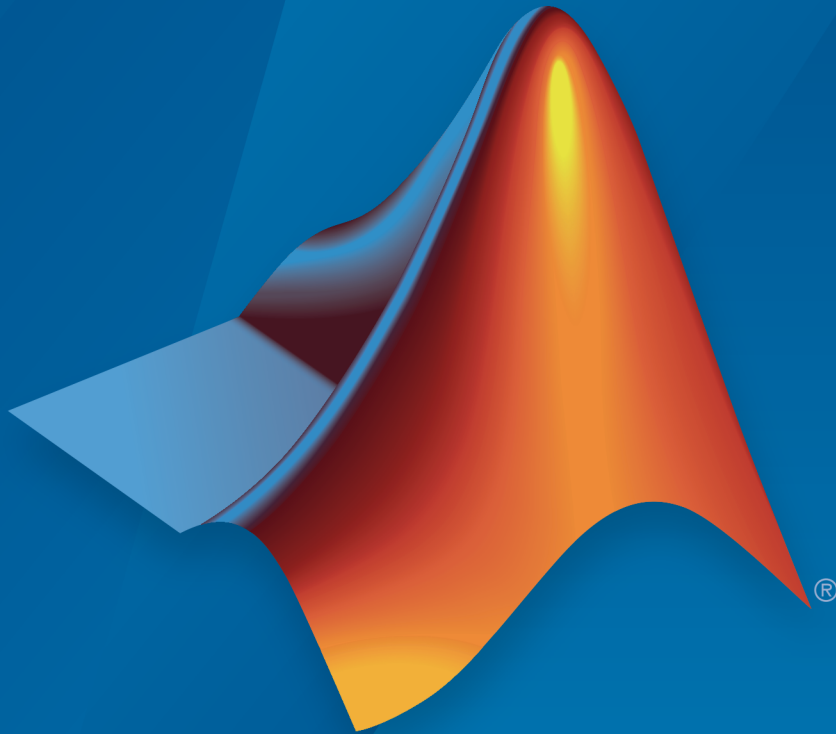


Polyspace[®] Bug Finder[™] Release Notes



MATLAB[®]&SIMULINK[®]

How to Contact MathWorks



Latest news: www.mathworks.com
Sales and services: www.mathworks.com/sales_and_services
User community: www.mathworks.com/matlabcentral
Technical support: www.mathworks.com/support/contact_us



Phone: 508-647-7000



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

Polyspace[®] Bug Finder[™] Release Notes

© COPYRIGHT 2013–2016 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

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

Analysis Setup	1-2
Diab Compiler Support: Set up Polyspace analysis easily for code compiled with Wind River Diab compiler	1-2
Multitasking Code Analysis Setup: Specify cyclic tasks and nonpreemptable interrupts directly as analysis options ...	1-2
Improved source and include folder management	1-2
Writable Examples: Modify example projects and restore original versions	1-3
Run analysis on <code>.psprj</code> file from the command line	1-3
DOS or UNIX Command Line	1-3
MATLAB Command Prompt	1-4
Support for local threads	1-4
Polyspace API in MATLAB: Configure and run Polyspace using MATLAB objects	1-4
Configuration Parameters Help: View descriptions of Polyspace options in Simulink configuration parameters	1-5
Eclipse Build Support: Set up Polyspace analysis from Eclipse build command	1-6
Visual Studio 2010 add-in support to be removed from installation	1-6
Support for Rhapsody 8.1	1-6
DOS Mode Warning on Linux: Compilation warning for DOS inconsistencies	1-6
Faster Restart for Remote Verification: Reuse compilation results from a previous analysis	1-7
Changes in Target & Compiler analysis options	1-7
Changes in analysis options and binaries	1-9
Analysis Results	1-12
CERT C Support: Identify CERT C violations using defect checkers and coding rules	1-12

Local Variable Size Estimation: Find total size of local variables in a function	1-14
Metrics for C++ Templates: View code complexity metrics for instances of C++ templates	1-14
Changes to coding rule checking	1-15
Expanded MISRA C++ Support	1-15
Updated Specifications	1-15
Updated Bug Finder defects	1-16
Changes in supported CWE IDs	1-17
Reviewing Results	1-21
Data Race Graphs: Fix data race defects easily using graphical view of function call sequence	1-21
Interactive Graphical Display: Click graphs on Dashboard to filter results	1-22
Event History for Coding Rules: Navigate easily between two locations in code that together cause a rule violation	1-23
Results in Macros Consolidated: View coding rule violations and defects on macro definitions instead of macro instances . .	1-23
Analysis Objectives in Eclipse: Create review scopes to focus your review	1-23
Filtered Report: Reuse result filters for generated report . . .	1-24
Results Export: Export results to text file for computing graphs and statistics	1-24
Coding Rules in Report: View improved presentation of coding rules violations in report	1-24
Coding Rule Graphs	1-24
Coding Rule Template	1-25
English Reports in Non-English Locales: Generate English reports on operating systems with a different language . .	1-25
Change in report template location	1-26
Improved PDF Report Generation	1-26
Changes in Polyspace User Interface	1-26

R2016a

Analysis Setup	2-2
---------------------------------	------------

Files to Review: Generate results for only specified files and folders	2-2
Faster MISRA Checking: Check coding rules more quickly and efficiently	2-2
S-Function Analysis: Launch analysis of S-Function code from Simulink	2-3
Import signal ranges from model for generated code analysis	2-3
Polyspace Metrics Tomcat Upgrade: Use upgraded default Tomcat server or custom Tomcat version	2-3
Polyspace Metrics Interface Updated: View project and metrics summary and defect impact	2-4
Source Code Search: Search huge applications more quickly	2-4
Default Layouts: Switch easily between project setup and results review in user interface	2-4
Files Not Compiled: Receive alerts about compilation errors in dashboard and reports	2-5
Project Language Flexibility: Change your project language at any time	2-5
Improvements in automatic project creation from build command	2-5
Polyspace TargetLink plug-in supports data from structures	2-6
Changes in analysis options	2-6
Analysis Results	2-9
Improvements to defect checkers	2-9
Improvements in checking of previously supported MISRA C rules	2-9
MISRA C:2004 Rules	2-9
MISRA C:2012 Rules	2-10
Standards Mapped to Defects: Observe coding standards using Polyspace Bug Finder	2-10
CERT C mapping	2-10
CWE ID mapping	2-10
Reviewing Results	2-12
More results available in real time	2-12
Autocompletion for Review Comments: Partially type previous comment to select complete comment	2-12
Persistent Filter States: Apply filters once and view filtered results across multiple runs	2-12
Polyspace Eclipse plug-in results location moved	2-13

Bug Fixes**R2015b**

Analysis Setup	4-2
Mixed C/C++ Code: Run analysis on entire project with C and C++ source files	4-2
Autodetection of Multitasking Primitives: Analyze source code with multitasking primitives from POSIX and VxWorks without manual setup	4-2
Microsoft Visual C++ 2013: Analyze code developed in Microsoft Visual C++ 2013	4-3
GNU 4.9 and Clang 3.5 Support: Analyze code compiled with GNU 4.9 or Clang 3.5	4-3
Improvements to automatic project creation from build command	4-3
Start Page: Get oriented with Polyspace Bug Finder	4-5
Saved Layouts: Save your preferred layouts of the Polyspace user interface	4-5
Renaming of labels in Polyspace user interface	4-6
Including options multiple times	4-6
Updated Support for TargetLink	4-7
Changes in analysis options	4-7
Binaries removed	4-11
Support for Visual Studio 2008 to be removed	4-11
Import Visual Studio project removed	4-11
Analysis Results	4-12
More Defect Categories: Detect security vulnerabilities, resource management issues, object oriented design issues	4-12
Complete MISRA C:2012 Support: Detect violations of all MISRA C:2012 rules	4-12

Improvements in checking of previously supported MISRA C rules	4-13
MISRA C:2004	4-13
MISRA C:2012	4-14
Checking Coding Rules Using Text Files	4-15
Changes to Bug Finder Defects	4-15
New Defects	4-16
Updated Defects	4-21
Reviewing Results	4-23
Results in Real Time: View results as they are produced . . .	4-23
Improved Eclipse Support: View results embedded in source code and context-sensitive help	4-23
Defects Classified by Impact: Prioritize defect review by using the impact attribute assigned to each defect type	4-24
Improved Review Capability: View result details and add review comments in one window	4-25
Enhanced Review Scope: Filter coding rule violations from display in one click	4-25
Configuration Associated with Result Not Opened by Default	4-26
Improvements in Report Templates	4-26
XML and RTF report formats removed	4-27

R2015a

Analysis Setup	5-2
Simplified workflow for project setup and results review with a unified user interface	5-2
Search improvements in the user interface	5-3
Option to specify program termination functions	5-3
Support for GCC 4.8	5-3
Polyspace plug-in for Simulink improvements	5-4
Integration with Simulink projects	5-4
Back-to-model available when Simulink is closed	5-4
Polyspace binaries being removed	5-4
Import Visual Studio project being removed	5-5
Analysis Results	5-6

Changes to Bug Finder defects	5-6
Improvements in coding rules checking	5-6
Reviewing Results	5-9
Code complexity metrics available in user interface	5-9
Context-sensitive help for code complexity metrics, MISRA- C:2012, and custom coding rules	5-9
Review of latest results compared to the last run	5-9
Simplified results infrastructure	5-10
Default statuses to justify results	5-10
Filters to limit display of results	5-10

R2014b

Analysis Setup	6-2
Parallel compilation for faster analysis	6-2
Support for Mac OS	6-2
Support for C++11	6-2
Code editor in Polyspace interface	6-3
Ignore files and folders during analysis	6-3
Simulink plug-in support for custom project files	6-3
TargetLink support updated	6-3
AUTOSAR support added	6-4
Remote launcher and queue manager renamed	6-4
Improved global menu in user interface	6-4
Improved Project Manager perspective	6-5
Polyspace binaries being removed	6-6
Import Visual Studio project being removed	6-6
Analysis Results	6-7
Support for MISRA C:2012	6-7
Additional concurrency issue detection (deadlocks, double locks, and others)	6-7
Data race errors	6-7
Locking errors	6-7
New and updated defect checkers	6-8

Reviewing Results	6-10
Context-sensitive help for analysis options and defects	6-10
Improved Results Manager perspective	6-10
Error mode removed from coding rules checking	6-11

R2014a

Analysis Setup	7-2
Automatic project setup from build systems	7-2
Support for GNU 4.7 and Microsoft Visual Studio C++ 2012 dialects	7-2
Simplification of coding rules checking	7-3
Preferences file moved	7-4
Security level support for batch analysis	7-4
Interactive mode for remote analysis	7-5
Default text editor	7-5
Support for Windows 8 and Windows Server 2012	7-5
Function replacement in Simulink plug-in	7-6
Check model configuration automatically before analysis . . .	7-6
Data range specification support	7-7
Polyspace binaries being removed	7-7
Analysis Results	7-8
Classification of bugs according to the Common Weakness Enumeration (CWE) standard	7-8
Additional coding rules support (MISRA-C:2004 Rule 18.2, MISRA-C++ Rule 5-0-11)	7-8
Additional analysis checkers	7-8
Improvement of floating point precision	7-9
Reviewing Results	7-10
Results folder appearance in Project Browser	7-10
Results manager improvements	7-11
Additional back-to-model support for Simulink plug-in	7-13

Analysis Setup	8-2
Introduction of Polyspace Bug Finder	8-2
Fast analysis of large code bases	8-2
Eclipse integration	8-2
Analysis Results	8-3
Detection of run-time errors, data flow problems, and other defects in C and C++ code	8-3
Compliance checking for MISRA-C:2004, MISRA-C++:2008, JSF++, and custom naming conventions	8-3
Cyclomatic complexity and other code metrics	8-4
Reviewing Results	8-5
Traceability of code analysis results to Simulink models	8-5
Access to Polyspace Code Prover results	8-5

R2016b

Version: 2.2

New Features

Bug Fixes

Compatibility Considerations

Analysis Setup

Diab Compiler Support: Set up Polyspace analysis easily for code compiled with Wind River Diab compiler

If you build your source code with the Wind River® Diab compiler, in R2016b, you can easily set up a Polyspace® project to verify your code. After you specify the Diab compiler and your target processor, the verification:

- Implicitly defines macros that are defined for the Diab compiler. Previously, you defined the macros in your Polyspace project explicitly to avoid compilation errors.
- Understands language extensions such as keywords and pragmas that are specific to the Diab compiler. Previously, you removed unknown language extensions explicitly from the preprocessed code in your Polyspace project to avoid compilation errors.

You can now set up a Polyspace project manually without knowing the internal workings of your Diab compiler. Specify the Diab compiler and your target processor, and run an analysis without facing compilation errors. See Diab Compiler (-compiler diab).

The software supports version 5.9 and older versions of the Diab compiler.

Multitasking Code Analysis Setup: Specify cyclic tasks and nonpreemptable interrupts directly as analysis options

In R2016b, you can specify which entry points in your code represent cyclic tasks and nonpreemptable interrupts. Previously, to emulate the cyclic behavior of a task, you embedded instructions in a loop. To emulate a nonpreemptable interrupt, you specified temporally exclusive pairs where the interrupt was paired with the other interrupts.

For more information, see Cyclic tasks (-cyclic-tasks) and Interrupts (-interrupts).

Improved source and include folder management

Before R2016b, when you created a project, you added and removed source files and include folders individually. If you moved your source files or added new files to your programming project, you re-added the files into your Polyspace project.

Starting in R2016b, you create Polyspace projects with root source folders and include folders. The root folder location represents the top of the hierarchy for your source files.

Polyspace shows all files relative to the root source locations. When you add a root source location, you can:

- See all source files under the root folder (and subfolders)
- Exclude files and subfolders in the hierarchy to change the active list of source files to analyze.
- Refresh the source file list to see new files or folders in the root source hierarchy.
- Modify the root source folder path.
- If you use a revision control system, change the root folder location to point to different versions of your source files.

For include folders, instead of adding individual folders, you add a root include folder location. Polyspace adds all include folders underneath the root include location that contains include files. You can refresh and modify the include folder path.

For more information, see “Update Project”.

Writable Examples: Modify example projects and restore original versions

The examples projects under **Help > Examples** are now easier to use. The first time that you open an example project, a writable version is saved in your *Polyspace_Workspace*. In the writable project, you can test configuration options, change sources, and rerun the example. If you want to refresh the example with a clean version, select **Help > Examples > Restore Default Examples**.

Run analysis on .psprj file from the command line

If you already have a project created in the Polyspace Interface, you can now use that .psprj file to run your analysis from a command line.

DOS or UNIX Command Line

Use the new option `polyspace-bug-finder -generate-launching-script-for <PSPRJ FILE>` to generate the files to run the analysis from the command line. These files are generated:

- `source_command.txt` — List of source files in the project
- `options_command.txt` — List of analysis option settings

- `launchingCommand.sh` or `launchingCommand.bat` — Script that runs the analysis using `options_command.txt`, `source_command.txt`, and `.polyspace_conf.psprj`. The script can also take additional analysis options as parameters.

For more information, see “Create Command-Line Script from Project File”.

MATLAB Command Prompt

At the MATLAB® command prompt, you can now give a `.bf.psprj` file as an argument to `polyspaceBugFinder`.

The syntax `polyspaceBugFinder(PSPRJ file, '-nodesktop')` runs an analysis using the files and options from the *PSPRJ file*.

Support for local threads

Starting in R2016b, Polyspace adds support for these local thread modifiers:

- `__thread` — requires Compiler (-compiler) `gnu4.8`
- `__declspec(thread)` — requires **Compiler** (-compiler) `visual`
- `thread_local` — only for C++ code.

This support may eliminate compilation errors or false Data race results.

