolySpace Viewer.

PolySpace Viewer - C:\PolySpace\_Results\RTE\_px\_02\_Example\_Project\_LAST\_RESULTS.rte

File Edit Reports Windows Help

Launch the PolySpace Automatic Orange Tester.

| Coding review progress                              |         | Count | Progress |
|-----------------------------------------------------|---------|-------|----------|
| num F-OVFL reviewed / num F-OVFL to review (Orange) | 0/7     |       | 0        |
| num reviewed / num to review (Orange)               | 0/52    |       | 0        |
| Software reliability indicator                      | 366/441 |       | 82       |

example.c / Close\_To\_Zero / line 43 / column 12

```
if ((xmax < xmin) < 1.0E-37f)
```

Warning : float variable may overflow on [-], range :  
 {3.4029E+38 >= [expr]}  
 operator - on type float 32  
 left: full-range [-3.4029E+38 .. 3.4029E+38]  
 right: full-range [-3.4029E+38 .. 3.4029E+38]

| Procedural entities    | ? | X  | ?  | ✓   |    |
|------------------------|---|----|----|-----|----|
| Example_Project        | 5 | 18 | 52 | 388 |    |
| -__polyspace_main.c    |   |    |    | 29  |    |
| example.c              | 4 | 11 | 14 | 94  |    |
| -Close_To_Zero ()      |   |    | 6  | 11  |    |
| ✓ IRV.0                |   |    |    | 1   |    |
| ✓ IRV.1                |   |    |    | 1   |    |
| ✓ NIVL.2               |   |    |    | 1   |    |
| ? OVFL.3               |   |    |    | 1   |    |
| ? UNFL.4               |   |    |    | 1   |    |
| ✓ NIVL.5               |   |    |    | 1   |    |
| ✓ NIVL.6               |   |    |    | 1   |    |
| ? OVFL.7               |   |    |    | 1   |    |
| ? UNFL.8               |   |    |    | 1   |    |
| ✓ NIVL.9               |   |    |    | 1   |    |
| ✓ ZDV.12               |   |    |    | 1   |    |
| ? OVFL.10              |   |    |    | 1   |    |
| ? UNFL.11              |   |    |    | 1   |    |
| ✓ NIVL.13              |   |    |    | 1   |    |
| ✓ OVFL.14              |   |    |    | 1   |    |
| ✓ UNFL.15              |   |    |    | 1   |    |
| ✓ NIVL.16              |   |    |    | 1   |    |
| -Non_Infinite_Loop ()  |   |    |    | 12  |    |
| -Pointer_Arithmetic () | 1 | 4  | 2  | 23  |    |
| -RTE ()                | 1 |    |    | 3   |    |
| -Recursion ()          |   |    |    | 3   | 14 |
| -Recursion_caller ()   | 1 |    |    | 4   |    |
| -Square_Root ()        | 1 | 3  |    | 5   |    |
| -Square_Root_conv ()   |   |    |    | 11  |    |

**Variables View**

Written by: Example\_Project, -initialisations.arr, -initialisations.current\_data, -initialisations.first\_payload, -initialisations.second\_payload, -initialisations.tab, -single\_file\_analysis.output, -single\_file\_analysis.output, -single\_file\_analysis.output, -single\_file\_analysis.saved


**Call Tree View**

Both  
 Called by  
 Calls  
 Complete  
 Update on selection

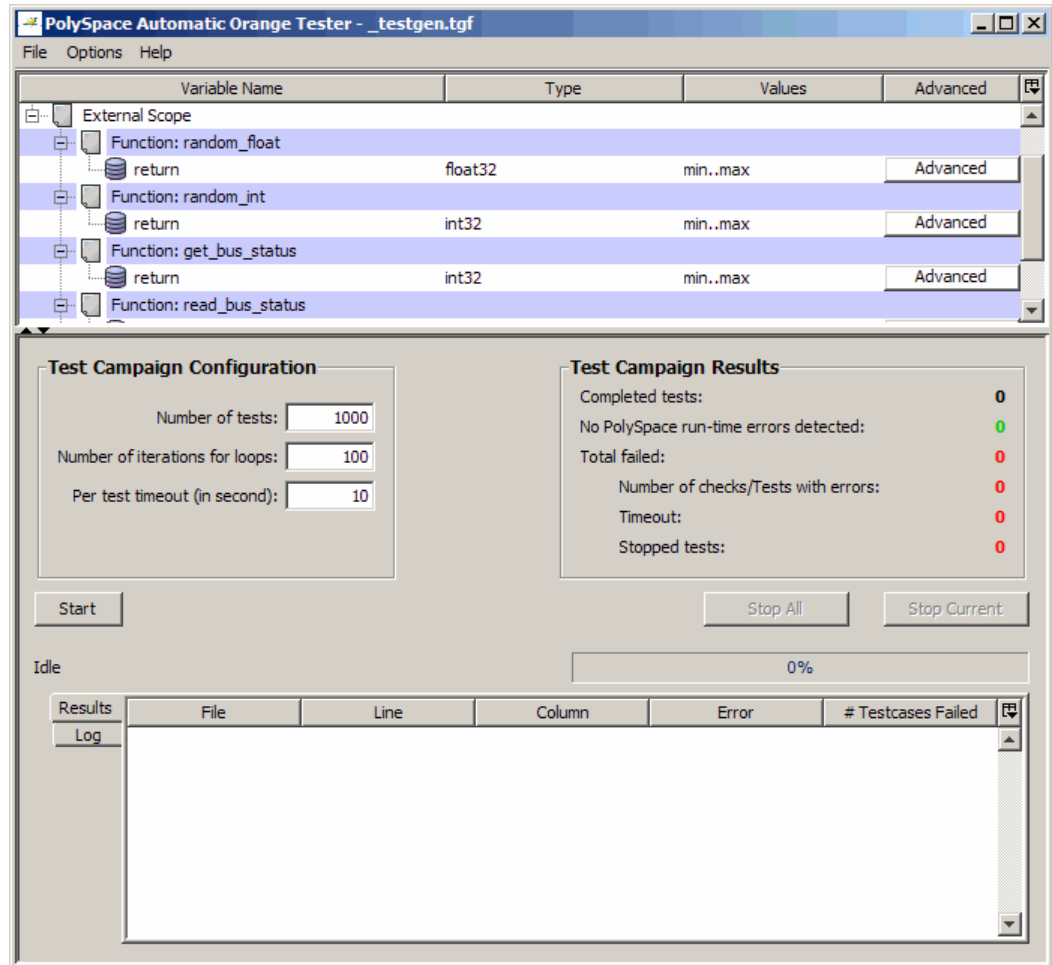
**example.c**

```
37 static void Close_To_Zero (void)
38 {
39 float xmin = random_float();
40 float xmax = random_float();
41 float y;
42
43 if ((xmax < xmin) < 1.0E-37f)
44 {
45 y = 1.0f;
46 }
47 else
48 { /* division by zero is impossible here */
49 y = (xmax + xmin) / (xmax - xmin);
50 }
51 }
```

Example\_Project    Source file: example.c    example.c    Line: 137    Column: 12

- 2 Click  (Launch the PolySpace Automatic Orange Tester) in the toolbar to open the Automatic Orange Tester.

The Automatic Orange Tester opens.



- 3 In the Test Campaign Configuration window, specify the following parameters:

- **Number of tests** – Specifies the total number of test cases you want to run. Running more tests increases the chances of finding a runtime error, but also takes more time to complete.
  - **Number of iterations for infinite loops** – Specifies the maximum number of loop iterations to perform before the Automatic Orange Tester identifies an infinite loop. A larger number of iterations decreases the chances of incorrectly identifying an infinite loop, but also may take more time to complete.
  - **Per test timeout** – Specifies the maximum time that an individual test can run (in seconds) before the Automatic Orange Tester moves on to the next test. Increasing the time limit reduces the number of tests that timeout, but can also increase the total verification time.
- 4** Click **Start** to begin testing.

The Automatic Orange Tester generates test cases and runs the dynamic tests.



The screenshot shows the PolySpace Automatic Orange Tester interface. The top section displays a list of variables and their values:

| Variable Name             | Type    | Values   | Advanced |
|---------------------------|---------|----------|----------|
| External Scope            |         |          |          |
| Function: random_float    |         |          |          |
| return                    | float32 | min..max | Advanced |
| Function: random_int      |         |          |          |
| return                    | int32   | min..max | Advanced |
| Function: get_bus_status  |         |          |          |
| return                    | int32   | min..max | Advanced |
| Function: read_bus_status |         |          |          |

The middle section shows the Test Campaign Configuration and Test Campaign Results:

**Test Campaign Configuration**

- Number of tests: 1000
- Number of iterations for loops: 100
- Per test timeout (in second): 10

**Test Campaign Results**

- Completed tests: 640
- No PolySpace run-time errors detected: 122
- Total failed: 518
- Number of checks/Tests with errors: 15/518
- Timeout: 0
- Stopped tests: 0

Buttons: Start, Stop All, Stop Current

Running... Time Remaining: 00:00:08 64%

**Results**

| File                   | Line | Column | Error                      | # Testcases Failed |
|------------------------|------|--------|----------------------------|--------------------|
| example.c              | 114  | 19     | OVFL (Scalar Overflow)     | 12                 |
| initialisations.c      | 89   | 7      | NIVL (Non Initialised ...) | 70                 |
| initialisations.c      | 47   | 6      | IDP (Illegal Derefe...     | 139                |
| example.c              | 43   | 12     | OVFL (Float Overflow)      | 21                 |
| example.c              | 26   | 2      | ASRT (User Assertio...     | 24                 |
| single_file_analysis.c | 26   | 137    | ASRT (User Assertio...     | 101                |
| example.c              | 104  | 10     | IDP (Illegal Derefe...     | 27                 |
| single file analysis.c | 25   | 137    | ASRT (User Assertio...     | 53                 |

5 If you want to stop the testing before it completes:

- Click **Stop Current** to stop the current test and move on to the next one.
- Click **Stop All** to immediately stop all tests.

## Reviewing the Test Results

When testing is complete, the Automatic Orange Tester displays an overview of the testing results, along with detailed information about each failed test.

**Test Campaign Configuration**

Number of tests:

Number of iterations for loops:

Per test timeout (in second):

**Test Campaign Results**

Completed tests: **1000**

No PolySpace run-time errors detected: **191**

Total failed: **809**

Number of checks/Tests with errors: **15/809**

Timeout: **0**

Stopped tests: **0**

Start Stop All Stop Current

Test Completed Time Remaining: 00:00:00 100%

| Results | File                   | Line | Column | Error                      | # Testcases Failed |
|---------|------------------------|------|--------|----------------------------|--------------------|
| Log     | example.c              | 114  | 19     | OVFL (Scalar Overflow)     | 23                 |
|         | initialisations.c      | 89   | 7      | NIVL (Non Initialised ...) | 130                |
|         | initialisations.c      | 47   | 6      | IDP (Illegal Derefe...     | 217                |
|         | example.c              | 43   | 12     | OVFL (Float Overflow)      | 29                 |
|         | example.c              | 26   | 2      | ASRT (User Assertio...     | 39                 |
|         | single_file_analysis.c | 26   | 137    | ASRT (User Assertio...     | 150                |
|         | example.c              | 104  | 10     | IDP (Illegal Derefe...     | 38                 |
|         | single file analysis.c | 25   | 137    | ASRT (User Assertio...     | 80                 |

## Test Campaign Results

The Test Campaign Results window displays overview information about the results of your dynamic tests, including:

- **Completed tests** – Displays the total number of tests completed.
- **No PolySpace runtime errors detected** – Displays the number of tests that did not produce a runtime error.
- **Total failed** – Displays the number of tests that produced a runtime error.
- **Number of checks/Tests with errors** – Displays the number of PolySpace checks that produced at least one failed test, as well as the total number of tests that produced a runtime error.

- **Timeout** – Displays the number of tests that exceeded the specified **Per test timeout** limit.
- **Stopped tests** – The number of tests that were stopped manually.

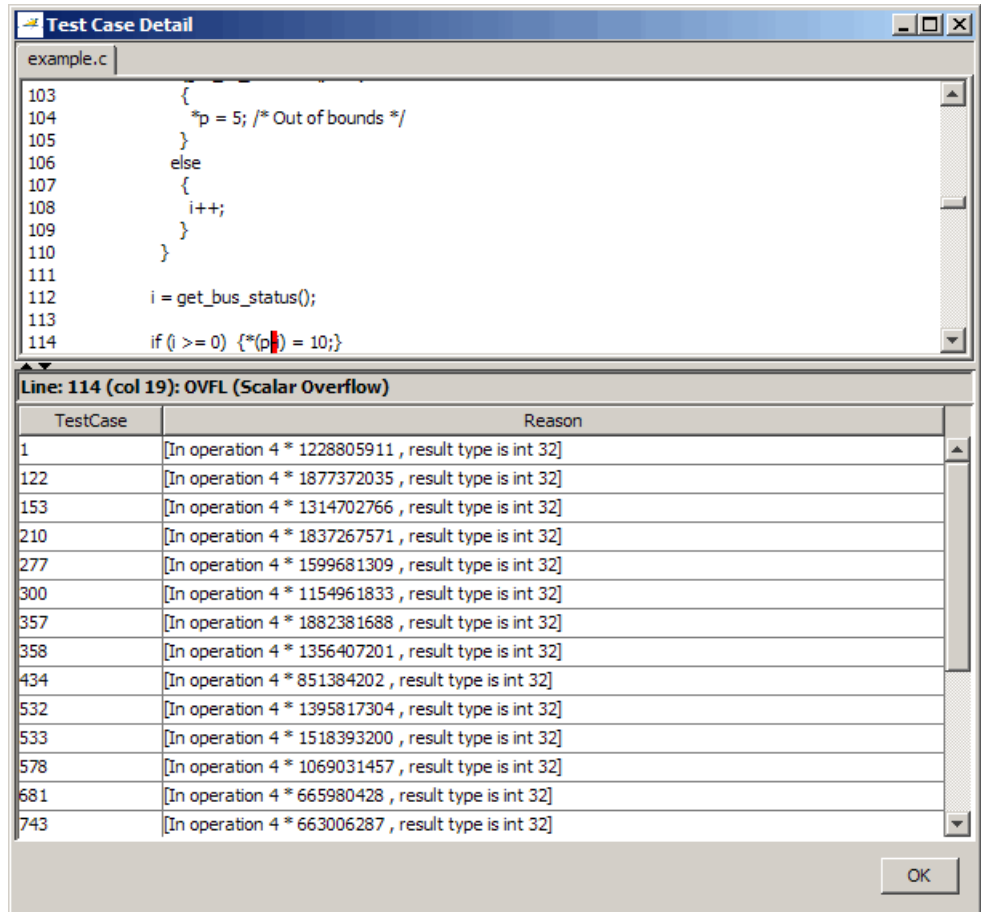
Use the Test Campaign Results Window to see an overall assessment of your test results, as well as to decide if you need to increase the **Per test timeout** value.

### **Results Table**

The Results table displays detailed information about each failed test, to help you identify the cause of the runtime error. This information includes:

- The filename, line number, and column in which the error was found.
- The type of error that occurred.
- The number of test cases in which the error occurred.

In addition, You can view more details about any failed test by clicking on the appropriate row in the Results table. The Test Case Detail dialog box opens.



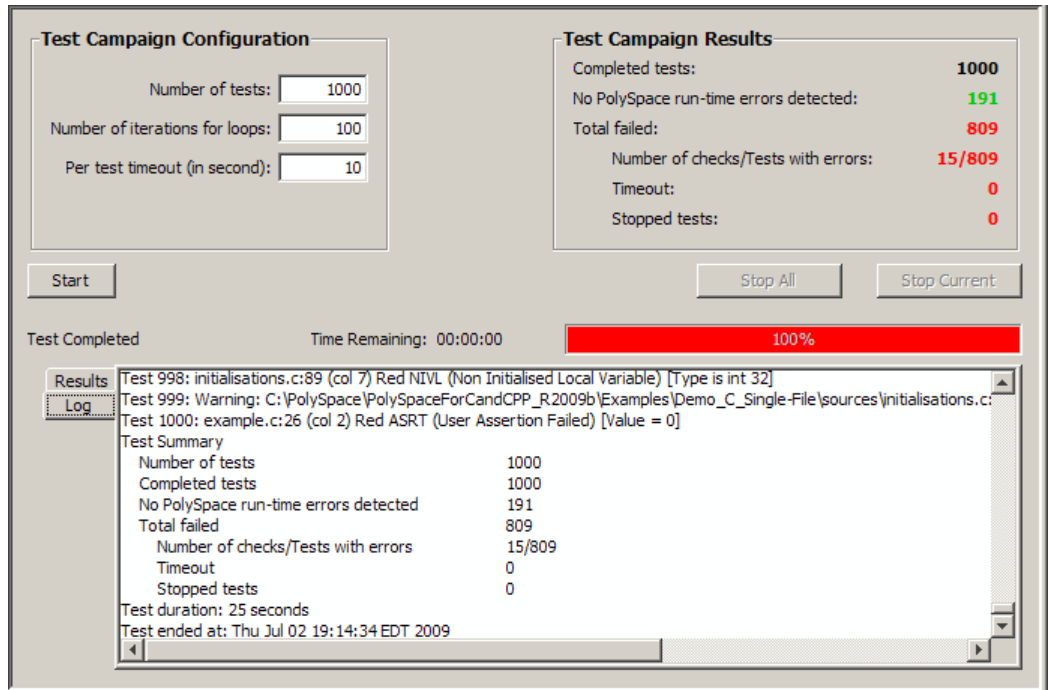
The Test Case Detail dialog box displays the portion of the code in which the error occurred, and gives detailed information about why each test case failed. Since the Automatic Orange Tester performs runtime tests, this information includes the actual values that caused the error.

