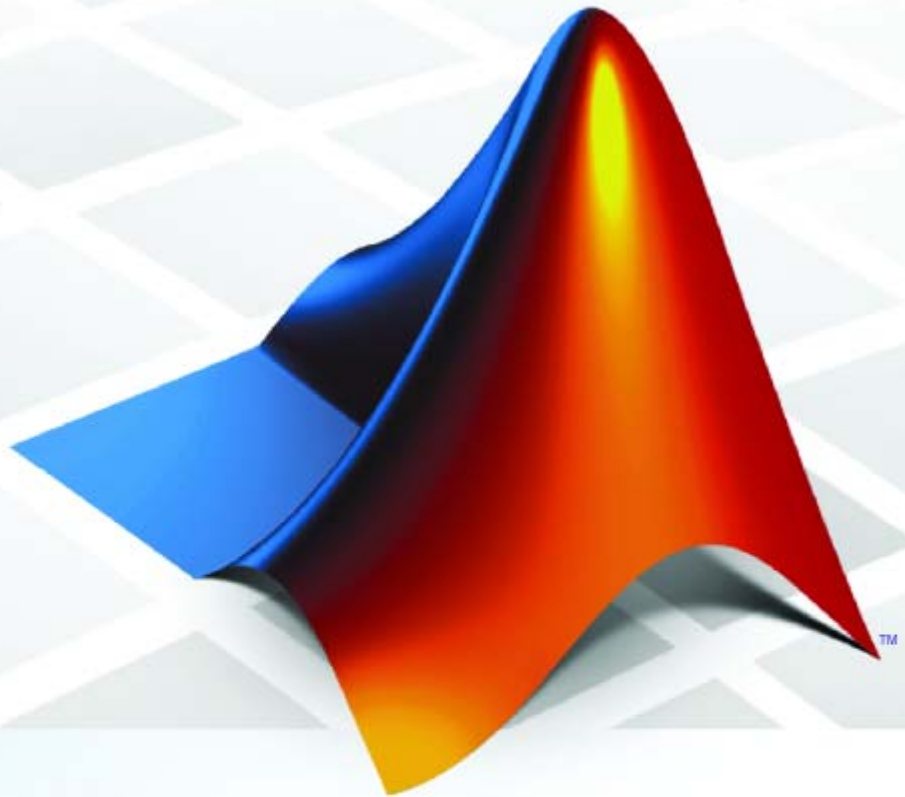


# PolySpace<sup>®</sup> Products for Ada 5 Reference



## How to Contact The MathWorks



[www.mathworks.com](http://www.mathworks.com) Web  
[comp.soft-sys.matlab](mailto:comp.soft-sys.matlab) Newsgroup  
[www.mathworks.com/contact\\_TS.html](http://www.mathworks.com/contact_TS.html) Technical Support



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



508-647-7000 (Phone)



508-647-7001 (Fax)



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

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

*PolySpace® Products for Ada Reference*

© COPYRIGHT 1999–2010 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](http://www.mathworks.com/trademarks) for a list of additional trademarks. Other product or brand names may be trademarks or registered trademarks of their respective holders.

### Patents

The MathWorks products are protected by one or more U.S. patents. Please see [www.mathworks.com/patents](http://www.mathworks.com/patents) for more information.

### Revision History

March 2009	Online Only	Revised for Version 5.3 (Release 2009a)
September 2009	Online Only	Revised for Version 5.4 (Release 2009b)
March 2010	Online Only	Revised for Version 5.5 (Release 2010a)

## Option Descriptions

1

<b>General Options</b> .....	1-2
Overview .....	1-2
Session identifier .....	1-2
Date .....	1-4
Author .....	1-5
Project version .....	1-6
Keep all preliminary results files .....	1-7
Report Generation .....	1-8
Report template name .....	1-8
Output format .....	1-8
Report name .....	1-9
-sources “list_of_files” .....	1-10
-extensions-for-spec-files and -ada-include-dir .....	1-11
-results-dir folder .....	1-12
<b>Target and Compiler Options</b> .....	1-13
Target processor type .....	1-14
Operating system target for Standard Libraries compatibility .....	1-15
Command/script to apply before start of the code verification .....	1-16
Command/script to apply after the end of the code verification .....	1-18
<b>Compliance with Standards Options</b> .....	1-19
Value of the constant Storage_Unit .....	1-20
Remove comparison operators ambiguities .....	1-21
Analysis Mode .....	1-23
<b>PolySpace Inner Settings Options</b> .....	1-24
Run a verification unit by unit .....	1-25
Unit common source .....	1-26
Name of the main subprogram .....	1-26
Generate a main .....	1-27

Stubbing .....	1-28
Assumptions .....	1-32
Run verification in 32 or 64-bit mode .....	1-36
Other options .....	1-36
<b>Precision Options .....</b>	<b>1-38</b>
Launch code verification from beginning of .....	1-39
To end of .....	1-41
Precision Level .....	1-43
Specific Precision .....	1-45
Max size of global array variables .....	1-46
Improve precision of interprocedural analysis .....	1-47
List of variables to expand .....	1-49
Expansion limit for a structured variable .....	1-50
<b>Multitasking Options (PolySpace Server Only) .....</b>	<b>1-52</b>
Implicit Tasks .....	1-52
Critical section details .....	1-53
Temporal exclusion tasks (separated by space characters) .....	1-54
<b>Batch Options .....</b>	<b>1-55</b>
-server server_name_or_ip[:port_number] .....	1-55
-h[elp] .....	1-55
-v   -version .....	1-56
-sources-list-file file_name .....	1-56

## Check Descriptions

# 2

<b>Colored Source Code for Ada .....</b>	<b>2-2</b>
Non-Initialized Variable: NIV/NIVL .....	2-3
Division by Zero: ZDV .....	2-7
Arithmetic Exceptions: EXCP .....	2-8
Scalar and Float Underflow/Overflow : UOVFL .....	2-11
Scalar and Float Overflow: OVFL .....	2-12
Scalar and Float Underflow: UNFL .....	2-13
Attributes Check: COR .....	2-15
Array Length Check: COR .....	2-17

DIGITS Value Check: COR .....	2-19
DELTA Value Length Check: COR .....	2-20
Static Range and Values Check: COR .....	2-21
Discriminant Check: COR .....	2-23
Component Check: COR .....	2-24
Dimension Versus Definition Check: COR .....	2-25
Aggregate Versus Definition Check: COR .....	2-26
Aggregate Array Length Check: COR .....	2-28
Sub-Aggregates Dimension Check: COR .....	2-29
Characters Check: COR .....	2-30
Accessibility Level on Access Type: COR .....	2-32
Explicit Dereference of a Null Pointer: COR .....	2-33
Accessibility of a Tagged Type: COR .....	2-34
Power Arithmetic: POW .....	2-36
User Assertion: ASRT .....	2-37
Non Terminations: Calls and Loops .....	2-39
Unreachable Code: UNR .....	2-49
Value on Assignment: VOA .....	2-51
Inspection Points: IPT .....	2-53

## Approximations Used During Verification

### 3

<b>Why PolySpace Verification Uses Approximations</b> ....	3-2
What is Static Verification .....	3-2
Exhaustiveness .....	3-3

## Examples

### 4

<b>Complete Examples</b> .....	4-2
Simple Ada Example .....	4-2
HDCA Server Example .....	4-2
airplane2 Example .....	4-3
High Speed Train Example .....	4-3



# Option Descriptions

---

- “General Options” on page 1-2
- “Target and Compiler Options” on page 1-13
- “Compliance with Standards Options” on page 1-19
- “PolySpace Inner Settings Options” on page 1-24
- “Precision Options” on page 1-38
- “Multitasking Options (PolySpace Server Only)” on page 1-52
- “Batch Options” on page 1-55

## General Options

In this section...
“Overview” on page 1-2
“Session identifier” on page 1-2
“Date” on page 1-4
“Author” on page 1-5
“Project version” on page 1-6
“Keep all preliminary results files” on page 1-7
“Report Generation” on page 1-8
“Report template name” on page 1-8
“Output format” on page 1-8
“Report name” on page 1-9
“-sources “list_of_files”” on page 1-10
“-extensions-for-spec-files and -ada-include-dir” on page 1-11
“-results-dir folder” on page 1-12

### Overview

This section describes all options relating to the identification of the verification, including the destination folder for the results and sources.

### Session identifier

Specify name of your application using any valid UNIX<sup>®</sup> file name

### Settings

No Default

### Command-Line Information

Parameter: prog



**Type:** string

**Value:** any valid UNIX file name

**Shell script example:** polyspace-ada -prog myApp ...

**See Also**

“Creating a Project” in PolySpace® Products for Ada documentation

## **Date**

Specify date stamp for verification

### **Settings**

**Default:** Date on which you launch verification, in *dd/mm/yyyy* format.

- You can change the default format of the date as follows:
  - 1** Select **Edit > Preferences**. The **Preferences** dialog box opens.
  - 2** Select **Miscellaneous**.
  - 3** From the **Date format** drop-down list, choose the format that you want.

### **Command-Line Information**

**Parameter:** date

**Type:** string

**Value:** any valid value in *dd/mm/yyyy* format

**Default:** Date on which you launch verification

**Shell script example:** `polyspace-ada -date "02/01/2002"`

### **See Also**

“Creating a Project” in PolySpace Products for Ada documentation

## **Author**

Specify author of verification

## **Settings**

**Default:** user ID

## **Command-Line Information**

**Parameter:** author

**Type:** string

**Value:** any valid value

**Default:** user ID

**Shell script example:** polyspace-ada -author "A. Tester"

## **See Also**

“Creating a Project” in PolySpace Products for Ada documentation

## **Project version**

Specify version ID for verification

### **Settings**

**Default:** 1.0

- Use this parameter to help you identify verifications.

### **Command-Line Information**

**Parameter:** `verif-version`

**Type:** string

**Value:** any valid value

**Default:** 1.0

**Shell script example:** `polyspace-ada -verif-version 1.3`

### **See Also**

“Creating a Project” in PolySpace Products for Ada documentation

## Keep all preliminary results files

Specify whether to retain all intermediate results and associated working files.

### Settings

**Default:** Off



On

Retain all intermediate results and associated working files. You can restart a verification from the end of any complete pass if the source code remains unchanged.



Off

Erase all intermediate results and associated working files. If you want to restart a verification, do so from the beginning.

### Tips

- This option is applicable only to client verifications. Intermediate results are always removed before results are downloaded from the PolySpace server.
- To cleanup intermediate files at a later time, you can select **Tools > Clean Results** in the Launcher. This option deletes the preliminary result files from the results folder.

### Command-Line Information

**Parameter:** `keep-all-files`

**Shell script example:** `polyspace-ada -keep-all-files`

### See Also

“Creating a Project” in PolySpace Products for Ada documentation

## Report Generation

Specify whether to create verification report using report generation options

### Settings

**Default:** Off

On  
Create report.

Off  
No report created.

## Report template name

Specify report template for generating verification report.

### Settings

**No Default**

- Report generated at the end of the verification process, before execution of any `post-analysis-command`.

### Command-Line Information

**Parameter:** `report-template`

**Type:** `string`

**Value:** any valid script file name

**Shell script example:** `polyspace-ada -report-template  
c:/polyspace/my_template`

## Output format

Specify output format of report

### Settings

**Default:** `RTF`

RTF  
Generate an .rtf format report.

HTML  
Generate an .html format report.

PDF  
Generate a .pdf format report.

Word  
Generate a .doc format report.

Word is not available on UNIX platforms. RTF is used instead.

XML  
Generate and .xml format report.

## Command-Line Information

**Parameter:** report-output-format

**Type:** string

**Value:** RTF | HTML | PDF | Word | XML

**Default:** RTF

### Shell script example:

```
polyspace-ada -report-template my_template -report-output-format pdf
```

## Report name

Specify name of verification report file

## Settings

**Default:** *Prog\_TemplateName.Format* where:

- *Prog* is the argument of the prog option
- *TemplateName* is the name of the report template specified by the report-template option
- *Format* is the file extension for the format specified by the report-output-format option.

## Command-Line Information

**Parameter:** report-output-name

**Type:** string

**Value:** any valid value

**Default:** *Prog\_TemplateName.Format*

### Shell script example:

```
polyspace-ada -report-template my_template -report-output-name Airbag_V3.rtf
```

### **-sources "list\_of\_files"**

For Windows<sup>®</sup>, Linux<sup>®</sup>, and Solaris<sup>™</sup>, use the form *file1[,file2[, ...]]* for *list\_of\_files*.

For example,

```
polyspace-ada -sources "spc/mod1.ads,bod/mod1.adb"
```

For Linux and Solaris, you can also use the form *file1[ file2[ ...]]* for *list\_of\_files*.

For example,

```
polyspace-ada -sources "my_folder/mod*.ad[sb]"
```

With the preceding syntax, the software analyzes only Ada files with the extensions. (A|a)d(a|b|s)

However, you can analyze Ada files with other extensions. If you also have, for example, files with the .sep extension, you can use the following syntax:

```
-sources "./sources/*.a* ,./sources/*.sep"
```

To analyse Ada files with any extension, use the following syntax:

```
-sources "./sources/*.*"
```

**Default:** sources/\*. (A|a)d(a|b|s)

For specifying files in batch mode, see “-sources-list-file file\_name” on page 1-56.



## **-extensions-for-spec-files and -ada-include-dir**

The `-extensions-for-specs-files` option specifies the file extension for files "*F*" which are verified to get the type and variables names but which are not part of the `-sources` list.

The result of specifying this option is similar to having a dictionary with only the list of words and their type (*verb, noun, adj*) without the definition. These files allow the product to know the name and the type, but not the values (*dictionary definitions*).

The `-ada-include-dir` specifies the folder where the *F* files are. However, you can use the option several times and you can specify more than one folder.

---

**Note** Use both options together.

---

### **Benefits:**

- Faster compilation on these packages to focus on the `-sources` packages specifications and bodies
- Full range for all constants defined in these packages. Consider 1 package body B and 2 specifications S1 and S2 in the following examples.