Polyspace API in MATLAB: Configure and run Polyspace using MATLAB objects

Polyspace scripting from the MATLAB command line is now easier and more MATLAB-friendly. R2016b introduces a set of classes, methods, and function improvements to help you run Polyspace from the MATLAB command line. For more information and examples, see the linked reference pages.

Classes

Name	Description
<code>polyspace.BugFinderOptions</code>	An options object with properties that map to the Polyspace environment configuration options. Use this object to customize analysis options and run analysis.

Name	Description
polyspace. ModelLinkBugFinderOptions	Another version of the <code>BugFinderOptions</code> object with properties specifically for model generated code. Use this object to customize analysis options and run analysis.
polyspace.GenericTargetOptions	A helper object for the <code>BugFinderOptions</code> classes. Use this object to customize a generic target.
polyspace.DefectsOptions	A helper object for the <code>BugFinderOptions</code> classes. Use this object to customize the list of defects checked during the analysis.
polyspace.CodingRulesOptions	A helper object for the <code>BugFinderOptions</code> object. Use this object to customize the list of coding rules checked during the analysis.

Methods

Name	Description
polyspace.Options.copyTo	Copy settings between options objects. You can use this method to copy options from a <code>BugFinderOptions</code> object to a <code>CodeProverOptions</code> object and vice versa.
polyspace.Options.generateProject	Generate a <code>.psprj</code> file from an options object to open in the Polyspace interface.

Functions

Name	Description
polyspaceBugFinder	Run an analysis using <code>BugFinderOptions</code> objects or <code>.psprj</code> files.

Configuration Parameters Help: View descriptions of Polyspace options in Simulink configuration parameters

When you use the Simulink[®] plugin, you must set Simulink configuration parameters to run your analysis. If you need help setting the configuration parameters, you can now right-click a configuration parameter and get **What's This** help. When you select **What's This**, a help window opens with details about the different settings and limitations of the parameter.

For more information about the configuration parameters, see “Configure Model Options”.

Eclipse Build Support: Set up Polyspace analysis from Eclipse build command

In R2016b, if you use a build command to build your source code in Eclipse™ or an IDE based on Eclipse, you can easily set up your Polyspace verification. To obtain the compiler options for the analysis, trace the build command inside the IDE. For more information, see “Customize Analysis Options”.

Visual Studio 2010 add-in support to be removed from installation

In a future release, the Polyspace add-in for Visual Studio® 2010 will no longer be included with the installation.

To run Polyspace on code from Visual Studio, use the automatic configuration tool instead. See “Create Project Using Visual Studio Information”.

If you still want to use the add-in, you will be able to download the add-in from MATLAB Answers.

Support for Rhapsody 8.1

The Polyspace plugin for IBM® Rational® Rhapsody® supports Rhapsody 8.1. For more information, see “Find Defects from IBM Rational Rhapsody”.

DOS Mode Warning on Linux: Compilation warning for DOS inconsistencies

When using Polyspace on Linux®, a new compilation warning may appear. On Windows®, DOS is case-insensitive meaning you cannot have two files with the same name but different capitalization. If you select the option Code from DOS or Windows file system (-dos), Polyspace simulates this DOS behavior on Linux. If your source files include header files with inconsistent capitalization and it is unclear which file should be included, Polyspace issues a compilation warning.

For example, consider these two situations:

	Include Statements	Include Files
Situation 1	<code>#include "myheader.h"</code> <code>#include "MYHEADER.h"</code> <code>#include "MyHeader.h"</code>	<code>myheader.h</code>
Situation 2	<code>#include "myheader.h"</code> <code>#include "MYHEADER.h"</code> <code>#include "MyHeader.h"</code>	<code>myheader.h</code> <code>MYHEADER.h</code>

In the first situation, only one file exists with the name `myheader.h`. Because these include statements can only refer to one file, there is no ambiguity about which file to include. No warning is issued.

In the second situation, two files exist: `myheader.h` and `MyHeader.h`. Because they have the same name and different capitalization, the capitalization in the include statement affects which file is included. Polyspace can find perfect matches for the first and second include statements. The last include statement is not a perfect match, so could refer to either header file. Because there is ambiguity with the last include statement, Polyspace issues this compilation warning: `warning: could not find include file "MyHeader.h"`.

In a future release, this compilation warning will become a compilation error.

Faster Restart for Remote Verification: Reuse compilation results from a previous analysis

In R2016b, if a remote analysis stops after compilation, for instance because of communication problems between the server and client computers, you do not have to restart the analysis from the beginning. You can reuse compilation results from the previous failed analysis.

For more information, see `-submit-job-from-previous-compilation-results`.

Changes in Target & Compiler analysis options

In R2016b, these **Target & Compiler** options have been added, changed, or removed.

Option	Change	More Information
Compiler (-compiler)	New option	

Option	Change	More Information
Dialect (-dialect)	Removed from the user interface. If you use the option in your scripts, you see a warning.	Option will be permanently removed in a future release. Replace <code>-dialect</code> with <code>-compiler</code> while retaining the option argument. In the user interface, this replacement is done automatically for existing projects. If you use the Wind River Diab compiler to build your source code, use the option <code>Compiler (-compiler)</code> with argument <code>diab</code> .
Target processor type (-target)	Updated for the Wind River Diab compiler.	In the user interface, if you select <code>diab</code> for <code>Compiler (-compiler)</code> , you see target processors that are tailored to the Diab compiler. For the processor specifications, see the contextual help.

Option	Change	More Information
Target operating system (-OS-target)	<p>Removed from the user interface.</p> <p>If you use the option in your scripts, you see a warning.</p>	<p>Option will be permanently removed in a future release.</p> <p>Remove the option from your scripts. For some option arguments, you might have to perform these additional steps:</p> <ul style="list-style-type: none"> • Linux: If you get compilation errors, use a <code>gnu.x</code> argument for Compiler (-compiler). <p>Sometimes, you might have to explicitly define operating-system-specific macros such as <code>linux</code>, <code>unix</code>, or <code>__linux__</code>. See Preprocessor definitions (-D).</p> <ul style="list-style-type: none"> • Visual: Use a <code>visualx.x</code> argument for Compiler (-compiler). • Vxworks: Use the options from the VxWorks[®] templates. <p>Create a Polyspace project using one of the VxWorks templates and generate a script from your project. Copy the options related to the VxWorks template from this script. For more information, see “Create Project Using Configuration Template” and the reference page for <code>-generate-launching-scripts-for</code>.</p> <ul style="list-style-type: none"> • Solaris: Just remove the option <code>-OS-target</code>. • no-predefined-OS: Just remove the option <code>-OS-target</code>.

Changes in analysis options and binaries

In R2016b, the following options have been added, changed, or removed.

For **Target & Compiler** options, see “Changes in Target & Compiler analysis options” on page 1-7. For other options, see here.

New Options

Option	Description
Cyclic tasks (-cyclic-tasks)	Specify functions that represent cyclic tasks.
Interrupts (-interrupts)	Specify functions that represent nonpreemptable interrupts.
-preemptable-interrupts	Specify functions that represent preemptable interrupts.
-non-preemptable-tasks	Specify functions that represent nonpreemptable tasks.

Updated Options

Option	Change	More Information
Coding rule subsets <code>single-unit-rules</code> and <code>system-decidable-rules</code>	Subsets now available from the drop-down list.	These subsets are available for Check MISRA C:2004 (-misra2), Check MISRA AC AGC (-misra-ac-age), and Check MISRA C:2012 (-misra3)

Removed Options

Option	Status	Description
Import Folder (-import-dir)	Warning	Option will be removed in a future release.
-easy-setup-preprocess	Warning	Option will be removed in a future release.
polyspace-automatic-verification	Warning	Binary will be removed in a future release.
polyspace-verifier	Warning	Binary will be removed in a future release.
rte-kernel	Warning	Binary will be removed in a future release.

Option	Status	Description
<code>polyspace-remote</code>	Warning	Binary will be removed in a future release.
<code>gui-api</code>	Warning	Binary will be removed in a future release. Use instead, <code>polyspace-comments-import</code> .
Files and folders to ignore (-includes-to-ignore)	Error	Use the option <code>Do not generate results for (-do-not-generate-results-for)</code> to suppress results from headers and sources in certain files or folders.
<code>-support-FX-option-results</code>	Error	Option will be removed in a future release.
<code>polyspace-vcproj</code>	Removed	Use <code>polyspace-configure</code> or the Polyspace Add-In for Visual Studio instead.

Compatibility Considerations

If you use scripts that contain the removed or updated options, change your scripts accordingly.

Analysis Results

CERT C Support: Identify CERT C violations using defect checkers and coding rules

In R2016b, you can comply with more CERT C Coding Standard rules using Polyspace defects and coding rules.

For more information, see “Mapping Between CERT C Standards and Polyspace Results”. The new defects added in R2016b specifically for CERT C support are listed here.

Concurrency

Name	Description	CERT C Rule
Data race through standard library function call	Certain standard library functions are called from multiple tasks without protection	CON33-C: Avoid race conditions when using library functions
Destruction of locked mutex	A task is trying to destroy a locked mutex that has not yet been unlocked	CON31-C: Do not destroy a mutex while it is locked

Good Practice

Name	Description	CERT C Rule
Bitwise and arithmetic operation on the same data	Code statement with mixed bitwise and arithmetic operations	INT14-C: Avoid performing arithmetic and bitwise operations on the same data
Missing reset of a freed pointer	Pointer free not followed by a reset statement to clear leftover data	MEM01-C: Store a new value in pointers immediately after free()
Missing break of switch case	No comments at the end of switch case without a break statement	MSC17-C: Finish every set of statements associated with a case label with a break statement

Name	Description	CERT C Rule
Hard-coded object size used to manipulate memory	Memory manipulation uses hard-coded size instead of <code>sizeof</code>	EXP09-C: Use <code>sizeof</code> to determine the size of a type or variable

Numerical

Name	Description	CERT C Rule
Use of plain char type for numerical value	Plain <code>char</code> variable used in arithmetic operation without explicit signedness	INT07-C: Use only explicitly signed or unsigned char type for numeric values
Bitwise operation on negative value	Undefined behavior for bitwise operations on signed values	INT13-C: Use bitwise operations only on unsigned operands

Programming

Name	Description	CERT C Rule
Unsafe conversion from string to numerical value	String to number conversion without validation checks	ERR34-C: Detect errors when converting a string to a number
Abnormal termination of exit handler	Exit handler function terminates incorrectly	ENV32-C: All exit handlers must return normally
Unsafe conversion between pointer and integer	Misaligned or invalid results from conversions between pointer and integer types	INT36-C: Unsafe conversion between pointer and integer

Resources

Name	Description	CERT C Rule
Opening previously opened resource	Opening an already opened file	FIO24-C: Do not open a file that is already open

Security

Name	Description	CERT C Rule
Returned value of a sensitive function not checked	Calls to sensitive or critical functions should be checked for	EXP12-C: Do not ignore values returned by functions

Name	Description	CERT C Rule
	unexpected return values and errors	ERR33-C: Detect and handle standard library errors
Bad order of dropping privileges	Dropped user or primary group privileges before dropping primary/supplementary group privileges	POS36-C: Observe correct revocation order while dropping privileges
Privilege drop not verified	Verify privilege relinquishment	POS37-C: Ensure that privilege relinquishment is successful

Local Variable Size Estimation: Find total size of local variables in a function

In R2016b, you can compute the total size of local variables in a function using the following two metrics:

- Lower Estimate of Local Variable Size: Total size of local variables taking nested scopes into account.

If a function has variable definitions in nested scopes, the software computes the total variable size in each scope and uses whichever total is greatest. For instance, if a conditional statement has variables definitions, the software computes the total variable size in each branch and then uses whichever total is greatest.

- Higher Estimate of Local Variable Size: Total size of all local variables.

Metrics for C++ Templates: View code complexity metrics for instances of C++ templates

In R2016b, you can compute code complexity metrics for C++ templates. If you instantiate a C++ template function and specify the option Calculate code metrics (-code-metrics), you can now see function metrics for the template in your analysis results.

The metrics appear on the template definition. The software uses the first instance of the template to calculate the metrics. If you specialize a template, you see separate metrics for the original template and its specialization.

For more information, see “Code Metrics”.

Changes to coding rule checking

Expanded MISRA C++ Support

The following MISRA C++:2008 rules are now supported.

- 0-1-9: There shall be no dead code.
- 0-1-11: There shall be no unused parameters (named or unnamed) in nonvirtual functions.
- 0-1-12: There shall be no unused parameters (named or unnamed) in the set of parameters for a virtual function and all the functions that override it.
- 0-2-1: An object shall not be assigned to an overlapping object.
- 16-6-1: All uses of the `#pragma` directive shall be documented.

Updated Specifications

The Polyspace specifications for the following rules have been updated.

Standard	Rule	Change
MISRA C++:2008	5-0-3	If two types have the same size in the target configuration, Polyspace no longer raises a violation.
	5-0-6	If two types have the same size in the target configuration, Polyspace no longer raises a violation.
	5-0-8	If two types have the same size in the target configuration, Polyspace no longer raises a violation.
MISRA C:2004 and MISRA AC AGC	10.1	If two types have the same size in the target configuration, Polyspace no longer raises a violation.
	10.2	If two types have the same size in the target configuration, Polyspace no longer raises a violation.
	10.3	If two types have the same size in the target configuration, Polyspace no longer raises a violation.
	10.4	If two types have the same size in the target configuration, Polyspace no longer raises a violation.
MISRA C:2012	10.3	If two types have the same size in the target configuration, Polyspace no longer raises a violation.
	10.6	If two types have the same size in the target configuration, Polyspace no longer raises a violation.

Standard	Rule	Change
	10.7	If two types have the same size in the target configuration, Polyspace no longer raises a violation.
	10.8	If two types have the same size in the target configuration, Polyspace no longer raises a violation.

Updated Bug Finder defects

For the new defects that explicitly correspond to CERT-C rules, see “CERT C Support: Identify CERT C violations using defect checkers and coding rules” on page 1-12.

Numerical

Name	Description	Update
Absorption of float operand	In an addition or subtraction, one operand is absorbed by the other and has no effect on the result	New defect

Programming

Name	Description	Update
Typedef mismatch	Mismatch between <code>typedef</code> statements	New defect

Static Memory

Name	Description	Update
Unreliable cast of function pointer	A function pointer is cast to another function pointer with different argument or return type	You can check C++ code for this defect.

Concurrency

Name	Description	Update
Data race	Multiple tasks perform unprotected non-atomic operations on shared variables	You can see a graphical view of the call sequence leading to

Name	Description	Update
		<p>conflicting operations on the shared variable.</p> <p>If you have existing critical sections, this graph also shows you the critical sections. Using this information, you can easily identify how to protect the shared variable from concurrent access.</p>

Data Flow

Name	Description	Update
Write without a further read	Variable not read after assignment	The defect does not appear if the variable that is assigned the value NULL and not read again.

Changes in supported CWE IDs

In R2016b, the following changes have been made in the mapping between CWE IDs and Polyspace Bug Finder™ defects.