You can use this information to quickly identify the cause of the error, and determine if there is an actual bug in the code.

## Log

The Log window displays a complete list of all the tests which failed, as well as summary information.

You can copy information from the log window to paste into other applications, such as Microsoft® Excel®.



The log file is also saved in the PolySpace-Instrumented directory with the following filename:

`TestGenerator_day_month_year-time.out`

## Refining Data Ranges

The Automatic Orange Tester allows you to specify ranges for external variables. This allows you to perform runtime tests using real-world values for your variables, rather than randomly selected values.

Setting ranges for your variables reduces the number of tests that fail due to unrealistic data values, allowing you to focus on actual problems, rather than purely theoretical problems.

To refine your data ranges:

- 1 In the Variables section at the top of the Automatic Orange Tester, identify the variable for which you want to set a data range.

The screenshot shows the PolySpace Automatic Orange Tester interface. The top section displays a list of variables with their names, types, and current values. The 'Advanced' column for each variable has a button to open configuration options.

| Variable Name             | Type         | Values   | Advanced |
|---------------------------|--------------|----------|----------|
| External Scope            |              |          |          |
| Function: random_float    |              |          |          |
| return                    | float32      | min..max | Advanced |
| Function: random_int      |              |          |          |
| return                    | int32        | min..max | Advanced |
| Function: get_bus_status  |              |          |          |
| return                    | int32        | min..max | Advanced |
| Function: read_bus_status |              |          |          |
| return                    | int32        | min..max | Advanced |
| SEND_MESSAGE              |              |          |          |
| +1                        | const int8 * | min..max | Advanced |

The bottom section shows the Test Campaign Configuration and Test Campaign Results.

**Test Campaign Configuration**

- Number of tests: 1000
- Number of iterations for loops: 100
- Per test timeout (in second): 10

**Test Campaign Results**

- Completed tests: 1000
- No PolySpace run-time errors detected: 191
- Total failed: 809
- Number of checks/Tests with errors: 15/809
- Timeout: 0
- Stopped tests: 0

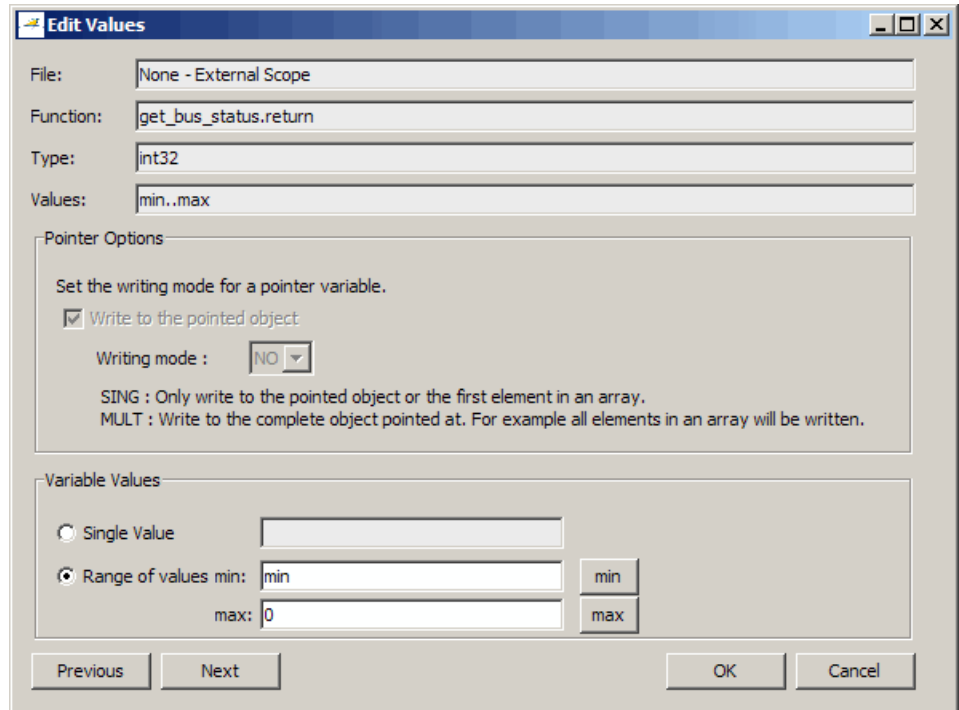
Buttons: Start, Stop All, Stop Current

Test Completed: Time Remaining: 00:00:00, Progress: 100%

**Results**

| File                   | Line | Column | Error                    | # Testcases Failed |
|------------------------|------|--------|--------------------------|--------------------|
| example.c              | 114  | 19     | OVFL (Scalar Overfl...   | 23                 |
| initialisations.c      | 89   | 7      | NIVL (Non Initialised... | 130                |
| initialisations.c      | 47   | 6      | IDP (Illegal Derefere... | 217                |
| example.c              | 43   | 12     | OVFL (Float Overflow)    | 29                 |
| example.c              | 26   | 2      | ASRT (User Assertio...   | 39                 |
| single_file_analysis.c | 26   | 137    | ASRT (User Assertio...   | 150                |

**2** Select **Advanced**. The Edit Values dialog box opens.



**3** Set the appropriate values for the variable:

**Single Value** – Specifies a constant value for the variable.

**Range of values**, – Specifies a minimum and maximum value for the variable.

---

**Note** For pointers, you can also specify the writing mode:

**SING** – The tests only write the object or first element in the array.

**MULT** – The tests write the complete object, or all elements in the array.

---

- 4 Click **Next** to edit the values for the next variable.
- 5 When you have finished setting values, click **OK** to save your changes and close the Edit Values dialog box.
- 6 Click **Start** to retest the code.

The Automatic Orange Tester generates test cases, runs the tests, and displays the updated results.



The screenshot displays the PolySpace Automatic Orange Tester interface. The top section shows a tree view of the test campaign configuration with the following details:

| Variable Name             | Type    | Values      | Advanced |
|---------------------------|---------|-------------|----------|
| External Scope            |         |             |          |
| Function: random_float    |         |             |          |
| return                    | float32 | 0..10000000 | Advanced |
| Function: random_int      |         |             |          |
| return                    | int32   | min..0      | Advanced |
| Function: get_bus_status  |         |             |          |
| return                    | int32   | -100..0     | Advanced |
| Function: read_bus_status |         |             |          |
| return                    | int32   | min..max    | Advanced |
| Function: read_on_bus     |         |             |          |

The bottom section shows the Test Campaign Configuration and Test Campaign Results:

**Test Campaign Configuration**

- Number of tests: 1000
- Number of iterations for infinite loops: 100
- Per test timeout (in second): 10

**Test Campaign Results**

- Completed tests: 1000
- No PolySpace run-time errors detected: 997
- Total failed: 3
- Number of checks/Tests with errors: 1/3
- Timeout: 0
- Stopped tests: 0

Buttons: Start, Stop All, Stop Current

Test Completed: Time Remaining: 0:0:0, 100%

| Results | File      | Line | Column | Error                     | # Testcases Failed |
|---------|-----------|------|--------|---------------------------|--------------------|
| Log     | example.c | 114  | 16     | IDP (Illegal Dereferen... | 3                  |

The updated results show fewer failed tests, allowing you to focus in on any actual code problems.

## Saving and Reusing Your Configuration

You can save your Automatic Orange Tester preferences and variable ranges for use in future dynamic testing.

To save your configuration:

- 1 Select **File > Save**.
- 2 Enter an appropriate name and click **Save**.

Your configuration is saved in a `.tgf` file.

To open a configuration from a previous verification:

- 1 Select **File > Open**.
- 2 Select the appropriate `.tgf` file, then click **Open**.

The configuration is opened.

When you open a previously saved configuration, the **Log** window displays any differences in the configuration files. For example:

- If a variable does not exist in the new configuration, a warning is displayed.
- If the ranges for a variable are no longer valid (if the variable type changes, for example), a warning is displayed and the range is changed to the largest valid range for the new data type (if possible).

### **Exporting Data Ranges for PolySpace Verification**

Once you have set the data ranges for your variables, you can export them to a Data Range Specifications (DRS) file for use in future PolySpace verifications. This allows you to reduce the number of orange checks identified in the PolySpace Viewer.

To export your data ranges:

- 1 Set the appropriate values for each variable you want to specify.
- 2 Select **File > Export DRS**.
- 3 Enter an appropriate name and click **Save**.

The DRS file is saved.

For information on using a DRS file for PolySpace verifications, see “Applying Data Ranges to External Variables and Stub Functions (DRS)” on page 4-26.

## **Configuring Compiler Options**

On UNIX, Solaris, or Linux systems, you must configure your compiler and linker options before using the Automatic Orange Tester.

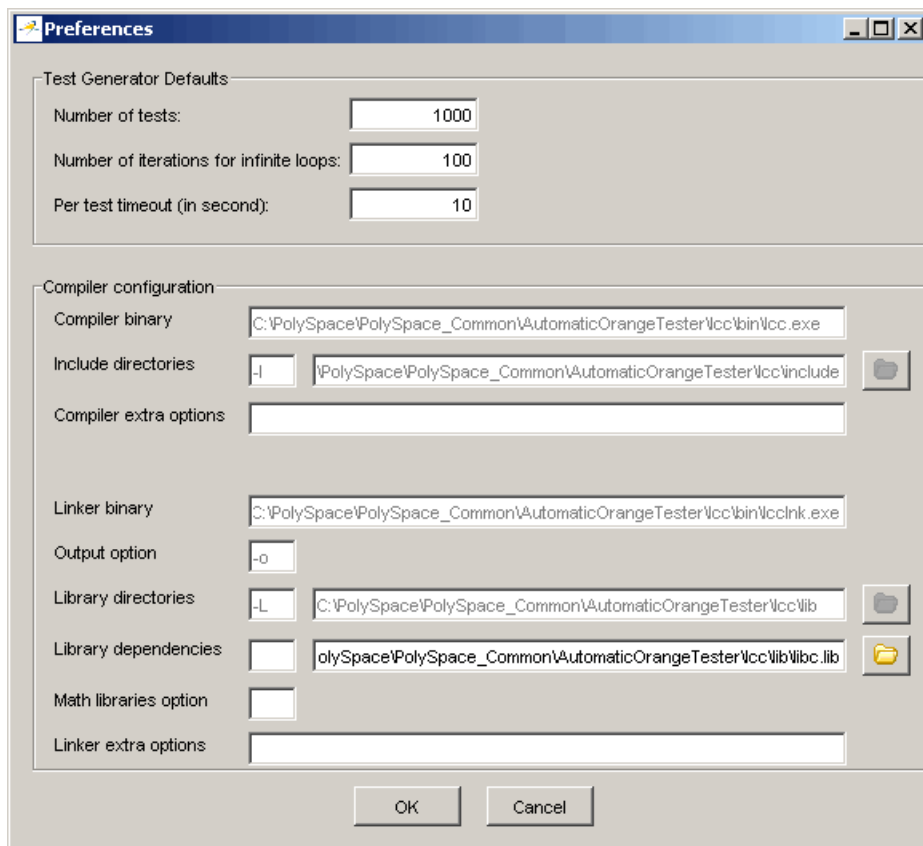
---

**Note** On Windows systems, the compiler options cannot be modified. You can only configure the library dependencies.

---

To set compiler and linker options:

- 1** Open the Automatic Orange Tester, as described above.
- 2** Select **Options > Configure**.
- 3** The Preferences dialog box opens.



**4** Set the appropriate parameters for your compiler.

## Technical Limitations

The Automatic Orange Tester has the following limitations:

- “Unsupported PolySpace Options” on page 9-59
- “Options with Limitations” on page 9-59
- “Unsupported C Language Constructions” on page 9-59

## Unsupported PolySpace Options

The following options are not supported when you select `-prepare-automatic-tests`.

- `-entry-points`
- `-dialect`
- `-ignore-float-rounding`
- `-div-round-down`
- `-char-is-16its`
- `-short-is-8bits`
- `-respect-types-in-globals`
- `-respect-types-in-fields`

In addition, Global asserts in the code of the form `Pst_Global_Assert(A,B)` are not supported with the Automatic Orange Tester.

## Options with Limitations

The following options cannot take specific values when you select `-prepare-automatic-tests`.

- `-target [tms320c3c | sharc21x61]`
- `-data-range-specification` (in global assert mode)

## Unsupported C Language Constructions

The code verification stops when any of the following characteristics are met:

- ANSI C99 long long and long double types are unsupported for Windows systems
- Calls to following routines are unsupported:
  - va\_start
  - va\_arg
  - va\_end
  - va\_copy
  - setjmp
  - sigsetjmp
  - longjmp
  - siglongjmp

The following C language constructions are ignored:

- The endianness of the target is not managed. The tests are performed as if the user-defined target has the same endianness as the hardware on which the Automatic Orange Tester is running
- Calls to the following routines are ignored:
  - signal
  - sigset
  - sighold
  - sigrelse
  - sigpause
  - sigignore
  - sigaction
  - sigpending
  - sigsuspend
  - sigvec
  - sigblock

- sigsetmask
- sigprocmask
- siginterrupt
- srand
- srandom
- initstate
- setstate





# Day to Day Use

---

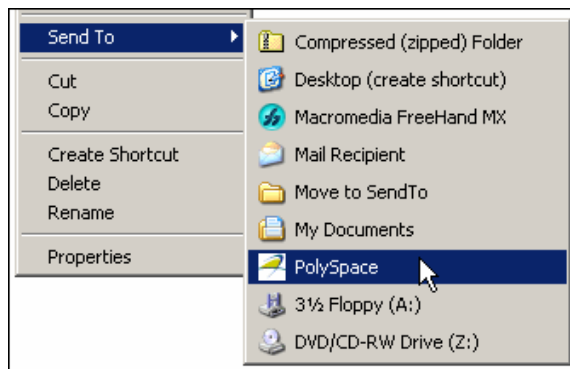
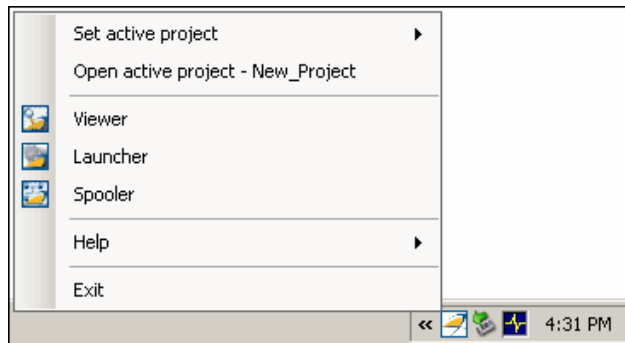
- “PolySpace In One Click Overview” on page 10-2
- “Using PolySpace In One Click” on page 10-3

## PolySpace In One Click Overview

Most developers verify the same files multiple times (writing new code, unit testing, integration), and usually need to run verifications on multiple project files using the same set of options. In a Microsoft Windows environment, PolySpace In One Click provides a convenient way to streamline your work when verifying several files using the same set of options.

Once you have set up a project file with the options you want, you designate that project as the *active project*, and then send the source files to PolySpace software for verification. You do not have to update the project with source file information.

On a Windows systems, the plug-in provides a PolySpace Toolbar in the Windows Taskbar, and a **Send To** option on the desktop pop-up menu:



## Using PolySpace In One Click

### In this section...

“PolySpace In One Click Workflow” on page 10-3

“Setting the Active Project” on page 10-3

“Launching Verification” on page 10-5

“Using the Taskbar Icon” on page 10-8

## PolySpace In One Click Workflow

Using PolySpace In One Click involves two steps:

- 1 Setting the active project.
- 2 Sending files to PolySpace software for verification.

## Setting the Active Project

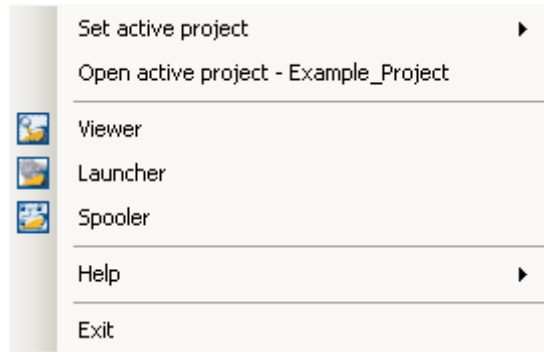
The active project is the project that PolySpace In One Click uses to verify the files that you select. Once you have set an active project, it remains active until you change the active project. PolySpace software uses the analysis options from the project; it does not use the source files or results directory from the project.