### **Usage examples using the graphical interface:**

configuration 1:

- `-sources` contains B.ada and S1.ada
- `-extensions-for-specs-files` contains the \*.ada filter
- `-ada-include-dir` contains the TEST folder and the TEST folder contains S2.ada

configuration 2:

- `-sources` contains B.ada, S1.ada, S2.ada
- If you use a constant S2.C:

- configuration 1: its value is its full range
- configuration 2: its value is the real constant value

### Usage examples in shell entry-script mode:

```
polyspace-desktop-ada -sources "B.ada,S1.ada"  
-extensions-for-specs-files "*.ada" -ada-include-dir  
./include_specs
```

```
polyspace-desktop-ada -sources sources/example.ad*  
-extensions-for-spec-files "*.ad?" -ada-include-dir "sources"
```

### **-results-dir folder**

This option specifies the folder in which PolySpace writes the results of the verification. Although you may specify relative folders, be careful with their use, especially if the tool launches remotely over a network, and when a project configuration file is copied using the "Save as" option.

**Default:** Folder in which tool is launched

**Shell Script:** Folder in which tool is launched

**From Graphical User Interface:** C:\PolySpace\_Results

### **Example Shell Script Entry:**

```
polyspace-ada -results-dir RESULTS ...  
export RESULTS=results_`date+%d%B_%HH%M_%A`  
polyspace-ada -results-dir `pwd`/$RESULTS ...
```

## Target and Compiler Options

<b>In this section...</b>
“Target processor type” on page 1-14
“Operating system target for Standard Libraries compatibility” on page 1-15
“Command/script to apply before start of the code verification” on page 1-16
“Command/script to apply after the end of the code verification” on page 1-18

## Target processor type

Specify the target processor type.

### Settings

**Default:** sparc

sparc

Sun® Microsystems SPARC® processor

m68k

Freescale™ ColdFire® m68k processor

1750a

MIL-STD-1750A 16-bit instruction set architecture

powerpc64bit

PowerPC® 64-bit instruction set architecture

powerpc32bit

PowerPC 32-bit instruction set architecture

i386

Intel® 80386 (i386) processor

### Command-Line Information

**Parameter:** target

**Type:** string

**Value:** sparc | m68k | 1750a | powerpc64bit | powerpc32bit | i386

**Default:** sparc

**Shell script example:** polyspace-ada -target m68k

### See Also

“Setting Up a Target” in PolySpace Products for Ada documentation

## Operating system target for Standard Libraries compatibility

Specify operating system target for which there are implementation-specific declarations in the Ada Standard Libraries

### Settings

PolySpace supplies only `gnat` include files, which you can find in the `ada` include folder within the installation folder. You can verify projects with other operating systems by using the corresponding include files (not supplied). For instance, to verify a `greenhills` project, use the option:

```
ada-include-dir path_to_the_greenhills_include_folder
```

### Default: no-predefined-OS

`no-predefined-OS`

No operating system (with implementation-specific declarations in Ada Standard Libraries) specified

`gnat`

GCC Ada95

`greenhills`

Greenhills® Software real-time operating system (RTOS)

### Command-Line Information

**Parameter:** OS-target

**Type:** string

**Value:** no-predefined-OS | gnat | greenhills

**Default:** no-predefined-OS

### Shell script examples:

```
polyspace-ada -OS-target gnat
```

```
polyspace-ada -OS-target greenhills -ada-include-dir /complete_path_to/greenhills_includes
```

### See Also

“Setting Up a Target” in PolySpace Products for Ada documentation

## Command/script to apply before start of the code verification

Specify script file or command to run before the verification of each source file.

### Settings

#### No Default

- Design the script or command to process the standard output from source code. For example, consider the following script `replace_keywords`:

```
#!/usr/bin/perl
my $TOOLS_VERSION = "V1_4_1";
binmode STDOUT;

# Process every line from STDIN until EOF
while ($line = <STDIN>)
{
    # Change Volatile to Import
    $line =~ s/Volatile/Import/;
    print $line;
}
```

To replace the keyword `Volatile` by `Import`, run the following command on a Linux machine:

```
polyspace-ada -pre-analysis-command `pwd`/replace_keywords
```

- If you are running PolySpace software Version 5.1 (r2008a) or later on a Windows system, you cannot use Cygwin™ shell scripts. Cygwin is no longer included with PolySpace software, so all files must be executable by Windows. To support scripting, the PolySpace installation includes Perl. You can access Perl using:

```
%POLYSPACE_ADA%\Verifier\tools\perl\win32\bin\perl.exe
```

To run the Perl script `replace_keywords` on a Windows machine, use the option `-pre-analysis-command` with the absolute path to the Perl script:

```
%POLYSPACE_ADA%\Verifier\bin\polyspace-cpp.exe
-pre-analysis-command
```

```
%POLYSPACE_ADA%\Verifier\tools\perl\win32\bin\perl.exe  
<absolute_path>\replace_keywords
```

### **Command-Line Information**

**Parameter:** pre-analysis-command

**Type:** string

**Value:** any valid script file name or command

### **See Also**

“Setting Up a Target” in PolySpace Products for Ada documentation

## Command/script to apply after the end of the code verification

Specify script file or command to run after the completion of verification.

### Settings

#### No Default

- You execute the script or command in the verification results folder from either the client or server side, depending your configuration.

To send an e-mail to the client indicating that the verification is complete, run the following command:

```
polyspace-ada -post-analysis-command `pwd`/end_mail
```

where `end_mail` is an appropriate Perl script.

- If you are running PolySpace software Version 5.1 (r2008a) or later on a Windows system, you cannot use Cygwin shell scripts. Cygwin is no longer included with PolySpace software, so all files must be executable by Windows. To support scripting, the PolySpace installation includes Perl. You can access Perl using:

```
%POLYSPACE_ADA%\Verifier\tools\perl\win32\bin\perl.exe
```

To run the Perl script `end_mail` on a Windows machine, use the option `-post-analysis-command` with the absolute path to the Perl script:

```
%POLYSPACE_ADA%\Verifier\bin\polyspace-cpp.exe
```

```
-post-analysis-command
```

```
%POLYSPACE_ADA%\Verifier\tools\perl\win32\bin\perl.exe
```

```
<absolute_path>\end_email
```

### Command-Line Information

**Parameter:** `post-analysis-command`

**Type:** string

**Value:** any valid script file name or command

### See Also

“Setting Up a Target” in PolySpace Products for Ada documentation



## Compliance with Standards Options

<b>In this section...</b>
“Value of the constant Storage_Unit” on page 1-20
“Remove comparison operators ambiguities” on page 1-21
“Analysis Mode” on page 1-23

## Value of the constant `Storage_Unit`

Specify a positive value for `SYSTEM.Storage_Unit`.

### Settings

**Default:** 8, except for target processor type 1750a whose default is 16

- If you do not specify a value, the default in the `SYSTEM` package is used.
- The value required depends on the code that you write. For example, if the value for `Storage_Unit` is 8, the following code generates an error message A overlaps B:

```
-- Definition of record type
type REC is record
  A : integer;
  B : boolean;
end REC;
-- Representation clause of this record
for REC use record
  A at 0 range 0 .. 31;
  B at 1 range 0 .. 31;
end record
```

In this case, set the value of `Storage_Unit` to 32.

### Command-Line Information

**Parameter:** `storage-unit`

**Type:** string

**Value:** any valid value

**Default:** 8, except for target processor type 1750a whose default is 16

### See Also

“Compile Errors” in PolySpace Products for Ada documentation

## Remove comparison operators ambiguities

Specify whether to remove ambiguities regarding the visibility of relational operators (=, /=, <=, =>, >, and <).

In the following code:

```
Package A is
  type T1 is new Integer range 0 .. 100; -- line 1
end A;
-- Other file:example1.adb
with A; use A;
Package B is
  subtype T2 is T1 range 2..80;
end B;

Package OTHER_IABC_ADA_4 is
  procedure Main;
end OTHER_IABC_ADA_4;

with B; use B;
Package body OTHER_IABC_ADA_4 is
  X, Y : T2;
  procedure Main is
  begin
    null;
    pragma Assert (TRUE);
  end Main;
  begin
    X := 12;
    Y := 10;
    if X > Y then -- line 21
      pragma Assert (True);
      null;
    end if;
  end OTHER_IABC_ADA_4;
```

If you select the check box, the software does not generate errors. If you do not select the check box, the software generates errors:

- PolySpace found an error in ./example1.adb:21:07: operator for type "T1" defined at ./example1.adb:1 is not directly visible.
- PolySpace found an error in /example1.adb:21:07: use clause would make operation legal

## Settings

**Default:** Off



On

Remove ambiguities.



Off

Do not remove ambiguities. The type of operand determines whether the operator is visible.

## Command-Line Information

**Parameter:** base-type-directly-visible

## See Also

“Compile Errors” in PolySpace Products for Ada documentation

## Analysis Mode

Select customize, permissive, or strict verification mode

### Settings

**Default:** Customize

Customize

Strict

Selects no-automatic-stubbing option

Permissive

Selects continue-with-in-out-niv option

### Command-Line Information

**Parameter:** strict | permissive

**Type:** string

**Value:** Strict | Customize | Permissive

**Default:** Customize

## **PolySpace Inner Settings Options**

<b>In this section...</b>
“Run a verification unit by unit” on page 1-25
“Unit common source” on page 1-26
“Name of the main subprogram” on page 1-26
“Generate a main” on page 1-27
“Stubbing” on page 1-28
“Assumptions” on page 1-32
“Run verification in 32 or 64-bit mode” on page 1-36
“Other options” on page 1-36

## Run a verification unit by unit

Specify separate verification job for each source file in the project

### Settings

**Default:** Off



On

Each file is compiled, sent to the PolySpace Server, and verified individually. You can view results for the entire project or for individual units.

Unit by unit verification is available only for verification on a server.



Off

No unit by unit verification.

### Command-Line Information

**Parameter:** `unit-by-unit`

**Shell script example:** `polyspace-ada -unit-by-unit`

## **Unit common source**

Specify list of files to include with each unit verification

### **Settings**

**No Default**

- Compile files in the list once, and then link to each unit before verification.
- Stub functions not included in the list.

### **Command-Line Information**

**Parameter:** unit-by-unit-common-source

**Type:** string

**Value:** any valid file name

**Shell script example:** polyspace-ada -unit-by-unit-common-source  
c:/polyspace/function.adb

## **Name of the main subprogram**

Specifies the name of the main subprogram

### **Settings**

**No Default**

- Verify procedure after package elaboration, and before tasks (for a multi-task application or if -entry-points option is specified).
- Cannot be used with the main-generator option.

### **Command-Line Information**

**Parameter:** main

**Shell script example:** polyspace-ada -main mainpackage.init

### **See Also**

“Verifying an Application Without a “Main”” in PolySpace Products for Ada documentation



## Generate a main

Specifies whether to automatically generate a main program.

The generated main program:

- Calls only procedures and functions that are specified in a package. PolySpace software assigns random, initialized values to all `in` and `in out` parameters for these procedures and functions.
- Assigns values to global variables that are specified in a package. If a global variable is initialized in a specification, then PolySpace software assigns this variable a random, initialized value. If a global variable is not initialized, PolySpace software assigns the global variable a random, possibly uninitialized, value (specifying the `init-stubbing-vars-random` or `init-stubbing-vars-zero-or-random` parameters has no effect).

This behavior models the fact that the variable can be changed outside the package.

- Assigns values to global variables that are declared in a package body. If a global variable is initialized in a package body, then PolySpace software assigns this variable a random, initialized value. If a global variable is not initialized, PolySpace software leaves it uninitialized except when you specify the `init-stubbing-vars-random` or `init-stubbing-vars-zero-or-random` parameters. In this case, the variable is assigned a random, initialized value.

This behavior models the fact that the variable can only be changed inside the package, but the functions of the package can be called several times.

You cannot use this option with the `main` option.

### Settings

**Default:** On for PolySpace® Client™; Off for PolySpace® Server™



On

Create a procedure that calls every uninvoked procedure in the code.

Deactivates `main` option for PolySpace Server.



Off

Selected by PolySpace Client if main option is activated

## Command-Line Information

**Parameter:** main-generator

### Shell script examples:

```
polyspace-ada -main-generator ...  
polyspace-desktop-ada ... (implicit -main-generator active)  
polyspace-desktop-ada -main myPack.main ...  
(implicit -main-generator canceled by the usage of -main)
```

## See Also

“Initialization of uninitialized global variables” on page 1-32 in Products for Ada documentation

## Stubbing

- “Treat import as non volatile” on page 1-29
- “Treat export as non volatile” on page 1-30
- “No automatic stubbing” on page 1-31
- “Initialization of uninitialized global variables” on page 1-32

## Treat import as non volatile

Specify whether pragma import variable is volatile

**Settings.** Default: Off



On

Consider imported variable to be regular.



Off

Consider imported variable to be volatile.

### Command-Line Information.

**Parameter:**import-are-not-volatile

**Shell script example:** polyspace-ada -import-are-not-volatile

**See Also.** “Stubbing” and “Volatile Variables” in Products for Ada documentation

### **Treat export as non volatile**

Specify whether pragma export variable is volatile

**Settings.** Default: Off



On

Consider exported variable to be regular.



Off

Consider exported variable to be volatile.

### **Command-Line Information.**

**Parameter:** export-are-not-volatile

**Shell script example:** polyspace-ada -export-are-not-volatile

**See Also.** “Stubbing” and “Volatile Variables” in Products for Ada documentation

## No automatic stubbing

Specify whether to stub a procedure or function without a body, to allow verification.

**Settings.** Default: Off



On

A procedure or function that has no body (a function that you declare but do not define) stops verification. Use this option when you want to :

- Make sure that all code is supplied, for example, when verifying a large piece of code.
- Write stubs yourself, to increase the selectivity and speed of verification



Off

Stub all procedures and functions automatically according to these rules:

- The generated stub is the most general body derived from its prototype.
- Implicit and explicit tasks are not stubbed.
- The main procedure is not stubbed.
- The generated stubs do not have side-effects on global variables. If a function affects global variables, then stub this function manually.

**Dependency.** This parameter cannot be used with **Initialization of uninitialized global variables** (-init-stubbing-vars-random or -init-stubbing-vars-zero-or-random).

### Command-Line Information.

**Parameter:** -no-automatic-stubbing

**Type:** string

**Value:** on | off

**Default:** off

**Shell script example:** polyspace-ada -no-automatic-stubbing

**See Also.** “Stubbing” in PolySpace Products for Ada documentation

## **Initialization of uninitialized global variables**

Specify how uninitialized global variables are initialized.