CWE ID	Description	Prior to R2016b	R2016b
20	Improper input validation	Not supported	Unsafe conversion from string to numerical value
250	Execution with unnecessary privileges	Not supported	<p>Bad order of dropping privileges</p> <p>Privilege drop not verified</p>
252	Unchecked return value	Not supported	Returned value of a sensitive function not checked
273	Improper check for dropped privileges	Not supported	Privilege drop not verified

CWE ID	Description	Prior to R2016b	R2016b
362	Concurrent execution using shared resource with improper synchronization ('Race Condition')	Not supported	Opening previously opened resource
366	Race condition within a thread	Data race including atomic operations Data race	Data race including atomic operations Data race Data race through standard library function call
415	Double free	Deallocation of previously deallocated pointer	Deallocation of previously deallocated pointer Missing reset of a freed pointer
416	Use after free	Use of previously freed pointer	Missing reset of a freed pointer Use of previously freed pointer
465	Pointer Issues	Not supported	Unsafe conversion between pointer and integer
466	Return of pointer value outside of expected range	Array access out of bounds Pointer access out of bounds	Array access out of bounds Pointer access out of bounds Unsafe conversion between pointer and integer
484	Omitted break statement in switch	Not supported	Missing break of switch case

CWE ID	Description	Prior to R2016b	R2016b
587	Assignment of a fixed address to a pointer	Function pointer assigned with absolute address	Function pointer assigned with absolute address Unsafe conversion between pointer and integer
675	Duplicate operations on resource	Not supported	Opening previously opened resource
676	Use of potentially dangerous function	Use of dangerous standard function	Unsafe conversion between pointer and integer Use of dangerous standard function
682	Incorrect calculation	Float overflow Invalid use of standard library floating point routine Invalid use of standard library integer routine Tainted modulo operand	Absorption of float operand Bitwise operation on negative value Float overflow Invalid use of standard library floating point routine Invalid use of standard library integer routine Tainted modulo operand Use of plain char type for numerical value
696	Incorrect behavior order	Not supported	Bad order of dropping privileges
705	Incorrect control flow scoping	Not supported	Abnormal termination of exit handler
710	Coding standard violation	Not supported	Bitwise and arithmetic operation on the same data

CWE ID	Description	Prior to R2016b	R2016b
754	Improper check for unusual or exceptional conditions	Not supported	Returned value of a sensitive function not checked
758	Reliance on undefined, unspecified, or implementation-defined behavior	Not supported	Bitwise operation on negative value Unsafe conversion between pointer and integer Use of plain char type for numerical value
805	Buffer access with incorrect length value	Not supported	Hard-coded object size used to manipulate memory
826	Premature release of resource during expected lifetime	Not supported	Destruction of locked mutex
873	CERT C++ Secure Coding Section 05 - Floating point arithmetic (FLP)	Float overflow Invalid use of floating point operation Invalid use of standard library floating point routine	Absorption of float operand Float overflow Invalid use of floating point operation Invalid use of standard library floating point routine

For more information, see “Mapping Between CWE Identifiers and Defects”.

Reviewing Results


Data Race Graphs: Fix data race defects easily using graphical view of function call sequence

In R2016b, you can use a new graphical view to determine fixes for concurrency defects such as Data race. For each pair of conflicting operations on a shared variable, the graphical view shows:

- Two function call sequences leading to the two operations.

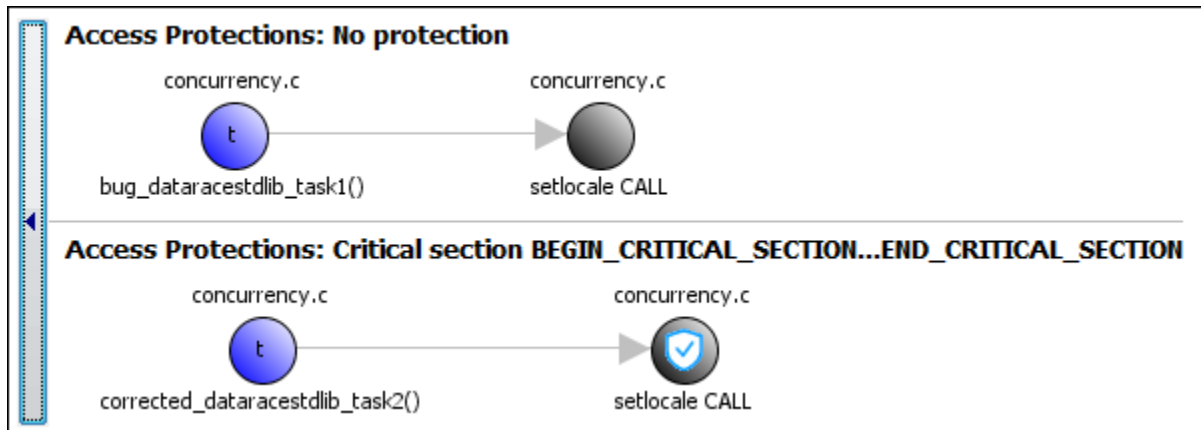
The first node in each sequence represents the entry point function. The last node represents the operation. The intermediate nodes represent functions call sequence leading from the entry point to the operations. To navigate to a function in your source code, click the corresponding node in the graph.

- Critical sections that are already active when a function is called.

If certain critical sections are active when a function is called, the corresponding node in the graph shows a  icon. To see which critical sections are active, place your cursor on the node.

Using this information, you can easily determine how to place appropriate protections and prevent two operations in different tasks/threads from conflicting with each other.

For instance, the following graph shows two tasks calling the function `setlocale`. The two calls are not protected by the same critical section even though the second call uses a critical section. To protect the two calls from interfering with each other, see the **Access Protections** entry for the critical section on the second call and reuse this critical section for the first call.



Interactive Graphical Display: Click graphs on Dashboard to filter results

In R2016b, you can narrow down the scope of your review by using a graphical display of analysis results. Previously you used the graphs to obtain an overview of the analysis results and determine which results to focus on. Now you can also select elements in the graphs to view only the results that you want to focus on. To see all results again, clear your filters in one click.

To filter results, you can use the following graphs:

- **Defect distribution by impact:** If you click a region on this pie chart that corresponds to the impact **High**, the **Results List** pane shows high-impact defects only.
- **Defect distribution by category (Top 10 only):** If you click a column corresponding to a defect, the **Results List** pane shows instances of that defect only.
- **Coding rule violations by rule (Top 10 only):** If you click a column corresponding to a coding rule, the **Results List** pane shows violations of that rule only.

For more information, see “Filter and Group Results”.

Event History for Coding Rules: Navigate easily between two locations in code that together cause a rule violation

In R2016b, for certain coding rules, the **Result Details** pane shows previous events causing the rule violation. You can click an event and navigate to the corresponding location in the source code.

MISRA C:2012 5.1 (Required) ? External identifiers shall be distinct. External variable engine_temperature_scaled conflicts with the external identifier engine_temperature_raw (file.c line 1).				
	Event	File	Scope	Line
1	Violation site	file.c	file.c	1
2	MISRA C:2012 5.1 ?	file.c	File Scope	2

This event history is shown for those rules which are related to more than one location in the code. For instance, the event history appears for the following rules:

- MISRA C[®]:2004 Rule 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.
- MISRA C:2012 Rule 5.1: External identifiers shall be distinct.
- MISRA[®] C++ Rule 2-10-1: Different identifiers shall be typographically unambiguous.
- JSF[®] C++ Rule 139: External objects will not be declared in more than one file.

Results in Macros Consolidated: View coding rule violations and defects on macro definitions instead of macro instances

When you run coding rules checking, violations from macro definitions can propagate throughout your code causing many results. In R2016b, coding rule violations and defects caused by a macro are now shown on the macro definition. This change reduces the number of results with the same root cause, making your review process simpler.

Analysis Objectives in Eclipse: Create review scopes to focus your review

From the Eclipse plugin, you can now create custom review scopes. Review scopes filter your results to only the defects, coding rules, or code metrics you want to see. For more information, see “Limit Display of Defects”.

Filtered Report: Reuse result filters for generated report

In R2016b, if you apply filters to your results, you can reuse those filters for the generated report. For instance, you can use filters to view only the following subset of results on the **Results List** pane and then reuse those filters for the report.

- View only high-impact defects and create a report with those defects only.
- View only new results found since the last analysis and create a report with the new results only.
- View only code metrics that exceed specified thresholds and create a report with those metrics only.

On the **Results List** pane, you can apply complicated filtering criteria to show only the results that are most meaningful to you. You can reuse these criteria for your generated report and show only the results that you want the report reviewer to focus on. For more information on the filters you can use, see “Filter and Group Results”.

The report shows which filters you have applied. Another person reviewing your report can see your filtering criteria.

Results Export: Export results to text file for computing graphs and statistics

In R2016b, you can export your results to a tab delimited text file. You can parse the text file using MATLAB or Excel[®] and generate graphs or statistics about your results that you cannot obtain readily from the user interface.

For more information, see “Export Results to Text File”.

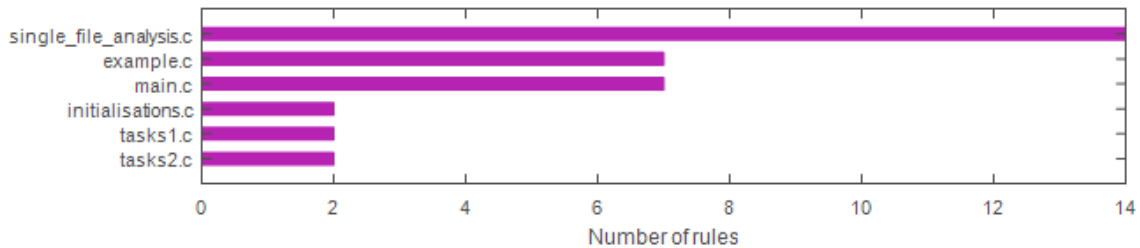
Coding Rules in Report: View improved presentation of coding rules violations in report

In R2016b, the following improvements have been made in how coding rule violations appear in the report.

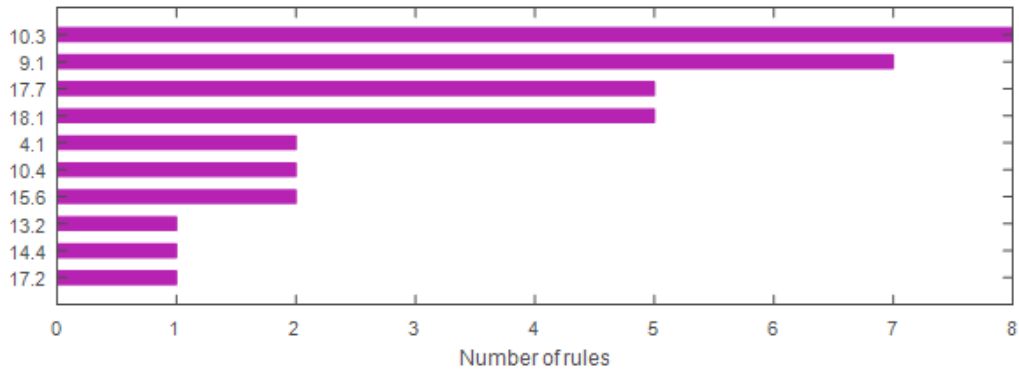
Coding Rule Graphs

If you choose to report coding rule violations, the report contains two new graphs.

- The first graph shows the number of coding rule violations broken down by file.



- The second graph shows the number of violations broken down by rule number.



Coding Rule Template

You can now create a report that shows coding rules violation only. The report does not show other Polyspace Bug Finder results.

For more information, see the description of template `CodingRules` in Report template (-report-template).

English Reports in Non-English Locales: Generate English reports on operating systems with a different language

In R2016b, even if your operating system has a display language (Windows) or locale (Linux) other than English, you can generate English reports. See “Generate Reports from Command Line”.

Change in report template location

The location of the report template files has changed to *matlabroot*/toolbox/polyspace/psrptgen/templates. Here, *matlabroot* is the MATLAB installation folder.

If you use the report templates provided by Polyspace, the change does not impact you. If you use MATLAB Report Generator™ to modify the Polyspace report templates, you can open the templates from this new location.


Improved PDF Report Generation

In R2016b, the generation of PDF reports is improved.

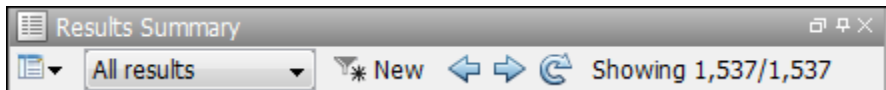
- The report generation is faster. For large results, the report generation is much less likely to cause out-of-memory errors.
- The reports use an improved visual display.

Changes in Polyspace User Interface

The following table lists minor changes to the user interface including new pane names and new icons.

- **Results List** — Window showing list of results, previously called **Results Summary**.
-  — Button to remove items in the configuration or projects.
- The icons on the **Results List** pane have been rearranged.

In R2016a, the icons were arranged as below.



In R2016b, the same icons are arranged as below.



R2016a

Version: 2.1

New Features

Bug Fixes

Compatibility Considerations

Analysis Setup

Files to Review: Generate results for only specified files and folders

In R2016a, you have greater control over the files on which you want analysis results. The default project configuration displays results on the set of files that are likely to be most relevant to you. You can add files or folders to this set based on your requirements.

For instance, by default, coding rule violations and code metrics are generated on header files that are located in the same folder as the source files. Often, other header files belong to a third-party library. Though these header files are required for a precise analysis, you are not interested in reviewing findings in those headers. Therefore, by default, results are not generated for those headers. If you are interested in certain headers from third-party libraries, you can add those headers to the subset on which results are generated.

For more information, see:

- Generate results for sources and (-generate-results-for)
- Do not generate results for (-do-not-generate-results-for)

Compatibility Considerations

In R2016a, by default, results are not generated for headers unless they are in the same location as source files. Previously, if you ran an analysis at the command line, by default, results were generated for all headers.

Due to the change in default behavior, if you rerun the analysis on a pre-R2016a project without explicitly changing the options, you can lose review comments on findings in some header files. To avoid losing the comments, set the option Generate results for sources and (-generate-results-for) to `all-headers`.

Faster MISRA Checking: Check coding rules more quickly and efficiently

In R2016a, you can use two predefined subsets to perform a quicker and more efficient check for coding rule violations. The new subsets turn on rules that have the same scope.

- `single-unit-rules` — Check rules that apply only to single translation units.

- **system-decidable-rules** — Check rules in the **single-unit-rules** subset and some rules that apply to the collective set of program files. The additional rules can be checked only at the integration level because the rules involve more than one translation unit.

Polyspace finds these subsets of rules in the early phases of the analysis. If your project is large, before checking all rules, you can check these subsets of rules for a quick preliminary analysis.

For more information, see [Coding Rule Subsets Checked Early in Analysis](#).

S-Function Analysis: Launch analysis of S-Function code from Simulink

With the Polyspace plug-in for Simulink, you can now start a Polyspace analysis on S-Functions directly from an S-Function block.

To analyze an S-Function, right-click the S-Function block and select **Polyspace > Verify S-Function**. If the S-Function occurs in your model multiple times, you can choose to analyze every instance of the S-Function by analyzing with the different signal range inputs, or just a single instance of the S-Function analyzing with the specific signal ranges for that block.

Import signal ranges from model for generated code analysis

When you run a Polyspace Bug Finder analysis from Simulink, you can now include the signal range information with your analysis. The signal ranges become constraint specifications (formerly called DRS) for the variables in your analysis. For more information see, [Configure Data Range Settings and Constraints](#).

Polyspace Metrics Tomcat Upgrade: Use upgraded default Tomcat server or custom Tomcat version

Polyspace Metrics now uses Tomcat 8.0.22 to run the Polyspace Metrics web interface.

If you want to use your own version of Tomcat, you can now specify a custom Tomcat server in the daemon configuration file. To add your custom tomcat web server, add the following line to the daemon configuration file.

```
tomcat_install_dir = <path/to/tomcat>
```

The daemon configuration file is located in:

- Windows — `\\%APPDATA%\\Polyspace_RLData\\polyspace.conf`
- Linux — `/etc/Polyspace/polyspace.conf`

Polyspace Metrics Interface Updated: View project and metrics summary and defect impact

The Polyspace Metrics web interface has been updated to include new features:

- The Bug Finder analysis uploaded to Polyspace Metrics now includes new metrics summarizing the number of defects with High, Medium, and Low impact. For more information on the impact classification, see [Classification of Defects by Impact](#).
- You can now view project-level metric summaries from the main Polyspace Metrics page using one of the following methods:
 - On the **Projects** tab, roll your mouse over the list of projects to open a window displaying a summary of the project and project metrics.
 - On the **Projects** or **Runs** tab, right-click the column headers to add new columns to the table. new columns you can add include Coding Rules, Bug-Finder Checks, Code Metrics, and Review Progress.