To set the active project:

- 1 Right-click the PolySpace In One Click icon in the taskbar area of your Windows desktop:

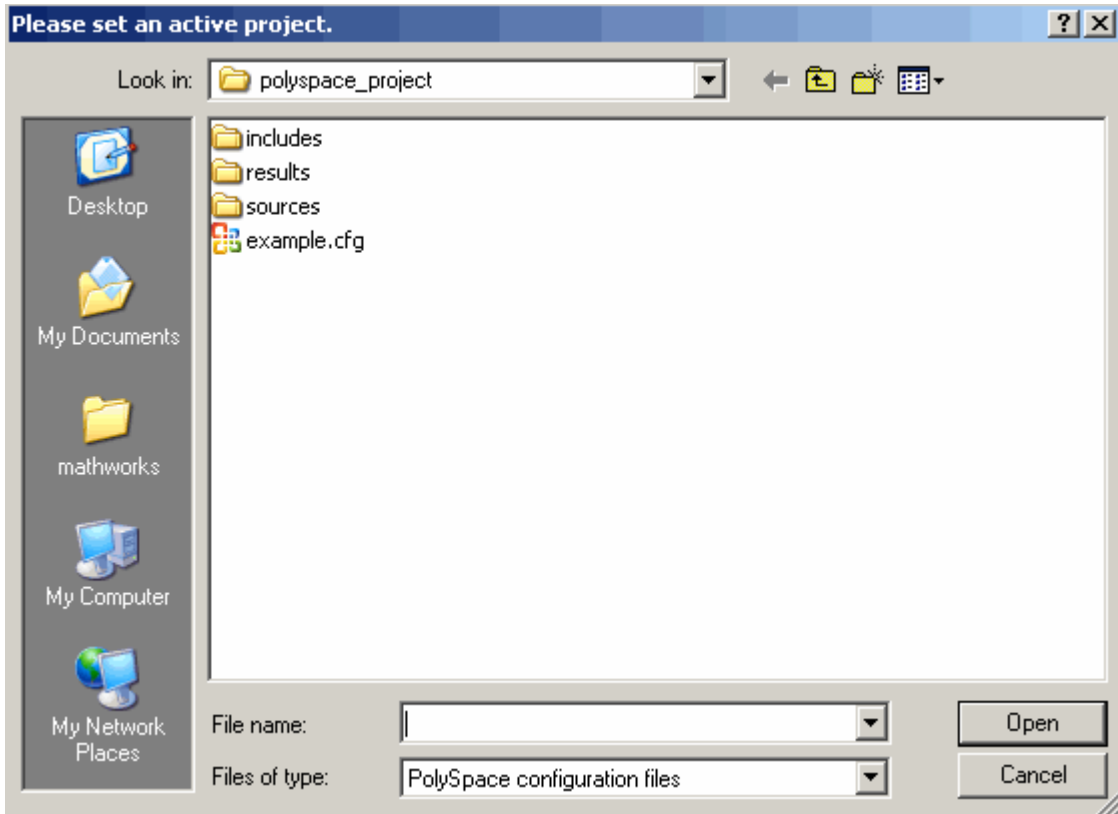


The context menu appears.



**2** Select **Set active project > Browse** from the menu.

The **Please set an active project** dialog box appears:



- 3 Select the project you want to use as the active project.
- 4 Click **Open** to apply the changes and close the dialog box.

---

**Note** You can also set the active project by right-clicking on a project file (.cfg or .dsk) file and selecting **Send To > PolySpace**.

---

## Launching Verification

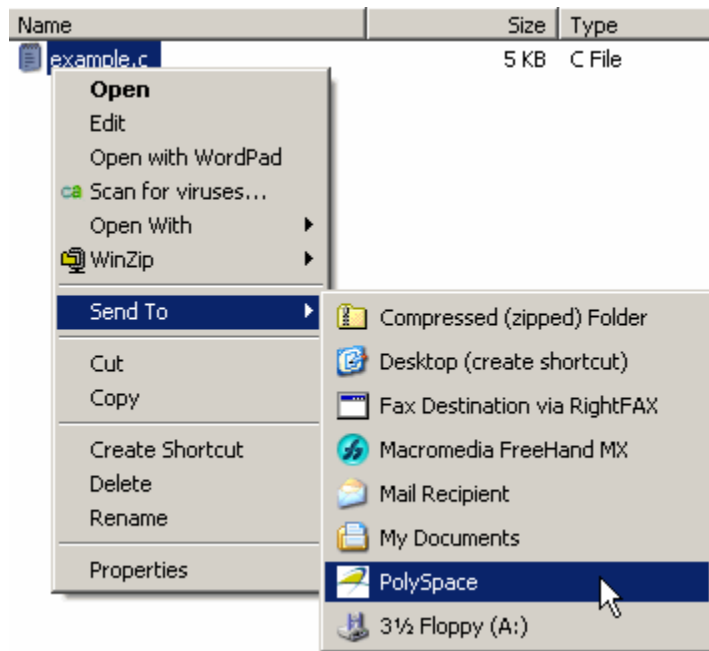
PolySpace in One Click allows you to send multiple files to PolySpace software for verification.

To send a file to PolySpace software for verification:

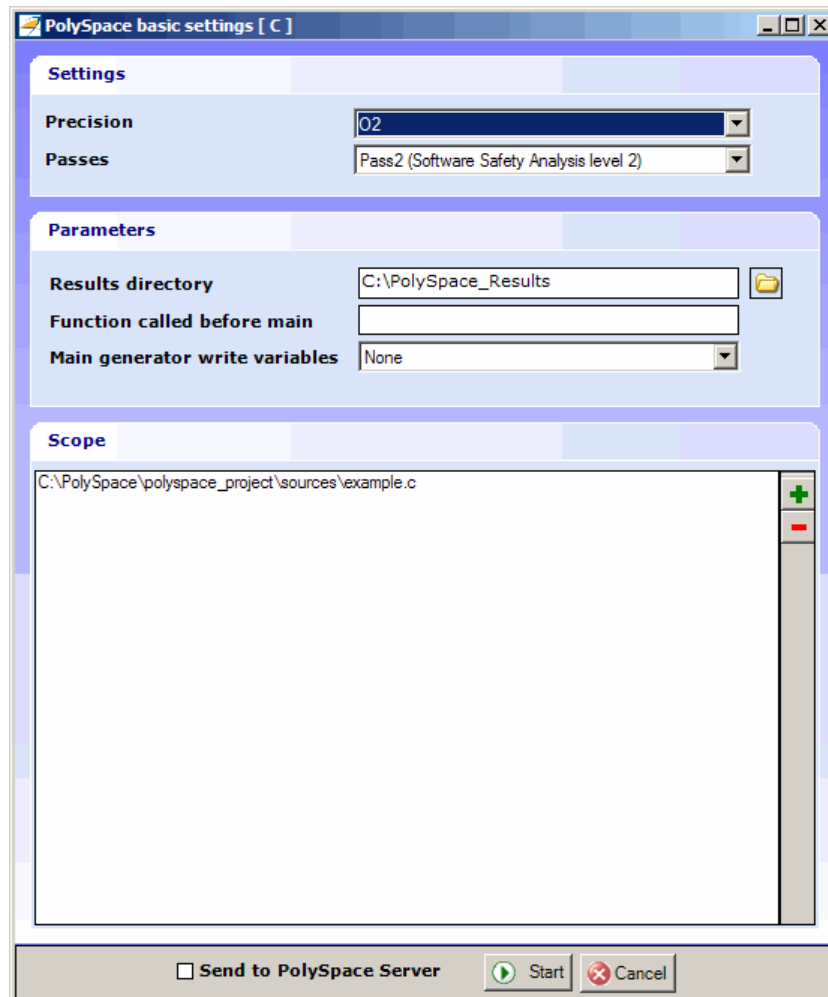
- 1** Navigate to the directory containing the source files you want to verify.
- 2** Right-click the file you want to verify.

The context menu appears.

- 3** Select **Send To > PolySpace**.



The **PolySpace basic settings** dialog box appears.



---

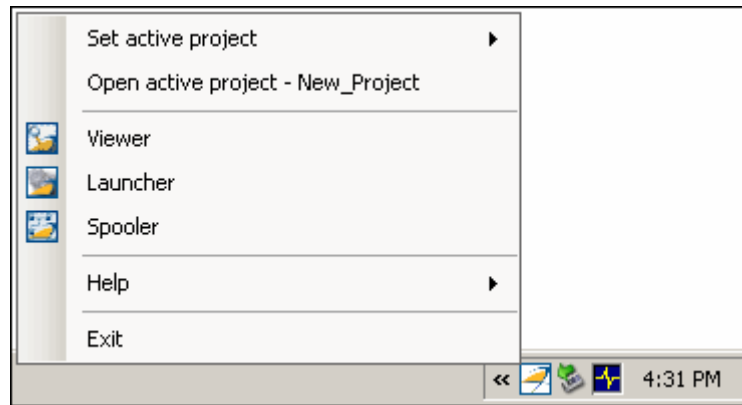
**Note** The options you specify the basic settings dialog box override any options set in the configuration file. These options are also preserved between verifications.

---

- 4 Enter the appropriate parameters for your verification.



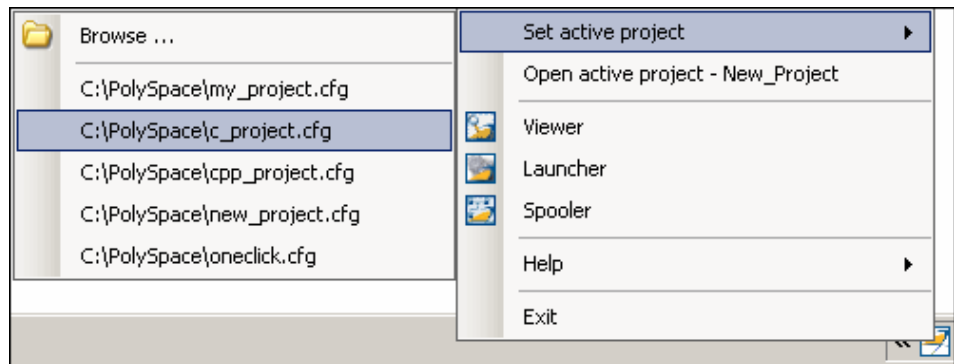




Click the PolySpace Taskbar Icon, then select one of the following options:

- **Set active project** — Allows you to set the active configuration file. Before you start, you have to choose a PolySpace configuration file which contains the common options. You can choose a template of a previous project and move it to your working directory.

A standard file browser allows you to choose the configuration file. If you have multiple configuration files, you can quickly switch between them using the browse history.



---

**Note** No configuration file is selected by default. You can create an empty file with a .cfg extension.

---

- **Open active project** — Opens the active configuration file. This allows you to update the project using the standard PolySpace Launcher graphical interface. It allows you to specify all PolySpace common options, including directives of compilation, options, and paths of standard and specific headers. It does not affect the precision of a verification or the results directory.
- **Viewer** — Opens the PolySpace viewer. This allows you to review verification results in the standard graphical interface. In order to load results into the viewer, you must choose a verification to review in the Verification Log window.
- **Launcher** — Opens the PolySpace Launcher. This allows you to launch a verification using the standard PolySpace graphical interface.
- **Spooler** — Opens the PolySpace Spooler. If you selected a server verification in the “PolySpace Preferences” dialog box, the spooler allows you to follow the status of the verification.

# MISRA Checker

---

- “PolySpace MISRA Checker Overview” on page 11-2
- “Setting Up MISRA C Checking” on page 11-4
- “Running a Verification with MISRA C Checking” on page 11-10
- “Rules Supported” on page 11-14
- “Rules Partially Supported” on page 11-40
- “Rules Not Checked” on page 11-51

## PolySpace MISRA Checker Overview

PolySpace software can check that C code complies with MISRA C 2004 standards.<sup>10</sup>

---

**Note** The PolySpace MISRA checker is based on MISRA C:2004 (<http://www.misra-c.com>).

---

The MISRA checker enables PolySpace software to provide messages when MISRA C rules are not respected. Most messages are reported during the compile phase of a verification. The MISRA checker can check nearly all of the 141 MISRA C:2004 rules.

These 142 rules are divided in three categories:

- **102** required and advisory rules fully supported. PolySpace software can check all these rules without any limitations. See “Rules Supported” on page 11-14.
- **20** required and advisory rules partially supported. PolySpace software can check all these rules with some limitations. These limitations are described in the associated “**Note**” paragraph for each rule. See “Rules Partially Supported” on page 11-40.
- **20** required and advisory rules which cannot be verified by PolySpace software. These rules cannot be verified because they are outside the scope of PolySpace verification. They may concern documentation, dynamic aspects or functional aspects of MISRA rules. These rules are not checked. The “**comment**” column details the reason. See “Rules Not Checked” on page 11-51.

---

10. MISRA and MISRA C are registered trademarks of MISRA Ltd., held on behalf of the MISRA Consortium.

---

**Note** Every violation, warning or error, will be written in the log file at compilation time of a PolySpace verification, except for rules 9.1 (NIV checks), 12.11 (OVFL check using `-detect-unsigned-overflows`), 13.7 (gray checks), 14.1 (gray checks), 16.2 (Call graph) and 21.1 (all runtime errors).

---

You will find a set of required and advisory MISRA rules in “Applying Coding Rules to Reduce Orange Checks” on page 9-12 which can have direct or indirect impact on the PolySpace selectivity (reliability percentage).

---

**Note** If any of the input source files do not compile, MISRA C checking will be incomplete.

---

## Setting Up MISRA C Checking

### In this section...

“Checking Compliance with MISRA C Coding Rules” on page 11-4

“Creating a MISRA C Rules File” on page 11-5

“Excluding Files from the MISRA C Checking” on page 11-7

“Configuring Text and XML Editors” on page 11-8

### Checking Compliance with MISRA C Coding Rules

To check MISRA C compliance, you set an option in your project before running a verification. PolySpace software finds the violations during the compile phase of a verification. When you have addressed all MISRA C violations, you run the verification again.

To set the MISRA C checking option:

- 1 In the Analysis options section of the Launcher window, expand **Compliance with standards**.

The Compliance with standards options appear.

- 2 Select the **Check MISRA-C:2004 rules** check box.
- 3 Expand the **Check MISRA-C:2004 rules** option.

Two options, **Rules configuration** and **Files and directories to ignore**, appear.

| Name                                  | Value                               |     | Internal name       |
|---------------------------------------|-------------------------------------|-----|---------------------|
| Analysis options                      |                                     |     |                     |
| + General                             |                                     |     |                     |
| + Target/Compilation                  |                                     |     |                     |
| - Compliance with standards           |                                     |     |                     |
| - Code from DOS or Windows filesystem | <input checked="" type="checkbox"/> |     | -dos                |
| + Embedded assembler                  |                                     |     |                     |
| + Strict                              | <input type="checkbox"/>            |     | -strict             |
| + Permissive                          | <input type="checkbox"/>            |     | -permissive         |
| - Check MISRA-C:2004 rules            | <input checked="" type="checkbox"/> |     |                     |
| - Rules configuration                 |                                     | ... | -misra2             |
| - Files and directories to ignore     |                                     | ... | -includes-to-ignore |
| + KeilMAR support                     | default                             | ▼   | -dialect            |
| + PolySpace inner settings            |                                     |     |                     |
| + Precision/Scaling                   |                                     |     |                     |
| + Multitasking                        |                                     |     |                     |


- 4** Specify which MISRA C rules to check and which, if any, files to exclude from the checking.

## Creating a MISRA C Rules File

You must have a rules file to run a verification with MISRA C checking.

### Opening a New Rules File

To open a new rules file:

- 1 Click the button  to the right of the **Rules configuration** option.

A window for opening or creating a MISRA C rules file appears.

- 2 Select **File > New File**.