**Settings.** Default: No initialization

The following setting descriptions apply only when the `-main-generator` option (**Generate a main** check box) is *not* selected. For information on how the settings apply when you select the `-main-generator` option, see “Generate a main” on page 1-27.

No initialization

Uninitialized global variables produce warnings or errors. No values assigned.

With random value

Assign random values to uninitialized global variables.

With zero or random value

Assign zero to uninitialized global variables if the type contains zero. Otherwise, assign random values.

**Dependency.** You cannot use this parameter with `-no-automatic-stubbing`.

### **Command-Line Information.**

**Parameter:** `init-stubbing-vars-random |  
init-stubbing-vars-zero-or-random`

**Shell script example:** `polyspace-ada -init-stubbing-vars-random`

**See Also.** “Stubbing” in PolySpace Products for Ada documentation

## **Assumptions**

- “Continue after non initialized variables” on page 1-33
- “Continue with non-initialized in/out parameters” on page 1-33
- “Ignore float rounding” on page 1-34
- “Procedures known to cause NTC” on page 1-35

## Continue after non initialized variables

Specify whether verification detects all non-initialized variables

**Settings.** Default: Off



Detect all non-initialized variables (NIV). In the following code, the software detects all three NIVs in the first verification run.

```

procedure Main is
  I,T,No: Integer;
begin
  if (No = 0)  -- red NIV, with or without option
  then
    I := 1/I;  -- red NIV with option, grey otherwise
  end if;
  if (T = 0)  -- red NIV with option, grey otherwise
  then
    I := 12312409 /120;
  end if;
end Main;

```

You lose precision when using this option. Use this option only for the first verification run of a project.



Verification stops after the first red non-initialized variable (NIV).

### Command-Line Information.

**Parameter:** continue-with-all-niv

## Continue with non-initialized in/out parameters

Specify whether to continue with verification if in and out parameters of a procedure are not initialized.

**Settings.** Default: Off



On

In Ada, the in and out parameters of a procedure must be initialized. With this option, if the software detects one of the parameters as a red NIV, then subsequent code is *not* declared unreachable (the software does not color the code gray). The red error does not affect the verification.

```
procedure test(x : in out Integer) is
begin
  x := 10;
end
procedure main is
  T : integer;
begin
  test(T); -- red NIV on T with or without the option
  T := T + 1; -- green with -continue-with-in-out-niv, gray otherwise
end Main;
```



Off

Verification stops if in and out parameters of a procedure are not initialized.

### Command-Line Information.

**Parameter:** `continue-with-in-out-niv`

### Ignore float rounding

Specify whether to round data type `float` according to the IEEE® 754 standard

**Settings.** Default: Off



On

No rounding. Computation is exact.



Off

Round data type `float` according to IEEE 754 standard: simple precision on 32-bit targets and double precision on targets that define `double` as 64-bit.



**Command-Line Information.**

**Parameter:** ignore-float-rounding

**Shell script example:** polyspace-ada -ignore-float-rounding

**See Also.** “Float Rounding” in PolySpace Products for Ada documentation

**Procedures known to cause NTC**

Filter known non-terminating calls (NTC) to functions

**Settings. Default:** Empty. All NTCs appear as red errors.

- There can be functions that "never terminate". Some functions, such as tasks and threads, contain infinite loops by design, while functions that halt the program, such as `kill_task`, `exit`, or `Terminate_Thread` are often stubbed by an infinite loop. If there are many of these functions, or you want to present results to a third party, you may want to filter certain types of NTCs in the Viewer. Specify these NTCs before a verification. They appear in the Viewer within the known-NTC category.

**Command-Line Information.**

**Parameter:** known-NTC

**Type:** string

**Value:** any valid value, for example, "kill\_task,exit",

**Default:** Empty

**Shell script examples:**

```
polyspace-ada -known-NTC "kill_task,exit"  
polyspace-ada -known-NTC "Exit,Terminate_Thread"
```

**See Also.** “Preparing Multitasking Code” in PolySpace Products for Ada documentation

## Run verification in 32 or 64-bit mode

Specify whether verification runs in 32-bit or 64-bit mode

### Settings

**Default:** auto

auto

Verification runs in 32-bit mode.

32

Verification runs in 32-bit mode.

64

Verification runs in 64-bit mode. Use this option only if 32-bit verification fails due to insufficient memory.

### Command-Line Information

**Parameter:** machine-architecture

**Type:** string

**Value:** auto | 32 | 64

**Default:** auto

**Shell script example:** polyspace-ada -machine-architecture auto

### Other options

Specify extra PolySpace options

### Settings

**Default:** None

- Add expert option flags to verification. Place the option `-extra-flags` before each flag (parameter or value), for example:

```
-extra-flags -param1 -extra-flags -param2 -extra-flags 10
```

and

```
-ada95-extra-flags -param1 -ada95-extra-flags -param2
```

- PolySpace supplies these flags, which depend on your verification requirements.
- Use `ada95-extra-flags` for Ada95 only.

### **Command-Line Information**

**Parameter:** `extra-flags` | `ada95-extra-flags`

**Value:** Supplied by PolySpace but depend on your requirements

**Default:** None

### **See Also**

“Preparing Source Code for Verification” in PolySpace Products for Ada documentation

## Precision Options

<b>In this section...</b>
“Launch code verification from beginning of” on page 1-39
“To end of” on page 1-41
“Precision Level” on page 1-43
“Specific Precision” on page 1-45
“Max size of global array variables” on page 1-46
“Improve precision of interprocedural analysis” on page 1-47
“List of variables to expand” on page 1-49
“Expansion limit for a structured variable” on page 1-50

## Launch code verification from beginning of

Specify starting point of verification

### Settings

- Use with the `to` option.
- Use only on a verification that you have run partially, to specify the restart point of the verification. For example, if you have previously run a verification to `Software Safety Analysis level 1 (pass1)`, you can restart the verification at this point. You do not have to run the verification from scratch.
- Use only for client-based verification (server-based verification always starts from scratch).
- Use only for restarting a verification launched with the option `keep-all-files` (unless you restart from scratch).
- You cannot use this option if you modify the source code between verifications.

**Default:** `scratch`

`scratch`

The starting point for a new verification

`Source Compliance Checking`

Corresponds to the command-line option `compile`

`Control and Data Flow Analysis`

Corresponds to the command-line option `pass0` or `CDFA`

`Software Safety Analysis level 1`

Corresponds to the command-line option `pass1`

`Software Safety Analysis level 2`

Corresponds to the command-line option `pass2`

`Software Safety Analysis level 3`

Corresponds to the command-line option `pass3`

`Software Safety Analysis level 4`

Corresponds to the command-line option `pass4`

Other

For levels greater than pass4 but less than pass20

### **Command-Line Information**

**Parameter:** from

**Type:** string

**Value:** scratch | compile | pass0 | pass1 | pass2 | pass3 | pass4  
| other

**Default:** scratch

**Shell script example:** polyspace-ada -from pass0

### **See Also**

“Reducing Orange Checks in Your Results” in PolySpace Products for Ada documentation

## To end of

Specify the end point of verification

### Settings

- Use with the `from` option.
- Specifies the point at which the verification ends.
- Allows you to have a higher selectivity to find more bugs within the code. A higher integration level contributes to a higher selectivity rate. However, a higher integration level also leads to a longer verification time

**Default:** Software Safety Analysis level 4

Source Compliance Checking

Corresponds to the command-line option `compile`

Control and Data Flow Analysis

Corresponds to the command-line option `pass0` or `CDFA`

Software Safety Analysis level 1

Corresponds to the command-line option `pass1`

Software Safety Analysis level 2

Corresponds to the command-line option `pass2`

Software Safety Analysis level 3

Corresponds to the command-line option `pass3`

Software Safety Analysis level 4

Corresponds to the command-line option `pass4`

Other

The verification continues until you halt it manually (through `kill-rte-kernel`) or it reaches `pass20`.

## **Command-Line Information**

**Parameter:** to

**Type:** string

**Value:** compile | pass0 | pass1 | pass2 | pass3 | pass4 | other

**Default:** pass4

pass4

### **Shell script examples:**

```
polyspace-ada -to "Software Safety Analysis level 3"
```

```
polyspace-ada -to pass0
```

## **See Also**

“Reducing Orange Checks in Your Results” in PolySpace Products for Ada documentation



## Precision Level

Specify precision level used in verification

### Settings

The precision level determines the algorithm used to model the program state space during verification. A higher precision level contributes to a higher selectivity rate, which makes reviewing results more efficient and isolating bugs easier. However, a higher precision level also results in a longer verification time.

**Default:** 2

0

Static interval verification. MathWorks™ recommends that you begin verification at this level. Once you have addressed red errors and gray code from a verification at this level, you can relaunch the verification with a higher precision level.

1

Complex polyhedron model of domain values

2

Complex algorithms that closely model domain values (a mixed approach with integer lattices and complex polyhedrons)

3

Suitable for code that is less than 1000 lines long. For such code, the selectivity can be very high, for example, 98%. This high selectivity results in a very long verification time, for example, an hour for 1000 lines of code.

### Command-Line Information

**Parameter:** 0

**Value:** 0 | 1 | 2 | 3

**Default:** 2

**Shell script example:** polyspace-ada -01

**See Also**

“Reducing Orange Checks in Your Results” in PolySpace Products for Ada documentation

## Specific Precision

Specify Ada packages to verify with a different precision from the general precision level (defined by the 0 option)

### Settings

**Default** Verify all packages or modules with the same precision

To apply different precision levels to Ada packages in the Specific Precision dialog box:

- Under **Ada Package name**, specify the name of package or module.
- Under **Precision**, specify the required level: 0, 1, 2, or 3

### Command-Line Information

**Parameter:** modules-precision

**Type:** string

**Value:** *package\_name1:0(precision1),  
package\_name2:0(precision2), package\_name3:0(precision3) ...  
package\_nameN:0(precisionN)*

**Shell script example:** polyspace-ada -01 -modules-precision  
myMath:02,myText:01

### See Also

“Reducing Orange Checks in Your Results” in PolySpace Products for Ada documentation

## **Max size of global array variables**

Force PolySpace software to verify each cell of global variable arrays as a separate variable, if length is less than or equal to threshold value

### **Settings**

**Default:** 3

- Threshold value.
- Increasing the number of global variables to verify affects verification time.
- Affects only Global Data Dictionary results.

### **Command-Line Information**

**Parameter:** array-expansion-size

**Value:** any valid value

**Default:** 3

**Shell script example:** polyspace-ada -01 -array-expansion-size 8

### **See Also**

“Expansion of Sizes” in PolySpace Products for Ada documentation

## Improve precision of interprocedural analysis

Improve inter-procedural verification precision within a pass

### Settings

The propagation of information within procedures happens earlier than usual with this option, which results in improved selectivity but a longer verification time.

Consider two cases, one where you set this option (`-path-sensitivity-delta`) to 1, and another where you do not set this option, that is, the option value is 0.

- A level 1 verification with this option set provides results equivalent to a level 1 or 2 verification without the option.
- A level 1 verification with this option set can be many times longer than a cumulative level 1 and 2 verification without the option.

The same effect and results apply to a level 2 verification with this option set. A level 2 verification is equivalent to a level 3 or 4 verification without the option. Verification time also increases correspondingly.

Using this option results in the following:

- The highest selectivity is achieved in level 2, so you do not need to wait until level 4.
- Verification time can increase exponentially and result in an even longer verification time than that for the cumulative level 1, 2, 3, and 4 verification.

Use this option only for packages with fewer than 1000 lines of code.

**Default:** 0

### Command-Line Information

**Parameter:** `path-sensitivity-delta`

**Value:** any valid value

**Default:** 0

**Shell script example:** `polyspace-ada -path-sensitivity-delta 1`

**See Also**

“Expansion of Sizes” in PolySpace Products for Ada documentation

## List of variables to expand

Specify aggregate variables to split into independent variables during verification

### Settings

**Default** Do not split aggregate variables into independent variables

- Use together with `-variable-expansion-depth` option.
- Affects the Global Data Dictionary results.

### Command-Line Information

**Parameter:** `variables-to-expand`

**Type:** string

**Value:** list of aggregate variables, for example, `var1, var2,`

### Shell script example:

```
polyspace-ada -variables-to-expand pkg.rec1,pkg2.recF \
  -variable-expansion-depth 4
```

### See Also

“Expansion of Sizes” in PolySpace Products for Ada documentation

## Expansion limit for a structured variable

Specify maximum depth for expansion of variables

### Settings

In the following code:

```
Package foo is
  Type Internal is
    Record
      FieldI : Integer;
      FieldII : Integer;
    End Record ;
  Type External is
    Record
      Data : Internal ;
      FieldE : Integer;
    End Record ;
  myVar : External ;
End foo;
```

the effects of using different expansion depths are:

- `-variable-expansion-depth 1` — The concurrent access verification is done on `foo.myVar.FieldE` and `foo.myVar.Data`. If each access on `Data` is protected by critical section but `FieldE` is not protected, then `Data` is flagged as protected (a green entry in the Global Data Dictionary) and `FieldE` is flagged as not protected (an orange entry).
- `-variable-expansion-depth 2` — The verification is done on `foo.myVar.FieldE`, `foo.myVar.Data.FieldI` and `foo.myVar.Data.FieldII`. Each variable is flagged independently.  
  
`foo.myVar` is flagged as shared if any of its fields are shared. It is flagged as non-protected if any of its fields are not protected.

### No Default:

- Use with `-variables-to-expand` option
- Increasing the number of global variables to verify extends verification time.



- This option affects only the Global Data Dictionary results.

### **Command-Line Information**

**Parameter:** variable-expansion-depth

**Value:** any valid value, for example, 1, 2

### **Shell script example:**

```
polyspace-ada -variables-to-expand package_foo.myVar -variable-expansion-depth 1
```

### **See Also**

“Expansion of Sizes” in PolySpace Products for Ada documentation

## Multitasking Options (PolySpace Server Only)

In this section...
“Implicit Tasks” on page 1-52
“Critical section details” on page 1-53
“Temporal exclusion tasks (separated by space characters)” on page 1-54

---

**Note** Concurrency options are not compatible with the `main-generator` option.

---

### Implicit Tasks

Specify tasks/entry points to verify

#### Settings

##### No Default

- The entry points must not take parameters. If the task entry points are functions with parameters, encapsulate the entry points in functions with no parameters and pass the parameters through global variables.
- If you declare tasks with the Ada keyword `task`, the software takes the tasks into account automatically.