For more information, see [View Projects in Polyspace Metrics](#).

Source Code Search: Search huge applications more quickly

In R2016a, search results are produced more quickly. If you search for a string in a huge application, it takes less time for search results to appear.

You can search for a string either by entering the search string in the box on the **Search** pane, or by right-clicking a word in your code on the **Source** pane, and then selecting a search option.

Default Layouts: Switch easily between project setup and results review in user interface

In R2016a, you have two default layouts of panes in the Polyspace user interface, one for project setup and another for results review.

When setting up your projects, select **Window > Reset Layout > Project Setup**. When reviewing results, select **Window > Reset Layout > Results Review**.

For more information, see *Organize Layout of Polyspace User Interface*.

Files Not Compiled: Receive alerts about compilation errors in dashboard and reports

If some of your source files contain compilation errors, Polyspace Bug Finder analyzes those files only for code metrics and some coding rules.

In R2016a, if some of your files are analyzed only partially because of compilation errors:

- On the **Dashboard** pane, you can see that some files failed to compile. Further information about the compilation errors is available on the **Output Summary** pane. For more information, see *Dashboard*.
- If you generate reports by using the `BugFinderSummary` or `BugFinder` template, the chapter **Polyspace Bug Finder Summary** lists the files that are partially analyzed. For more information, see *Report template (-report-template)*.

Project Language Flexibility: Change your project language at any time

Projects in the Polyspace interface are no longer fixed to one language.

When you create your projects, you can add any file to the project. After you add files, select the language (C, C++, or C/C++) for your analysis using the Source code language (-lang) option. If you add or change the files in your project, you can change the language to reflect the most suitable analysis type.

Many options that were C only or C++ only are now available for both languages. To see which analysis options have changed, see “Changes in analysis options” on page 2-6.

Improvements in automatic project creation from build command

In R2016a, automatic project creation from build command is improved.

- If you trace your build command and create a Polyspace project from the command line, you do not have to specify a product name or project language. You can open the project in Polyspace Bug Finder or Polyspace Code Prover™. The project language is determined by using the following rules:
 - If all your files are compiled as C, as C++03, or C++11, the corresponding language is assigned to the project.

Language	Options Set in Project
C	Source code language: c
C++03	Source code language: cpp
C++11	Source code language: cpp C++11 Extensions: On

- If some files are compiled as C and the remaining files as C++03 or C++11, the **Source code language** option is set to `c-cpp`.

The option **C++11 Extensions** is also enabled.

For more information, see Source code language (-lang) and C++11 Extensions (-cpp11-extensions).

Previously, you specified the product name by using options `-bug-finder` or `-code-prover`. If you did not specify a project language and your source code consisted of both `.c` and `.cpp` files, the language `cpp` was assigned to the project. The options `-bug-finder` and `-code-prover` have been removed.

For more information, see Create Project Automatically at Command Line.

- The support for IAR compilers has improved. All variations of IAR compilers are now supported for automatic project creation from build command.

Polyspace TargetLink plug-in supports data from structures

The Polyspace plug-in for TargetLink[®] can now import data from structures in the constraint specifications (formerly called DRS) for your analysis.

Changes in analysis options

In R2016a, the following options have been added, changed, or removed.

New Options

Option	Description
Generate results for sources and (-generate-results-for)	Specify files on which you want analysis results.

Option	Description
Do not generate results for (-do-not-generate-results-for)	Specify files on which you do not want analysis results.

Updated Options

Option	Change	More Information
Source code language (-lang)	New value c	Select your project language to set compilation rules and enable language specific analysis options.
Dialect (-dialect)	Unified dialects for C, C/C++, and C++ projects. All projects can use any dialect option.	
Target processor type (-target)	Targets i386 and x86_64 now allow any alignment value.	
Sfr type support (-sfr-types)	Allowed for C, C++, C/C++	
Respect C90 standard (-no-language-extensions)	Allowed for mixed C/C++ projects	
Pack alignment value (-pack-alignment-value)	Allowed for C, C++, C/C++	
Import folder (-import-dir)	Allowed for C, C++, C/C++	
Ignore pragma pack directives (-ignore-pragma-pack)	Allowed for C, C++, C/C++	
Division round down (-div-round-down)	Allowed for C, C++, C/C++	

Removed Options

Option	Status	Description
Files and folders to ignore (-includes-to-ignore)	Warning	Use the option Do not generate results for (-do-not-generate-results-for) to

Option	Status	Description
		suppress results from headers and sources in certain files or folders.
-support-FX-option-results	Warning	Option will be removed in a future release.

Compatibility Considerations

If you use scripts that contain the removed or updated options, change your scripts accordingly.

Analysis Results

Improvements to defect checkers

In R2016a, there are improvements in detection of certain defects. For instance, with the checkers for defects Dead code and Useless if:

- You see the code sequence leading to the defect in a greater number of situations. For more information, see Navigate to Root Cause of Defect.
- You see fewer false positives. For instance, you do not see false **Dead code** or **Useless if** defects associated with the following constructs:
 - `_setjmp`
 - Pointer parameter pointing to a global variable
- You do not see defects in templates.

Improvements in checking of previously supported MISRA C rules

In R2016a, the following changes have been made in checking of previously supported MISRA C rules.

MISRA C:2004 Rules

Rule	Description	Improvement
MISRA C:2004 Rule 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.	The rule checker no longer raises a violation of this rule if an expression with a Boolean result is cast to a type that is also effectively Boolean. For instance, in your code, you define a type <code>myBool</code> using a <code>typedef</code> and cast the result of <code>(a && b)</code> to <code>myBool</code> . If you specify to Polyspace that <code>myBool</code> is effectively Boolean, the rule checker does not consider this cast as a violation of rule 10.3. For more information on how to specify effectively Boolean types, see

Rule	Description	Improvement
		Effective boolean types (-boolean-types).
MISRA C:2004 Rule 12.2	The value of an expression shall be the same under any order of evaluation that the standard permits.	The rule checker no longer flags expressions with the comma operator that can be evaluated in only one order. For instance, the statement <code>ans = (val++, val++)</code> does not violate this rule.

MISRA C:2012 Rules

Rule	Description	Improvement
MISRA C:2012 Rule 13.2	The value of an expression and its persistent side effects shall be the same under all permitted evaluation orders.	The rule checker no longer flags expressions with the comma operator that can be evaluated in only one order. For instance, the statement <code>ans = (val++, val++)</code> does not violate this rule.

Standards Mapped to Defects: Observe coding standards using Polyspace Bug Finder

CERT C mapping

In R2016a, you can now observe coding standards such as SEI CERT C Coding Standards by using Polyspace Bug Finder.

For more information, see Mapping Between CERT C Standards and Defects.

CWE ID mapping

In R2016a, the following changes have been made in the mapping between CWE IDs and Polyspace Bug Finder defects.

Defect	CWE ID: Prior to R2016a	CWE ID: R2016a
Invalid use of standard library integer routine	CWE-369: Divide By Zero	<ul style="list-style-type: none">• CWE-227: Improper fulfillment of API contract• CWE-369: Divide By Zero• CWE-682: Incorrect Calculation• CWE-872: CERT C++ Secure Coding Section 04 - Integers (INT)

For more information, see Mapping Between CWE Identifiers and Defects.

Reviewing Results

More results available in real time

When you run a Bug Finder analysis, more results for blocks of code are now available while the analysis is running. For information about how to open results during the analysis, see Open Results.

Autocompletion for Review Comments: Partially type previous comment to select complete comment

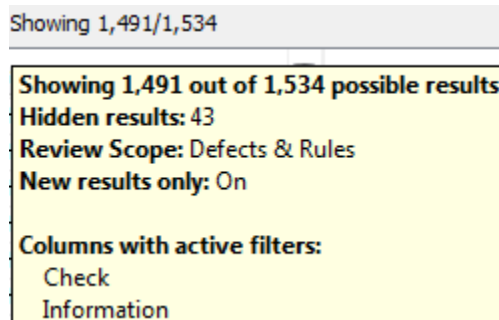
In R2016a, on the **Results Summary** or **Result Details** pane, if you start typing a review comment that you have previously entered, a drop-down list shows the previous entry. Select the previous comment from this list instead of retyping the comment.

If you want the autocompletion to be case sensitive, select **Tools > Preferences**. On the **Miscellaneous** tab, select **Autocomplete on Results Summary or Details is case sensitive**.


Persistent Filter States: Apply filters once and view filtered results across multiple runs

In R2016a, if you apply a set of filters to your analysis results and rerun analysis on the project, your filters are also applied to the new results. You can specify your filters once and suppress results that are not relevant for you across multiple runs.

The **Results Summary** pane shows the number of results filtered from the display. If you place your cursor on this number, you can see the applied filters.



For instance, in the image, you can see that the following filters have been applied:

- The **Defects & Rules** filter to suppress code metrics and global variables.
- The  filter to suppress results found in a previous analysis.
- Filters on the **Information** and **Check** columns.

For more information, see Filter and Group Results.

Polyspace Eclipse plug-in results location moved

When you analyze projects using the Polyspace plug-in for Eclipse, your results used to be stored inside your Eclipse project under *eclipse project folder*\polyspace. For new Eclipse projects, Polyspace now stores results in the Polyspace Workspace under *Polyspace_Workspace*\EclipseProjects*Eclipse Project Name*, where *Polyspace_Workspace* is the default project location specified in your Polyspace Interface preferences. For more information, see Results Location.

R2015aSP1

Version: 1.3.1

Bug Fixes

R2015b

Version: 2.0

New Features

Bug Fixes

Compatibility Considerations

Analysis Setup

Mixed C/C++ Code: Run analysis on entire project with C and C++ source files

If your coding project contains C and C++ files, you can now analyze the entire project in one Polyspace project. Use the new C/C++ setting to compile `.c` files with C compilation rules and compile `.cpp` and other files with C++ compilation rules.

To create a mixed C and C++ project:

- At the command line, use the option `-lang C-CPP`.
- In the user interface:
 - 1 Select **File > New Project**.
 - 2 In the Project properties window, select **Project Language > C++** as the main project language. Enter your other project properties as before.
 - 3 When adding source files, add your `.c` and `.cpp` files with their include files.
 - 4 In the configuration, on the **Target & Compiler** pane, set **Source code language > C-CPP**. This setting indicates to the compiler to use C compilation rules for `.c` files and C++ compilation rules for `.cpp` files. For other file extensions, Polyspace uses C++ compilation rules.
 - 5 Set your other options as required. Some limitations to consider:
 - Coding rules — You can select only one C coding rule set and one C++ coding rule set.
 - Bug Finder Defects — You can select C/C++ or C++ defects. The C++ defects are checked only on `.cpp` files.

Autodetection of Multitasking Primitives: Analyze source code with multitasking primitives from POSIX and VxWorks without manual setup

If you use POSIX[®] or VxWorks to perform multitasking, Polyspace can now interpret your multitasking code more easily.

Functions Polyspace can interpret:

POSIX

- `pthread_create`
- `pthread_mutex_lock`
- `pthread_mutex_unlock`

VxWorks

- `taskSpawn`
- `semTake`
- `semGive`

By default in R2015b, Polyspace detects thread creating and critical sections from supported multitasking functions.

For more information, see [Modeling Multitasking Code](#).

Microsoft Visual C++ 2013: Analyze code developed in Microsoft Visual C++ 2013

You can analyze code developed in the Microsoft® Visual C++® 2013 dialect.

To analyze code compiled with Microsoft Visual C++ 2013, set your dialect to `visual12.0`. Once you specify your dialect, Microsoft Visual C++ allows language extensions specific to Microsoft Visual C++ 2013. For more information, see [Dialect \(C\)](#) or [Dialect \(C++\)](#).

GNU 4.9 and Clang 3.5 Support: Analyze code compiled with GNU 4.9 or Clang 3.5

Polyspace now supports the GNU 4.9 and Clang 3.5 dialects for C and C++ projects.

To analyze code compiled with one of these dialects, set the **Target & Compiler > Dialect** option to `gnu4.9` or `clang3.5`.

For more information, see [Dialect \(C\)](#) or [Dialect \(C++\)](#).

Improvements to automatic project creation from build command

In R2015b, automatic project creation from your build command is improved:

- If you build your source code from the Cygwin™ environment (using either a 32-bit or 64-bit installation), Polyspace can trace your build and to create a Polyspace project or options file.
- Support for the following compilers has improved:

- Texas Instruments™ C2000 compiler

This compiler is available with Code Composer Studio™.

- Cosmic HC08 C compiler
- MPLAB XC8 C Compiler
- With certain compilers, the speed of tracing your build command has improved. The software now stores build information in the system temporary folder, thereby allowing faster access during the build.

If you still encounter a slow build, use the advanced option `-cache-path ./ps_cache` when tracing your build. For more information, see [Slow Build Process When Polyspace Traces the Build](#).

- If the software detects target settings that correspond to a standard processor type, it assigns that standard target processor type to your project. The target processor type defines the size of fundamental data types and the endianness of the target machine. For more information, see [Target processor type \(C/C++\)](#).

Previously, when you created a project from your build command, the software assigned a custom target processor type. Although you saw the processor type in the form of an option such as `-custom-target true,8,2,4,-1,4,8,4,8,8,4,8,1,little,unsigned_int,int,unsigned_short`, you could not identify easily how many bits were associated with each fundamental type. With this enhancement, when the software assigns a processor type, you can identify the number of bits for each type. Click the **Edit** button for the option **Target processor type**.

- Automatic project creation uses a configuration file written for specific compilers. If your compiler is not supported, you can adapt one of the existing configuration files for your compiler. The configuration file, written in XML, is now simplified with some new elements, macros and attributes.
 - The `preprocess_options_list` element supports a new `$(OUTPUT_FILE)` macro when the compiler does not allow sending the preprocessed file to the standard output.

- A new `preprocessed_output_file` element allows the preprocessed file name to be adapted from the source file name.
- The `semantic_options` element supports a new `isPrefix` attribute. This attribute provides a shortcut to specify multiple semantic options that begin with the same prefix.
- The `semantic_options` element supports a new `numArgs` attribute. This attribute provides a shortcut to specify semantic options that take one or more arguments.

For more information, see `Compiler Not Supported for Project Creation from Build Systems`.

- Sometimes, the build command returns a non-zero status even when the command succeeds. The non-zero status can result from warnings in the build process. However, Polyspace does not trace the build and create a Polyspace project. You can now use an option `-allow-build-error` to create a Polyspace project even if the build command returns an exit status or error level different from zero. This option helps you understand the error in the build process.

For more information, see `-option value` arguments of `polyspaceConfigure`.

Start Page: Get oriented with Polyspace Bug Finder

In R2015b, when you open Polyspace Bug Finder for the first time, a **Start Page** pane appears. From this pane, you can:

- Open Polyspace recent results and examples.
- Start a new project.
- Get additional help using the **Getting Started**, **What's New**, and **Learn More** tabs.

If you select the **Show on startup** box, the pane appears each time you open Polyspace Bug Finder. Otherwise, if you close the pane once, it does not reopen. To open the pane, select **Window > Show/Hide View > Start Page**.

Saved Layouts: Save your preferred layouts of the Polyspace user interface

In R2015b, if you reorganize the Polyspace user interface and place the various panes in more convenient locations, you can save your new layout. If you change your layout, you can quickly revert to a saved layout.

With this modification, you can create customized layouts suitable for different requirements. You can switch between saved layouts quickly. For instance:

- You can have separate layouts for project configuration and results review.
- You can have a minimal layout with only the frequently used panes.