A table of rules appears.

| Rules                                                                                                   | Error                            | Warning                          | Off                              |
|---------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|----------------------------------|
| MISRA C rules                                                                                           |                                  |                                  |                                  |
| — Number of rules by mode :                                                                             | 7                                | 1                                | 134                              |
| +1 Environment                                                                                          |                                  |                                  |                                  |
| +2 Language extensions                                                                                  |                                  |                                  |                                  |
| +3 Documentation                                                                                        |                                  |                                  |                                  |
| +4 Character sets                                                                                       |                                  |                                  |                                  |
| +5 Identifiers                                                                                          |                                  |                                  |                                  |
| +6 Types                                                                                                |                                  |                                  |                                  |
| +7 Constants                                                                                            |                                  |                                  |                                  |
| +8 Declarations and definitions                                                                         |                                  |                                  |                                  |
| +9 Initialisation                                                                                       |                                  |                                  |                                  |
| +10 Arithmetic type conversions                                                                         |                                  |                                  |                                  |
| +11 Pointer type conversions                                                                            |                                  |                                  |                                  |
| +12 Expressions                                                                                         |                                  |                                  |                                  |
| +13 Control statement expressions                                                                       |                                  |                                  |                                  |
| +14 Control flow                                                                                        |                                  |                                  |                                  |
| +15 Switch statements                                                                                   |                                  |                                  |                                  |
| -16 Functions                                                                                           |                                  |                                  |                                  |
| —16.1 Functions shall not be defined with variable numbers of arguments.                                | <input type="radio"/>            | <input type="radio"/>            | <input checked="" type="radio"/> |
| —16.2 Functions shall not call themselves, either directly or indirectly.                               | <input type="radio"/>            | <input type="radio"/>            | <input checked="" type="radio"/> |
| —16.3 Identifiers shall be given for all of the parameters in a function prototype.                     | <input checked="" type="radio"/> | <input type="radio"/>            | <input type="radio"/>            |
| —16.4 The identifiers used in the declaration and definition of a function shall match.                 | <input type="radio"/>            | <input type="radio"/>            | <input checked="" type="radio"/> |
| —16.5 Functions with no parameters shall be declared with parameter type void.                          | <input type="radio"/>            | <input type="radio"/>            | <input checked="" type="radio"/> |
| —16.6 The number of arguments passed to a function shall match the number in the function prototype.    | <input type="radio"/>            | <input type="radio"/>            | <input checked="" type="radio"/> |
| —16.7 A pointer parameter in a function prototype should be declared as pointer to const.               | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> |
| —16.8 All exit paths from a function with non-void return type shall have an explicit return statement. | <input type="radio"/>            | <input type="radio"/>            | <input checked="" type="radio"/> |
| —16.9 A function identifier shall only be used with either a preceding &, or with a preceding *.        | <input type="radio"/>            | <input type="radio"/>            | <input checked="" type="radio"/> |
| —16.10 If a function returns error information, then that error information shall be checked.           | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> |
| -17 Pointer and arrays                                                                                  |                                  |                                  |                                  |
| —17.1 Pointer arithmetic shall only be applied to pointers that address an array.                       | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> |
| —17.2 Pointer subtraction shall only be applied to pointers that address elements of an array.          | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> |
| —17.3 >, >=, <, <= shall not be applied to pointer types except where they point to the same object.    | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> |
| —17.4 Array indexing shall be the only allowed form of pointer arithmetic.                              | <input type="radio"/>            | <input checked="" type="radio"/> | <input type="radio"/>            |
| —17.5 The declaration of objects should contain no more than 2 levels of pointer indirection.           | <input type="radio"/>            | <input type="radio"/>            | <input checked="" type="radio"/> |
| —17.6 The address of an object with automatic storage shall not be assigned to a pointer.               | <input type="radio"/>            | <input type="radio"/>            | <input checked="" type="radio"/> |
| +18 Structures and unions                                                                               |                                  |                                  |                                  |
| +19 Preprocessing directives                                                                            |                                  |                                  |                                  |
| +20 Standard libraries                                                                                  |                                  |                                  |                                  |
| +21 Run-time failures                                                                                   |                                  |                                  |                                  |



**3** For each rule, you specify one of these states:

| State   | Causes the verification to...                                                 |
|---------|-------------------------------------------------------------------------------|
| Error   | End after the compile phase when this rule is violated.                       |
| Warning | Display warning message and continue verification when this rule is violated. |
| Off     | Skip checking of this rule.                                                   |

**Note** The default state for most rules is **Warning**. The state for rules that have not yet been implemented is **Off**. Some rules always have state **Error** (you cannot change the state of these).

**4** Click **OK** to save the rules and close the window.


The **Save as** dialog box opens.

**5** In **File**, enter a name for the rules file.

**6** Click **OK** to save the file and close the dialog box.

## Excluding Files from the MISRA C Checking

You can exclude files from MISRA C checking. You might want to exclude some included files. To exclude `math.h` from the MISRA C checking of the project `example.cfg`:

**1** Click the button  to the right of the **Files and directories to ignore** option.

**2** Click the folder icon.



The **Select a file or directory to include** dialog box appears.

**3** Select the files or directories (such as include files) you want to ignore.

**4** Click **OK**.

The selected files appear in the list of files to ignore.

**5** Click **OK** to close the dialog box.

## **Configuring Text and XML Editors**

Before you check MISRA rules, you should configure your text and XML editors in the Launcher. Configuring text and XML editors in the Launcher allows you to view source files and MISRA reports directly from the MISRA-C log in the launcher.

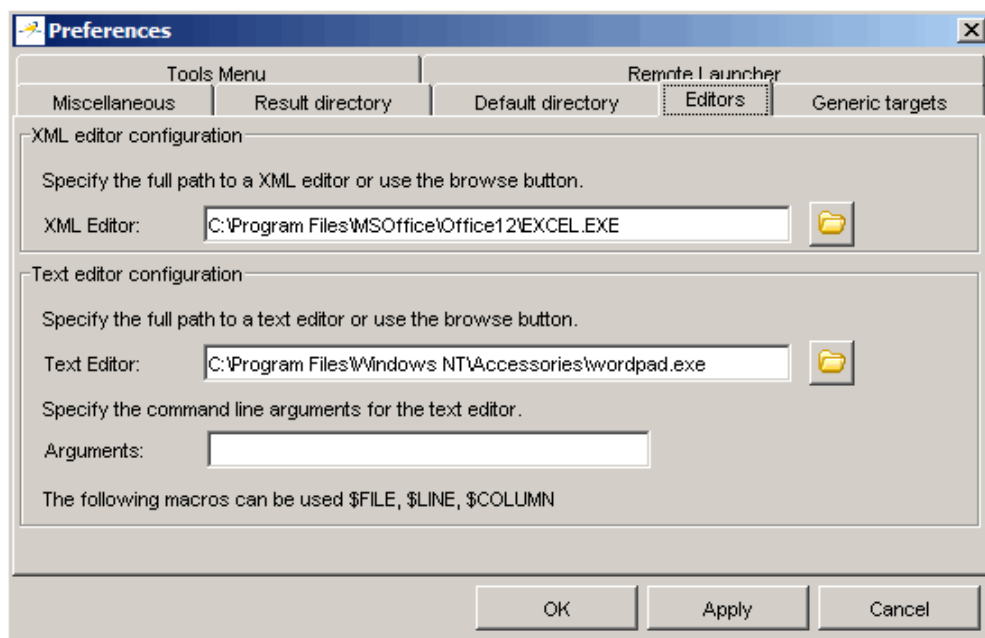
To configure your text and .XML editors:

**1** Select **Edit > Preferences**.

The Preferences dialog box opens.

**2** Select the **Editors** tab.

The Editors tab opens.



- 3** Specify an XML editor to use to view MISRA-C reports.
- 4** Specify a Text editor to use to view source files from the Launcher logs.
- 5** Click **OK**.

## Running a Verification with MISRA C Checking

### In this section...

“Starting the Verification” on page 11-10

“Examining the MISRA C Log” on page 11-11

“Opening MISRA-C Report” on page 11-12

### Starting the Verification

When you run a verification with the MISRA C option selected, the verification checks most of the MISRA C rules during the compile phase.<sup>11</sup>

---

**Note** Some rules address run-time errors.

---

The verification stops if there is a violation of a rule with state Error.

To start the verification:

1 Click the **Start** button

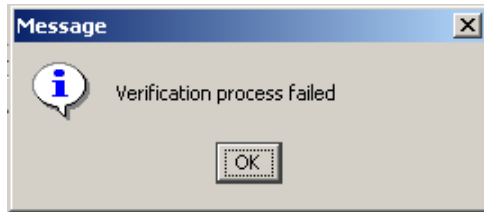


2 If you see a caution that PolySpace software will remove existing results from the results directory, click **Yes** to continue and close the message dialog box.

If the verification fails because of MISRA C violations. A message dialog box appears.

---

11. MISRA and MISRA C are registered trademarks of MISRA Ltd., held on behalf of the MISRA Consortium.



**3** Click **OK**.

---

**Note** If any of the input source files do not compile, MISRA C checking will be incomplete.

---

## Examining the MISRA C Log

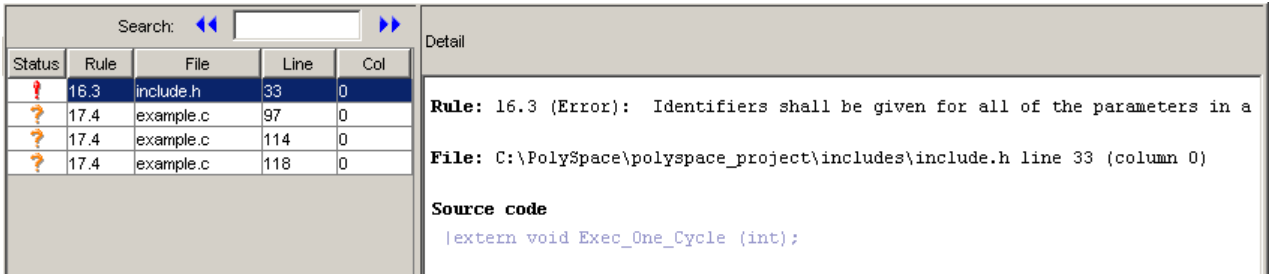
To examine the MISRA C violations:

**1** Click the **MISRA-C** button in the log area of the Launcher window.

A list of MISRA C violations appear in the log part of the window.

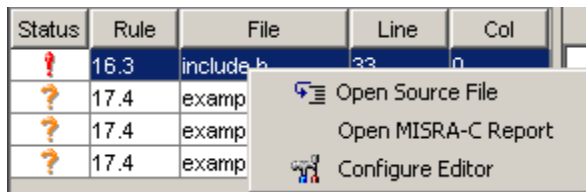
```
ERROR : rule 16.3 (required) violated. At : C:\po:
 | identifiers shall be given for all of the
WARNING : rule 17.4 (required) violated. At : exar
 | array indexing shall be the only allowed
WARNING : rule 17.4 (required) violated. At : exar
 | array indexing shall be the only allowed
```

**2** Click on any of the violations to see a description of the violated rule, the full path of the file in which the violation was found, and the source code containing the violation.



In this example, the log reports a violation of rule 16.3. A function prototype declaration in `include.h` is missing an identifier.

- 3 Right click the row containing the violation, then select Open Source File.



The appropriate file opens in your text editor.

---

**Note** You must configure a text editor before you can open source files. See “Configuring Text and XML Editors” on page 11-8.

---

- 4 Correct the MISRA violation and run the verification again.

## Opening MISRA-C Report

After you check MISRA rules, you can generate an XML report containing all the errors and warnings reported by the MISRA-C checker.

---

**Note** You must configure an XML editor before you can open a MISRA-C report. See “Configuring Text and XML Editors” on page 11-8.

---

To view the MISRA-C report:

- 1 Click the **MISRA-C** button in the log area of the Launcher window.

A list of MISRA C violations appear in the log part of the window.

- 2 Right click any row in the log, and select **Open MISRA-C Report**.

| Status | Rule | File      | Line | Col |
|--------|------|-----------|------|-----|
| !      | 16.3 | include.h | 33   | 0   |
| ?      | 17.4 | examp     |      |     |
| ?      | 17.4 | examp     |      |     |
| ?      | 17.4 | examp     |      |     |

|                     |
|---------------------|
| Open Source File    |
| Open MISRA-C Report |
| Configure Editor    |

The report opens in your XML editor.

The screenshot shows a Microsoft Excel spreadsheet with the following data:

| Name | Mode     | Report  | File                                              | Line | Column | Message                                                                  |
|------|----------|---------|---------------------------------------------------|------|--------|--------------------------------------------------------------------------|
| 16.3 | required | error   | C:\PolySpace\polyspace_project\includes\include.h | 33   | 0      | Identifiers shall be given for all of the parameters in a function proto |
| 17.4 | required | warning | example.c                                         | 97   | 0      | Array indexing shall be the only allowed form of pointer arithmetic.     |
| 17.4 | required | warning | example.c                                         | 114  | 0      | Array indexing shall be the only allowed form of pointer arithmetic.     |
| 17.4 | required | warning | example.c                                         | 118  | 0      | Array indexing shall be the only allowed form of pointer arithmetic.     |

## Rules Supported

| <b>In this section...</b>                     |
|-----------------------------------------------|
| “Language Extensions” on page 11-15           |
| “Character Sets” on page 11-15                |
| “Identifiers” on page 11-15                   |
| “Types” on page 11-17                         |
| “Constants” on page 11-17                     |
| “Declarations and Definitions” on page 11-18  |
| “Initialization” on page 11-20                |
| “Arithmetic Type Conversion” on page 11-20    |
| “Pointer Type Conversion” on page 11-24       |
| “Expressions” on page 11-25                   |
| “Control Statement Expressions” on page 11-28 |
| “Control Flow” on page 11-29                  |
| “Switch Statements” on page 11-31             |
| “Functions” on page 11-32                     |
| “Pointers and Arrays” on page 11-33           |
| “Structures and Unions” on page 11-33         |
| “Preprocessing Directives” on page 11-34      |
| “Standard Libraries” on page 11-37            |
| “runtime Failures” on page 11-39              |



## Language Extensions

| N.  | MISRA Definition                                             | Messages in log file                                         | Detailed PolySpace Specification                                                        |
|-----|--------------------------------------------------------------|--------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 2.2 | source code shall only use /* */ style comments              | C++ comments shall not be used.                              | C++ comments are handled as comments but lead to a violation of this MISRA rule         |
| 2.3 | The character sequence /* shall not be used within a comment | The character sequence /* shall not appear within a comment. | This rule violation is also raised when the character sequence /* inside a C++ comment. |

## Character Sets

| N.  | MISRA Definition                                                                    | Messages in log file                                                                                                               | Detailed PolySpace Specification                                                                          |
|-----|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| 4.1 | Only those escape sequences which are defined in the ISO® C standard shall be used. | \<character> is not an ISO C escape sequence<br>Only those escape sequences which are defined in the ISO C standard shall be used. |                                                                                                           |
| 4.2 | Trigraphs shall not be used.                                                        | Trigraphs shall not be used.                                                                                                       | Trigraphs are handled and converted to the equivalent character but lead to a violation of the MISRA rule |

## Identifiers

| N.  | MISRA Definition                                                                                  | Messages in log file                                                            | Detailed PolySpace Specification                        |
|-----|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|---------------------------------------------------------|
| 5.1 | Identifiers (internal and external) shall not rely on the significance of more than 31 characters | Identifier 'XX' should not rely on the significance of more than 31 characters. | All identifiers (global, static and local) are checked. |

| N.  | MISRA Definition                                                                                                                                              | Messages in log file                                                                                                                                                           | Detailed PolySpace Specification                                  |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 5.2 | Identifiers in an inner scope shall not use the same name as an identifier in an outer scope, and therefore hide that identifier.                             | <ul style="list-style-type: none"> <li>• Local declaration of XX is hiding another identifier.</li> <li>• Declaration of parameter XX is hiding another identifier.</li> </ul> | Assumes that rule 8.1 is not violated.                            |
| 5.3 | A typedef name shall be a unique identifier                                                                                                                   | { typedef name }'%s' should not be reused. (already used as { typedef name } at %s:%d)                                                                                         | Warning when a typedef name is reused as another identifier name. |
| 5.4 | A tag name shall be a unique identifier                                                                                                                       | { tag name }'%s' should not be reused. (already used as { tag name } at %s:%d)                                                                                                 | warning when a tag name is reused as another identifier name      |
| 5.5 | No object or function identifier with a static storage duration should be reused.                                                                             | { static identifier/parameter name }'%s' should not be reused. (already used as { static identifier/parameter name } at %s:%d)                                                 | warning when a static name is reused as another identifier name   |
| 5.6 | No identifier in one name space should have the same spelling as an identifier in another name space, with the exception of structure and union member names. | { member name }'%s' should not be reused. (already used as { member name } at %s:%d)                                                                                           | warning when a idf in a namespace is reused in another namespace  |
| 5.7 | No identifier name should be reused.                                                                                                                          | { identifier }'%s' should not be reused. (already used as { identifier } at %s:%d)                                                                                             | warning on other conflicts (including member names)               |

## Types

| N.  | MISRA Definition                                                                             | Messages in log file                                                                   | Detailed PolySpace Specification                                                                                                   |
|-----|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| 6.1 | The plain char type shall be used only for the storage and use of character values           | Only permissible operators on plain chars are '=', '==' or '!=' operators.             | There is a warning when a plain char is used with an operator other than =, == or !=.                                              |
| 6.3 | <i>typedefs</i> that indicate size and signedness should be used in place of the basic types | typedefs that indicate size and signedness should be used in place of the basic types. | No warning is given in typedef definition. There is no exception on bitfields.                                                     |
| 6.4 | Bit fields shall only be defined to be of type <i>unsigned int</i> or <i>signed int</i> .    | Bit fields shall only be defined to be of type unsigned int or signed int.             |                                                                                                                                    |
| 6.5 | Bit fields of type <i>signed int</i> shall be at least 2 bits long.                          | Bit fields of type signed int shall be at least 2 bits long.                           | No warning on anonymous signed int bitfields of width 0 - Extended to all signed bitfields of size <= 1 (if Rule 6.4 is violated). |