#### Command-Line Information

**Parameter:** `entry-points`

**Type:** `string`

**Value:** any valid name, for example, `str1`, `str2`, `str3`

**Shell script example:** `polyspace-ada -entry-points pack1.proc1, pack2.proc2, pack3.proc3`

#### See Also

“Preparing Multitasking Code” in PolySpace Products for Ada documentation

## Critical section details

Specify critical sections in procedures

### Settings

You can use critical sections to model, for example, protection of shared resources or interruption enabling and disabling.

**Default** No critical sections

- The options `critical-section-begin` and `critical-section-end` use lists to specify the procedures that begin and end critical sections.
- A list holds pairs of values. Each pair contains a procedure name along with the name of the critical section, for example, `"package1.proc1:cs1,package2.proc2:cs2"`. Do not put spaces in a list.

### Command-Line Information

**Parameter:** `critical-section-begin`

**Type:** string

**Value:** any valid list, for example, `"package1.proc1:cs1,package2.proc2:cs2"`

**Parameter:** `critical-section-end`

**Type:** string

**Value:** any valid list, for example, `"proc3:cs1,proc4:cs2"`

### Shell script example:

```
polyspace-ada -critical-section-begin "start_my_semaphore:cs" \  
-critical-section-end "end_my_semaphore:cs"
```

### See Also

“Preparing Multitasking Code” in PolySpace Products for Ada documentation

## Temporal exclusion tasks (separated by space characters)

Specify file that lists sets of temporally exclusive tasks (tasks that never execute at the same time)

### Settings

**Default** No temporally exclusive tasks

Format of file:

- Use one line for each group of temporally exclusive tasks
- On each line, use spaces to separate tasks

For example, the file `exclusions` in the `sources` folder contains the following lines:

- `task1_group1 task2_group1`
- `task1_group2 task2_group2 task3_group2`

### Command-Line Information

**Parameter:** `temporal-exclusions-file`

**Type:** `string`

**Value:** any valid file name, including path, for example,

```
sources/exclusions -entry-points task1_group1,task2_group1,task1_group2
```

### Shell script example:

```
polyspace-ada -temporal-exclusions-file sources/exclusions \  
-entry-points task1_group1,task2_group1,task1_group2,\  
task2_group2,task3_group2
```

### See Also

“Preparing Multitasking Code” in PolySpace Products for Ada documentation

## Batch Options

### In this section...

“-server server\_name\_or\_ip[:port\_number]” on page 1-55

“-h[elp]” on page 1-55

“-v | -version” on page 1-56

“-sources-list-file file\_name” on page 1-56

### **-server server\_name\_or\_ip[:port\_number]**

Using `polyspace-remote[-desktop]-[ada] [server [name or IP address][[:port number]]]` allows you to send a verification to a specific or referenced PolySpace server.

---

**Note** If you do not specify the option `server`, the default server referenced in the `PolySpace-Launcher.prf` configuration file is used as the server.

---

When you use the `server` option in the batch launching command, you must specify the name or IP address and a port number. If the port number does not exist, the 12427 value is used as the default.

`polyspace-remote-` accepts all other options.

#### **Option Example Shell Script Entry:**

```
polyspace-remote-desktop-ada server 192.168.1.124:12400
```

```
polyspace-remote-ada
```

```
polyspace-remote-ada server Bergeron
```

### **-h[elp]**

Displays simple help in the shell window that provides information on all options.

**Example Shell Script Entry:**

```
polyspace-ada h
```

**-v | -version**

Displays the PolySpace version number.

**Example Shell Script Entry:**

```
polyspace-ada v
```

produces an output like the following:

```
PolySpace r2008b
```

```
Copyright (c) 1999-2008 The Mathworks, Inc.
```

**-sources-list-file file\_name**

This option is available only in batch mode.

*file\_name* specifies:

- The name of one file
- The absolute or relative path of the file

**Example Shell Script Entry for -sources-list-file:**

```
polyspace-ada -sources-list-file "C:\Analysis\files.txt"
```

```
polyspace-ada -sources-list-file "files.txt"
```

# Check Descriptions

---

## Colored Source Code for Ada

**In this section...**

“Non-Initialized Variable: NIV/NIVL” on page 2-3

“Division by Zero: ZDV” on page 2-7

“Arithmetic Exceptions: EXCP” on page 2-8

“Scalar and Float Underflow/Overflow : UOVFL” on page 2-11

“Scalar and Float Overflow: OVFL” on page 2-12

“Scalar and Float Underflow: UNFL” on page 2-13

“Attributes Check: COR” on page 2-15

“Array Length Check: COR” on page 2-17

“DIGITS Value Check: COR” on page 2-19

“DELTA Value Length Check: COR” on page 2-20

“Static Range and Values Check: COR” on page 2-21

“Discriminant Check: COR” on page 2-23

“Component Check: COR” on page 2-24

“Dimension Versus Definition Check: COR” on page 2-25

“Aggregate Versus Definition Check: COR” on page 2-26

“Aggregate Array Length Check: COR” on page 2-28

“Sub-Aggregates Dimension Check: COR” on page 2-29

“Characters Check: COR” on page 2-30

“Accessibility Level on Access Type: COR” on page 2-32

“Explicit Dereference of a Null Pointer: COR” on page 2-33

“Accessibility of a Tagged Type: COR” on page 2-34

“Power Arithmetic: POW” on page 2-36

“User Assertion: ASRT” on page 2-37

“Non Terminations: Calls and Loops” on page 2-39

“Unreachable Code: UNR” on page 2-49



**In this section...**

“Value on Assignment: VOA” on page 2-51

“Inspection Points: IPT” on page 2-53

**Non-Initialized Variable: NIV/NIVL**

Check to establish whether a variable is initialized before being read.

**Examples****Ada Example.**

```

1  package NIV is
2    type Pixel is
3      record
4        X : Integer;
5        Y : Integer;
6      end record;
7    procedure MAIN;
8    function Random_Bool return Boolean;
9  end NIV;
10
11 package body NIV is
12
13   type TwentyFloat is array (Integer range 1.. 20) of Float;
14
15   procedure AddPixelValue(Vpixel : Pixel) is
16     Z : Integer;
17   begin
18     if (Vpixel.X < 3) then
19       Z := Vpixel.Y + Vpixel.X; -- NIV error: Y field
20 not initialized
21     end if;
22   end AddPixelValue;
23
24   procedure MAIN is
25     B : Twentyfloat;
26     Vpixel : Pixel;

```

```
27  begin
28  if (Random_Bool) then
29  Vpixel.X := 1;
30  AddPixelValue(Vpixel); -- NTC Error: because of NIV error
31  in call
32  end if;
33
34  for I in 2 .. Twentyfloat'Last loop
35  if ((I mod 2) = 0) then
36  B(I) := 0.0;
37  end if;
38  end loop;
39  B(2) := B(4) + B(5); -- NIV Warning because
40 B(odd) not initialized
41  end MAIN;
42
43  end NIV;
```

**Explanation.** The result of the addition is unknown at line 19 because *Vpixel.Y* is not initialized (gray code on "+" operator). In addition, line 37 shows how PolySpace prompts the user to investigate further (orange NIV warning on *B(I)*) when all fields have not been initialized.

**NIV Check vs. IN OUT Parameter Mode.** Standard Ada83 says: For a scalar parameter, the above effects are achieved by copy: at the start of each call, if the mode is in or in out, the value of the actual parameter is copied into the associated formal parameter; then after normal completion of the subprogram body, if the mode is in out or out, the value of the formal parameter is copied back into the associated actual parameter.

Clearly, in out parameters necessitate initialization before call.

### Ada Example.

```
1  package NIVIO is
2  procedure MAIN;
3  function Random_Boolean return Boolean;
4  end NIVIO;
5
6  package body NIVIO is
```

```

7
8  Y : Integer := 3;
9  procedure Niv_Not_Dangerous(X : in out integer) is
10 begin
11   X := 2;
12   if (Y > 2) then
13     Y := X + 3;
14   end if ;
15 end Niv_Not_Dangerous;
16
17 procedure Niv_Dangerous(X : in out integer) is
18 begin
19   if (Y /= 3) then
20     Y := X + 3;
21   end if ;
22 end Niv_Dangerous;
23
24 procedure MAIN is
25   X : Integer;
26 begin
27   if (Random_Boolean) then
28     Niv_Dangerous(X); -- NIV ERROR: certainly dangerous
29   end if ;
30   if (Random_Boolean) then
31     Niv_Not_dangerous(X); -- NIV ERROR: not dangerous
32   End if ;
33 end MAIN;
34
35 end NIVIO;

```

**Explanation.** In the previous example, as shown at line 28, PolySpace highlights a dangerous non-initialized variable. Even if it is not dangerous, as shown in the *Niv\_Not\_Dangerous* procedure, PolySpace also highlights the non-initialized variable at line 30. To be more permissive with standard, the **-continue-with-in-out-niv** option permits to continuation of the verification for the rest of the sources even if a red error stays in place at lines 28 and 31.

### Pragma Interface/Import

The following table illustrates how variables are regarded when:

- A pragma is used to interface the code;
- An address clause is applied;
- A pointer type is declared.

	<b>Records and Other Variable Types</b>	<b>Integer Variable Types</b>	<b>Function</b>
<pre>pragma interface (C, variable_name) pragma import (C, variable_name)</pre>	<ul style="list-style-type: none"> <li>• green NIV</li> <li>• Permanent random value</li> </ul>	<ul style="list-style-type: none"> <li>• No NIV check</li> <li>• Permanent random value</li> </ul>	<ul style="list-style-type: none"> <li>• same behavior as - automatic-stubbing</li> <li>• in/out and out variables are written within their entire type range</li> </ul>

In this case, a permanent random value means that the variable is always equivalent to the full range of its type. It is almost equivalent to a volatile variable except for the color of the NIV.

### **Type Access Variables**

The following table illustrates how variables are verified by PolySpace when a type access is used:

	<b>Records and Other Variable Types</b>	<b>Integer Variable Types</b>
<pre>Type a_new_type is access another_type;</pre>	<ul style="list-style-type: none"> <li>• orange NIV</li> <li>• Permanent random value</li> </ul>	<ul style="list-style-type: none"> <li>• No NIV check</li> <li>• Permanent random value</li> </ul>

In this case, a Permanent Random Variable is exactly equivalent to a volatile variable - that is, it is assumed that the value can have been changed to anywhere within its whole range between one read access and the next.

## Address Clauses

The following table illustrates how variables are regarded by PolySpace where an address clause is used.

Address Clause	Records and Other Variable Types	Integer Variable Types
<pre>for variable_name'address use 16#1234abcd#; for variable_name'other'address use;</pre>	<ul style="list-style-type: none"> <li>• orange NIV</li> <li>• Permanent random value</li> </ul>	<ul style="list-style-type: none"> <li>• No NIV check</li> <li>• Permanent random value</li> </ul>

In this case, a Permanent Random Variable is exactly equivalent to a pvolatile variable - that is, it is assumed that the value can have been changed to anything within its whole range between one read access and the next.

## Division by Zero: ZDV

Check to establish whether the right operand of a division (denominator) is different to 0[.0].

### Ada Example:

```

1  package ZDV is
2    function Random_Bool return Boolean;
3    procedure ZDVS (X : Integer);
4    procedure ZDVF (Z : Float);
5    procedure MAIN;
6  end ZDV;
7
8  package body ZDV is
9
10   procedure ZDVS(X : Integer) is
11     I : Integer;
12     J : Integer := 1;
13   begin
14     I := 1024 / (J-X); -- ZDV ERROR: Scalar Division by Zero
15   end ZDVS;
```

```
16
17 procedure ZDVF(Z : Float) is
18   I : Float;
19   J : Float := 1.0;
20 begin
21   I := 1024.0 / (J-Z); -- ZDV ERROR: float Division by Zero
22 end ZDVF;
23
24 procedure MAIN is
25 begin
26   if (random_bool) then
27     ZDVS(1); -- NTC ERROR: ZDV.ZDVS call never terminates
28   end if ;
29   if (Random_Bool) then
30     ZDVF(1.0); -- NTC ERROR: ZDV.ZDVF call never terminates
31   end if;
32 end MAIN;
33
34 end ZDV;
35
36
37
```

### Arithmetic Exceptions: EXCP

Check to establish whether standard arithmetic functions are used with good arguments:

- Argument of *sqrt* must be positive
- Argument of *tan* must be different from  $\pi/2$  modulo  $\pi$
- Argument of *log* must be strictly positive
- Argument of *acos* and *asin* must be within  $[-1..1]$
- Argument of *exp* must be less than or equal to a specific value which depends on the processor target: 709 for 64/32 bit targets and 88 for 16 bit targets

Basically, an error occurs if an input argument is outside the domain over which the mathematical function is defined.