For more information, see [Organize Layout of Polyspace User Interface](#).

Renaming of labels in Polyspace user interface

In the Polyspace user interface, the following labels have been renamed:

- On the **Configuration** pane, the **Coding Rules** node is renamed **Coding Rules & Code Metrics**.

The new **Coding Rules & Code Metrics** node now contains the option **Calculate Code Metrics**, which previously appeared in the **Advanced Settings** node.

- On the **Results Summary** pane, the **Category** column title is changed to **Group**. This change avoids confusion with coding rule categories.
- On the **Results Summary** and **Result Details** pane, the field **Classification** is changed to **Severity**. You assign a **Severity** such as **High**, **Medium** and **Low** to a defect to indicate how critical you consider the issue.
- The labels associated with specifying constraints have changed as follows:
 - On the **Configuration** pane, the field **Variable/function range setup** is changed to **Constraint setup**.
 - When you click **Edit** beside the **Constraint Setup** field, a new window opens. The window name is changed from **Polyspace DRS Configuration** to **Constraint Specification**.

For more information, see [Specify Constraints](#).

Including options multiple times

You can specify analysis options multiple times. This new capacity is available only at the command line or using the command-line names in the **Advanced options** pane in the user interface. You can customize pre-made configurations without having to remove options.

If you specify an option multiple times, only the last setting is used. For example, if your configuration is:

```
-lang c
-prog test_bf_cp
-verif-version 1.0
-author username
-sources-list-file sources.txt
-OS-target no-predefined-OS
-target i386
-dialect none
-misra-cpp required-rules
-target powerpc
```

Polyspace uses the last target setting, **powerpc**, and ignores the other target specified, **i386**.

In the user interface, if you specify **c18** as the target on the Target and Compiler pane and in **Advanced options** enter **-target i386**, these two targets count as multiple analysis option specifications. Polyspace uses the target specified in the Advanced options dialog box, **i386**.

Updated Support for TargetLink

The Polyspace plug-in for TargetLink now supports versions 3.5 and 4.0 of the dSPACE® Data Dictionary and TargetLink Code Generator.

dSPACE and TargetLink version 3.4 is no longer supported.

For more information, see TargetLink Considerations.

Changes in analysis options

In R2015b, the following options have been added, changed, or removed.

New Options

Option	Status	Description
Respect C90 Standard	New	The analysis does not allow C language extensions that do not follow the ISO/IEC 9899:1990 standard.

Option	Status	Description
(-no-language-extensions)		
Dialect visual12.0	New	Allows Microsoft Visual C++ 2013 (visual 12) language extensions.
Dialect gnu4.9	New	Allows GCC 4.9 language extensions.
Dialect clang3.5	New	Allows Clang 3.5 language extensions.
Source code language (C++) (-lang)	New in the user interface	The <code>-lang</code> option is now available in the Polyspace user interface. It is on the Target & compiler tab and called Source code language .
Source code language (C++) > C-CPP (-lang C-CPP)	New option setting	For C++ projects, you can choose C-CPP to analyze a mix of <code>.c</code> and <code>.cpp</code> source files.
Configure multitasking manually (C/C++)	New	A user interface option only. This option enables the previous multitasking options <ul style="list-style-type: none"> • Entry points • Critical section details • Temporally exclusive tasks
Disable automatic concurrency detection (C/C++)	New	By default, the new automatic concurrency detection is enabled. If you want to turn it off, select this option.

Updated Options

Option	Change	Description
Calculate Code Metrics (C/C++)	Moved in user interface	The option has been moved in the Configuration panel from the Advanced Settings pane to the Coding Rules and Code Metrics pane.
Signed right shift (C/C++) (-logical-signed-right-shift)	Now available in C++ projects	

Option	Change	Description
Division round down (C/C++) (-div-round-down)	Now available in C++ projects	
Targets: <ul style="list-style-type: none"> • tms320c3x • sharc21x61 • necv850 • hc08 • hc12 • mpc5xx • c18 	Now available in C++ projects	
Enum type definition (C/C++) (-enum-type-definition)	Possible values updated	The possible values for -enum-type-definition now match for C and C++. Available values: <ul style="list-style-type: none"> • defined-by-standard (default) • auto-signed-first • auto-unsigned-first
-support-FX-option-results	No longer available in the user interface	
-pointer-is-24bits	Available in C++ projects	Available only if you use the Target setting c18 .
-asm-begin -asm-end	Now available in C++ projects	
Check MISRA C:2004	Now available in C++ projects	Available only if you select Source code language > C-CPP .
Check MISRA AC AGC	Now available in C++ projects	Available only if you select Source code language > C-CPP .

Option	Change	Description
Check MISRA C:2012 and Use generated code requirements (C)	Now available in C++ projects	Available only if you select Source code language > C-CPP .
Effective boolean types (C)	Now available in C++ projects	Available only if you select Source code language > C-CPP .
Allowed pragmas (C)	Now available in C++ projects	Available only if you select Source code language > C-CPP .
Output format (C/C++) -report-output-format	Possible values updated	The output format RTF is deprecated and not available on the Configuration pane.

Removed Options

Option	Status	Description
-dialect cfront2	Removed	Choose a different dialect.
-dialect cfront3	Removed	Choose a different dialect.
-passes-time	Removed	Polyspace includes this behavior by default. Remove this option from existing configurations.
-include-headers-once	Removed	Polyspace includes this behavior by default. Remove this option from existing configurations.
-discard-asm	Removed	This option is no longer supported. Remove this option from existing configurations.
-misra2 AC-AGC-OBL-subset	Removed	Use -misra-ac-agc OBL-rules instead.

Compatibility Considerations

If you use scripts that contain the removed or updated options, change your scripts accordingly.

Binaries removed

The following binaries have been removed.

Removed binary	Use instead
<code>polyspace-rl-manager.exe</code>	<code>polyspace-server-settings.exe</code>
<code>polyspace-spooler.exe</code>	<code>polyspace-job-monitor.exe</code>
<code>polyspace-ver.exe</code>	<code>polyspace-bug-finder-nodesktop -ver</code>

The binaries to use instead are located in `matlabroot/polyspace/bin`.

Support for Visual Studio 2008 to be removed

The Polyspace Add-In for Visual Studio 2008 is no longer supported and will be removed in a future release.

Compatibility Considerations

To analyze your Visual Studio projects, use either:

- The Polyspace Add-in for Visual Studio 2010. See [Install Polyspace Add-In for Visual Studio](#).
- The `polyspace-configure` tool to create a project using your build command. See [Create Project Using Visual Studio Information](#).

Import Visual Studio project removed

The **Tools > Import Visual Studio project** has been removed.

To import your project information from Visual Studio, use the **Create from build system** option during new project creation. For more information, see [Create Project Using Visual Studio Information](#).

Analysis Results

More Defect Categories: Detect security vulnerabilities, resource management issues, object oriented design issues

You can check your code against five new categories of defects:

- Resource management — Defects related to resource handling such as detection of unclosed file descriptors or use of a closed file descriptor.
- Object oriented — Defects related to C++ object-oriented programming such as detection of class design issues or issues in the inheritance hierarchy.
- Security — Defects related to security vulnerabilities such as vulnerable standard functions, use of sensitive data, and pseudo-random number generation.
- Tainted data — Defects related to using variables that someone outside your program can manipulate and externally controlled resources.
- Good practice — Defects that allow you to observe good coding practices such as detection of hard-coded memory buffer size or unused function parameters.

For information about the new defects, see “Changes to Bug Finder Defects” on page 4-15.

Complete MISRA C:2012 Support: Detect violations of all MISRA C:2012 rules

In R2015b, Polyspace Bug Finder supports the following MISRA C: 2012 coding rules.

Rule	Description
MISRA C:2012 Directive 2.1	All source files shall compile without any compilation errors.
MISRA C:2012 Directive 4.5	Identifiers in the same name space with overlapping visibility should be typographically unambiguous.
MISRA C:2012 Directive 4.13	Functions which are designed to provide operations on a resource should be called in an appropriate sequence.
MISRA C:2012 Rule 2.6	A function should not contain unused label declarations.

Rule	Description
MISRA C:2012 Rule 2.7	There should be no unused parameters in functions.
MISRA C:2012 Rule 17.5	The function argument corresponding to a parameter declared to have an array type shall have an appropriate number of elements.
MISRA C:2012 Rule 17.8	A function parameter should not be modified.
MISRA C:2012 Rule 21.12	The exception handling features of <code><fenv.h></code> should not be used.
MISRA C:2012 Rule 22.1	All resources obtained dynamically by means of Standard Library functions shall be explicitly released.
MISRA C:2012 Rule 22.2	A block of memory shall only be freed if it was allocated by means of a Standard Library function.
MISRA C:2012 Rule 22.3	The same file shall not be open for read and write access at the same time on different streams.
MISRA C:2012 Rule 22.4	There shall be no attempt to write to a stream which has been opened as read-only.
MISRA C:2012 Rule 22.5	A pointer to a <code>FILE</code> object shall not be dereferenced.
MISRA C:2012 Rule 22.6	The value of a pointer to a <code>FILE</code> shall not be used after the associated stream has been closed.

Improvements in checking of previously supported MISRA C rules

In R2015b, the following changes have been made in MISRA C checking:

MISRA C:2004

Rule	Description	Improvement
MISRA C:2004 Rule 2.1	Assembly language shall be encapsulated and isolated.	If an assembly language statement is entirely encapsulated in macros, Polyspace no longer considers that the statement violates this rule.
MISRA C:2004 Rule 8.8	An external object or function shall be declared in one file and only one file.	Polyspace considers that variables or functions declared <code>extern</code> in a non-header file violate this rule.

Rule	Description	Improvement
MISRA C:2004 Rule 10.1	The value of an expression of integer type shall not be implicitly converted to a different underlying type if it is not a conversion to a wider integer type of the same signedness.	Polyspace no longer raises violation of this rule on operations involving pointers.
MISRA C:2004 Rule 19.2	Nonstandard characters should not occur in header file names in <code>#include</code> directives.	<p>If the character <code>\</code> or <code>\\</code> occurs between the <code><</code> and <code>></code> in <code>#include <filename></code> (or between <code>"</code> and <code>"</code> in <code>#include "filename"</code>), Polyspace no longer raises violation of this rule.</p> <p>Therefore, you can use Windows paths to files in place of <code>filename</code> without triggering a rule violation.</p>

MISRA C:2012

Rule	Description	Improvement
MISRA C:2012 Directive 4.3	Assembly language shall be encapsulated and isolated.	If an assembly language statement is entirely encapsulated in macros, Polyspace no longer considers that the statement violates this rule.
MISRA C:2012 Rule 1.1	The program shall contain no violations of the standard C syntax and constraints, and shall not exceed the implementation's translation limits.	<p>If a rule violation occurs because your <code>.c</code> file contains too many macros, Polyspace places the rule violation at the beginning of the file instead on the last macro usage.</p> <p>Therefore, you can add a comment before the first line of the <code>.c</code> file justifying the violation. Previously, if you placed a justification comment before the last macro usage and</p>

Rule	Description	Improvement
		later added another macro usage, the comment no longer applied. For information on adding code comments to justify results, see Annotate Code for Rule Violations.
MISRA C:2012 Rule 10.4	Both operands of an operator in which the usual arithmetic conversions are performed shall have the same essential type category.	<ul style="list-style-type: none"> • If one of the operands is the constant zero, Polyspace does not raise a violation of this rule. • If one of the operands is a signed constant and the other operand is unsigned, the rule violation is not raised if the signed constant has the same representation as its unsigned equivalent. <p>For instance, the statement <code>u8b = u8a + 3;</code>, where <code>u8a</code> and <code>u8b</code> are unsigned char variables, does not violate the rule because the constants <code>3</code> and <code>3U</code> have the same representation.</p>

Checking Coding Rules Using Text Files

In R2015b, if your coding rules configuration text file has an incorrect syntax, the analysis stops with an error message. The error message states the line numbers in the configuration file that contain the incorrect syntax.

For more information on checking for coding rules using text files, see [Format of Custom Coding Rules File](#).

Changes to Bug Finder Defects

- “New Defects” on page 4-16
- “Updated Defects” on page 4-21

The following tables list updates and additions to the list of Bug Finder defect checkers.

New Defects

Tainted Data Defects

Name	Description
Array access with tainted index	Array index from unsecure source possibly outside array bounds
Command executed from externally controlled path	Path argument from an unsecure source
Execution of externally controlled command	Command argument from an unsecure source is vulnerable to OS command injection
Host change using externally controlled elements	Changing host id from an unsecure source
Library loaded from externally controlled path	Library argument from an externally controlled path
Loop bounded with tainted value	Loop controlled by a value from an unsecure source
Memory allocation with tainted size	Size argument to memory function is from an unsecure source
Pointer dereference with tainted offset	Offset is from an unsecure source and dereference may be out of bounds
Tainted division operand	Division operands from an unsecure source
Tainted modulo operand	Remainder operands from an unsecure source
Tainted NULL or non-null-terminated string	Argument is from an unsecure source and may be NULL or not NULL-terminated
Tainted sign change conversion	Value from an unsecure source changes sign
Tainted size of variable length array	Size of the variable-length array (VLA) is from an unsecure source and may be zero, negative, or too large
Tainted string format	Input format argument is from an unsecure source
Use of externally controlled environment variable	Value of environment variable from an unsecure source

Name	Description
Use of tainted pointer	Pointer from an unsecure source may be NULL or point to unknown memory

Good Practice Defects

Name	Description
Delete of void pointer	<code>delete</code> operates on a <code>void*</code> pointer pointing to an object
Hard coded buffer size	Size of memory buffer is a numerical value instead of symbolic constant
Hard coded loop boundary	Loop boundary is a numerical value instead of symbolic constant
Unused parameter	Function prototype has parameters not read or written in function body
Use of <code>setjmp/longjmp</code>	<code>set jmp</code> and <code>long jmp</code> cause deviation from normal control flow

Programming Defects

Name	Description
Bad file access mode or status	Access mode argument of function in <code>fopen</code> or <code>open</code> group is invalid
Call to <code>memset</code> with unintended value	<code>memset</code> or <code>wmemset</code> used with possibly incorrect arguments
Copy of overlapping memory	Source and destination arguments of a copy function have overlapping memory
Exception caught by value	<code>catch</code> statement accepts an object by value
Exception handler hidden by previous handler	<code>catch</code> statement is not reached because of an earlier <code>catch</code> statement for the same exception
Improper array initialization	Incorrect array initialization when using initializers
Incorrect pointer scaling	Implicit scaling in pointer arithmetic might be ignored
Invalid assumptions about memory organization	Address is computed by adding or subtracting from address of a variable

Name	Description
Invalid <code>va_list</code> argument	Variable argument list used after invalidation with <code>va_end</code> or not initialized with <code>va_start</code> or <code>va_copy</code>
Modification of internal buffer returned from nonreentrant standard function	Function attempts to modify internal buffer returned from a nonreentrant standard function
Overlapping assignment	Memory overlap between left and right sides of an assignment
Possible misuse of <code>sizeof</code>	Use of <code>sizeof</code> operator can cause unintended results
Possibly unintended evaluation of expression because of operator precedence rules	Operator precedence rules cause unexpected evaluation order in arithmetic expression
Standard function call with incorrect arguments	Argument to a standard function does not meet requirements for use in the function
Use of <code>memset</code> with size argument zero	Size argument of function in <code>memset</code> family is zero
Variable length array with nonpositive size	Size of variable-length array is zero or negative
Writing to <code>const</code> qualified object	Object declared with a <code>const</code> qualifier is modified