## Constants

| N.  | MISRA Definition                                                                | Messages in log file                                                                                                                                                                                                                                     | Detailed PolySpace Specification |
|-----|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| 7.1 | Octal constants (other than zero) and octal escape sequences shall not be used. | <ul style="list-style-type: none"> <li>• Octal constants other than zero and octal escape sequences shall not be used.</li> <li>• Octal constants (other than zero) should not be used.</li> <li>• Octal escape sequences should not be used.</li> </ul> |                                  |

## Declarations and Definitions

| N.  | MISRA Definition                                                                                                         | Messages in log file                                                                                                                                                                                                                                                                                                         | Detailed PolySpace Specification                                                                                                 |
|-----|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 8.1 | Functions shall have prototype declarations and the prototype shall be visible at both the function definition and call. | <ul style="list-style-type: none"> <li>• Function XX has no complete prototype visible at call.</li> <li>• Function XX has no prototype visible at definition.</li> </ul>                                                                                                                                                    | Prototype visible at call must be complete.                                                                                      |
| 8.2 | Whenever an object or function is declared or defined, its type shall be explicitly stated                               | Whenever an object or function is declared or defined, its type shall be explicitly stated.                                                                                                                                                                                                                                  |                                                                                                                                  |
| 8.4 | If objects or functions are declared more than once their types shall be compatible.                                     | <ul style="list-style-type: none"> <li>• If objects or functions are declared more than once their types shall be compatible.</li> <li>• Global declaration of 'XX' function has incompatible type with its definition.</li> <li>• Global declaration of 'XX' variable has incompatible type with its definition.</li> </ul> | During link phase, errors are converted into warnings with <code>-permissive-link</code> option.<br><b>Cannot be turned Off.</b> |
| 8.5 | There shall be no definitions of objects or functions in a header file                                                   | <ul style="list-style-type: none"> <li>• Object 'XX' should not be defined in a header file.</li> <li>• Function 'XX' should not be defined in a header file.</li> </ul>                                                                                                                                                     | Tentative of definitions are considered as definitions.                                                                          |

| N.   | MISRA Definition                                                                                                                            | Messages in log file                                                                                                                                                                                                                      | Detailed PolySpace Specification                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.6  | Functions shall always be declared at file scope.                                                                                           | Function 'XX' should be declared at file scope.                                                                                                                                                                                           |                                                                                                                                                                            |
| 8.9  | Definition: An identifier with external linkage shall have exactly one external definition.                                                 | <ul style="list-style-type: none"> <li>• Procedure/Global variable XX multiply defined.</li> <li>• Forbidden multiple tentative of definition for object XX.</li> <li>• Global variable has multiples tentative of definitions</li> </ul> | Tentative of definitions are considered as definitions, No warning on undefined objects with <code>-allow-undef-variables</code> option, No warning on predefined symbols. |
| 8.10 | All declarations and definitions of objects or functions at file scope shall have internal linkage unless external linkage is required      | Function/Variable XX should have internal linkage.                                                                                                                                                                                        | Not checked if <code>-main-generator</code> option is set. Assumes that 8.1 is not violated. No warning if 0 uses.                                                         |
| 8.11 | The <i>static</i> storage class specifier shall be used in definitions and declarations of objects and functions that have internal linkage | static storage class specifier should be used on internal linkage symbol XX.                                                                                                                                                              |                                                                                                                                                                            |
| 8.12 | When an array is declared with external linkage, its size shall be stated explicitly or defined implicitly by initialization                | Array XX has unknown size.                                                                                                                                                                                                                |                                                                                                                                                                            |

## Initialization

| N.  | MISRA Definition                                                                                                                                             | Messages in log file                                                                                                                                         | Detailed PolySpace Specification                         |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| 9.1 | All automatic variables shall have been assigned a value before being used.                                                                                  |                                                                                                                                                              | Done by PolySpace (NIV Checks).<br><b>Cannot be Off.</b> |
| 9.2 | Braces shall be used to indicate and match the structure in the nonzero initialization of arrays and structures.                                             | Braces shall be used to indicate and match the structure in the nonzero initialization of arrays and structures.                                             |                                                          |
| 9.3 | In an enumerator list, the = construct shall not be used to explicitly initialize members other than the first, unless all items are explicitly initialized. | In an enumerator list, the = construct shall not be used to explicitly initialize members other than the first, unless all items are explicitly initialized. |                                                          |

## Arithmetic Type Conversion

| N.   | MISRA Definition                                                                                                                                                                                                                                                                                                                                                 | Messages in log file                                                                                                                                                                                                                                                                                                                        | Detailed PolySpace Specification                                                                                                                                                                                                                                                                                                           |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10.1 | <p>The value of an expression of integer type shall not be implicitly converted to a different underlying type if:</p> <ul style="list-style-type: none"> <li>it is not a conversion to a wider integer type of the same signedness, or</li> <li>the expression is complex, or</li> <li>the expression is not constant and is a function argument, or</li> </ul> | <ul style="list-style-type: none"> <li>Implicit conversion of the expression of underlying type ?? to the type ?? that is not a wider integer type of the same signedness.</li> <li>Implicit conversion of one of the binary operands whose underlying types are ?? and ??</li> <li>Implicit conversion of the binary right hand</li> </ul> | <ol style="list-style-type: none"> <li>ANSI C base types order (signed char, short, int, long) defines that T2 is wider than T1 if T2 is on the right hand of T1 or T2 = T1. The same interpretation is applied on the unsigned version of base types.</li> <li>An expression of bool or enum types has int as underlying type.</li> </ol> |

| N.           | MISRA Definition                                                                                            | Messages in log file                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Detailed PolySpace Specification                                                                                                                                                                                                                                                                                                                                                                      |
|--------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | <ul style="list-style-type: none"> <li>the expression is not constant and is a return expression</li> </ul> | <p>operand of underlying type ?? to ?? that is not an integer type.</p> <ul style="list-style-type: none"> <li>Implicit conversion of the binary left hand operand of underlying type ?? to ?? that is not an integer type.</li> <li>Implicit conversion of the binary right hand operand of underlying type ?? to ?? that is not a wider integer type of the same signedness or Implicit conversion of the binary ? left hand operand of underlying type ?? to ??, but it is a complex expression.</li> </ul> | <p><b>3</b> Plain char may have signed or unsigned underlying type (depending on PolySpace target configuration or option setting).</p> <p><b>4</b> The underlying type of a simple expression of struct.bitfield is the base type used in the bitfield definition, the bitfield width is not taken into account and it assumes that only signed   unsigned int are used for bitfield (Rule 6.4).</p> |
| 10.1 (cont.) |                                                                                                             | <ul style="list-style-type: none"> <li>Implicit conversion of complex integer expression of underlying type ?? to ??.</li> <li>Implicit conversion of non-constant integer expression of underlying type ?? in function return whose expected type is ??.</li> <li>Implicit conversion of non-constant integer expression of underlying type ?? as argument of function whose</li> </ul>                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                       |

| N.   | MISRA Definition                                                                                                                                                                                                                                                                                                                                                   | Messages in log file                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Detailed PolySpace Specification                                                                                      |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                                                                                                                                                                                                    | corresponding parameter type is ??.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                       |
| 10.2 | <p>The value of an expression of floating type shall not be implicitly converted to a different type if</p> <ul style="list-style-type: none"> <li>• it is not a conversion to a wider floating type, or</li> <li>• the expression is complex, or</li> <li>• the expression is a function argument, or</li> <li>• the expression is a return expression</li> </ul> | <ul style="list-style-type: none"> <li>• Implicit conversion of the expression from ?? to ?? that is not a wider floating type.</li> <li>• Implicit conversion of the binary ? right hand operand from ?? to ??, but it is a complex expression.</li> <li>• Implicit conversion of the binary ? right hand operand from ?? to ?? that is not a wider floating type or Implicit conversion of the binary ? left hand operand from ?? to ??, but it is a complex expression.</li> <li>• Implicit conversion of complex floating expression from ?? to ??.</li> <li>• Implicit conversion of floating expression of ?? type in function return whose expected type is ??.</li> <li>• Implicit conversion of floating expression of ?? type as argument of function whose</li> </ul> | ANSI C base types order (float, double) defines that T2 is wider than T1 if T2 is on the right hand of T1 or T2 = T1. |



| N.   | MISRA Definition                                                                                                                                                  | Messages in log file                                                                                                                       | Detailed PolySpace Specification                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                   | corresponding parameter type is ??.                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 10.3 | The value of a complex expression of integer type may only be cast to a type that is narrower and of the same signedness as the underlying type of the expression | Complex expression of underlying type ?? may only be cast to narrower integer type of same signedness, however the destination type is ??. | <ul style="list-style-type: none"> <li>• ANSI C base types order (signed char, short, int, long) defines that T1 is narrower than T2 if T2 is on the right hand of T1 or T1 = T2. The same methodology is applied on the unsigned version of base types.</li> <li>• An expression of bool or enum types has int as underlying type.</li> <li>• Plain char may have signed or unsigned underlying type (depending on target configuration or option setting).</li> <li>• The underlying type of a simple expression of struct.bitfield is the base type used in the bitfield definition, the bitfield width is not taken into account and it assumes that only signed, unsigned int are used for bitfield (Rule 6.4).</li> </ul> |

| N.   | MISRA Definition                                                                                                                                                                                         | Messages in log file                                                                                                                                     | Detailed PolySpace Specification                                                                                         |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| 10.4 | The value of a complex expression of float type may only be cast to narrower floating type                                                                                                               | Complex expression of ?? type may only be cast to narrower floating type, however the destination type is ??.                                            | ANSI C base types order (float, double) defines that T1 is narrower than T2 if T2 is on the right hand of T1 or T2 = T1. |
| 10.5 | If the bitwise operator ~ and << are applied to an operand of underlying type <i>unsigned char</i> or <i>unsigned short</i> , the result shall be immediately cast to the underlying type of the operand | Bitwise [<< ~] is applied to the operand of underlying type [unsigned char unsigned short], the result shall be immediately cast to the underlying type. |                                                                                                                          |
| 10.6 | The “U” suffix shall be applied to all constants of <i>unsigned</i> types                                                                                                                                | No explicit ‘U suffix on constants of an unsigned type.                                                                                                  |                                                                                                                          |

### Pointer Type Conversion

| N.   | MISRA Definition                                                                                                                                                 | Messages in log file                                                                                                                                              | Detailed PolySpace Specification                            |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| 11.1 | Conversion shall not be performed between a pointer to a function and any type other than an integral type                                                       | Conversion shall not be performed between a pointer to a function and any type other than an integral type.                                                       | Casts and implicit conversions involving a function pointer |
| 11.2 | Conversion shall not be performed between a pointer to an object and any type other than an integral type, another pointer to a object type or a pointer to void | Conversion shall not be performed between a pointer to an object and any type other than an integral type, another pointer to a object type or a pointer to void. | There is also a warning on qualifier loss                   |

| N.   | MISRA Definition                                                                                                                  | Messages in log file                                                                                                              | Detailed PolySpace Specification                        |
|------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| 11.3 | A cast should not be performed between a pointer type and an integral type                                                        | A cast should not be performed between a pointer type and an integral type.                                                       | Exception on zero constant. Extended to all conversions |
| 11.4 | A cast should not be performed between a pointer to object type and a different pointer to object type.                           | A cast should not be performed between a pointer to object type and a different pointer to object type.                           | Extended to all conversions                             |
| 11.5 | A cast shall not be performed that removes any <i>const</i> or <i>volatile</i> qualification from the type addressed by a pointer | A cast shall not be performed that removes any <i>const</i> or <i>volatile</i> qualification from the type addressed by a pointer | Extended to all conversions                             |

## Expressions

| N.   | MISRA Definition                                                                        | Messages in log file                                                                  | Detailed PolySpace Specification                    |
|------|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|-----------------------------------------------------|
| 12.1 | Limited dependence should be placed on C's operator precedence rules in expressions     | Limited dependence should be placed on C's operator precedence rules in expressions   |                                                     |
| 12.3 | The <i>sizeof</i> operator should not be used on expressions that contain side effects. | he size of operator should not be used on expressions that contain side effects.      | No warning on volatile accesses and function calls  |
| 12.4 | The right hand operand of a logical && or    operator shall not contain side effects.   | The right hand operand of a logical && or    operator shall not contain side effects. | No warning on volatile accesses and function calls. |

| N.   | MISRA Definition                                                                                                                                                                          | Messages in log file                                                                                                                                                                                                                                                                                                                                                          | Detailed PolySpace Specification                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.5 | The operands of a logical && or    shall be primary-expressions.                                                                                                                          | <ul style="list-style-type: none"> <li>• operand of logical &amp;&amp; is not a primary expression</li> <li>• operand of logical    is not a primary expression</li> <li>• The operands of a logical &amp;&amp; or    shall be primary-expressions.</li> </ul>                                                                                                                | <p>During preprocessing, violations of this rule are detected on the expressions in #if directives.</p> <p>Allowed exception on associatively (a &amp;&amp; b &amp;&amp; c), (a    b    c).</p>                                                                                                                                                                                                                                                                              |
| 12.6 | Operands of logical operators (&&,    and !) should be effectively Boolean. Expression that are effectively Boolean should not be used as operands to operators other than (&&,    or !). | <ul style="list-style-type: none"> <li>• Operand of '!' logical operator should be effectively Boolean. Left operand of '%s' logical operator should be effectively Boolean.</li> <li>• Right operand of '%s' logical operator should be effectively Boolean.</li> <li>• Boolean should not be used as operands to operators other than '&amp;&amp;', '  ' or '!'.</li> </ul> | <p>"the operand of a logical operator should be a Boolean". As there are no Boolean in "C" but as the standard assumes it, some operator return Boolean like expression (var == 0).</p> <p><b>Example:</b></p> <pre>unsigned char flag; if (!flag) raises the rule: the operand of "!" is "flag". And "flag" is not a Boolean but an unsigned char. To be 12.6 MISRA compliant, the code need to be written like this:</pre> <pre>if (!( flag != 0)) or if (flag == 0)</pre> |

| N.   | MISRA Definition                                                                                                                                       | Messages in log file                                                                                                                                                                                                                                                                                                                                                | Detailed PolySpace Specification                                                                                                                                                                                                                                          |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.7 | Bitwise operators shall not be applied to operands whose underlying type is signed                                                                     | <ul style="list-style-type: none"> <li>• [~/Left Shift/Right shift/&amp;] operator applied on an expression whose underlying type is signed.</li> <li>• Bitwise ~ on operand of signed underlying type ??.</li> <li>• Bitwise [&lt;&lt; &gt;&gt;] on left hand operand of signed underlying type ??.</li> <li>• Bitwise [&amp;   ^] on two operands of s</li> </ul> | <p>The underlying type for an integer used in a re-processor expression is signed when :</p> <ul style="list-style-type: none"> <li>• it does not have a u or U suffix</li> <li>• it is small enough to fit into a 64 bits signed number</li> </ul>                       |
| 12.8 | The right hand operand of a shift operator shall lie between zero and one less than the width in bits of the underlying type of the left hand operand. | <ul style="list-style-type: none"> <li>• shift amount is negative</li> <li>• shift amount is bigger than 64</li> <li>• Bitwise [&lt;&lt; &gt;&gt;] count out of range [0 ..X] (width of the underlying type ?? of the left hand operand - 1)..</li> </ul>                                                                                                           | <p>The numbers that are manipulated in preprocessing directives are 64 bits wide so that valid shift range is between 0 and 63</p> <p>Check is also extended onto bitfields with the field width or the width of the base type when it is within a complex expression</p> |

| N.    | MISRA Definition                                                                                          | Messages in log file                                                                                                                                                                        | Detailed PolySpace Specification                                                                                                                                                                                                            |
|-------|-----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.9  | The unary minus operator shall not be applied to an expression whose underlying type is unsigned.         | <ul style="list-style-type: none"> <li>• Unary - on operand of unsigned underlying type ??.</li> <li>• Minus operator applied to an expression whose underlying type is unsigned</li> </ul> | The underlying type for an integer used in a re-processor expression is signed when: <ul style="list-style-type: none"> <li>• it does not have a u or U suffix</li> <li>• it is small enough to fit into a 64 bits signed number</li> </ul> |
| 12.10 | The comma operator shall not be used.                                                                     | The comma operator shall not be used.                                                                                                                                                       |                                                                                                                                                                                                                                             |
| 12.13 | The increment (++) and decrement (--) operators should not be mixed with other operators in an expression | The increment (++) and decrement (--) operators should not be mixed with other operators in an expression                                                                                   | warning when ++ or -- operators are not used alone.                                                                                                                                                                                         |