## Ada Example

```
1
2 With Ada.Numerics; Use Ada.Numerics;
3 With Ada.Numerics.Aux; Use Ada.Numerics.Aux;
4
5 package EXCP is
6   function Bool_Random return Boolean;
7   procedure MAIN;
8 end EXCP;
9
10 package body EXCP is
11
12 -- implementation dependant in Ada.Numerics.Aux: subtype
Double is Long_Float;
13   M_PI_2 : constant Double := Pi/2.0; -- pi/2
14
15   procedure MAIN is
16     IRes, ILeft, IRight : Integer;
17     Db1_Random : Double;
18     pragma Volatile_ada.htm (dbl_Random);
19
20     SP : Double := Db1_Random;
21     P : Double := Db1_Random;
22     SN : Double := Db1_Random;
23     N : Double := Db1_Random;
24     NO_TRIG_VAL : Double := Db1_Random;
25     res : Double;
26     Fres : Long_Float;
27   begin
28     -- assert is used to redefine range values of a variable.
29     pragma assert(SP > 0.0);
30     pragma assert(P >= 0.0);
31     pragma assert(SN < 0.0);
32     pragma assert(N <= 0.0);
33     pragma assert(NO_TRIG_VAL < -1.0 or NO_TRIG_VAL > 1.0);
34
35     if (bool_random) then
36       res := sqrt(sn); -- EXCP ERROR: argument of SQRT must be
positive.
```

```
37  end if ;
38  if (bool_random) then
39    res := tan(M_PI_2);
        -- EXCP Warning: Float argument of TAN
40        -- may be different than pi/2 modulo pi.
41  end if;
42  if (bool_random) then
43    res := asin(no_trig_val); --EXCP ERROR: float argument of
ASIN is not in -1..1
44  end if;
45  if (bool_random) then
46    res := acos(no_trig_val); --EXCP ERROR: float argument of
ACOS is not in -1..1
47  end if;
48  if (bool_random) then
49    res := log(n); -- EXCP ERROR: float argument of LOG is not
strictly positive
50  end if;
51  if (bool_random) then
52    res := exp(710.0); -- EXCP ERROR: float argument of EXP
is not less than or equal to 709 or 88
53  end if;
54
55  -- range results on trigonometric functions
56  if (Bool_Random) then
57    Res := Sin (dbl_random); -- -1 <= Res <= 1
58    Res := Cos (dbl_random); -- -1 <= Res <= 1
59    Res := atan(dbl_random); -- -pi/2 <= Res <= pi/2
60  end if;
61
62  -- Arithmetic functions where there is no check currently
implemented
63  if (Bool_Random) then
64    Res := cosh(dbl_random);
65    Res := tanh(dbl_random);
66  end if;
67  end MAIN;
68  end EXCP;
```



## Explanation

The arithmetic functions *sqrt*, *tan*, *sin*, *cos*, *asin*, *acos*, *atan* and *log* are derived directly from mathematical definitions of functions.

Standard *cosh* and *tanh* hyperbolic functions are currently assumed to return the full range of values mathematically possible, regardless of the input parameters. The Ada83 standard gives more details about domain and range error for each maths function.

## Scalar and Float Underflow/Overflow : UOVFL

Check to simultaneously establish whether an arithmetic expression on a float value overflows and/or underflows.

### Ada Example

```

1  package UOVFL is
2    function Bool_Random return Boolean;
3    procedure MAIN;
4  end UOVFL;
5
6  package body UOVFL is
7
8    procedure MAIN is
9      I : Integer;
10     DValue : Long_float;
11   begin
12     if (Bool_Random) then
13       I := 2**30;
14       I := 2 * (I - 1); --integer UOVFL verified on "*" and "-"
15     end if;
16     if (Bool_Random) then
17       DValue := Long_float(Float'Last);
18       DValue := 2.0 * DValue + 1.0; --float UOVFL verified on "*"
and "+"
19     end if;
20   end MAIN;
21 end UOVFL;
```

## Explanation

PolySpace can detect that there is neither an underflow nor an overflow on \* and - operators at lines 16 and 18.

## Scalar and Float Overflow: OVFL

Check to establish whether an arithmetic expression overflows. This is a scalar check with integer types and a float check for floating point expressions.

An overflow is also detected should an array index\_ada.htm be out of bounds.

## Ada Example

```
1  package OVFL is
2    procedure MAIN;
3    function Bool_Random return Boolean;
4  end OVFL;
5
6  package body OVFL is
7
8    procedure OVFL_ARRAY is
9      A : array(1..20) of Float;
10     J : Integer;
11     begin
12       for I in A'First .. A'Last loop
13         A(I) := 0.0 ;
14         J := I + 1;
15       end loop;
16       A(J) := 0.0; -- OVFL ERROR: Overflow array index_ada.htm
17     end OVFL_ARRAY;
18
19     procedure OVFL_ARITHMETIC is
20       I : Integer;
21       FValue : Float;
22     begin
23
24       if (Bool_Random) then
25         I := 2**30;
26         I := 2 * (I - 1) + 2 ; -- OVFL ERROR: 2**31 is an overflow
```

```

value for Integer
27   end if;
28   if (Bool_Random) then
29     FValue := Float'Last;
30     FValue := 2.0 * FValue + 1.0; -- OVFL ERROR: float
variable is overflow
31   end if;
32   end OVFL_ARITHMETIC;
33
34   procedure MAIN is
35   begin
36     if (Bool_Random) then OVFL_ARRAY; end if; -- NTC
propagation because of OVFL ERROR
37     if (Bool_Random) then OVFL_ARITHMETIC; end if;
38   end MAIN;
39
40 end OVFL;
41
42

```

## Explanation

In Ada, the bounds of an array can be considered with reference to a new type or subtype of an existing one. Line 16 shows an overflow error resulting from an attempt to access element 21 in an array subtype of range *1..20*.

A different example is shown by the overflow on line 26, where adding 1 to *Integer'Last* (the maximum integer value being  $2^{*}31-1$  on a 32 bit architecture platform). Similarly, if *OVFL\_ARITHMETIC.FValue* represents the max floating value,  $2*FValue$  cannot be represented with the same type and so raises an overflow at line 30.

## Scalar and Float Underflow: UNFL

Check to establish whether an arithmetic expression underflows. This is a scalar check with integer types and a float check for floating point expressions.

An underflow is also detected should an array index\_ada.htm be out of bounds.

## Ada Example

```
1 package UNFL is
2   function Bool_Random return Boolean;
3   procedure MAIN;
4 end UNFL;
5
6 package body UNFL is
7
8   procedure UNFL_ARRAY is
9     A : array(1..20) of Float;
10    J : Integer;
11    begin
12      for I in A'Last.. A'First loop
13        A(I) := 0.0 ;
14        J := I - 1;
15      end loop;
16      A(J) := 0.0; -- UNFL ERROR: underflow array index_ada.htm
17    end UNFL_ARRAY;
18
19    procedure UNFL_ARITHMETIC is
20      I : Integer;
21      FValue : Float;
22    begin
23
24      if (Bool_Random) then
25        I := -2**31;
26        I := I - 1 ; -- UNFL ERROR: -2**31-1 is integer underflow
27      end if;
28      if (Bool_Random) then
29        FValue := Float'First;
30        FValue := -2.0 * FValue; -- UNFL ERROR: float variable is
overflow
31      end if;
32    end UNFL_ARITHMETIC;
33
34    procedure MAIN is
35    begin
36      if (Bool_Random) then UNFL_ARRAY; end if;
-- NTC propagation because of UNFL ERROR
```

```

37   if (Bool_Random) then UNFL_ARITHMETIC; end if;
38   end MAIN;
39
40 end UNFL;

```

## Explanation

In Ada, the bounds of an array can be considered with reference to a new type or subtype of an existing one. Line 16 shows an underflow error resulting from an attempt to access element 0 in an array subtype of range *1..20*.

A different example is shown by the underflow on line 26, where subtracting 1 from *Integer.First* (the minimum integer value being  $-2^{**31}-1$  on a 32 bit architecture platform). Similarly, if *UNFL\_ARITHMETIC.FValue* represents the minimum floating value,  $-2^{*FValue}$  cannot be represented with the same type and so raises an underflow at line 30.

## Attributes Check: COR

PolySpace encourages the user to investigate the attributes *SUCC*, *PRED*, *VALUE* and *SIZE* further, thanks to a COR check (failure of CORrectness condition).

## Ada Example

```

1
2 package CORS is
3   function Bool_Random return Boolean;
4   procedure MAIN;
5   function INT_VALUE (S : String) return Integer;
6   type PSTCOLORS is (ORANGE, RED, GREY, GREEN);
7   type ADCFUZZY is (LOW, MEDIUM, HIGH);
8 end CORS;
9
10 package body CORS is
11
12   type STR_ENUM is (AA,BB);
13
14   function INT_VALUE (S : String) return Integer is
15     X : Integer;

```

```
16  begin
17  X := Integer'Value (S); -- COR Warning: Value parameter
might not be in range integer
18  return X;
19  end INT_VALUE;
20
21  procedure MAIN is
22  E : PSTCOLORS := GREEN;
23  F : PSTCOLORS;
24  ADCVAL : ADCFUZZY := ADCFUZZY'First;
25  StrVal : STR_ENUM;
26  X : Integer;
27  begin
28  if (Bool_Random) then
29  F := PSTCOLORS'PRED(E); -- COR Verified: Pred attribute
is not used on the first element of pstcolors
30  E := PSTCOLORS'SUCC(E); -- COR ERROR: Succ attribute is
used on the last element of pstcolors
31  end if;
32  if (Bool_Random) then
33  ADCVAL := ADCFUZZY'PRED(ADCVAL); -- COR ERROR: Pred
attribute is used on the first element of adcfuzzy
34  end if ;
35
36  StrVal := STR_ENUM'Value ("AA"); -- COR Warning: Value
parameter might not be in range str_enum
37  StrVal := STR_ENUM'Value ("AC"); -- COR Warning: Value
parameter might not be in range str_enum
38  X := INT_VALUE ("123"); --X info: -2**31<=[expr]<=2**31-1
39  end MAIN;
40  end CORS;
41
```

### Explanation

At line 36 and 37, the COR warning (orange) prompts the user to check whether the *VALUE* attribute is correct or not.

In fact, standard ADA generates a "CONSTRAINT\_ERROR" exception when the string does not correspond to one of the possible values of the type.

Also note that in this case, PolySpace results assume the full possible range of the returned type, regardless of the input parameters. In this example, *strVal* has a range in  $[aa,bb]$  and *X* in  $[Integer'First, Integer'Last]$ .

The incorrect use of *PRED* and *SUCC* attributes on type is indicated by PolySpace.

### SIZE Attribute Error: COR

```

1
2 with Ada.Text_IO; use Ada.Text_IO;
3
4 package SIZE is
5   PROCEDURE Main;
6 end SIZE;
7
8 PACKAGE BODY SIZE IS
9
10  TYPE unSTab is array (Integer range <>) of Integer;
11
12  PROCEDURE MAIN is
13    X : Integer;
14  BEGIN
15    X := unSTab'Size; -- COR ERROR: Size attribute must not be
16    Put_Line (Integer'Image (X));
17  END MAIN;
18
19 END SIZE;
```

### Explanation

At line 15, PolySpace shows the error on the *SIZE* attribute. In this case, it cannot be used on an unconstrained array.

### Array Length Check: COR

Checks the correctness condition of an array length, including *Strings*.

## Ada Example

```
1
2 with Dname;
3 package CORL is
4   function Bool_Random return Boolean;
5   type Name_Type is array (1 .. 6) of Character;
6   procedure Put (C : Character);
7   procedure Put (S : String);
8   procedure MAIN;
9 end CORL;
10
11 package body CORL is
12
13   STR_CST : constant NAME_TYPE := "String";
14
15   procedure MAIN is
16     Str1,Str2,Str3 : String(1..6);
17     Arr1 : array(1..10) of Integer;
18   begin
19
20     if (Bool_Random) then
21       Str1 := "abcdefg"; -- COR ERROR: Too many elements in
array must have 6
22     end if;
23     if (Bool_Random) then
24       Arr1 := (1,2,3,4,5,6,7,8,9); -- COR ERROR: Not enough
elements in array, must have 10
25     end if ;
26     if (Bool_Random) then
27       Str1 := "abcdef";
28       Str2 := "ghijkl";
29       Str3 := Str1 & Str2; -- COR Warning: Length might not be
compatible with 1 .. 6
30       Put(Str3);
31       if Bool_Random then
32         DName.DISPLAY_NAME (DNAME.NAME_TYPE(STR_CST));
33         -- COR ERROR: String Length is not correct, must be 4
34       end if;
35     end if ;
```



```
35   end MAIN;
36
37   end CORL;
38
39   package DName is
40     type Name_Type is array (1 .. 4) of Character;
41     PROCEDURE DISPLAY_NAME (Str : Name_Type);
42   end DName;
43
```

## Explanation

At lines 21 and 24, PolySpace gives the exact value needed to match the two arrays. On the other hand, PolySpace prompts the user to investigate the compatibility of concatenated arrays, by means of an **orange** check at line 29.

Moreover at line 32, the string length is being put forward even if it depends on another package.

## DIGITS Value Check: COR

Checks the length of *DIGITS* constructions.

## Ada Example

```
1   package DIGIT is
2     procedure MAIN;
3   end DIGIT;
4
5   package body DIGIT is -- NTC ERROR: COR propagation
6
7     type T is digits 4 range 0.0 .. 100.0;
8     subtype T1 is T
9       digits 1000 range 0.0 .. 100.0; -- COR ERROR: digits value
is too large, highest possible value is 4
10
11    procedure MAIN is
12      begin
13        null;
14      end MAIN;
```

```
15 end DIGIT;
```

### Explanation

At line 9, PolySpace shows an error on the *digits* value. It indicates in its associated message the highest available value, 4 in this case.

### DELTA Value Length Check: COR

Checks the length of *DELTA* constructions.

### Ada Example

```
1
2 package FIXED is
3   procedure MAIN;
4   procedure FAILED(STR : STRING);
5   function Random return Boolean;
6 end FIXED;
7
8 package body FIXED is
9
10  PROCEDURE FIXED_DELTA IS
11
12    GENERIC
13      TYPE FIX IS DELTA <>;
14    PROCEDURE PROC (STR : STRING);
15
16    PROCEDURE PROC (STR : STRING) IS
17      SUBTYPE SFIX IS FIX DELTA 0.1 RANGE -1.0 .. 1.0; -- COR
18      ERROR: delta is too small, smallest possible value is 0.5E0
19    BEGIN
20      FAILED ( "NO EXCEPTION RAISED FOR " & STR );
21    END PROC;
22  BEGIN
23
24    IF RANDOM THEN
25      DECLARE
26        TYPE NFIX IS DELTA 0.5 RANGE -2.0 .. 2.0;
```

```

27     PROCEDURE NPROC IS NEW PROC (NFIX);
28     BEGIN
29         NPROC ( "INCOMPATIBLE DELTA" ); --NTC ERROR: propagation
of COR Error
30     END;
31     END IF ;
32
33     END FIXED_DELTA;
34
35     procedure MAIN is
36     begin
37         FIXED_DELTA;
38     end MAIN;
39
40 end FIXED;

```

## Explanation

At line 17, PolySpace Server shows an error on the *DELTA* value. The message gives the smallest available value, *0.5* in this case.

## Static Range and Values Check: COR

Checks if constant values and variable values correspond to their range definition and construction.