Resource Management Defects

Name	Description
Closing a previously closed resource	Function closes a previously closed stream
Resource leak	File stream not closed before <code>FILE</code> pointer scope ends or pointer is reassigned
Use of previously closed resource	Function operates on a previously closed stream
Writing to read-only resource	File opened earlier as read-only is modified

Security Defects

Name	Description
Deterministic random output from constant seed	Seeding routine uses a constant seed making the output deterministic
Execution of a binary from a relative path can be controlled by an external actor	Command with relative path is vulnerable to malicious attack
File access between time of check and use (TOCTOU)	File/directory may have changed state due to access race
File manipulation after chroot() without chdir("/")	Path-related vulnerabilities for file manipulated after call to chroot
Function pointer assigned with absolute address	Constant expression is used as function address is vulnerable to code injection
Incorrect order of network connection operations	Socket is not correctly established due to bad order of connection steps or missing steps
Load of library from a relative path can be controlled by an external actor	Library loaded with relative path is vulnerable to malicious attacks
Mismatch between data length and size	Data size argument is not computed from actual data length
Missing case for switch condition	Default case is missing and may be reached
Predictable random output from predictable seed	Seeding routine uses a predictable seed making the output predictable
Sensitive data printed out	Function prints out sensitive data
Sensitive heap memory not cleared before release	Sensitive data not cleared or released by memory routine
Umask used with chmod-style arguments	Unsafe argument to umask allows external user too much control

Name	Description
Uncleared sensitive data in stack	Variable in stack is not cleared and contains sensitive data
Unsafe standard encryption function	Function is not reentrant or uses a risky encryption algorithm
Unsafe standard function	Function unsafe for security-related purposes
Use of dangerous standard function	Dangerous functions cause possible buffer overflow in destination buffer
Vulnerable path manipulation	Path argument with <code>././</code> , <code>/abs/path/</code> , or other unsecure elements
Vulnerable permission assignments	Argument gives read/write/search permissions to external users
Vulnerable pseudo-random number generator	Using a cryptographically weak pseudo-random number generator
Use of non-secure temporary file	Temporary generated file name is unsecure
Use of obsolete standard function	Obsolete routines can cause security vulnerabilities and/or portability issues

Object-Oriented Defects

Name	Description
*this not returned in copy assignment operator	<code>operator=</code> method does not return a pointer to the current object
Base class assignment operator not called	Copy assignment operator does not call copy assignment operators of base subobjects
Base class destructor not virtual	Class cannot behave polymorphically for deletion of derived class objects
Copy constructor not called in initialization list	Copy constructor does not call copy constructors of some members or base classes
Incompatible types prevent overriding	Derived class method hides a <code>virtual</code> base class method instead of overriding it
Missing explicit keyword	Constructor missing the <code>explicit</code> specifier

Name	Description
Missing virtual inheritance	A base class is inherited both virtually and non-virtually in the same hierarchy
Member not initialized in constructor	Constructor does not initialize some members of a class
Object slicing	Derived class object passed by value to function with base class parameter
Partial override of overloaded virtual functions	Class overrides a fraction of the inherited virtual functions with a given name
Return of non const handle to encapsulated data member	Method returns pointer or reference to internal member of object
Self assignment not tested in operator	Copy assignment operator does not test for self-assignment

Updated Defects

Name	Status	Additional Information
Integer conversion overflow Integer overflow Invalid use of standard library routine Shift operation overflow Sign change integer conversion overflow Shift of a negative value Unsigned integer conversion overflow Unsigned integer overflow	Updated	The defects do not appear on computations involving constants only. For instance, the assignment <code>unsigned int var = -1;</code> does not show a Sign change integer conversion overflow defect.
Format string specifiers and arguments mismatch	New category	Moved from Other to Programming
Invalid use of standard library routine	New category	Moved from Other to Programming

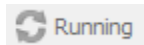
Name	Status	Additional Information
Assertion	New category	Moved from Other to Good practice
Large pass-by-value argument	New category	Moved from Other to Good practice
Line with more than one statement	New category	Moved from Other to Good practice

Reviewing Results

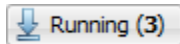
Results in Real Time: View results as they are produced

Previously, you could not review results until the analysis was complete. For local analyses in R2015b, you can start reviewing results as soon as they are available.

When you run a local analysis, a new button appears on the toolbar.

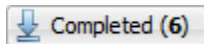


When results are available, this button becomes active.



To start reviewing available results, click this button. The button reactivates every time results are available. To load additional results, click the button again.

When the analysis is complete, to load all your results, click the button.






For more information, see [Open Results](#).

Improved Eclipse Support: View results embedded in source code and context-sensitive help


In R2015b, the following improvements have been made to the Polyspace plugin for Eclipse:

- Polyspace Bug Finder highlights defects in your source code in the following ways:
 - For defects, an ! mark appears before the line number on the left. For coding rule violations, a ▾ or ▼ mark appears before the line number on the left.
 - The operation containing the defect has a wavy red underlining.







- For defects, a  icon appears in the overview ruler to the right of the line containing the defect. For coding rule violations, a  icon appears in the overview ruler to the right of the line containing the rule violation. If you place your cursor on the icon, a tooltip shows a brief description of the defect or coding rule.

In addition, a  icon appears at the top of the overview ruler. If you place your cursor on the icon, a tooltip states the total number of defects and coding rule violations in the file.

Using these indicators, you can track defects in your source code more easily. For more information, see [Review and Fix Results](#).

- When you select a result in the **Results Summary - Bug Finder** view, the **Result Details** view displays additional information about the result. In the **Result Details** view, if you click the  button next to the result name, you can see a brief description and examples of the result. For defects, you can sometimes see the risk associated with not fixing the defect and the most common fix for the defect.
- You can switch to a Polyspace perspective that shows only the information relevant to a Polyspace Bug Finder analysis. To open the perspective, select **Window > Open Perspective > Other**. In the Open Perspective dialog box, select **Polyspace**.

Once you switch to the Polyspace perspective, the source code shows the Polyspace Bug Finder defects only in this perspective.

- You can view results as they are produced instead of waiting till end of the analysis.
 - When you begin an analysis, a  icon appears next to the  button.
 - If results are available, the icon turns to . Click the  icon to load available results.
 - With your results open, if additional results are available, the  icon is still visible. Click the  icon to load all available results.

Defects Classified by Impact: Prioritize defect review by using the impact attribute assigned to each defect type

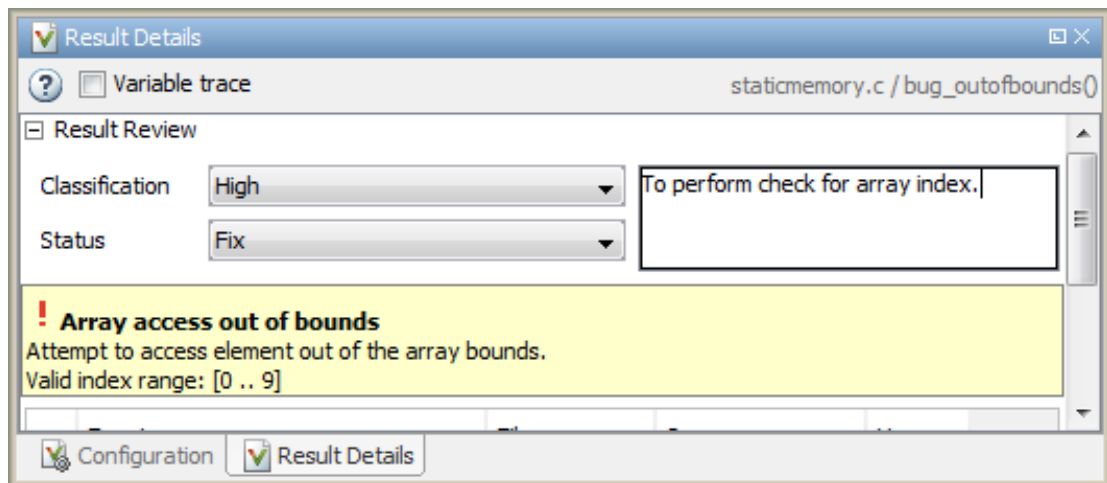
You can prioritize your result review using an **Impact** attribute assigned to the defects. The attribute is assigned based on the following considerations:

- Criticality, or whether the defect is likely to cause a code failure.
- Certainty, or the rate of false positives.

You can filter results on the **Results Summary** pane using the **Impact** attribute. Or, you can obtain a graphical visualization of the **Defect distribution by impact** on the **Dashboard** pane. For more information, see [Classification of Defects by Impact](#).

Improved Review Capability: View result details and add review comments in one window

In R2015b, the **Check Details** pane is renamed as **Result Details**. On this pane, you can now enter review information such as **Classification**, **Status**, and comments. For more information, see [Review and Fix Results](#).



Previously, to enter review information while keeping the **Results Summary** pane collapsed, you used the **Check Review** pane. This pane has been removed.

Enhanced Review Scope: Filter coding rule violations from display in one click

Previously, using custom options on the **Show** menu, you suppressed only defects and code metrics (if they fell below a certain threshold). In R2015b, you can suppress a

certain number or percentage of coding rule violations from the display. You use custom options in the **Show** menu on the **Results Summary** pane. You can:

- Suppress violations of coding rules that are not relevant.
- Focus your results review by seeing only a certain number of coding rule violations in your display.
- Predefine a percentage of coding rule violations that you intend to review and view only that percentage in your analysis results.

You define an option on the **Show** menu only once. The option is available for one-click use every time that you open your results. For information on how to create an option to suppress coding rule violations, see [Suppress Certain Rules from Display in One Click](#).

Configuration Associated with Result Not Opened by Default

In R2015b, when you open your result, the **Configuration** pane does not automatically display a read-only form of the associated configuration.

To view the configuration associated with the result, select the link **View configuration for results** on the **Dashboard** pane. If a corresponding project is open in the **Project Browser**, you can also right-click the **Results** node in the project and select **Open Configuration**.

Improvements in Report Templates

In R2015b, the major improvements in report templates include the following:

- The summary chapter in the template **BugFinder** now contains a breakup of Polyspace Bug Finder results by file, in addition to the project-wide summary.
- The summary now shows the total number of results along with the number of results reviewed.
- Instead of filenames, absolute paths to files appear in the reports.
- If you check for coding rules, the appendix about coding rules configuration states all rules along with the information whether they were enabled or disabled. Previously, the appendix only stated the enabled rules.
- The reports display the impact attribute associated with a defect.

For more information on this attribute, see [Classification of Defects by Impact](#).

For more information on templates, see [Report template \(C/C++\)](#).

XML and RTF report formats removed

The formats XML and RTF for report generation are not available from R2016a onwards. If you generated reports using one of these formats, use an alternative format instead.

For more information, see [Output format \(C/C++\)](#).

R2015a

Version: 1.3

New Features

Bug Fixes

Compatibility Considerations

Analysis Setup

Simplified workflow for project setup and results review with a unified user interface

In R2015a, the Project and Results Manager perspectives have been unified. You can run the analysis and review results without switching between two perspectives.

The unification has resulted in the following major changes:

- After an analysis, the result opens automatically.

Previously, after an analysis, you had to double-click the result in the **Project Browser** to open your new results.

- You can have any of the panes open in the unified interface.

Previously, you could open the following panes only in one of the two perspectives.

Project Manager	Results Manager
<ul style="list-style-type: none"> • Project Browser: Set up project. • Configuration: Specify analysis options for your project. • Output Summary: Monitor progress of analysis. • Run Log: Find information about an analysis. 	<ul style="list-style-type: none"> • Results Summary: View Polyspace results. • Source: View read-only form of source code color coded with Polyspace results. • Check Details: View details of a particular result. • Results Properties: Same as Run Log, but associated with results instead of a project. This pane has been removed. <p>To open the log associated with a result, with the results open, select Window > Show/Hide View > Run Log.</p> <ul style="list-style-type: none"> • Settings: Same information as Configuration, but associated with

Project Manager	Results Manager
	<p>results instead of a project. This pane has been removed.</p> <p>To open the configuration associated with a result, with the results open, select Window > Show/Hide View > Configuration.</p>

Search improvements in the user interface

In R2015a, the **Search** pane allows you to search for a string in various panes of the user interface.

To search for a string in the new user interface:

- 1 If the **Search** pane is not visible, open it. Select **Window > Show/Hide View > Search**.
- 2 Enter your string in the search box.
- 3 From the drop-down list beside the box, select names of panes you want to search.

The **Search** pane consolidates the previously available search options.

Option to specify program termination functions

In R2015a, you can specify functions that behave like the exit function and terminate your program.

- At the command line, use the flag `-termination-functions`.
- In the user interface, on the **Configuration** pane, select **Advanced Settings**. Enter `-termination-functions` in the **Other** field.

For more information, see `-termination-functions`.

Support for GCC 4.8

Polyspace now supports the GCC 4.8 dialect for C and C++ projects.

To allow GCC 4.8 extensions in your Polyspace Bug Finder analysis, set the **Target & Compiler > Dialect** option to `gnu4.8`.

For more information, see [Dialect \(C\)](#) and [Dialect \(C++\)](#).

Polyspace plug-in for Simulink improvements

In R2015a, there are three improvements to the Polyspace Simulink plug-in.

Integration with Simulink projects

You can now save your Polyspace results to a Simulink project. Using this feature, you can organize and control your Polyspace results alongside your model files and folders.

To save your results to a Simulink project:

- 1 Open your Simulink project.
- 2 From your model, select **Code > Polyspace > Options**.
- 3 In the Polyspace parameter configuration tab, select the **Save results to Simulink project** option.

For more information, see [Save Results to a Simulink Project](#).

Back-to-model available when Simulink is closed

In the Polyspace plug-in for Simulink, the back-to-model feature now works even when your model is closed. When you click a link in your Polyspace results, MATLAB opens your model and highlights the related block.

Note: This feature works only with Simulink R2013b and later.

For more information about the back-to-model feature, see [Review Generated Code Results](#).

Polyspace binaries being removed

The following binaries will be removed in a future release. The binaries to use are located in `matlabroot/polyspace/bin`. You get a warning if you run them.

Binary name	Use instead
polyspace-rl-manager.exe	polyspace-server-settings.exe
polyspace-spooler.exe	polyspace-job-monitor.exe
polyspace-ver.exe	polyspace-bug-finder-nodesktop -ver

Import Visual Studio project being removed

The **Tools > Import Visual Studio project** will be removed in a future release. Instead, use the **Create from build system** option during new project creation. For more information, see [Create Project Automatically](#).

Analysis Results

Changes to Bug Finder defects

Defect	R2015a change
Invalid use of floating point operation	Off by default.
Line with more than one statement	Off by default.
Invalid use of = (assignment) operator	On by default for handwritten code (analyses started at the command-line or Polyspace environment). Off by default for generated code (analyses started from the Simulink plug-in).
Invalid use of == (equality) operator	On by default for handwritten code. Off by default for generated code.
Missing null in string array	On by default for handwritten code. Off by default for generated code.
Partially accessed array	On by default for handwritten code. Off by default for generated code.
Variable shadowing	On by default for handwritten code. Off by default for generated code.
Write without further read	On by default for handwritten code. Off by default for generated code.
Wrong type used in sizeof	On by default for handwritten code. Off by default for generated code.