### Control Statement Expressions

| N.   | MISRA Definition                                                                 | Messages in log file                                                             | Detailed PolySpace Specification |
|------|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------|----------------------------------|
| 13.1 | Assignment operators shall not be used in expressions that yield Boolean values. | Assignment operators shall not be used in expressions that yield Boolean values. |                                  |

| N.   | MISRA Definition                                                                                 | Messages in log file                                                                             | Detailed PolySpace Specification                                                                                                                         |
|------|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 13.2 | Tests of a value against zero should be made explicit, unless the operand is effectively Boolean | Tests of a value against zero should be made explicit, unless the operand is effectively Boolean | No warning is given on integer constants. Example: if (2)                                                                                                |
| 13.7 | Boolean operations whose results are invariant shall not be permitted                            | Boolean operator '%s' should not have invariant result. (Result is always 'true/false').         | Done by PolySpace (gray Checks). It is also checked during compilation on comparison between with a least one constant operand.<br><b>Cannot be Off.</b> |

## Control Flow

| N.   | MISRA Definition                                                                                                     | Messages in log file                                                                                                                                                                            | Detailed PolySpace Specification                          |
|------|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| 14.1 | There shall be no unreachable code.                                                                                  |                                                                                                                                                                                                 | Done by PolySpace (gray checks).<br><b>Cannot be Off.</b> |
| 14.2 | All non-null statements shall either have at least one side effect however executed, or cause control flow to change | <ul style="list-style-type: none"> <li>• All non-null statements shall either:</li> <li>• have at least one side effect however executed, or</li> <li>• cause control flow to change</li> </ul> |                                                           |
| 14.4 | The <i>goto</i> statement shall not be used.                                                                         | The <i>goto</i> statement shall not be used.                                                                                                                                                    |                                                           |
| 14.5 | The <i>continue</i> statement shall not be used.                                                                     | The <i>continue</i> statement shall not be used.                                                                                                                                                |                                                           |

| N.    | MISRA Definition                                                                                                                                                                        | Messages in log file                                                                                                                                                                                                                                              | Detailed PolySpace Specification |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| 14.6  | For any iteration statement there shall be at most one <i>break</i> statement used for loop termination                                                                                 | For any iteration statement there shall be at most one break statement used for loop termination                                                                                                                                                                  |                                  |
| 14.7  | A function shall have a single point of exit at the end of the function                                                                                                                 | A function shall have a single point of exit at the end of the function                                                                                                                                                                                           |                                  |
| 14.8  | The statement forming the body of a <i>switch</i> , <i>while</i> , <i>do while</i> or <i>for</i> statement shall be a compound statement                                                | <ul style="list-style-type: none"> <li>• The body of a do while statement shall be a compound statement.</li> <li>• The body of a for statement shall be a compound statement.</li> <li>• The body of a switch statement shall be a compound statement</li> </ul> |                                  |
| 14.9  | An <i>if (expression)</i> construct shall be followed by a compound statement. The <i>else</i> keyword shall be followed by either a compound statement, or another <i>if</i> statement | <ul style="list-style-type: none"> <li>• An if (expression) construct shall be followed by a compound statement.</li> <li>• The else keyword shall be followed by either a compound statement, or another if statement</li> </ul>                                 |                                  |
| 14.10 | All <i>if else if</i> constructs should contain a final <i>else</i> clause.                                                                                                             | All if else if constructs should contain a final else clause.                                                                                                                                                                                                     |                                  |



## Switch Statements

| N.   | MISRA Definition                                                                                                                            | Messages in log file                                                                                                   | Detailed PolySpace Specification                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------|---------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15.0 | <p>Unreachable code is detected between switch statement and first case.</p> <hr/> <p><b>Note</b> this is not a MISRA C2004 rule.</p> <hr/> | switch statements syntax normative restrictions.                                                                       | <p>Warning on declarations or any statements before the first switch case.</p> <p>Warning on label or jump statements in the body of switch cases.</p> <p>On the following example, the rule is displayed in the log file at line 3:</p> <pre> 1 ... 2 switch(index) { 3   var = var + 1;   // RULE 15.0   // violated 4 case 1: ... </pre> <p>The code between switch statement and first case is checked as gray by PolySpace verification. It follows ANSI standard behavior.</p> |
| 15.1 | A switch label shall only be used when the most closely-enclosing compound statement is the body of a <i>switch</i> statement               | A switch label shall only be used when the most closely-enclosing compound statement is the body of a switch statement |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 15.2 | An unconditional <i>break</i> statement shall terminate every non-empty switch clause                                                       | An unconditional break statement shall terminate every non-empty switch clause                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| N.   | MISRA Definition                                                                    | Messages in log file                                                         | Detailed PolySpace Specification |
|------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------|----------------------------------|
| 15.3 | The final clause of a <i>switch</i> statement shall be the <i>default</i> clause    | The final clause of a switch statement shall be the default clause           |                                  |
| 15.4 | A <i>switch</i> expression should not represent a value that is effectively Boolean | A switch expression should not represent a value that is effectively Boolean |                                  |
| 15.5 | Every <i>switch</i> statement shall have at least one <i>case</i> clause            | Every switch statement shall have at least one case clause                   |                                  |

### Functions

| N.   | MISRA Definition                                                                          | Messages in log file                                                                      | Detailed PolySpace Specification                                                                                                                                                  |
|------|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 16.1 | Functions shall not be defined with variable numbers of arguments.                        | Function XX should not be defined as varargs.                                             |                                                                                                                                                                                   |
| 16.2 | Functions shall not call themselves, either directly or indirectly.                       | Function %s should not call itself.                                                       | Done by PolySpace software (Call graph in the viewer gives the information). PolySpace verification also checks that partially during compilation phase.<br><b>Cannot be Off.</b> |
| 16.3 | Identifiers shall be given for all of the parameters in a function prototype declaration. | Identifiers shall be given for all of the parameters in a function prototype declaration. | Assumes Rule 8.6 is not violated.                                                                                                                                                 |
| 16.4 | The identifiers used in the declaration and definition of a function shall be identical.  | The identifiers used in the declaration and definition of a function shall be identical.  | Assumes that rules 8.8, 8.1 and 16.3 are not violated. All occurrences are detected.                                                                                              |

| <b>N.</b> | <b>MISRA Definition</b>                                                                                                         | <b>Messages in log file</b>                                                       | <b>Detailed PolySpace Specification</b>                                                             |
|-----------|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| 16.5      | Functions with no parameters shall be declared with parameter type <i>void</i> .                                                | Functions with no parameters shall be declared with parameter type void.          | Definitions are also checked.                                                                       |
| 16.8      | All exit paths from a function with non-void return type shall have an explicit return statement with an expression.            | Missing return value for non-void function XX.                                    | Warning when a non-void function is not terminated with an unconditional return with an expression. |
| 16.9      | A function identifier shall only be used with either a preceding &, or with a parenthesized parameter list, which may be empty. | Function identifier XX should be preceded by a & or followed by a parameter list. |                                                                                                     |

## Pointers and Arrays

| <b>N.</b> | <b>MISRA Definition</b>                                             | <b>Messages in log file</b>                                         | <b>Detailed PolySpace Specification</b> |
|-----------|---------------------------------------------------------------------|---------------------------------------------------------------------|-----------------------------------------|
| 17.5      | A type should not contain more than 2 levels of pointer indirection | A type should not contain more than 2 levels of pointer indirection |                                         |

## Structures and Unions

| <b>N.</b> | <b>MISRA Definition</b>                                                          | <b>Messages in log file</b>                                                      | <b>Detailed PolySpace Specification</b> |
|-----------|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------|-----------------------------------------|
| 18.1      | All structure or union types shall be complete at the end of a translation unit. | All structure or union types shall be complete at the end of a translation unit. |                                         |
| 18.4      | Unions shall not be used                                                         | Unions shall not be used.                                                        |                                         |

## Preprocessing Directives

| N.   | MISRA Definition                                                                                   | Messages in log file                                                                                                                                                                                                                                        | Detailed PolySpace Specification |
|------|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| 19.1 | #include statements in a file shall only be preceded by other preprocessors directives or comments | A message is displayed when a #include directive is preceded by other things than preprocessor directives, comments, spaces or “new lines”.                                                                                                                 |                                  |
| 19.2 | Nonstandard characters should not occur in header file names in #include directives                | <ul style="list-style-type: none"> <li>• A message is displayed on characters ', \, " or /* between &lt; and &gt; in #include &lt;filename&gt;</li> <li>• A message is displayed on characters ', \ or /* between " and " in #include "filename"</li> </ul> |                                  |
| 19.3 | The #include directive shall be followed by either a <filename> or "filename" sequence.            | <ul style="list-style-type: none"> <li>• #include' expects "FILENAME" or &lt;FILENAME&gt;</li> <li>• #include_next' expects "FILENAME" or &lt;FILENAME&gt;</li> </ul>                                                                                       | <b>Cannot be Off.</b>            |
| 19.5 | Macros shall not be #defined and #undefd within a block.                                           | <ul style="list-style-type: none"> <li>• Macros shall not be #defined within a block.</li> <li>• Macros shall not be #undef'd within a block.</li> </ul>                                                                                                    |                                  |
| 19.6 | #undef shall not be used.                                                                          | #undef shall not be used.                                                                                                                                                                                                                                   |                                  |

| N.    | MISRA Definition                                                                                                                                               | Messages in log file                                                                                                                                                                                                                                                             | Detailed PolySpace Specification                                                                                              |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| 19.7  | A function should be used in preference to a function like-macro.                                                                                              | Message on all function-like macros expansions                                                                                                                                                                                                                                   |                                                                                                                               |
| 19.8  | A function-like macro shall not be invoked without all of its arguments                                                                                        | <ul style="list-style-type: none"> <li>• arguments given to macro '&lt;name&gt;'</li> <li>• macro '&lt;name&gt;' used without args.</li> <li>• macro '&lt;name&gt;' used with just one arg.</li> <li>• macro '&lt;name&gt;' used with too many (&lt;number&gt;) args.</li> </ul> | <b>Cannot be Off.</b>                                                                                                         |
| 19.9  | Arguments to a function-like macro shall not contain tokens that look like preprocessing directives.                                                           | Macro argument shall not look like a preprocessing directive.                                                                                                                                                                                                                    | This rule is detected as violated when the '#' character appears in a macro argument (outside a string or character constant) |
| 19.10 | In the definition of a function-like macro each instance of a parameter shall be enclosed in parentheses unless it is used as the operand of # or ##.          | Parameter instance shall be enclosed in parentheses.                                                                                                                                                                                                                             |                                                                                                                               |
| 19.11 | All macro identifiers in preprocessor directives shall be defined before use, except in #ifdef and #ifndef preprocessor directives and the defined() operator. | '<name>' is not defined.                                                                                                                                                                                                                                                         |                                                                                                                               |

| N.    | MISRA Definition                                                                                                                            | Messages in log file                                                                                                                                                                                                                                                                                                                                                                  | Detailed PolySpace Specification |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| 19.12 | There shall be at most one occurrence of the # or ## preprocessor operators in a single macro definition.                                   | More than one occurrence of the # or ## preprocessor operators.                                                                                                                                                                                                                                                                                                                       |                                  |
| 19.13 | The # and ## preprocessor operators should not be used                                                                                      | Message on definitions of macros using # or ## operators                                                                                                                                                                                                                                                                                                                              |                                  |
| 19.14 | The defined preprocessor operator shall only be used in one of the two standard forms.                                                      | 'defined' without an identifier.                                                                                                                                                                                                                                                                                                                                                      | <b>Cannot be Off.</b>            |
| 19.16 | Preprocessing directives shall be syntactically meaningful even when excluded by the preprocessor.                                          | directive is not syntactically meaningful.                                                                                                                                                                                                                                                                                                                                            |                                  |
| 19.17 | All #else, #elif and #endif preprocessor directives shall reside in the same file as the #if or #ifdef directive to which they are related. | <ul style="list-style-type: none"> <li>• #elif not within a conditional.</li> <li>• #else not within a conditional.</li> <li>• #elif not within a conditional.</li> <li>• #endif not within a conditional.</li> <li>• unbalanced #endif.</li> <li>• unterminated #if conditional.</li> <li>• unterminated #ifdef conditional.</li> <li>• unterminated #ifndef conditional.</li> </ul> | <b>Cannot be Off.</b>            |

## Standard Libraries

| N.   | MISRA Definition                                                                                                  | Messages in log file                                                                                                                                           | Detailed PolySpace Specification                                                                                                                                                                                  |
|------|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 20.1 | Reserved identifiers, macros and functions in the standard library, shall not be defined, redefined or undefined. | <ul style="list-style-type: none"> <li>• The macro ‘&lt;name&gt; shall not be redefined.</li> <li>• The macro ‘&lt;name&gt; shall not be undefined.</li> </ul> |                                                                                                                                                                                                                   |
| 20.2 | The names of standard library macros, objects and functions shall not be reused.                                  | Identifier XX should not be used.                                                                                                                              | In case a macro whose name corresponds to a standard library macro, object or function is defined, the rule that is detected as violated is <b>20.1</b> . Tentative of definitions are considered as definitions. |
| 20.4 | Dynamic heap memory allocation shall not be used.                                                                 | <ul style="list-style-type: none"> <li>• The macro ‘&lt;name&gt; shall not be used.</li> <li>• Identifier XX should not be used.</li> </ul>                    | In case the dynamic heap memory allocation functions are actually macros and the macro is expanded in the code, this rule is detected as violated. Assumes rule <b>20.2</b> is not violated.                      |
| 20.5 | The error indicator errno shall not be used                                                                       | The error indicator errno shall not be used                                                                                                                    | Assumes that rule <b>20.2</b> is not violated                                                                                                                                                                     |
| 20.6 | The macro <i>offsetof</i> , in library <stddef.h>, shall not be used.                                             | <ul style="list-style-type: none"> <li>• The macro ‘&lt;name&gt; shall not be used.</li> <li>• Identifier XX should not be used.</li> </ul>                    | Assumes that rule <b>20.2</b> is not violated                                                                                                                                                                     |

| N.    | MISRA Definition                                                                     | Messages in log file                                                                                                                        | Detailed PolySpace Specification                                                                                                                                              |
|-------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 20.7  | The <i>setjmp</i> macro and the <i>longjmp</i> function shall not be used.           | <ul style="list-style-type: none"> <li>• The macro ‘&lt;name&gt; shall not be used.</li> <li>• Identifier XX should not be used.</li> </ul> | In case the longjmp function is actually a macro and the macro is expanded in the code, this rule is detected as violated. Assumes that rule <b>20.2</b> is not violated      |
| 20.8  | The signal handling facilities of <signal.h> shall not be used.                      | <ul style="list-style-type: none"> <li>• The macro ‘&lt;name&gt; shall not be used.</li> <li>• Identifier XX should not be used.</li> </ul> | In case some of the signal functions are actually macros and are expanded in the code, this rule is detected as violated. Assumes that rule <b>20.2</b> is not violated       |
| 20.9  | The input/output library <stdio.h> shall not be used in production code.             | <ul style="list-style-type: none"> <li>• The macro ‘&lt;name&gt; shall not be used.</li> <li>• Identifier XX should not be used.</li> </ul> | In case the input/output library functions are actually macros and are expanded in the code, this rule is detected as violated. Assumes that rule <b>20.2</b> is not violated |
| 20.10 | The library functions atof, atoi and toll from library <stdlib.h> shall not be used. | <ul style="list-style-type: none"> <li>• The macro ‘&lt;name&gt; shall not be used.</li> <li>• Identifier XX should not be used.</li> </ul> | In case the atof, atoi and atoll functions are actually macros and are expanded, this rule is detected as violated. Assumes that rule <b>20.2</b> is not violated             |



| N.    | MISRA Definition                                                                                | Messages in log file                                                                                                                         | Detailed PolySpace Specification                                                                                                                                            |
|-------|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 20.11 | The library functions abort, exit, getenv and system from library <stdlib.h> shall not be used. | <ul style="list-style-type: none"> <li>• The macro '&lt;name&gt;' shall not be used.</li> <li>• Identifier XX should not be used.</li> </ul> | In case the abort, exit, getenv and system functions are actually macros and are expanded, this rule is detected as violated. Assumes that rule <b>20.2</b> is not violated |
| 20.12 | The time handling functions of library <time.h> shall not be used.                              | <ul style="list-style-type: none"> <li>• The macro '&lt;name&gt;' shall not be used.</li> <li>• Identifier XX should not be used.</li> </ul> | In case the time handling functions are actually macros and are expanded, this rule is detected as violated. Assumes that rule <b>20.2</b> is not violated                  |

## runtime Failures

| N.   | MISRA Definition                                                                                                                                                                                                                                                                            | Messages in log file | Detailed PolySpace Specification                                   |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|--------------------------------------------------------------------|
| 21.1 | Minimization of runtime failures shall be ensured by the use of at least one of: <ul style="list-style-type: none"> <li>• static verification tools/techniques;</li> <li>• dynamic verification tools/techniques;</li> <li>• explicit coding of checks to handle runtime faults.</li> </ul> |                      | Done by PolySpace (runtime error checks).<br><b>Cannot be Off.</b> |