## Ada Example

```

1
2 package SRANGE is
3   procedure Main;
4   function IsNatural return Boolean;
5
6   SUBTYPE INT IS INTEGER RANGE 1 .. 3;
7   TYPE INF_ARRAY IS ARRAY(INT RANGE <>, INT RANGE <>) OF INTEGER;
8   SUBTYPE DINT IS INTEGER RANGE 0 .. 10;
9 end SRANGE;
10
11 package body SRANGE is
12

```

```
13  TYPE SENSOR IS NEW INTEGER RANGE 0 .. 10;
14
15  TYPE REC2(D : DINT := 1) IS RECORD -- COR Warning: Value
might not be in range
1 .. 3
16  U : INF_ARRAY(1 .. D, D .. 3) := (1 .. D =>
17      (D .. 3 => 1));
18  END RECORD;
19  TYPE REC3(D : DINT := 1) IS RECORD -- COR Error: Value is
not in range 1 .. 3
20  U : INF_ARRAY(1 .. D, D .. 3) := (1 .. D =>
21      (D .. 3 => 1));
22  END RECORD;
23
24  PROCEDURE VALUE_RANGE is
25  VAL : INTEGER;
26  pragma Volatile(VAL);
27  SLICE_A2 : REC2(VAL); -- NIV and COR warning: Value might
not be in range 0 ..
28  SLICE_A3 : REC3(4); -- Unreacheable code: because of COR
Error in REC3
29  BEGIN
30  NULL;
31  END VALUE_RANGE;
32
33  PROCEDURE MAIN is
34  Digval : Sensor;
35  begin
36  if IsNatural then
37  declare
38  TYPE Sub_sensor is new Natural range -1 .. 5; -- COR
Error: Static value is not in range of 0 .. 16#7FFF_FFFF#
39  begin
40  null;
41  end;
42  end if;
43  if IsNatural then
44  declare
45  TYPE NEW_ARRAY IS ARRAY (NATURAL RANGE <>) OF INTEGER;
```

```

46     subtype Sub_Sensor is New_Array (Integer RANGE -1 .. 5);
-- COR Error: Static range is not in range 0 .. 16#7FFF_FFFF#
47     begin
48         null;
49     end;
50 end if ;
51 if IsNatural then
52     VALUE_RANGE; -- NTC Error: propagation of the COR error
in VALUE_RANGE
53     else
54     Digval := 11; -- COR Error: Value is not in range of 0..10
55     end if;
56 END Main;
57 end SRANGE;
58
59

```

## Explanation

PolySpace checks the compatibility between range and value. Moreover, it tells in its associated message the expected length.

Example is shown on the record types *REC2* and *REC3*. PolySpace cannot determine the exact value of the volatile variable *VAL* at line 27, because some paths lead to a **safe** definition, others to a **red** one. The results is an **orange** warning at line 15.

At lines 19, 38, 46 and 54 PolySpace displays errors on out of range values.

## Discriminant Check: COR

Checks the usage of a discriminant in a record declaration.

## Ada Example

```

1
2 package DISC is
3     PROCEDURE MAIN;
4
5     TYPE T_Record(A: Integer) is record -- COR Verified: Value

```

```
is in range of 1 .. 16#7FFF_FFFF#
6   Sa: String(1..A);
7   END RECORD;
8   end DISC;
9
10  package body DISC is
11
12    PROCEDURE MAIN is
13    begin
14      declare
15        T_STRING6 : T_RECORD(6) := (6, "abcdef"); --COR Verified:
Discriminant is compatible
16        T_StringOther : T_RECORD(6); -- COR Verified:
Discriminant is compatible
17        T_STRING5 : T_RECORD(5) := (5, "abcde"); -- COR Verified:
Discriminant is compatible
18      begin
19        T_StringOther := T_STRING6; -- COR Verified: Discriminant
is compatible
20        T_string5 := T_Record(T_STRING6); -- COR ERROR:
Discriminant is not compatible
21      end;
22    END Main;
23
24  END DISC;
```

### Explanation

At line 20, PolySpace shows an error while using a discriminant. *T\_String6* discriminant of length 6 cannot match *T\_String5* discriminant of length 5.

### Component Check: COR

Checks whether each component of a record given is being used accurately.

### Ada Example

```
1  package COMP is
2
3  PROCEDURE MAIN;
```

```
4  SUBTYPE DINT IS INTEGER RANGE 0..1;
5  TYPE COMP_RECORD ( D : DINT := 0) is record
6    X : INTEGER;
7    CASE D IS
8      WHEN 0 => ZERO : BOOLEAN;
9      WHEN 1 => UN : INTEGER;
10   END CASE;
11  END RECORD;
12
13  end COMP;
14
15  package body COMP is
16
17    PROCEDURE MAIN is
18      CZERO : COMP_RECORD(0);
19    BEGIN
20      CZERO.X := 0;
21      CZERO.ZERO := FALSE; -- COR Verified: zero is a component
of the variable
22      CZERO.UN := CZERO.X; -- COR ERROR: un is not a component
of the variable
23    END MAIN;
24  END COMP;
25
```

## Explanation

At line 22, PolySpace Server shows an error. According to the declaration of *CZERO* (line 18), *UN* is not a valid field record component of the variable.

## Dimension Versus Definition Check: COR

Checks the compatibility of array dimension in relation to their definition.

## Ada Example

```
1  package DIMDEF is
2    PROCEDURE MAIN;
3    FUNCTION Random RETURN boolean;
4  end DIMDEF;
```

```
5
6 package body DIMDEF is
7
8   SUBTYPE ST IS INTEGER RANGE 4 .. 8;
9   TYPE BASE IS ARRAY(ST RANGE <>, ST RANGE <>) OF INTEGER;
10  SUBTYPE TBASE IS BASE(5 .. 7, 5 .. 7);
11
12  FUNCTION IDENT_INT(VAL : INTEGER) RETURN INTEGER IS
13  BEGIN
14    RETURN VAL;
15  END IDENT_INT;
16
17  PROCEDURE MAIN IS
18    NEWARRAY : TBASE;
19  BEGIN
20    IF RANDOM THEN
21      NEWARRAY := (7 .. IDENT_INT(9) => (5 .. 7 => 4)); --
COR Error: Dimension is not compatible with definition
22    END IF;
23    IF Random THEN
24      NEWARRAY := (5 .. 7 => (IDENT_INT(3) .. 5 => 5)); --
COR Error: Dimension is not compatible with definition
25    END IF;
26  END MAIN;
27
28 END DIMDEF;
```

### Explanation

At lines 21 and 24, PolySpace Server indicates the incorrect dimension of the double array *Newarray* of type *TBASE*.

### Aggregate Versus Definition Check: COR

Checks the correctness condition on aggregate declaration in relation to their definition.

### Ada Example

1



```
2 package AGGDEF is
3   PROCEDURE MAIN;
4   PROCEDURE COMMENT (A: STRING);
5   function RANDOM return BOOLEAN;
6 end AGGDEF;
7
8 package body AGGDEF is
9
10  TYPE REC1 (DISC : INTEGER := 5) IS RECORD
11    NULL;
12  END RECORD;
13
14  TYPE REC2 (DISC : INTEGER) IS RECORD
15    NULL;
16  END RECORD;
17
18  TYPE REC3 is RECORD
19    COMP1 : REC1(6);
20    COMP2 : REC2(6);
21  END RECORD;
22
23  FUNCTION IDENT_INT(VAL : INTEGER) RETURN INTEGER IS
24  BEGIN
25    RETURN VAL;
26  END IDENT_INT;
27
28  PROCEDURE AGGDEF_INIT is -- AGGREGATE INITIALISATION
29    OBJ3 : REC3;
30  BEGIN
31    if random then
32      OBJ3 :=
33        ((DISC => IDENT_INT(7)), (DISC => IDENT_INT(7))); --
COR ERROR: Aggregate is not compatible with definition
34    end if;
35    IF OBJ3 = ((DISC => 7), (DISC => 7)) then -- COR ERROR:
Aggregate is not compatible with definition
36      COMMENT ("PREVENTING DEAD VARIABLE OPTIMIZATION");
37    END IF;
38  END AGGDEF_INIT;
39
```

```
40  PROCEDURE MAIN IS
41  BEGIN
42  AGGDEF_INIT; -- NTC ERROR: propagation of COR ERROR
43  END MAIN;
44  end AGGDEF;
```

### Explanation

At lines 33 and 35, PolySpace indicates the incompatible aggregate declaration on *OBJ3*. The aggregate definition with a discriminant of value 6, is not compatible with a discriminant of value 7.

### Aggregate Array Length Check: COR

Checks the length for array aggregate.

### Ada Example

```
1  package AGGLEN is
2  PROCEDURE MAIN;
3  PROCEDURE COMMENT(A: STRING);
4  end AGGLEN;
5
6  package body AGGLEN is
7
8  SUBTYPE SLENGTH IS INTEGER RANGE 1..5;
9  TYPE SL_ARR IS ARRAY (SLENGTH RANGE <>) OF INTEGER;
10
11  F1_CONS : INTEGER := 2;
12  FUNCTION FUNC1 RETURN INTEGER IS
13  BEGIN
14  F1_CONS := F1_CONS - 1;
15  RETURN F1_CONS;
16  END FUNC1;
17
18
19  TYPE CONSR (DISC : INTEGER := 1) IS
20  RECORD
21  FIELD1 : SL_ARR (FUNC1 .. DISC); -- FUNC1 EVALUATED.
22  END RECORD;
```

```

23
24  PROCEDURE MAIN IS
25
26  BEGIN
27  DECLARE
28    TYPE ACC_CONSR IS ACCESS CONSR;
29    X : ACC_CONSR;
30  BEGIN
31    X := NEW CONSR;
32    BEGIN
33      IF X.ALL /= (3, (5 => 1)) THEN -- COR ERROR: Illegal
Length for array aggregate
34        COMMENT ("IRRELEVANT");
35      END IF;
36    END;
37  END;
38  END MAIN;
39
40  END AGGLEN;

```

### Explanation

At line 33, PolySpace shows an error. The static aggregate length is not compatible with the definition of the component FIELD1 at line 21.

## Sub-Aggregates Dimension Check: COR

Checks the dimension of sub-aggregates.

### Ada Example

```

1
2  package SUBDIM is
3    PROCEDURE MAIN;
4    FUNCTION EQUAL ( A : Integer; B : Integer) return Boolean;
5  end SUBDIM;
6
7  package body SUBDIM is
8
9

```

```
10  TYPE DOUBLE_TABLE IS ARRAY(INTEGER RANGE <>, INTEGER
RANGE <>) OF INTEGER;
11  TYPE CHOICE_INDEX IS (H, I);
12  TYPE CHOICE_CNTR IS ARRAY(CHOICE_INDEX) OF INTEGER;
13
14  CNTR : CHOICE_CNTR := (CHOICE_INDEX => 0);
15
16  FUNCTION CALC (A : CHOICE_INDEX; B : INTEGER)
17    RETURN INTEGER IS
18  BEGIN
19    CNTR(A) := CNTR(A) + 1;
20    RETURN B;
21  END CALC;
22
23  PROCEDURE MAIN IS
24    A1 : DOUBLE_TABLE(1 .. 3, 2 .. 5);
25  BEGIN
26    CNTR := (CHOICE_INDEX => 1);
27    if (EQUAL(CNTR(H),CNTR(I))) then
28      A1 := ( -- COR ERROR: Sub-aggregates do not
have the same dimension
29      1 => (CALC(H,2) .. CALC(I,5) => -4),
30      2 => (CALC(H,3) .. CALC(I,6) => -5),
31      3 => (CALC(H,2) .. CALC(I,5) => -3) );
32    END IF;
33  END MAIN;
34
35  end SUBDIM;
```

### Explanation

At line 28, PolySpace shows an error. One of the sub-aggregates declarations of *A1* is not compatible with its definition. The second sub-aggregates does not respect the dimension defined at line 24.

Sub-aggregates must be singular.

### Characters Check: COR

Checks the construction using the *character* type.

## Ada Example

```
1
2 package CHAR is
3   procedure Main;
4   function Random return Boolean;
5 end CHAR;
6
7
8 package body CHAR is
9
10  type ALL_Char is array (Integer) of Character;
11  TYPE Sub_Character is new Character range 'A' .. 'E';
12  TYPE TabC is array (1 .. 5) of Sub_Character;
13
14  FUNCTION INIT return character is
15    VAR : TabC := "abcdf"; -- COR Error: Character is not in
range 'A' .. 'E'
16  begin
17    return 'A';
18  end;
19
20  procedure MAIN is
21    Var : ALL_Char;
22  BEGIN
23    IF RANDOM THEN
24      Var(1) := Init; --NTC ERROR: propagation of the COR err
25    ELSE
26      Var(Integer) := ""; -- COR ERROR: the 'null' string
literal is not allowed here
27    END IF;
28  END MAIN;
29 END CHAR;
```

## Explanation

At line 15, PolySpace indicates that the assigned array is not within the range of the *Sub\_Character* type. Moreover, any of the character values of *VAR* does not match any value in the range 'A'..'E'.

At line 26, a particular detection is made by PolySpace when the *null string literal* is assigned incorrectly.

## Accessibility Level on Access Type: COR

Checks the accessibility level on an access type. This check is defined in Ada Standard at chapter 3.10.2-29a1. It detects errors when an access pointer refers to a bad reference.

### Ada Example

```
1
2 package CORACCESS is
3   procedure main;
4   function Brand return Boolean;
5 end CORACCESS;
6
7 package body CORACCESS is
8   procedure main is
9
10    type T is new Integer;
11    type A is access all T;
12    Ref : A;
13
14    procedure Proc1(Ptr : access T) is
15    begin
16      Ref := A(Ptr); -- COR Verified: Accessibility level deeper
than that of access type
17    end;
18
19    procedure Proc2(Ptr : access T) is
20    begin
21      Ref := A(Ptr); -- COR ERROR: Accessibility level not
deeper than that of access type
22    end;
23
24    procedure Proc3(Ptr : access T) is
25    begin
26      Ref := A(Ptr); -- COR Warning: Accessibility level might
be deeper than that of access type
```

```

27   end;
28
29   X : aliased T := 1;
30   begin
31   declare
32     Y : aliased T := 2;
33   begin
34     Proc1(X'Access);
35     if BAnd then
36       Proc2(Y'Access); -- NTC ERROR: propagation of error
at line 22
37     elsif BAnd then
38       Proc3(Y'Access); -- NTC ERROR: propagation of error
at line 27
39     end if;
40   end;
41   Proc3(X'Access);
42   end main;
43   end CORACCESS;
44

```

### Explanation

In the example above at line 16: *Ref* is set to *x'access* and *Ref* is defined in same block or in a deeper one. This is authorized.