Improvements in coding rules checking

MISRA C:2004 and MISRA AC AGC

Rule Number	Effect	More Information
Rule 12.6	More results on noncompliant <code>#if</code> preprocessor directives. Fewer results for variables cast to effective Boolean types.	MISRA C:2004 Rules — Chapter 12: Expressions
Rule 12.12	Fewer results when converting to an array of <code>float</code>	MISRA C:2004 Rules — Chapter 12: Expressions

MISRA C:2012

Rule Number	Effect	More Information
Rules 10.3	Fewer results on enumeration constants when the type of the constant is a named enumeration type. Fewer results on user-defined effective Boolean types.	MISRA C:2012 Rule 10.3
Rule 10.4	Fewer results on enumeration constants when the type of the constant is a named enumeration type. Fewer results for casts to user-defined effective Boolean types.	MISRA C:2012 Rule 10.4
Rule 10.5	Fewer results on enumeration constants when the type of the constant is a named enumeration type. Fewer results on user-defined effective Boolean types.	MISRA C:2012 Rule 10.5
Rule 12.1	More results on expressions with <code>sizeof</code> operator and on expressions with <code>?</code> operators. Fewer results on operators of the same precedence and in preprocessing directives.	MISRA C:2012 Rule 12.1
Rule 14.3	No results for non-controlling expressions.	MISRA C:2012 Rule 14.3

MISRA C++:2008

Rule Number	Effect	More Information
Rule 5-0-3	Fewer results on enumeration constants when the type of the constant is the enumeration type.	MISRA C++ Rules — Chapter 5
Rule 6-5-1	Fewer results on compliant vector variable iterators.	MISRA C++ Rules — Chapter 6
Rule 14-8-2	Fewer results for functions contained in the Files and folders to ignore (C++) option.	MISRA C++ Rules — Chapter 14
Rule 15-3-2	Fewer results for user-defined return statements after a <code>try</code> block.	MISRA C++ Rules — Chapter 15

Reviewing Results

Code complexity metrics available in user interface

In R2015a, code complexity metrics can be viewed in the Polyspace user interface. For more information, see [Code Metrics](#). Previously, this information was available only in the Polyspace Metrics web interface.

In the user interface, you can:

- Specify a limit for the value of a metric. If the metric value for your source exceeds this limit, the metric appears red in **Results Summary**.
- Comment and justify the value of a metric. If a metric value exceeds specified limits and appears red, you can add a comment with the rationale.

Using Polyspace results in this way, you can enforce coding standards across your organization. For more information, see [Review Code Metrics](#).

Reducing the complexity of your code improves code readability, reduces the possibility of coding errors, and allows more precise Polyspace analysis.

Context-sensitive help for code complexity metrics, MISRA-C:2012, and custom coding rules

In R2015a, context-sensitive help is available in the user interface for code metrics results, MISRA C:2012 rule violations, and custom coding rule violations.

To access the contextual help, see [Getting Help](#).

For information about these results, see:

- [Code Metrics](#)
- [MISRA C:2012 Directives and Rules](#)
- [Custom Coding Rules](#)

Review of latest results compared to the last run

In R2015a, you can review only new results compared to the previous run.

If you rerun your analysis, the new results are displayed with an asterisk (*) against them on the **Results Summary** pane. To display only these results, select the **New results** box.

If you make changes in your source code, you can use this feature to see only the results introduced due to those changes. You can avoid reviewing the results in your existing source code.

Simplified results infrastructure

Polyspace results folders are reorganized and simplified. Files have been removed, combined, renamed, or moved. The infrastructure changes do not change the analysis results that you see in the Polyspace environment.

Some important changes and file locations:

- The main results file is now encrypted and renamed `ps_results.psbf`. You can view results only in the Polyspace environment.
- The log file, `Polyspace_R2015a_project_date-time.log` has not changed.

For more information, see Results Folder Contents.

Default statuses to justify results

Polyspace Bug Finder results use certain statuses to calculate the number of justified results in Polyspace Metrics.

In R2015a, the default statuses that mark results as justified are:

- **Justified** — Previously called **Justify**, renamed in R2015a.
- **No action planned** — Existing status added to justified list in R2015a.

You can change which statuses mark results as justified from the Polyspace preferences. For more information, see Define Custom Review Status.

Filters to limit display of results

In R2015a, you can use the **Show** menu on the **Results Summary** pane to suppress certain Polyspace Bug Finder results from display.

- To suppress code complexity metrics from display, select **Show > Defects & Rules**.
- Create your own options on the **Show** menu. Select **Tools > Preferences** and create new options through the **Review Scope** tab.

For more information, see [Limit Display of Defects](#).

R2014b

Version: 1.2

New Features

Bug Fixes

Compatibility Considerations

Analysis Setup

Parallel compilation for faster analysis

Starting in R2014b, Polyspace Bug Finder can run the compilation phase of your analysis in parallel on multiple processors. The software detects available processors and uses them to compile different source files in parallel.

Previously, the software ran post-compilation phases in parallel but compiled the source files sequentially. Starting in R2014b, the software can use multiple processors for the entire analysis process.

To explicitly specify the number of processors, use the command-line option `-max-processes`. For more information, see `-max-processes`.

Support for Mac OS

You can install and run Polyspace on Mac OS X. Polyspace is supported for Mac OS 10.7.4+, 10.8, and 10.9.

You can use Polyspace Metrics on Safari and set up your Mac as a Metrics server. However, if you restart your Mac machine that is setup as a Metrics server, you must restart the Polyspace server daemon.

Support for C++11

Polyspace can now fully analyze C++ code that follows the ISO[®]/IEC 14882:2011 standard, also called C++11.

Use two new analysis options when analyzing C++11 code. On the **Target & Compiler** pane, select:

- **C++11 extensions** to allow the standard C++11 libraries and functions during your analysis.
- **Block char 16/32_t types** to not allow `char16_t` or `char32_t` types during the analysis.

For more information, see [C++11 Extensions \(C++\)](#) and [Block char16/32_t types \(C++\)](#).

Code editor in Polyspace interface

In R2014b, you can edit your source files inside the Polyspace user interface.

- In the Project Manager perspective, on the **Project Browser** tree, double-click your source file.
- In the Results Manager perspective, right-click the **Source** pane and select **Open Source File**.

Your source files appear on a **Code Editor** tab. On this tab, you can edit your source files and save them.

Ignore files and folders during analysis

You can now use the analysis option **Files and folders to ignore** (command line - `includes-to-ignore`) to ignore files and folders during defect checking. Previously, the **Files and folders to ignore** option (command line - `includes-to-ignore`) ignored files and folders during coding rule checking. In R2014b, Polyspace Bug Finder uses this option to ignore specified files or folders for coding rule checking AND defect analysis.

For more information, see `Files and folders to ignore (C)` or `Files and folders to ignore (C++)`.

Simulink plug-in support for custom project files

With the Polyspace plug-in for Simulink, you can now use a project file to specify the analysis options.

On the **Polyspace** pane of the Configuration Parameters window, with the **Use custom project file** option you can enter a path or browse for a `.psprj` project file.

For more information, see `Configure Polyspace Analysis Options`.

TargetLink support updated

The Polyspace plug-in for Simulink now supports TargetLink 3.4 and 3.5. Older versions of TargetLink are no longer supported.

For more information, see `TargetLink Considerations`.

AUTOSAR support added

In R2013b, the Polyspace plug-in for Simulink added support for AUTOSAR generated code with Embedded Coder[®]. If you use `autosar.tlc` as your **System target file** for code generation, Polyspace can analyze this generated code. Polyspace uses the same default analysis options and parameters as Embedded Coder.

For more information, see Embedded Coder Considerations.

Remote launcher and queue manager renamed

Polyspace renamed the remote launcher and the queue manager.

Previous name	New name	More information
<code>polyspace-rl-manager</code>	<code>polyspace-server-settings</code>	Only the binary name has changed. The interface title, Metrics and Remote Server Settings , is unchanged.
<code>polyspace-spooler</code>	<code>polyspace-job-monitor</code>	The binary and the interface titles have changed. Interface labels have changed in the Polyspace interface and its plugins.
Queue Manager or Spooler	Job Monitor	
<code>pslinkfun('queuemanager')</code>	<code>pslinkfun('jobmonitor')</code>	See <code>pslinkfun</code>

Compatibility Considerations

If you use the old binaries or functions, you receive a warning.

Improved global menu in user interface

The global menu in the Polyspace user interface has been updated. The following table lists the current location for the existing global menu options.

Goal	Prior to R2014b	R2014b
Open the Polyspace Metrics interface in your web browser.	File > Open Metrics Web Interface	Metrics > Open Metrics

Goal	Prior to R2014b	R2014b
Upload results from the Polyspace user interface to Polyspace Metrics.	File > Upload in Polyspace Metrics repository	Metrics > Upload to Metrics
Update results stored in Polyspace Metrics with your review comments and justifications.	File > Save in Polyspace Metrics repository	Metrics > Save comments to Metrics
Generate a report from results after analysis.	Run > Run Report > Run Report	Reporting > Run Report
Open a generated report.	Run > Run Report > Open Report	Reporting > Open Report
Import review comments from a previous analysis.	Review > Import	Tools > Import Comments
Specify code generator for generated code.	Review > Code Generator Support	Tools > Code Generator Support
Specify settings that apply to every Polyspace project.	Options > Preferences	Tools > Preferences
Specify settings for remote analysis.	Options > Metrics and Remote Server Settings	Metrics > Metrics and Remote Server Settings

Improved Project Manager perspective

The following changes have been made in the Project Manager perspective:

- The **Progress Monitor** tab does not exist anymore. Instead, after you start an analysis, you can view its progress on the **Output Summary** tab.
- In the **Project Browser**, projects appear sorted in alphabetical order instead of order of creation.
- On the **Configuration** pane, the **Interactive** option has been removed from the graphical interface. To use the interactive mode, use the `-interactive` flag at the command line, or in the **Advanced Settings > Other** text field. For more information, see `-interactive`

Polyspace binaries being removed

The following binaries will be removed in a future release. Unless otherwise noted, the binaries to use are located in *matlabroot/polyspace/bin*.

Binary name	What happens	Use instead
<code>polyspace-rl-manager.exe</code>	Warning	<code>polyspace-server-settings.exe</code>
<code>polyspace-spooler.exe</code>	Warning	<code>polyspace-job-monitor.exe</code>
<code>polyspace-ver.exe</code>	Warning	<code>polyspace-bug-finder-nodesktop -ver</code>
<code>setup-remote-launcher.exe</code>	Warning	<code>matlabroot/toolbox/polyspace / psdistcomp/bin/setup-polyspace-cluster</code>

Import Visual Studio project being removed

The **File > Import Visual Studio project** will be removed in a future release. Instead, use the **Create from build system** option during New Project creation. For more information, see [Create Projects Automatically from Your Build System](#).

Analysis Results

Support for MISRA C:2012

Polyspace can now check your code against MISRA C:2012 directives and coding rules. To check for MISRA C:2012 coding rule violations:

- 1 On the **Configuration** pane, select **Coding Rules**.
- 2 Select **Check MISRA C:2012**.
- 3 The MISRA C:2012 guidelines have different categories for handwritten and automatically generated code.

If you want to use the settings for automatically generated code, also select **Use generated code requirements**.

For more information about supported rules, see MISRA C:2012 Coding Directives and Rules.

Additional concurrency issue detection (deadlocks, double locks, and others)

Data race errors

The following defects deal with unprotected access of shared variables by multiple tasks.

Defect name	Status	More information
Race conditions	Removed	Replaced by Data race and Data race including atomic operations.
Data race	New	Checks for unprotected operations on variables shared by multiple tasks. This check applies to non-atomic operations only.
Data race including atomic operations	New	Checks for unprotected operations on variables shared by multiple tasks. This check applies to all operations, including atomic ones.

Locking errors

The following defects deal with incorrect design of critical sections. For multitasking analysis, to mark a section of code as a critical section, you must place it between two

function calls. A lock function begins a critical section. An unlock function ends a critical section.

Defect name	Status	More information
Deadlock	New	Checks whether the sequence of calls to lock functions is such that two tasks block each other.
Missing lock	New	Checks whether an unlock function has a corresponding lock function.
Missing unlock	New	Checks whether a lock function has a corresponding unlock function.
Double lock	New	Checks whether a lock function is called twice in a task without an unlock function being called in between.
Double unlock	New	Checks whether an unlock function is called twice in a task without a lock function being called in between.

For more information, see:

- Set Up Multitasking Analysis
- Review Concurrency Defects

New and updated defect checkers

Defect name	Status	More information
Dead code	Updated	Checks for non-executed code. No longer checks for: <ul style="list-style-type: none"> • <code>if</code> conditions that are always true without a corresponding <code>else</code>. This check is covered by the Useless if defect. • Code following control-flow statements such as <code>break</code>, <code>return</code>, or <code>goto</code> defect. This check is covered by the Unreachable code defect.
Useless if	New	Checks for if-conditions that are always true.

Defect name	Status	More information
Unreachable code	New	Checks for code following control-flow statements such as <code>break</code> , <code>return</code> , or <code>goto</code> .
Declaration mismatch	Updated	Updated for <code>#pragma</code> packing statements.
Race conditions	Removed	Replaced by Data race and Data race including atomic operations.
Data race	New	Checks for unprotected operations on variables shared by multiple tasks. This check applies to non-atomic operations only.
Data race including atomic operations	New	Checks for unprotected operations on variables shared by multiple tasks. This check applies to all accesses, including atomic ones.
Deadlock	New	Checks whether the sequence of calls to lock functions is such that two tasks block each other.
Missing lock	New	Checks whether an unlock function has a corresponding lock function.
Missing unlock	New	Checks whether a lock function has a corresponding unlock function.
Double lock	New	Checks whether a lock function is called twice in a task without an unlock function being called in between.
Double unlock	New	Checks whether an unlock function is called twice in a task without a lock function being called in between.

Reviewing Results


Context-sensitive help for analysis options and defects

Contextual help is available for analysis options in the Polyspace interface and its plug-ins. To view the contextual help for analysis options:

- 1 Hover your cursor over an analysis option in the **Configuration** pane.
- 2 Inside the tooltip, select the “More Help” link.

The documentation for that analysis option appears in a dockable window.

Contextual help is available for defects in the Polyspace interface. To view the contextual help:

- 1 In the Results Manager perspective, select a defect from the Results Summary.
- 2 Inside the **Check Details** pane, select .

The documentation for that Bug Finder defect appears in a dockable window.

For more information, see Getting Help.

Improved Results Manager perspective

The following changes have been made in the Results Manager perspective:

- To group your defects, use the **Group by** menu on the **Results Summary** pane.
 - To leave your defects ungrouped, instead of **List of Checks**, select **Group by > None**.
 - To group defects by category, instead of **Checks by Family**, select **Group by > Family**.
 - To group defects by file and function, instead of **Checks by File/Function**, select **Group by > File**.
- On the **Source** pane:
 - If a color appears on a brace enclosing a code block, double-click the brace to highlight the block. If no color appears, click the brace once to highlight the code block.

- If a code block is deactivated due to conditional compilation, it appears gray.

Error mode removed from coding rules checking

In R2014b, the **Error** mode has been removed from coding rules checking. Therefore, coding rule violations cannot stop an analysis.

Compatibility Considerations

For existing coding rules files, coding rules that use the keyword `error` are treated in the same way as that with keyword `warning`. For more information on `warning`, see [Format of Custom Coding Rules File](#).

R2014a

Version: 1.1

New Features

Bug Fixes

Compatibility Considerations

Analysis Setup


Automatic project setup from build systems

In R2014a, you can set up a Polyspace project from build automation scripts that you use to build your software application. The automatic project setup runs your automation scripts to determine:

- Source files
- Includes
- **Target & Compiler** options

To set up a project from your build automation scripts:

- At the command line: Use the `polyspace-configure` command. For more information, see [Create Project from DOS and UNIX Command Line](#).
- In the user interface: When creating a new project, in the **Project – Properties** window, select **Create from build command**. In the following window, enter:
 - The build command that you use.
 - The folder from which you run your build command.
 - Additional options. For more information, see [Create Project in User Interface](#).

Click . In the **Project Browser**, you see your new Polyspace project with the required source files, include folders, and **Target & Compiler** options.

- On the MATLAB command line: Use the `polyspaceConfigure` function. For more information, see [Create Project from MATLAB Command Line](#).