## Rules Partially Supported

| In this section...                            |
|-----------------------------------------------|
| “Environment” on page 11-40                   |
| “Language Extension” on page 11-41            |
| “Declarations and Definitions” on page 11-42  |
| “Expressions” on page 11-43                   |
| “Control Statement Expressions” on page 11-44 |
| “Control Flow” on page 11-46                  |
| “Functions” on page 11-47                     |
| “Pointers and Arrays” on page 11-47           |
| “Preprocessing Directives” on page 11-48      |

## Environment

| Rule                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Description                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.1<br>(Required)                                                                                                                                                                                                                                                                                                                                                                                                                                       | All code shall conform to ISO 9899:1990 “Programming languages - C”, amended and corrected by ISO/IEC 9899/COR1:1995, ISO/IEC 9899/AMD1:1995, and ISO/IEC 9899/COR2:1996. |
| Messages in log:                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                           |
| <ul style="list-style-type: none"> <li>• ANSI C does not allow ‘#include_next’</li> <li>• ANSI C does not allow macros with variable arguments list</li> <li>• ANSI C does not allow ‘#assert’</li> <li>• ANSI C does not allow ‘#unassert’</li> <li>• ANSI C does not allow testing assertions</li> <li>• ANSI C does not allow ‘#ident’</li> <li>• ANSI C does not allow ‘#sccs’</li> <li>• text following ‘#else’ violates ANSI standard.</li> </ul> |                                                                                                                                                                           |

| Rule | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <ul style="list-style-type: none"> <li>• text following <code>#endif</code> violates ANSI standard.</li> <li>• text following <code>#else</code> or <code>#endif</code> violates ANSI standard.</li> <li>• ANSI C90 forbids 'long long int' type.</li> <li>• ANSI C90 forbids 'long double' type.</li> <li>• ANSI C90 forbids long long integer constants.</li> <li>• Keyword 'inline' should not be used.</li> <li>• Array of zero size should not be used.</li> <li>• Integer constant does not fit within unsigned long int.</li> <li>• Integer constant does not fit within long int.</li> </ul> |
|      | <hr/> <p><b>Note</b> All the supported extensions lead to a violation of this MISRA rule. Standard compilation error messages do not lead to a violation of this MISRA rule and remain unchanged. Can be turned to Off (see <code>-misra2</code> option).</p> <hr/>                                                                                                                                                                                                                                                                                                                                  |

## Language Extension

| Rule              | Description                                           |
|-------------------|-------------------------------------------------------|
| 2.1<br>(Required) | Assembly language shall be encapsulated and isolated. |

| Rule | Description                                                                                                                                                                                     |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <p>Message in log:</p> <ul style="list-style-type: none"> <li>• Assembly language shall be encapsulated and isolated.</li> </ul>                                                                |
|      | <p><b>Note</b> no warnings if code is encapsulated in asm functions or in asm pragma (only warning is given on asm statements even if it is encapsulated by a MACRO). Can be turned to Off.</p> |

## Declarations and Definitions

| Rule              | Description                                                                                                                                    |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.3<br>(Required) | For each function parameter the type given in the declaration and definition shall be identical, and the return types shall also be identical. |
|                   | <p>Message in log:</p> <ul style="list-style-type: none"> <li>• Definition of function 'XX' incompatible with its declaration.</li> </ul>      |
|                   | <p><b>Note</b> Assumes that rule 8.1 is not violated. The rule is restricted to compatible types. Can be turned to Off</p>                     |
| 8.7<br>(Required) | Objects shall be defined at block scope if they are only accessed from within a single function                                                |
|                   | <p>Message in log:</p> <ul style="list-style-type: none"> <li>• Object 'XX' should be declared at block scope.</li> </ul>                      |
|                   | <p><b>Note</b> Restricted to static objects. Can be turned to Off</p>                                                                          |

| Rule                                                                                                                                      | Description                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| 8.8<br>(Required)                                                                                                                         | An external object or function shall be declared in one file and only one file |
| Message in log:<br><ul style="list-style-type: none"> <li>• Function/Object 'XX' has external declarations in multiples files.</li> </ul> |                                                                                |
| <hr/> <p><b>Note</b> Restricted to explicit extern declarations (tentative of definitions are ignored). Can be turned to Off</p> <hr/>    |                                                                                |

## Expressions

| Rule                                                                                                                                                                                                                                                                                                                                     | Description                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| 12.2<br>(Required)                                                                                                                                                                                                                                                                                                                       | The value of an expression shall be the same under any order of evaluation that the standard permits. |
| Messages in log:<br><ul style="list-style-type: none"> <li>• The value of 'sym' depends on the order of evaluation.</li> <li>• The value of volatile 'sym' depends on the order of evaluation because of multiple accesses.</li> </ul>                                                                                                   |                                                                                                       |
| <hr/> <p><b>Note</b> The expression is a simple expression of symbols (Unlike <code>i = i++</code>; no detection on <code>tab[2] = tab[2]++</code>);. Rule 12.2 check assumes that no assignment in expressions that yield a Boolean values (rule 13.1) and the comma operator is not used (rule 12.10). Can be turned to Off.</p> <hr/> |                                                                                                       |
| 12.11<br>(Advisory)                                                                                                                                                                                                                                                                                                                      | Evaluation of constant unsigned expression should not lead to wraparound.                             |
| No message.                                                                                                                                                                                                                                                                                                                              |                                                                                                       |

| Rule                                                                                                                                                                                                                                                                                                           | Description                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <p><b>Note</b> This rule is partially implemented with the <code>-detect-unsigned-overflows</code> option in PolySpace software. Concerning possible preprocessing overflows, PolySpace preprocessor does not take into account target basic types and considers always 32-Bit long int. Cannot be ticked.</p> |                                                                                       |
| <p>12.12<br/>(Required)</p>                                                                                                                                                                                                                                                                                    | <p>The underlying bit representations of floating-point values shall not be used.</p> |
| <p>Message in log:</p> <ul style="list-style-type: none"> <li>• The underlying bit representations of floating-point values shall not be used.</li> </ul>                                                                                                                                                      |                                                                                       |
| <p><b>Note</b> Warning on casts with float pointers (excepted with void *). Can be turned to Off.</p>                                                                                                                                                                                                          |                                                                                       |

## Control Statement Expressions

| Rule                                                                                                                                                  | Description                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| <p>13.3<br/>(Required)</p>                                                                                                                            | <p>Floating-point expressions shall not be tested for equality or inequality.</p>                          |
| <p>Message in log:</p> <ul style="list-style-type: none"> <li>• Floating-point expressions shall not be tested for equality or inequality.</li> </ul> |                                                                                                            |
| <p><b>Note</b> Warning on directs tests only. Can be turned to Off.</p>                                                                               |                                                                                                            |
| <p>13.4<br/>(Required)</p>                                                                                                                            | <p>The controlling expression of a <i>for</i> statement shall not contain any objects of floating type</p> |

| Rule               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <p>Message in log:</p> <ul style="list-style-type: none"> <li>• The controlling expression of a <i>for</i> statement shall not contain any objects of floating type</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                    | <p><b>Note</b> If <i>for</i> index is a variable symbol, checked that it is not a float. Can be turned to Off.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 13.5<br>(Required) | The three expressions of a <i>for</i> statement shall be concerned only with loop control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                    | <p>Messages in log:</p> <ul style="list-style-type: none"> <li>• 1st expression should be an assignment.</li> <li>• Bad type for loop counter (XX).</li> <li>• 2nd expression should be a comparison.</li> <li>• 2nd expression should be a comparison with loop counter (XX).</li> <li>• 3rd expression should be an assignment of loop counter (XX).</li> <li>• 3rd expression: assigned variable should be the loop counter (XX).</li> </ul> <p><b>Note</b> Checked if the <i>for</i> loop index (V) is a variable symbol; checked if V is the last assigned variable in the first expression (if present). Checked if, in first expression, if present, is assignment of V; checked if in 2nd expression, if present, must be a comparison of V; Checked if in 3rd expression, if present, must be an assignment of V. Can be turned to Off.</p> |
| 13.6<br>(Required) | Numeric variables being used within a <i>for</i> loop for iteration counting should not be modified in the body of the loop.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Rule | Description                                                                                                                                                                                      |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <p>Message in log:</p> <ul style="list-style-type: none"> <li>• Numeric variables being used within a for loop for iteration counting should not be modified in the body of the loop.</li> </ul> |
|      | <hr/> <p><b>Note</b> Detect only direct assignments if the for loop index is known and if it is a variable symbol. Can be turned to Off.</p> <hr/>                                               |

## Control Flow

| Rule                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>14.3<br/>(Required)</p> | <p>All non-null statements shall either</p> <ul style="list-style-type: none"> <li>• have at least one side effect however executed, or</li> <li>• cause control flow to change</li> </ul>                                                                                                                                                                                                                                                  |
|                            | <p>Message in log:</p> <ul style="list-style-type: none"> <li>• A null statement shall appear on a line by itself</li> </ul>                                                                                                                                                                                                                                                                                                                |
|                            | <hr/> <p><b>Note</b> We assume that a ';' is a null statement when it is the first character on a line (excluding comments). The rule is violated when:</p> <ul style="list-style-type: none"> <li>• there are some comments before it on the same line.</li> <li>• there is a comment immediately after it</li> <li>• there is something else than a comment after the ';' on the same line.</li> </ul> <p>Can be turned to Off.</p> <hr/> |



## Functions

| Rule                                                                                                                                              | Description                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| 16.6<br>(Required)                                                                                                                                | The number of arguments passed to a function shall match the number of parameters. |
| Messages in log: <ul style="list-style-type: none"> <li>• Too many arguments to XX.</li> <li>• Insufficient number of arguments to XX.</li> </ul> |                                                                                    |
| <hr/> <b>Note</b> Assumes that rule 8.1 is not violated. Can be turned to Off.                                                                    |                                                                                    |

## Pointers and Arrays

| Rule                                                                                                                                               | Description                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 17.4<br>(Required)                                                                                                                                 | Array indexing shall be the only allowed form of pointer arithmetic.                                                                      |
| Message in log: <ul style="list-style-type: none"> <li>• Array indexing shall be the only allowed form of pointer arithmetic.</li> </ul>           |                                                                                                                                           |
| <hr/> <b>Note</b> Warning on operations on pointers. ( $p+I$ , $I+p$ and $p-I$ , where $p$ is a pointer and $I$ an integer). Can be turned to Off. |                                                                                                                                           |
| 17.6<br>(Required)                                                                                                                                 | The address of an object with automatic storage shall not be assigned to an object that may persist after the object has ceased to exist. |

| Rule | Description                                                                                                                                                                  |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <p>Message in log:</p> <ul style="list-style-type: none"> <li>• Pointer to a parameter is an illegal return value. Pointer to a local is an illegal return value.</li> </ul> |
|      | <p><b>Note</b> Warning when returning a local variable address or a parameter address. Can be turned to Off.</p>                                                             |

## Preprocessing Directives

| Rule               | Description                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 19.4<br>(Required) | C macros shall only expand to a braced initializer, a constant, a parenthesized expression, a type qualifier, a storage class specifier, or a do-while-zero construct. |
|                    | <p>Message in log:</p> <ul style="list-style-type: none"> <li>• Macro '&lt;name&gt;' does not expand to a compliant construct.</li> </ul>                              |

| Rule                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | <p><b>Note</b> We assume that a macro definition does not violate this rule when it expands to:</p> <ul style="list-style-type: none"> <li>• a braced construct (not necessarily an initializer)</li> <li>• a parenthesized construct (not necessarily an expression)</li> <li>• a number</li> <li>• a character constant</li> <li>• a string constant (can be the result of the concatenation of string field arguments and literal strings)</li> <li>• the following keywords: typedef, extern, static, auto, register, const, volatile, __asm__ and __inline__</li> <li>• a do-while-zero construct</li> </ul> <p>Can be turned to Off.</p> |
| 19.15<br>(Required) | Precautions shall be taken in order to prevent the contents of a header file being included twice.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Rule | Description                                                                                                                                                                                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <p>Message in log:</p> <ul style="list-style-type: none"><li>• Precautions shall be taken in order to prevent multiple inclusions.</li></ul>                                                                                                                                                                                                                        |
|      | <p><b>Note</b> When a header file is formatted as follows:</p> <pre data-bbox="427 499 771 621">#ifndef &lt;control macro&gt; #define &lt;control macro&gt; &lt;contents&gt; #endif</pre> <p>It is assumed that precautions have been taken to prevent multiple inclusions. Otherwise, a violation of this MISRA rule is detected.</p> <p>Can be turned to Off.</p> |

## Rules Not Checked

| In this section...                    |
|---------------------------------------|
| “Environment” on page 11-51           |
| “Language Extensions” on page 11-52   |
| “Documentation” on page 11-52         |
| “Types” on page 11-53                 |
| “Functions” on page 11-54             |
| “Pointers and Arrays” on page 11-54   |
| “Structures and Unions” on page 11-55 |
| “Standard Libraries” on page 11-55    |

### Environment

| Rule              | Description                                                                                                                                                               | Comments                                                                          |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| 1.2<br>(Required) | No reliance shall be placed on undefined or unspecified behavior                                                                                                          | Not statically checkable unless the data dynamic properties is taken into account |
| 1.3<br>(Required) | Multiple compilers and/or languages shall only be used if there is a common defined interface standard for object code to which the language/compiler/assemblers conform. | It is a process rule method.                                                      |

| <b>Rule</b>       | <b>Description</b>                                                                                                                                                                                                                                                        | <b>Comments</b>                                                                              |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| 1.4<br>(Required) | The compiler/linker/Identifiers (internal and external) shall not rely on significance of more than 31 characters. Furthermore the compiler/linker shall be checked to ensure that 31 character significance and case sensitivity are supported for external identifiers. | The documentation of compiler must be checked.                                               |
| 1.5<br>(Advisory) | Floating point implementations should comply with a defined floating point standard.                                                                                                                                                                                      | The documentation of compiler must be checked as this implementation is done by the compiler |

## Language Extensions

| <b>Rule</b>       | <b>Description</b>                             | <b>Comments</b>                                                              |
|-------------------|------------------------------------------------|------------------------------------------------------------------------------|
| 2.4<br>(Advisory) | Sections of code should not be “commented out” | It might be some pseudo code or code that does not compile inside a comment. |

## Documentation

| <b>Rule</b>       | <b>Description</b>                                                | <b>Comments</b>                                                                                                                                                    |
|-------------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.1<br>(Required) | All usage of implementation-defined behavior shall be documented. | The documentation of compiler must be checked. Error detection is based on undefined behavior, according to choices made for implementation-defined constructions. |

| Rule              | Description                                                                                                                                                   | Comments                                       |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
|                   |                                                                                                                                                               | Documentation can not be checked.              |
| 3.2<br>(Required) | The character set and the corresponding encoding shall be documented.                                                                                         | The documentation of compiler must be checked. |
| 3.3<br>(Advisory) | The implementation of integer division in the chosen compiler should be determined, documented and taken into account.                                        | The documentation of compiler must be checked. |
| 3.4<br>(Required) | All uses of the <i>#pragma</i> directive shall be documented and explained.                                                                                   | The documentation of compiler must be checked. |
| 3.5<br>(Required) | The implementation-defined behavior and packing of bitfields shall be documented if being relied upon.                                                        | The documentation of compiler must be checked. |
| 3.6<br>(Required) | All libraries used in production code shall be written to comply with the provisions of this document, and shall have been subject to appropriate validation. | The documentation of compiler must be checked. |

## Types

| Rule              | Description                                                                                 | Comments                                                                                                           |
|-------------------|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| 6.2<br>(Required) | Signed and unsigned char type shall be used only for the storage and use of numeric values. | Consider an external function returning a char is been used and increased. There is no mean without the functional |

| Rule | Description                                                             | Comments                                                      |
|------|-------------------------------------------------------------------------|---------------------------------------------------------------|
|      | <hr/> <b>Note</b> this rule is partially implemented in Rule 6.1. <hr/> | knowledge that this function stores a character value or not. |

## Functions

| Rule                | Description                                                                                                                                   | Comments                                                                |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| 16.7<br>(Advisory)  | A pointer parameter in a function prototype should be declared as pointer to const if the pointer is not used to modify the addressed object. | Not statically checkable unless the pointer verification has been done. |
| 16.10<br>(Required) | If a function returns error information, then that error information shall be tested.                                                         | Not statically checkable unless type defining error is standardized.    |

## Pointers and Arrays

| Rule               | Description                                                                                    | Comments                                                               |
|--------------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| 17.1<br>(Required) | Pointer arithmetic shall only be applied to pointers that address an array or array element.   | Not statically checkable unless the pointer verification has been done |
| 17.2<br>(Required) | Pointer subtraction shall only be applied to pointers that address elements of the same array. | Not statically checkable unless the pointer verification has been done |
| 17.3<br>(Required) | >, >=, <, <= shall not be applied to pointer types except where they point to the same array.  | Not statically checkable unless the pointer verification has been done |



## Structures and Unions

| Rule               | Description                                                   | Comments                                                                          |
|--------------------|---------------------------------------------------------------|-----------------------------------------------------------------------------------|
| 18.2<br>(Required) | An object shall not be assigned to an overlapping object.     | Not statically checkable unless the data dynamic properties is taken into account |
| 18.3<br>(Required) | An area of memory shall not be reused for unrelated purposes. | "purpose" is functional design issue.                                             |

## Standard Libraries

| Rule               | Description                                                          | Comments                                                              |
|--------------------|----------------------------------------------------------------------|-----------------------------------------------------------------------|
| 20.3<br>(Required) | The validity of values passed to library functions shall be checked. | Not statically checkable unless all library function are standardized |



# Using PolySpace Software in the Eclipse IDE

---

## Verifying Code in the Eclipse IDE

| In this section...                                                   |
|----------------------------------------------------------------------|
| “Creating an Eclipse Project” on page 12-3                           |
| “Setting Up PolySpace Verification with Eclipse Editor” on page 12-4 |
| “Launching Verification from Eclipse Editor” on page 12-5            |
| “Reviewing Verification Results from Eclipse Editor” on page 12-5    |
| “Using the PolySpace Spooler” on page 12-6                           |

You can apply the powerful code verification of PolySpace software to code that you develop within the Eclipse Integrated Development Environment (IDE).