On the other hand, *y* is not defined in a block deeper or inside the one in which *Ref* is defined. So, at the end of block, *y* does not exist any more and *Ref* is supposed to points to on *y*. It is prohibited and PolySpace checks at lines 21 and 26.

---

**Note** The **warning** at line 26 is due to the combination of a **red** check because of *y'access* at line 38 and a **green** one for *x'access* at line 41.

---

### Explicit Dereference of a Null Pointer: COR

When a pointer is dereferenced, PolySpace checks whether or not it is a null pointer.

## Ada Example

```
1 package CORNULL is
2   procedure main;
3 end CORNULL;
4
5 package body CORNULL is
6   type ptr_type is access all integer;
7   ptr : ptr_type;
8   A : aliased integer := 10;
9
10  procedure main is
11  begin
12    ptr := A'access;
13    if (ptr /= null) then
14      ptr.all := ptr.all + 1; -- COR Warning: Explicit
15      pragma assert (ptr.all = 10); -- COR Warning: Explicit
16      null;
17    end if;
18  end main;
19 end CORNULL;
20
```

## Explanation

At line 14 and line 15, PolySpace checks the null value of *ptr* pointer. As PolySpace does not perform pointer verification, it is not able to be precise on such a construction.

These checks are currently always **orange**.

## Accessibility of a Tagged Type: COR

Checks if a tag belongs to a tagged type hierarchy. This check is defined in Ada Standard at chapter 4.6 (paragraph 42).

It detects errors when a Tag of an operand does not refer to class-wide inheritance hierarchy.



## Ada Example

```
1  package TAG is
2
3  type Tag_Type is tagged record
4    C1 : Natural;
5  end record;
6
7  type DTag_Type is new Tag_Type with record
8    C2 : Float;
9  end record;
10
11 type DDTag_Type is new DTag_Type with record
12   C3 : Boolean;
13 end record;
14
15 procedure Main;
16
17 end TAG;
18
19
20 package body TAG is
21
22   procedure Main is
23     Y : DTag_Type := DTag_Type'(C1 => 1, C2 => 1.1);
24     Z : DTag_Type := DTag_Type'(C1 => 2, C2 => 2.2);
25
26     W : Tag_Type'Class := Z; -- W can represent any object
27         -- in the hierarchy rooted at Tag_Type
28   begin
29     Y := DTag_Type(W); -- COR Warning: Tag might be correct
30     null;
31   end Main;
32
33 end TAG;
```

## Explanation

In the previous example *W* represents any object in the hierarchy rooted at *Tag\_Type*.

At line 29, a check is made that the tag of *W* is either a tag of *DTag\_Type* or *DDTag\_Type*. In this example, the check should be green, *W* belongs to the hierarchy.

PolySpace is not precise on tagged types and currently always flags each one with a **COR warning**.

## Power Arithmetic: POW

Check to establish whether the standard power integer or float function is used with an acceptable (positive) argument.

### Ada Example

```
1 With Ada.Numerics; Use Ada.Numerics;
2 With Ada.Numerics.Aux; Use Ada.Numerics.Aux;
3
4 package POWF is
5   function Bool_Random return Boolean;
6   procedure MAIN;
7 end POWF;
8
9 package body POWF is
10
11   procedure MAIN is
12     IRes, ILeft, IRight : Integer;
13     Res, Dbl_Random : Double ;
14     pragma Volatile(Dbl_Random);
15   begin
16     -- Implementation of Power arithmetic function with **
17     if (Bool_Random) then
18       ILeft := 0;
19       IRight := -1;
20       IRes:= ILeft ** IRight; -- POW ERROR: Power must
be positive
21     end if;
22     if (Bool_Random) then
23       ILeft := -2;
24       IRight := -1;
25       IRes:= ILeft ** IRight; -- POW ERROR: Power must
```

```

be positive
26   end if;
27
28   ILeft := 2e8;
29   IRight := 2;
30   IRes:= ILeft ** IRight; -- otherwise OVFL Warning
31
32   -- Implementation with double
33   Res := Pow (dbl_Random, dbl_Random); -- POW Warning :
may be not positive
34   end MAIN;
35   end POWF;

```

## Explanation

An error occurs on the power function on integer values `**` with respect to the values of the left and right parameters when *left*  $\leq 0$  and *right*  $< 0$ . Otherwise, PolySpace prompts the user to investigate further by means of an **orange** check.

---

**Note** As recognized by the Standard, PolySpace places a **green** check on the instruction `left**right` with `left:=right:=0`.

---

## User Assertion: ASRT

Check to establish whether a user assertion is valid. If the assumptions implied by an assertion are invalid, then the standard behavior of the pragma assert is to abort the program. PolySpace therefore considers a failed assertion to be a runtime error.

## Ada Example

```

1
2  package ASRT is
3  function Bool_Random return Boolean;
4  procedure MAIN;
5  end ASRT;
6

```

```
7 package body ASRT is
8
9 subtype Intpos is Integer range 0..Integer'Last;
10 subtype TenInt is Integer range 1..10;
11
12 Val_Constant : constant Boolean := True;
13 procedure MAIN is
14   -- Init variables
15   Flip_Flop, Flip_Or_val : Boolean;
16   Ten_Random, Ten_Positive : TenInt;
17   pragma Volatile_ada.htm (ten_random);
18 begin
19
20   if (Bool_Random) then
21     -- Flip_Flop is randomly be True or False
22     Flip_Flop := bool_random;
23
24     -- Flip_Or_Val is always True
25     Flip_Or_Val := Flip_Flop or Val_Constant;
26     pragma assert(flip_flop=True or flip_flop=False); --
User assertion is verified
27     pragma assert(Flip_Or_Val=False); -- ASRT ERROR: User
assertion fails
28   end if;
29   if (Bool_Random) then
30     ten_positive := Ten_random;
31     pragma assert(ten_positive > 5); -- ASRT Warning: User
assertion may fail
32     pragma assert(ten_positive > 5); -- User assertion
is verified
33     pragma assert(ten_Positive <= 5); -- ASRT ERROR:
Failure User Assert
34   end if;
35
36 end MAIN;
37
38 end ASRT; -- End Package
```

## Explanation

In the *ASRT.ASRT* function, *pragma assert* is used in two different manners:

- To establish whether the values *flip\_flop* and *var\_flip* in the program are inside the domain which that the program is designed to handle. If the values were outside the range implied by the assert, then the program wouldn't be able to run properly. Thus they are flagged as runtime errors.
- To redefine the range of variables as shown at line 32 where *ASRT.Ten\_positive* is restrained to only a few values. PolySpace makes the assumption that if the program is executed with no runtime error at line 32, *Ten\_positive* can only have a value greater than 5 after the line.

## Non Terminations: Calls and Loops

NTC and NTL are only informative red checks.

- They are the only red errors which can be filtered out using the filters shown below
- They don't stop the verification
- As other reds, code placed after them are gray (unreachable): the only color they can take is red. They are not "orange" NTL or NTC
- They can reveal a bug, or can simply just be informative

Check	Description
NTL	<p>A NTL is a loop for which the break condition is never met. Among NTLs, you will find the following examples:</p> <ul style="list-style-type: none"> <li>• <code>while( 1=1 )loop function_call; end loop; // informative NTL</code></li> <li>• <code>while(x &gt;=0) loop x := x+1; end loop; // with x as an unsigned int could reveal a bug, or not (an unsigned is always positive)</code></li> <li>• <code>for I in 0 .. 10 loop my_array(i) = 10; end loop; // with "my_array is integer in 0..9" this red NTL reveals a bug in the array access, flagged in orange</code></li> </ul>

Check	Description
NTC	<p>Your function called "test" calls f;. And “f;” is flagged as a <b>red NTC</b>. Why? There could be five distinct explanations for this NTC:</p> <ul style="list-style-type: none"><li>• “f” contains a red error;</li><li>• “f” contains an NTL ;</li><li>• “f” contains an NTC;</li><li>• “f” contains an orange which is context dependant : it is either red or green: for this call, it makes the function crash.</li></ul> <hr/> <p><b>Note</b> Some information can be given when clicking on the NTC</p>

The list of so-called "non satisfiable constraints" represents the list of variables that cause the red error inside the function. The (potentially) long list of variables is useful to understand the cause of the red NTC, as it gives the conditions causing the NTC: it can be a list of variables (global or not):

- with a given value;
- which are not initialized. Perhaps the variables are initialized outside the set of verified files.

### Solution

Carefully check the reasons with relation to your situation.

---

**Note** If you can identify a function that does not terminate (loop, exit procedure) you may wish to use the -known-NTC function. You will find all the NTCs and their consequences in the known-NTC Viewer, allowing you to filter them. Benefit: you can focus on NTCs you did not expect.

---

## Non Termination of Call: NTC

Check to establish whether a procedure call returns. It is not the case when the procedure contains an endless loop or a certain error, or if the procedure calls another procedure which does not terminate. In the latter instance, the status of this check is propagated to the caller.

### Ada Example.

```
1 package NTC is
2   procedure MAIN;
3   -- Stubbed function
4   function Random_Boolean return Boolean;
5 end NTC;
6
7 package body NTC is
8
9   procedure F00 (X : Integer) is
10    Y : Integer;
11    begin
12    Y := 1 / X; -- ZDV Warning: Scalar division
13    by zero may occur
14    while (X >= 0) loop -- NTL ERROR: Loop never terminate
15      if ( Y /= X) then
16        Y := 1 / (Y-X);
17      end if;
18    end loop;
19  end F00;
20
21 procedure MAIN is
22 begin
23   if (Random_Boolean) then
24     F00(0); --NTC ERROR: Division by zero in NTC.F00 (ZDV)
25   end if ;
26   if (Random_Boolean) then
27     F00(2); --NTC ERROR: Non Termination Loop in NTC.F00 (NTL)
28   end if;
29 end MAIN;
30 end NTC;
```

**Explanation.** In this example, the function NTC.FOO is called twice and neither of these 2 calls ever terminates:

- The first never returns because of a division by zero (ZDV **warning**) at line 12 when  $X = 0$ .
- The second never terminates because of an infinite loop (**red NTL**) at line 13.

---

**Note** An NTC check can only be **red**.

---

### Non Termination of Call Due to Entry in Tasks

Tasks or entry points are called by PolySpace at the end of the main subprogram (which is executed sequentially) at the same time (the main subprogram must terminate).

In Ada language, explicit task constructs which are automatically detected by PolySpace are also called at the end of the main subprogram. An Ada program whose main subprogram calls a task entry, for instance, violates this model. PolySpace signals violations of this hypothesis, by indicating an NTC on an entry call performed in the main.

In the PolySpace model, the main procedure is executed first before any other task is started.

#### Example.

```
1 package NTC_entry is
2
3   TASK TYPE MyTask IS
4     ENTRY START;
5     ENTRY V842;
6   END MyTask;
7   procedure Main;
8     A : Integer;
9   end NTC_entry;
10
11 package body NTC_entry is
```



```

12
13  task body MyTask is
14  begin
15    accept Start;
16    A := A + 1; -- Gray code
17    accept V842;
18    A := A - 1; -- Gray code
19    accept V842;
20    A := A + 1; -- Gray code
21    accept V842;
22    A := A - 1; -- Gray code
23  end MyTask;
24
25  procedure Main is
26    T1 : MyTask;
27  begin
28    A := 0;
29    T1.Start;      -- NTC ERROR: entry task in the main
30    T1.V842;
31    T1.V842;
32    T1.V842;
33    pragma Assert(A=0); -- Gray code
34  end Main;
35 end NTC_entry;

```

Using the launching command `polyspace-ada95 -main NTC_entry.main` on the previous example leads to a red **NTC** in the main procedure and gray code on the main task body `MyTask`.

The only way to verify this code with PolySpace is to add another main procedure with a null body and to consider the `NTC_entry.main` as a task.

```
Package mymain is Procedure null_main; End mymain;
```

The previous small piece of code added and the usage of the launching command `polyspace-ada95 -main mymain.null_main. -entry-points NTC_entry.main` allow removing the red **NTC** in `NTC_entry.main` and gray code in the body of `MyTask`.

Another example concerns the call of an accept “rendez-vous” in the task body from the main (using `-main main.main`):

```
main main.main):
--package body main is
  procedure main is
  begin
    depend.controleur.demarrer; -- red NTC because of the call
to a task is called by the main
  end main;
--end main;
with Text_Io;
package body depend is
  task body controleur is
    date : Integer := 0;
    init_date: Integer;
    begin
      loop
        select
          accept demarrer;
          if (date = 0) then
            init_date := 10;
          end if ;
          date := init_date ;
          Text_Io.Put_Line ("bonjour ....");
        exit;
      end select;
    end loop;
  end;
end depend;
```

### **Known Non Termination of Call: k-NTC**

By using the `-known-NTC` option with a specified function at launch time, it is possible to transform an NTC Check for a non termination of call to a k-NTC check. Like an NTC check, k-NTC checks are propagated to their callers.

Functions which are designed to be non-terminating can be filtered out during the analysis of results through the use of the appropriate filter in the viewer, in conjunction with the `-known-NTC` option at launch.

**Ada Example.**

```
1 package KNTC is
2   procedure Put_io (X : Integer);
3   procedure get_data(Data : out Float; Status : out Integer);
4   procedure store_data(Data : in Float);
5   procedure SysHalt(Value : Integer);
6   procedure MAIN;
7 end KNTC;
8
9 package body KNTC is
10
11   -- known NTC function
12   procedure SysHalt(Value : Integer) is
13   begin
14     Put_io(Value);
15     loop -- Never terminate loop
16       null;
17     end loop;
18   end SysHalt;
19
20   procedure MAIN is
21     Status : Integer := 1;
22     Data : Float;
23   begin
24
25     while(Status = 1) loop
26       -- get data
27       get_data(Data, Status);
28       if (status = 1) then
29         store_data(data);
30       end if;
31       if (Status = 0) then
32         SysHalt(1); -- k-NTC check: Call never terminate
33       end if;
34     end loop;
35   end MAIN;
36 end KNTC;
```

**Explanation.** In the above example, the **-known-NTC "KNTC.SysHalt"** option has been added at launch time, transforming corresponding NTC checks to k-NTC one.