Support for GNU 4.7 and Microsoft Visual Studio C++ 2012 dialects

Polyspace supports two additional dialects: Microsoft Visual Studio C++ 2012 and GNU[®] 4.7. If your code uses language extensions from these dialects, specify the corresponding analysis option in your configuration. From the **Target & Compiler > Dialect** menu, select:

- `gnu4.7` for GNU 4.7

- `visual11.0` for Microsoft Visual Studio C++ 2012

For more information, see [Dialects for C](#) or [Dialects for C++](#).

Simplification of coding rules checking

In R2014a, the **Error** mode has been removed from coding rules checking. This mode applied only to:

- The option `Custom` for:
 - **Check MISRA C rules**
 - **Check MISRA AC AGC rules**
 - **Check MISRA C++ rules**
 - **Check JSF C++ rules**
- **Check custom rules**

The following table lists the changes that appear in coding rules checking.

Coding Rules Feature	R2013b	R2014a
New file wizard for custom coding rules.	<p>For each coding rule, you can select three results:</p> <ul style="list-style-type: none"> • Error: Analysis stops if the rule is violated. The rule violation is displayed on the Output Summary tab in the Project Manager perspective. • Warning: Analysis continues even if the rule is violated. The rule violation is displayed on the Results Summary pane in the Result Manager perspective. • Off: Polyspace does not check for violation of the rule. 	<p>For each coding rule, you can select two results:</p> <ul style="list-style-type: none"> • On: Analysis continues even if the rule is violated. The rule violation is displayed on the Results Summary pane in the Result Manager perspective. • Off: Polyspace does not check for violation of the rule.

Coding Rules Feature	R2013b	R2014a
Format of the custom coding rules file.	<p>Each line in the file must have the syntax:</p> <pre><i>rule</i> off error warning #<i>comments</i></pre> <p>For example:</p> <pre># MISRA configuration - Proj1 10.5 off #don't check 10.5 17.2 error 17.3 warning</pre>	<p>Each line in the file must have the syntax:</p> <pre><i>rule</i> off warning #<i>comments</i></pre> <p>For example:</p> <pre># MISRA configuration - Proj1 10.5 off #don't check 10.5 17.2 warning 17.3 warning</pre>

Compatibility Considerations

For existing coding rules files that use the keyword `error`:

- If you run analysis from the user interface, it will be treated in the same way as the keyword `warning`. The analysis will not stop even if the rule is violated. The rule violation will however be reported on the **Results Summary** pane.
- If you run analysis from the command line, the analysis will stop if the rule is violated.

Preferences file moved

In R2014a, the location of the Polyspace preferences file has been changed.

Operating System	Location before R2014a	Location in R2014a
Windows	%APPDATA%\Polyspace	%APPDATA%\MathWorks\MATLAB\R2014a\Polyspace
Linux	/home/\$USER/.polyspace	/home/\$USER/.matlab/\$RELEASE/Polyspace

For more information, see [Storage of Polyspace Preferences](#).

Security level support for batch analysis

When creating an MDCS server for Polyspace batch analyses, you can now add additional security levels through the **MATLAB Admin Center**. Using the **Metrics**

and Remote Server Settings, the MDCS server is automatically set to security level zero. If you want additional security for your server, use the **Admin Center** button. The additional security levels require authentication by user name, cluster user name and password, or network user name and password.

For more information, see Set MJS Cluster Security.

Interactive mode for remote analysis

In R2014a, you can select an additional **Interactive** mode for remote analysis. In this mode, when you run Polyspace Bug Finder on a cluster, your local computer is tethered to the cluster through Parallel Computing Toolbox™ and MATLAB Distributed Computing Server™.

- In the user interface: On the **Configuration** pane, under **Distributed Computing**, select **Interactive**.
- On the DOS or UNIX® command line, append `-interactive` to the `polyspace-bug-finder-nodesktop` command.
- On the MATLAB command line, add the argument `'-interactive'` to the `polyspaceBugFinder` function.

For more information, see Interactive.

Default text editor

In R2014a, Polyspace uses a default text editor for opening source files. The editor is:

- WordPad in Windows
- vi in Linux

You can change the text editor on the **Editors** tab under **Options > Preferences**. For more information, see Specify Text Editor.

Support for Windows 8 and Windows Server 2012

Polyspace supports installation and analysis on Windows Server® 2012 and Windows 8.

For installation instructions, see Installation, Licensing, and Activation.

Function replacement in Simulink plug-in

The following functions have been replaced in the Simulink plug-in by the function `pslinkfun`. These functions will be removed in a future release.

Function	What Happens?	Use This Function Instead
<code>PolyspaceAnnotation</code>	Warning	<code>pslinkfun('annotations',...)</code>
<code>PolySpaceGetTemplateCFGFile</code>	Warning	<code>pslinkfun('gettemplate')</code>
<code>PolySpaceHelp</code>	Warning	<code>pslinkfun('help')</code>
<code>PolySpaceEnableCOMServer</code>	Warning	<code>pslinkfun('enablebacktomodel')</code>
<code>PolySpaceSpooler</code>	Warning	<code>pslinkfun('queuemanager')</code>
<code>PolySpaceViewer</code>	Warning	<code>pslinkfun('openresults',...)</code>
<code>PolySpaceSetTemplateCFGFile</code>	Warning	<code>pslinkfun('settemplate',...)</code>
<code>PolySpaceConfigure</code>	Warning	<code>pslinkfun('advancedoptions')</code>
<code>PolySpaceKillAnalysis</code>	Warning	<code>pslinkfun('stop')</code>
<code>PolySpaceMetrics</code>	Warning	<code>pslinkfun('metrics')</code>

For more information, see `pslinkfun`

Check model configuration automatically before analysis

For the Polyspace Simulink plug-in, the **Check configuration** feature has been enhanced to automatically check your model configuration before analysis. In the **Polyspace** pane of the Model Configuration options, select:

- **On, proceed with warnings** to automatically check the configuration before analysis and continue with analysis when only warnings are found.
- **On, stop for warnings** to automatically check the configuration before analysis and stop if warnings are found.
- **Off** does not check the configuration before an analysis.

If the configuration check finds errors, Polyspace stops the analysis.

For more information about **Check configuration**, see [Check Simulink Model Settings](#).

Data range specification support

Data range specification (DRS) is available with Polyspace Bug Finder. You can add range information to global variables.

You can also use DRS information with Polyspace Code Prover. Similarly, you can use DRS information from Code Prover in Bug Finder.

For more information, see [Inputs & Stubbing](#).

Polyspace binaries being removed

The following Polyspace binaries will be removed in a future release:

- `polyspace-report-generator.exe`
- `polyspace-results-repository.exe`
- `polyspace-spooler.exe`
- `polyspace-ver.exe`

Analysis Results

Classification of bugs according to the Common Weakness Enumeration (CWE) standard

In R2014a, Polyspace Bug Finder associates CWE™ IDs with many defects. For the covered defects, the IDs are listed in the **CWE ID** column on the **Results Summary** pane. To view the **CWE ID** column, right-click the **Results Summary** tab and select the **CWE ID** column.

For more information, see Common Weakness Enumeration from Bug Finder Defects.

Additional coding rules support (MISRA-C:2004 Rule 18.2, MISRA-C++ Rule 5-0-11)

The Polyspace coding rules checker now supports two additional coding rules: MISRA C 18.2 and MISRA C++ 5-0-11.

- MISRA C 18.2 is a required rule that checks for assignments to overlapping objects.
- MISRA C++ 5-0-11 is a required rule that checks for the use of the plain `char` type as anything other than storage or character values.
- MISRA C++ 5-0-12 is a required rule that checks for the use of the signed and unsigned `char` types as anything other than numerical values.

For more information, see MISRA C:2004 Coding Rules or MISRA C++ Coding Rules.

Additional analysis checkers

Polyspace Bug Finder can now check for two additional defects in C and C++:

- **Wrong allocated object size for cast** checks for memory allocations that are not multiples of the pointer size.
- **Line with more than one statement** checks for lines that have additional statements after a semicolon.

For more information, see Wrong allocated object size for cast and Line with more than one statement.

Improvement of floating point precision

In R2013b, Polyspace improved the precision of floating point representation. Previously, Polyspace represented the floating point values with intervals, as seen in the tooltips. Now, Polyspace uses a rounding method.

For example, the analysis represents `float arr = 0.1;` as,

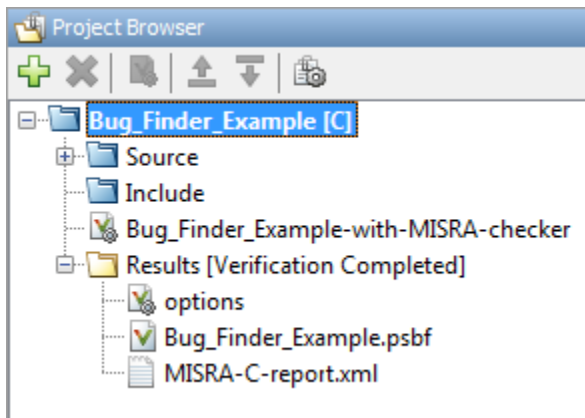
- Pre-R2013b, `arr = [9.9999E^-2,1.0001E-1]`.
- Now, `arr = 0.1`.

Reviewing Results

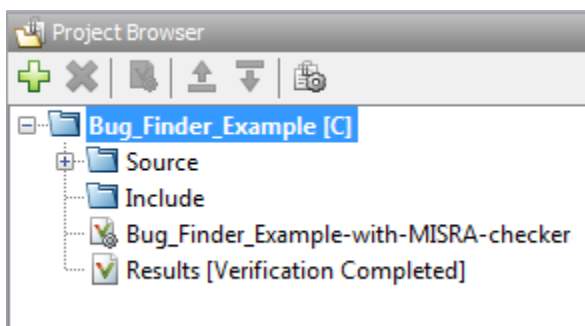
Results folder appearance in Project Browser

In R2014a, the results folder appears in a simplified form in the **Project Browser**. Instead of a folder containing several files, the result appears as a single file.

- Format before R2014a



- Format in R2014a



The following table lists the changes in the actions that you can perform on the results folder.

Action	R2013b	R2014a
Open results.	In the result folder, double-click result file with extension .psbf .	Double-click result file.
Open analysis options used for result.	In the result folder, select options .	Right-click result file and select Open Configuration .
Open metrics page for batch analyses if you had used the analysis option Distributed Computing > Add to results repository .	In the result folder, select Metrics Web Page .	Double-click result file. If you had used the option Distributed Computing > Add to results repository , double-clicking the results file for the first time opens the metrics web page instead of the Result Manager perspective.
Open results folder in your file browser.	Navigate to results folder. To find results folder location, select Options > Preferences . View result folder location on the Project and Results Folder tab.	Right-click result file and select Open Folder with File Manager .

Results manager improvements

- In R2014a, you can view the extent of a code block on the **Source** pane by clicking either its opening or closing brace.

```

Source
Dashboard x dataflow.c x
196  *-----*
197  int do_anything(void);
198
199  int bug_deactivatedcode(int val)
200  {
201      int retval;
202      retval = do_anything();
203
204      if (0 /*|| retval < 0*/) /* Defect: Deactivated (debug) code
205          retval = do_anything();
206      }
207
208      return retval;
209  }
210

```

Note: This action does not highlight the code block if the brace itself is already highlighted. The opening brace can be highlighted, for example, with a **Dead code** defect for the code block.

- In R2014a, the **Verification Statistics** pane in the Project Manager and the **Results Statistics** pane in the Results Manager have been renamed **Dashboard**.

On the **Dashboard**, you can obtain an overview of the results in a graphical format. You can see:

- Code covered by analysis.
- Defect distribution. You can choose to view the distribution by:
 - **File**
 - **Category** or defect name.
- Distribution of coding rule violations. You can choose to view the distribution by:
 - **File**

- **Category** or rule number.

The **Dashboard** displays violations of different types of rules such as MISRA C, JSF C++, or custom rules on different graphs.

For more information, see Dashboard.

- In R2014a, on the **Results Summary** pane, you can distinguish between violations of predefined coding rules such as MISRA C or C++ and custom coding rules.
 - The predefined rules are indicated by ▼.
 - The custom rules are indicated by ▼.

In addition, when you click the **Check** column header on the **Results Summary** pane, the rules are sorted by rule number instead of alphabetically.

- In R2014a, you can double-click a variable name on the **Source** pane to highlight other instances of the variable.

Additional back-to-model support for Simulink plug-in

In R2014a, the back-to-model feature is more stable. Additionally, support has been added for Stateflow® charts in Target Link and Linux operating systems.

For more information, see Identify Errors in Simulink Models.

R2013b

Version: 1.0

New Features

Analysis Setup

Introduction of Polyspace Bug Finder

Polyspace Bug Finder is a new companion product to Polyspace Code Prover. Polyspace Bug Finder analyzes C and C++ code to find possible defects and coding rule violations. Bug Finder can run fast analyses on large code bases with low false-positive results. Polyspace Bug Finder also calculates code complexity metrics with Polyspace Metrics.

Bug Finder integrates with Simulink, Eclipse, Visual Studio, and Rhapsody to help you analyze code from within your development environment.

Fast analysis of large code bases

Polyspace Bug Finder uses an efficient analysis method which produces results quickly, even from large code bases. Therefore you can fix errors and rerun the analysis without having to wait. You can find more issues early on in the development process and produce better quality code overall.

Eclipse integration

Polyspace Bug Finder comes with an Eclipse plug-in that integrates Polyspace into your development environment. You can set up options, run analyses, view results, and fix bugs in the Eclipse interface. Using the Polyspace plug-in, you can quickly find and fix bugs as you code.

For a tutorial on using the Polyspace Bug Finder plug-in, see [Find Defects from the Eclipse Plug-In](#).

Analysis Results

Detection of run-time errors, data flow problems, and other defects in C and C++ code

Polyspace Bug Finder uses static analysis to find various defects for C and C++ code with few false-positive results. The analysis does not require program execution, code instrumentation, or test cases.

Some categories of defects are:

- Numeric
- Programming
- Static memory
- Dynamic memory
- Data-flow

To see a list of defects you can find, see [Polyspace Bug Finder Defects](#).

Bug Finder analysis runs quickly, so you can fix errors and rerun analysis.

For information about running analyses, see [Find Bugs](#).

Compliance checking for MISRA-C:2004, MISRA-C++:2008, JSF++, and custom naming conventions

Polyspace Bug Finder can also check for compliance with coding rules. There are four industry-defined rules you can select:

- MISRA C
- MISRA AC-AGC
- MISRA C++
- JSF C++

In addition, you can define rules to check for naming conventions.

You can run the coding rules checker separately, or at the same time as your analysis.

For more information, see [Check Coding Rules](#).

Cyclomatic complexity and other code metrics

Using Polyspace Metrics, Polyspace Bug Finder calculates various code metrics, including cyclomatic complexity. These statistics are displayed using Polyspace Metrics, an integrated Web interface. You can use these results to track code quality over time. You can also share the code metrics, allowing others to track your project's progress.

Reviewing Results

Traceability of code analysis results to Simulink models

For generated code from Simulink models, Polyspace analysis results link directly back to your Simulink model. You can trace defects back to the block that is causing the bug.

In the Source Code view of the Results Manager, the block names appear as links. When you select a link, the corresponding block is highlighted in Simulink.

For a tutorial on using Polyspace Bug Finder with Simulink models, see [Find Defects from Simulink](#).

Access to Polyspace Code Prover results

A Polyspace Bug Finder installation also includes the Polyspace Code Prover user interface. With only a Polyspace Bug Finder license, you cannot run local Polyspace Code Prover verifications in the Polyspace Code Prover interface. However, you can use the Polyspace Code Prover interface to review results and upload comments to Polyspace Metrics.

For more information, see the [Polyspace Code Prover Documentation](#).