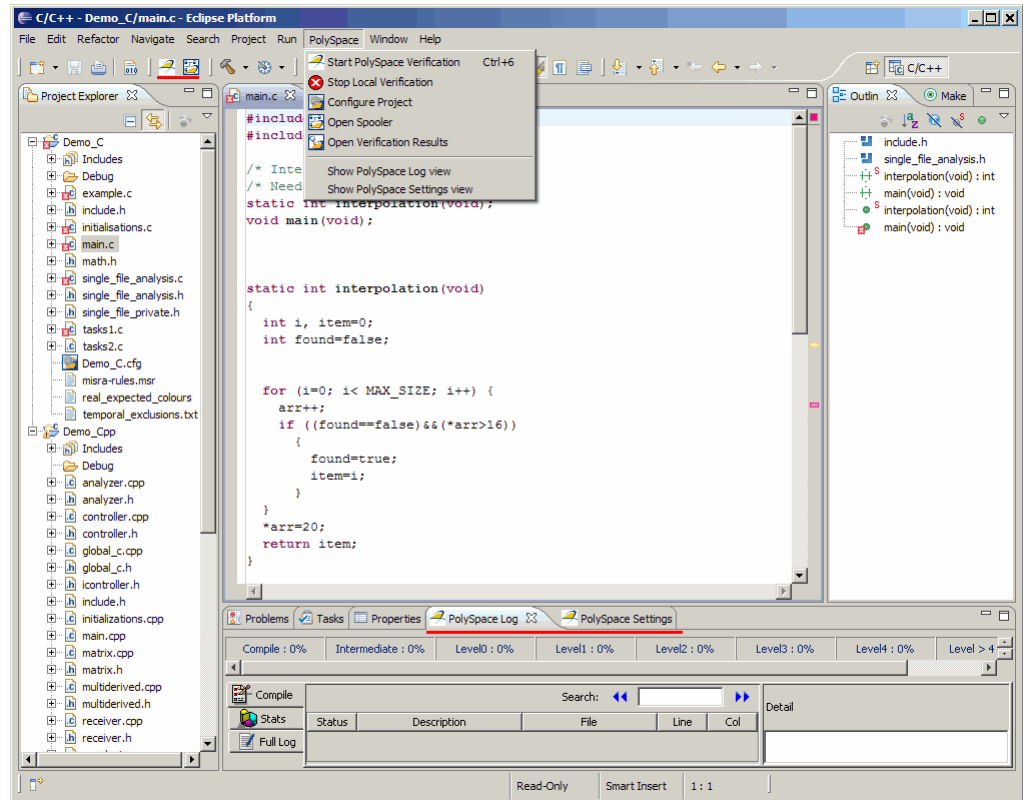
A typical workflow is:

- 1** Use the Eclipse™ editor to create an Eclipse project and develop code within your project.
- 2** Set up the PolySpace verification by configuring analysis options and settings.
- 3** Start the verification and monitor the process.
- 4** Review the verification results.

Install the PolySpace plug-in for Eclipse IDE before you verify code in Eclipse IDE. For more information, see “PolySpace Plug-In Requirements” and “Installing the PolySpace C/C++ Plug-In for Eclipse IDE” in the *PolySpace Installation Guide*.

Once you have installed the plug-in, in the Eclipse editor, you have access to:

- A **PolySpace** menu
- Toolbar buttons you use to launch a verification and open the PolySpace spooler
- **PolySpace Log** and **PolySpace Setting** views



## Creating an Eclipse Project

If your source files do not belong to an Eclipse project, then create one using the Eclipse editor:

- 1 Select **File > New > C Project**.
- 2 Clear the **Use default location** check box.
- 3 Click **Browse** to navigate to the folder containing your source files, for example, `C:\Test\Source_c`.
- 4 In the **Project name** field, enter a name, for example, `Demo_C`.

- 5 In the **Project Type** tree, under **Executable**, select **Empty Project** .
- 6 Under **Toolchains**, select your installed toolchain, for example, MinGW GCC.
- 7 Click **Finish**. An Eclipse project is created.

For information on developing code within Eclipse IDE, refer to [www.eclipse.org](http://www.eclipse.org).

## Setting Up PolySpace Verification with Eclipse Editor

### Analysis Options

To specify analysis options for your verification:

- 1 In **Project Explorer**, select the project or files that you want to verify.
- 2 Select **PolySpace > Configure Project** to open the PolySpace Launcher for C window.
- 3 Under **Analysis options**, select your options for the verification process.
- 4 Save your options.

For information on *how* to choose your options, see “Options Description” in the *PolySpace Products for C Reference Guide*

---

**Note** Your Eclipse compiler options for include paths (-I) and symbol definitions (-D) are automatically added to the list of PolySpace analysis options.

To view the -I and -D options in the Eclipse editor :

- 1 Select **Project > Properties** to open the Properties for Project dialog box.
  - 2 In the tree, under **C/C++ General** , select **Paths and Symbols** .
  - 3 Select **Includes** to view the -I options or **Symbols** to view the -D options.
-

## Other Settings

In the **PolySpace Settings** view, specify:

- In the **Results directory** field, the location of your results folder .
- The required **Verification level**, for example, **Level14**.

You can also do the following in the **PolySpace Settings** view :

- Generate a main (if the item you select does not contain one) by selecting the **Generate a main** check box. If you want to change the default behavior of the main generator, specify advanced settings through the `-main-generator-writes-variables` and `-main-generator-calls` options in the PolySpace Launcher for C window. Select **PolySpace > Configure Project** to open this window.
- Specify the `-function-called-before-main` option. In the **Startup function to call** field, enter the name of the function that you want to call before all selected functions in main.

## Launching Verification from Eclipse Editor

To launch a PolySpace verification from the Eclipse editor:

- 1 Select the file, files, or class that you want to verify.
- 2 Either right-click and select **Start PolySpace Verification**, or select **PolySpace > Start PolySpace Verification**.

You can see the progress of the verification in the **PolySpace Log** view. If you see an error or warning, double-click it to go to the corresponding location in the source code.

To stop a verification, select **PolySpace > Stop Local Verification**.

For more information on monitoring the progress of a verification, see Chapter 6, “Running a Verification” in the *PolySpace Products for C User Guide*.

## Reviewing Verification Results from Eclipse Editor

Use the PolySpace Viewer to examine results of the verification:

- 1 Select **PolySpace > Open Verification Results** to open the PolySpace Viewer.
- 2 If results are available in the specified **Results directory**, then these results appear automatically in the Viewer window.

For information on reviewing and understanding PolySpace verification results, see Chapter 8, “Reviewing Verification Results” in the *PolySpace Products for C User Guide*.

### Using the PolySpace Spooler

Use the PolySpace spooler to manage jobs running on remote servers. To open the spooler, select **PolySpace > Open Spooler** .

For more information, see “Managing Verification Jobs Using the PolySpace Queue Manager” on page 6-7 in the *PolySpace Products for C User Guide*.



**Atomic**

In computer programming, atomic describes a unitary action or object that is essentially indivisible, unchangeable, whole, and irreducible.

**Atomicity**

In a transaction involving two or more discrete pieces of information, either all of the pieces are committed or none are.

**Batch mode**

Execution of PolySpace from the command line, rather than via the launcher Graphical User Interface.

**Category**

One of four types of orange check: *potential bug*, *inconclusive check*, *data set issue* and *basic imprecision*.

**Certain error**

See "red check."

**Check**

A test performed by PolySpace during a verification and subsequently colored red, orange, green or gray in the viewer.

**Code verification**

The PolySpace process through which code is tested to reveal definite and potential runtime errors and a set of results is generated for review.

**Dead Code**

Code which is inaccessible at execution time under all circumstances due to the logic of the software executed prior to it.

**Development Process**

The process used within a company to progress through the software development lifecycle.

**Green check**

Code has been proven to be free of runtime errors.

**Gray check**

Unreachable code; dead code.

**Imprecision**

Approximations are made during a PolySpace verification, so data values possible at execution time are represented by supersets including those values.

**mcpu**

Micro Controller/Processor Unit

**Orange check**

A warning that represents a possible error which may be revealed upon further investigation.

**PolySpace Approach**

The manner of use of PolySpace to achieve a particular goal, with reference to a collection of techniques and guiding principles.

**Precision**

An verification which includes few inconclusive orange checks is said to be precise

**Progress text**

Output from PolySpace during verification to indicate what proportion of the verification has been completed. Could be considered as a “textual progress bar”.

**Red check**

Code has been proven to contain definite runtime errors (every execution will result in an error).

**Review**

Inspection of the results produced by a PolySpace verification.

**Scaling option**

Option applied when an application submitted to PolySpace proves to be bigger or more complex than is practical.

**Selectivity**

The ratio (green checks + gray checks + red checks) / (total amount of checks)

**Unreachable code**

Dead code.

**Verification**

The PolySpace process through which code is tested to reveal definite and potential runtime errors and a set of results is generated for review.



## A

- access sequence graph 8-31
- active project
  - definition 10-3
  - setting 10-3
- analysis options 3-16 3-19
  - generic targets 3-32
  - MISRA C compliance 3-24 11-4
- ANSI compliance 6-3
- assistant mode
  - criterion 8-20
  - custom methodology 8-23
  - methodology 8-20
  - methodology for C 8-20 to 8-21
  - overview 8-19
  - reviewing checks 8-24
  - selection 8-19
  - use 8-19 8-24

## C

- call graph 8-31
- call tree view 8-13
- calling sequence 8-31
- cfg. *See* configuration file
- client 1-6 6-2
  - installation 1-6
  - verification on 6-22
- Client
  - overview 1-6
- coding review progress view 8-13 8-32
- color-coding of verification results 1-3 8-15
- compile
  - log 7-8
- compile log
  - Launcher 6-24
  - Spooler 6-7
- compile phase 6-3
- compliance

- ANSI 6-3

- MISRA C 1-2 3-24 11-4

- composite filters 8-38
- configuration file
  - definition 3-2
- contextual verification 2-5
- criteria
  - quality 2-8
- custom methodology
  - definition 8-23

## D

- data range specifications 2-6
- default directory
  - changing in preferences 3-6
- desktop file
  - definition 3-2
- directories
  - includes 3-10 3-13 3-15
  - results 3-10 3-13 3-15
  - sources 3-10 3-13 3-15
- downloading
  - results 8-8
  - results to UNIX or Linux clients 8-11
  - unit-by-unit verification results 8-12
- DRS 2-6
- dsk. *See* desktop file

## E

- error call graph 8-31
- expert mode
  - filters 8-37
    - composite 8-38
    - individual 8-37
  - overview 8-27
  - selection 8-27
  - use 8-27

**F**

## files

- includes 3-10 3-13 3-15
- results 3-10 3-13 3-15
- source 3-10 3-13 3-15

## filters 8-37

- alpha 8-38
- beta 8-38
- custom
  - modification 8-38 to 8-39
  - use 8-38 to 8-39
- gamma 8-38
- individual 8-37
- user def 8-38

**G**

## generic target processors

- adding 3-31
- definition 3-32
- deleting 3-35

## global variable graph 8-31

**H**

## hardware requirements 7-2

## help

- accessing 1-8

**I**

## installation

- PolySpace Client for C/C++ 1-6
- PolySpace products 1-6
- PolySpace Server for C/C++ 1-6

**L**

## Launcher

- monitoring verification progress 6-24

- opening 3-3

- starting verification on client 6-22

- starting verification on server 6-3

- viewing logs 6-24

- window 3-3

- overview 3-3

- progress bar 6-24

## level

- quality 2-8

## licenses

- obtaining 1-6

## logs

## compile

- Launcher 6-24

- Spooler 6-7

## full

- Launcher 6-24

- Spooler 6-7

## stats

- Launcher 6-24

- Spooler 6-7

## viewing

- Launcher 6-24

- Spooler 6-7

**M**

- methodology for C 8-20 to 8-21

- MISRA C compliance 1-2

- analysis option 3-24 11-4

- checking 3-24 11-4

- file exclusion 3-28 11-7

- log 11-11

- rules file 3-26 11-5

**O**

## objectives

- quality 2-5

**P**

PolySpace Client  
     overview 1-6  
 PolySpace Client for C/C++  
     installation 1-6  
     license 1-6  
 PolySpace In One Click  
     active project 10-3  
     overview 10-2  
     sending files to PolySpace software 10-5  
     starting verification 10-5  
     use 10-2  
 PolySpace products for C  
     components 1-6  
     installation 1-6  
     licenses 1-6  
     overview 1-2  
     related products 1-6  
     user interface 1-6  
 PolySpace project model file  
     creation 3-31  
     definition 3-31  
     use 3-30  
 PolySpace Queue Manager Interface. *See* Spooler  
 PolySpace Server  
     overview 1-6  
 PolySpace Server for C/C++  
     installation 1-6  
     license 1-6  
 ppm. *See* PolySpace project model file  
 preferences  
     Launcher  
         default directory 3-6  
         default server mode 6-3  
         generic targets 3-31  
         server detection 7-4  
     Viewer  
         assistant configuration 8-21  
         display columns in RTE view 8-34  
 procedural entities view 8-13

        reviewed column 8-34  
 product overview 1-2  
 progress bar  
     Launcher window 6-24  
 project  
     creation 3-2  
     definition 3-2  
     directories  
         includes 3-3  
         results 3-3  
         sources 3-3  
     file types  
         configuration file 3-2  
         desktop file 3-2  
         PolySpace project model file 3-2  
         saving 3-18  
 project model file. *See* PolySpace project model file

**Q**

quality level 2-8  
 quality objectives 2-5 3-19

**R**

related products 1-6  
     PolySpace products for linking to Models 1-7  
     PolySpace products for verifying Ada  
         code 1-7  
     PolySpace products for verifying C++  
         code 1-7  
 reports  
     generation 8-44  
 results  
     directory 3-10 3-13 3-15  
     downloading from server 8-8  
     downloading to UNIX or Linux clients 8-11  
     opening 8-12  
     report generation 8-44

- unit-by-unit 8-12
- reviewed column 8-34
- robustness verification 2-5
- rte view. *See* procedural entities view

## S

- selected check view 8-13
- server 1-6 6-2
  - detection 7-4
  - information in preferences 7-4
  - installation 1-6 7-4
  - verification on 6-3
- Server
  - overview 1-6
- source code view 8-13
- Spooler
  - monitoring verification progress 6-7
  - removing verification from queue 8-8
  - use 6-7
  - viewing log 6-7

## T

- troubleshooting failed verification 7-2

## V

- variables view 8-13
- verification
  - Ada code 1-7
  - C code 1-2
  - C++ code 1-7
  - client 6-2
  - compile phase 6-3
  - contextual 2-5
  - failed 7-2

- monitoring progress
  - Launcher 6-24
  - Spooler 6-7
- phases 6-3
- results
  - color-coding 1-3
  - opening 8-12
  - report generation 8-44
  - reviewing 8-8
- robustness 2-5
- running 6-2
- running on client 6-22
- running on server 6-3
- starting
  - from Launcher 6-2 to 6-3 6-22
  - from PolySpace In One Click 6-2 10-5
- stopping 6-25
- troubleshooting 7-2
- with MISRA C checking 11-10

## Viewer

- modes
  - selection 8-16
- opening 8-12
- window
  - call tree view 8-13
  - coding review progress view 8-13
  - overview 8-13
  - procedural entities view 8-13
  - selected check view 8-13
  - source code view 8-13
  - variables view 8-13

## W

- workflow
  - setting quality objectives 2-5