### Non Termination of Loop: NTL

Check to establish whether a loop (for,do-while, while) terminates.

#### Ada Example.

```
1
2 package NTL is
3   procedure MAIN;
4   -- Prototypes stubbed as pure functions
5   procedure Send_Data (Data : in Float);
6   procedure Update_Alpha (A : in Float);
7   end NTL;
8
9 package body NTL is
10
11   procedure MAIN is
12     Acq, Vacq : Float;
13     pragma Volatile_ada.htm (Vacq);
14     -- Init variables
15     Alpha : Float := 0.85;
16     Filtered : Float := 0.0;
17   begin
18     loop    -- NTL information: Loop never terminates
19       -- Acquisition
20       Acq := Vacq;
21       -- Treatment
22       Filtered := Alpha * Acq + (1.0 - Alpha) * Filtered;
23       -- Action
24       Send_Data(Filtered);
25       Update_Alpha(Alpha);
26     end loop;
27   end MAIN;
28 end NTL;
29
```

**Explanation.** In the above example, the "continuation condition" of the while is always true and the loop will never exit. Thus PolySpace will raise an error.

In some case, the condition is not trivial and may depend on some program variables. Nevertheless, PolySpace is still able to treat those cases.

**Another NTL Example: Error Propagation.** As opposed to other red errors, PolySpace does not continue with the verification in the current branch. Due to the inside error, the (for, do-while, while) loop never terminates.

```
1 package NTLDO is
2   procedure MAIN;
3 end NTLDO;
4
5 package body NTLDO is
6   procedure MAIN is
7     A : array(1..20) of Float;
8     J : Integer;
9   begin
10    for I in A'First .. 21 loop -- NTL ERROR: propagation of
OVFL ERROR
11      A(I) := 0.0 ; -- OVFL Warning: 20 verification with
I in [1,20] and one ERROR with I = 21
12      J := I + 1;
13    end loop;
14  end MAIN;
15 end NTLDO;
```

---

**Note** A NTL check can only be red.

---

## Sqrt, Sin, Cos, and Generic Elementary Functions

When the verified code uses some mathematical functions which are not supported by PolySpace, there are always unproven checks about overflows when two variables which have been derived from the results of mathematical functions such as "cos" are summed. VOA checks display the *full range* for the potential return value of these functions.

This symptom can be seen when all mathematical functions are stubbed automatically which happens when the declarations of these functions for the compiler in use are slightly different from those assumed by PolySpace. The following solution matches the user's mathematical functions to PolySpace Server's equivalent function. Please note it has no impact on the original source code (no modification will be made).

### Original Code.

```
package Types is
  subtype My_Float is Float range -100.0 .. 100.0;
end Types;

3 package Main is
4   procedure Main;
5   end Main;
6
7
8   with New_Math; use New_Math;
9   with Types; use Types;
10
11  package body Main is
12    procedure Main is
13      X : My_float;
14      begin
15        X := Cos(12.3); --voa displays [-1.0 .. 1.0]
16        X := Sin(12.3); --voa displays [-1.0 .. 1.0]
17        X ::= Sqrt(-1.5); --is red: NTC Error
18      end;
19    end Main;
```

### Original Maths Package.

```
with My_Specific_Math_Lib;
with Types; use Types;

package New_Math is
  function COS (X : My_Float) return My_Float renames \
  My_specific_math_lib.
  Cos;
```

```

    function SQRT (X : My_Float) return My_Float renames \
My_specific_math_lib.
sqrt;
    function SIN (X : My_Float) return My_Float renames \
My_specific_math_lib.
sin;
end New_Math;

```

**Extra Package.** This package may be written by the user to include more precise modelling of the mathematical functions in the verification.

```

WITH Ada.Numerics.Generic_Elementary_Functions;
with Types; use Types;

package My_specific_math_lib is new Ada.Numerics.
Generic_Elementary_Functions(My_Float);

```

**Important.** Due to a lack of precision in some areas, PolySpace is not always able to indicate a **red** NTC check on mathematical functions even whereas a problem exists. By default it is important to consider each call to any mathematical functions as though it had been highlighted by an **unproven** check, and could therefore lead to a runtime error.

## Unreachable Code: UNR

Check to establish whether different code snippets (assignments, returns, conditional branches and function calls) are reached (Unreachable code is referred to as "dead code"). Dead code is represented by means of a **gray** color on every check and an UNR check entry.

### Ada Example

```

1 package UNR is
2   type T_STATE is (Init, Wait, Intermediate, EndState);
3   function STATE (State : in T_STATE) return Boolean;
4   function Intermediate_State(I : in Integer) return T_STATE;
5   function UNR_I return Integer;
6   procedure MAIN;
7 end UNR;
8

```

```
9 package body UNR is
10
11 function STATE (State : IN T_STATE) return Boolean is
12 begin
13   if State = Init then
14     return False;
15   end if ;
16   return True;
17 end STATE;
18
19 function UNR_I return Integer is
20   Res_End, Bool_Random : Boolean;
21   I : Integer;
22   Res_State : T_STATE;
23   pragma Volatile_ada.htm (bool_random);
24 begin
25   Res_End := STATE(Init);
26   if (Res_End = False) then
27     Res_End := State(EndState);
28     Res_State := Intermediate_State(0);
29     if (Res_End = True or else Res_State = Wait) then -- UNR code
30       Res_State := EndState;
31     end if;
32     -- Use of I which is not initialized
33     if (Bool_Random) then
34       Res_State := Intermediate_State(I); -- NIV ERROR
35       if (Res_State = Intermediate) then -- UNR code because
of NIV error
36         Res_State := EndState;
37       end if;
38     end if;
39   else
40     -- UNR code
41     I := 1;
42     Res_State := Intermediate_State(I);
43   end if;
44   return I; -- NIV ERROR: because of UNR code
45 end UNR_I;
46
47 procedure MAIN is
```



```
48   I : Integer;
49   begin
50     I := UNR_I; -- NTC ERROR because of propagation
51   end MAIN;
52
53   end UNR;
54
55
56
```

## Explanation

The example illustrates three possible reasons why code might be unreachable, and hence be colored gray.

- As shown at line 26, the first branch is always true (*if-then part*) and so the other branch is never executed (*else part* at lines 40 to 42).
- At line 29 a conditional part of a conditional branch is always true and the other part never evaluated because of the standard definition of logical operator *or else*.
- The piece of code after a red error is never evaluated by PolySpace Server. The call to the function and the lines following line 34 are considered to be dead code. Correcting the red error and relaunching would allow the color to be revised.

## Value on Assignment: VOA

Check to establish the value taken by a variable on assignment.

VOA checks are only available on scalar variables. Some examples are given below.

---

**Note** PolySpace software does not show VOA on all assignments. To optimize performance, the software may not show VOA in some cases.

---

## Ada Example

```
1
2
3 Package VOA is
4
5   subtype T_NBWAY is Integer range 1..8;
6   subtype T_DIGITAL is Integer range 0..1;
7   subtype T_ANALOGIC is Float range -10.0 .. 10.0;
8   Zero_analogic : constant T_ANALOGIC
9     := (T_ANALOGIC'Last - T_ANALOGIC'First)/ 2.0 - T_ANALOGIC'Last; --
10
11  function Get_Analogic (Way : T_NBWAY) return T_Analogic;
12  function Get_Digit (Way : T_NBWAY) return T_Digital;
13
14  type VerifierColor is (Red, Green, Orange, Black);
15  type RECOR is
16    record
17      A : Float;
18      B : VerifierColor;
19    end record;
20  Var_rec : RECOR;
21
22  Procedure MAIN;
23
24 end VOA;
25
26 package body VOA is
27
28  Procedure MAIN is
29    Way_io : T_NBWAY := T_NBWAY'First;
30    Val_Sensor : T_ANALOGIC;
31    Val_Digit : T_DIGITAL;
32    volatile_Color : VerifierColor;
33    pragma Volatile(Volatile_color);
34    Volatile_Float : Float;
35    pragma Volatile(Volatile_Float);
36  begin
37
38    for I in T_NBWAY'Range loop
```

```

39   Val_Sensor := Get_Analogic(I); --VOA: {-1E+1<=[expr]<=1E+1}
40   Val_Digit := Get_Digit(I); -- VOA: {0<=[expr]<=1}
41   if Val_Sensor < 0.0 then
42     Val_Sensor := Zero_Analogic; -- VOA: {[expr]=0.0}
43   end if;
44   end loop;
45
46   -- Example
47   Var_Rec.A := Volatile_Float; -- VOA: {[expr]=float(32)
range -3.41E+38..3.4E+38}
48   Var_Rec.B := Volatile_color; -- VOA: {red<=[expr]<=black}
49
50   -- Other possible but intrusive way to know a specific value
51   pragma Inspection_Point (Way_io); -- inspection point
computed range: {WAY_IO=1}
52
53   end MAIN;
54
55   End VOA;

```

## Explanation

As shown in the example, inspection points ( IPT ) can also be used to discover the range of a variable.

## Inspection Points: IPT

The use of *pragma Inspection\_Point (var)* as a code snippet ( where *(var)* is a scalar variable ) represents a request to compute the specific range of a variable by means of a pragma instruction. Refer to the example below.

## Ada Example

```

1
2
3 Package IPT is
4
5   subtype T_NBWAY is Integer range 1..8;
6   subtype T_DIGITAL is Integer range 0..1;
7   subtype T_ANALOGIC is Float range -10.0 .. 10.0;

```

```
8 Zero_analogic : constant T_ANALOGIC
9 := (T_ANALOGIC'Last - T_ANALOGIC'First)/ 2.0 - T_ANALOGIC'Last; --
10
11 function Get_Analogic (Way : T_NBWAY) return T_Analogic;
12 function Get_Digit (Way : T_NBWAY) return T_Digital;
13
14 type VerifierColor is (Red, Green, Orange, Black);
15 type RECOR is
16   record
17     A : Float;
18     B : VerifierColor;
19   end record;
20 Var_rec : RECOR;
21
22 Procedure MAIN;
23
24 end IPT;
25
26 package body IPT is
27
28   Procedure MAIN is
29     Way_io : T_NBWAY := T_NBWAY'First;
30     Val_Sensor : T_ANALOGIC;
31     Val_Digit : T_DIGITAL;
32     volatile_Color : VerifierColor;
33     pragma Volatile(Volatile_color);
34     Volatile_Float : Float;
35     pragma Volatile(Volatile_Float);
36   begin
37
38     for I in T_NBWAY'Range loop
39       Val_Sensor := Get_Analogic(I);
40       pragma Inspection_Point (Val_Sensor); --
41       IPT: {-1E+1<=VAL_SENSOR<=1E+1}
42       Val_Digit := Get_Digit(I);
43       pragma Inspection_Point (Val_Digit); --
44       IPT: {0<=VAL_DIGIT<=1}
45     end loop;
46
47     -- Example on record
```

```
46   Var_Rec.A := Volatile_Float;
47   Var_Rec.B := Volatile_color;
48   pragma Inspection_Point (Var_Rec); --IPT currently ignored
49   pragma Inspection_Point (Volatile_color); --
IPT: {VOLATILE_COLOR=red..
black}
50   pragma Inspection_Point (Way_io); -- IPT: {WAY_IO=1}
51
52   end MAIN;
53
54 End IPT;
```

### Explanation

Note that the inspection point at line 48 is ignored. Inspection points are available for scalar variables only.



# Approximations Used During Verification

---

## Why PolySpace Verification Uses Approximations

In this section...
“What is Static Verification” on page 3-2
“Exhaustiveness” on page 3-3

### What is Static Verification

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

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

For example, consider the following code:

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

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

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

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



to establish that – and hence the gain in efficiency compared to traditional approaches.

Static code verification does have an exact solution, but that solution is generally not practical, as it would generally require the enumeration of all possible test cases. As a result, approximation is required.

## **Exhaustiveness**

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

### **3** Approximations Used During Verification

---

# Examples

---

## Complete Examples

In this section...
“Simple Ada Example” on page 4-2
“HDCA Server Example” on page 4-2
“airplane2 Example” on page 4-3
“High Speed Train Example” on page 4-3

### Simple Ada Example

```
polyspace-ada \  
-main a_project.root_procedure \  
-prog myProject \  
-O1 \  
-sources directory/*.ad[bs] \  
-modules-precision sri:02,types:00
```

### HDCA Server Example

An Ada example. Note that we try to minimize verification time in going to pass2 and O0. Note also the list of files (no spaces in that file list!).

```
polyspace-ada \  
-prog HDCA_Server \  
-main hdca_main.HDCA_Server \  
-O0 \  
-from scratch -to pass2 \  
-keep-all-files \  
-no-automatic-stubbing \  
-continue-with-red-error \  
-results-dir RESULTS \  
-sources \  
$working_version/hdca/clock_and_date.ada,\  
$working_version/hdca/cpu_usage.ada,\  
$working_version/hdca/exception_log.ada,\  
$working_version/hdca/hdca_main.ada,\  
$working_version/screen/monitor.ada,\  
$working_version/common/utilities/letter_box.ada,\  

```

```
$working_version/common/utilities/library_functions.ada,\  
$working_version/common/utilities/catalog_tools.ada,\  
$working_version/common/utilities/configuration.ada,\  
$working_version/common/utilities/convertng.ads\  
$working_version/common/utilities/convertng.adb
```

## airplane2 Example

An Ada Example with Tasks

```
polyspace-ada \  
-target m68k \  
-entry-points Wings.wingSuperVisor,Tail.tailSuperVisor,\  
Rudder.rudderSuperVisor \  
-to pass2 \  
-from scratch \  
-prog airplane2 \  
-OO \  
-results-dir `pwd`/RESULTS_14_08 \  
-main main.pst_main
```

## High Speed Train Example

An Ada example.

```
polyspace-ada \  
-target sparc \  
-from scratch \  
-array-expansion-size 1 \  
-sources "sources/*. [aA]*[a-zA-Z]" \  
-prog high_speed_train \  
-OO \  
-keep-all-files \  
-results-dir RESULTS \  
-main root_package.start
```