Compass User Manual:
A Tool for Source Code Checking
(A ROSE Tool)
Draft User Manual
(Associated with ROSE Version 0.9.2a)

ROSE Team
Lawrence Livermore National Laboratory
Livermore, CA 94550
925-423-2668 (office) 925-422-6278 (fax)
dquinlan@llnl.gov
Project Web Page: http://www.rosecompiler.org
UCRL Number for ROSE User Manual: UCRL-SM-210137-DRAFT
UCRL Number for ROSE Tutorial: UCRL-SM-210032-DRAFT
UCRL Number for ROSE Source Code: UCRL-CODE-155962

ROSE User Manual (pdf)
ROSE Tutorial (pdf)
ROSE HTML Reference (html only)

June 26, 2008

Contents

Acknowledgments

This tool is the product of the entire ROSE team. Compass depends upon the ROSE open compiler infrastructure and is a simple application of mechanisms in ROSE which have been developed over several years and contributed to by a large number of people.

This currently includes:

- Staff: Dan Quinlan
- Post docs: Thomas Panas, Chunhua Liao, and Jeremiah Willcock
- Ex Post doc: Richard Vuduc
- Students:
  Gergo Barany, Michael Byrd, Valentin David, Han Kim, Robert Preissl, Andreas Saebjornsen, Jacob Sorensen, Ramakrishna Upadrasta, Jeremiah Willcock, Gary Yuan
- Internal LLNL Contributors: Greg White
- External Collaborators:
  We want to thank CERT, who has been particularly helpful and supportive both with the development of checkers for their Secure Coding Rules and with numerous suggestions.

Chapter 1

Introduction

1.1 Overview

Compass is a tool for the checking of source code. It is based on the ROSE compiler infrastructure and demonstrates to use of ROSE to build lots of simple pattern detectors for analysis of C, C++, and Fortran source code.

The purpose of this work is several fold:

- Provide a concrete tool to support interactions with lab customers.
- Provide a home for the security analysis specific detectors being built within external research projects.
- Provide an external tool for general analysis of software.
- Provide a tool to support improvements to the ROSE source code base.
- Define an infrastructure for an evolving and easily tailored program analysis tool.
- Provide a simple motivation for expanded use of ROSE by external users. Development, testing, and evaluation of ROSE infrastructure is best facilitated through its expanded use by others and this provides a specific and attractive tool that can provide feedback to users about their own code projects. Even though optimization research is our focus, this gets our supporting infrastructure for optimization research out and into use by others in the form of an extensible tool.

Note that as the collection of detectors grows we will periodically reorganize the collection. At some point soon we will build a hierarchy to organize the evolving collection.

A basis for other source analysis tools Input and output to ROSE is organized so that any number of sources could be used. So although we provide a compiler interface (for simplicity), we will also provide a GUI interface as an alternative interface to demonstrate that the detectors are orthogonal to there use in alternative tools. Alternative tool interfaces should be possible and will

further demonstrate the independence of the input and output mechanisms to the designs and implementation of the core detectors.

Add Your Own Detector Detectors written in Compass make direct use of ROSE and are designed to be copied and extended by users to develop their own detectors. We welcome the contribution of these detectors back to the ROSE team for inclusion into future releases of Compass; full credit for all work will be provide to all authors. Compass is an open source project using ROSE, an open source compiler infrastructure.

Each of the detectors are examples of how to add your own detector to **Compass**. If you build a detector that you would like to have be distributed with **Compass**, please send it to us and we will add your as an external contributor.

Guidelines for contributions:

- Use any Compass detector and an example.
- provide the documentation about your detector.
- Use any features in ROSE to support your detector; AST, Control Flow graph, System dependence Graph, Call Graph, Class Hierarchy Graph, etc.
- Your detector should have **NO** side-effects on the AST.

Chapter 2

Design and Verification

Compass is a tool is used to analyze software (both source code and binaries). A collection of *checkers* are built with each of them detecting the violation of a rule. By reporting on the violations of rules *Compass* provides a way to enforce predefined or arbitrary user specified properties on software. This chapter covers the design of *Compass* and the design of the verification in the *Compass Verifier*, used to verify properties of the checkers implemented and submitted to *Compass*.

2.1 Usage Model

Figure 2.1 shows the usage model (use cases) of *Compass*. The analysis is triggered by the user running *Compass* over an input file (source code or binary). The user implicitly selects which checkers to execute (defining what rules are to be enforced); by default all checkers are run. The user also specifies the input file to be checked; for source code the specification is similar to the command line required for the compilation in the case of a source file. Results of the analysis are presented to the user, a number of mechanisms can be used to display the results.

Either the same user or a different user/developer can also implement and submit checkers to be built into Compass. Since external users may contribute checker automatically via scripts, a verification of the validity and safety of these checkers is necessary. We provide a *Compass Verifier* that helps to check that all checkers are safe. Currently, the verifier is run by an administrative person but may run automatically in the future.

2.2 Trust Model

By design we make a few assumptions about the use of Compass in order to define a secure tool. We assume:

1. For now, there is an assuption of trust in the person writing the checker. We use the *Compass Verifier* as a way to double check the checkers so that we can eventually weaken the level of trust assumed for people writing checkers. However, the design of the *Compass Verifier* is not likely to ever

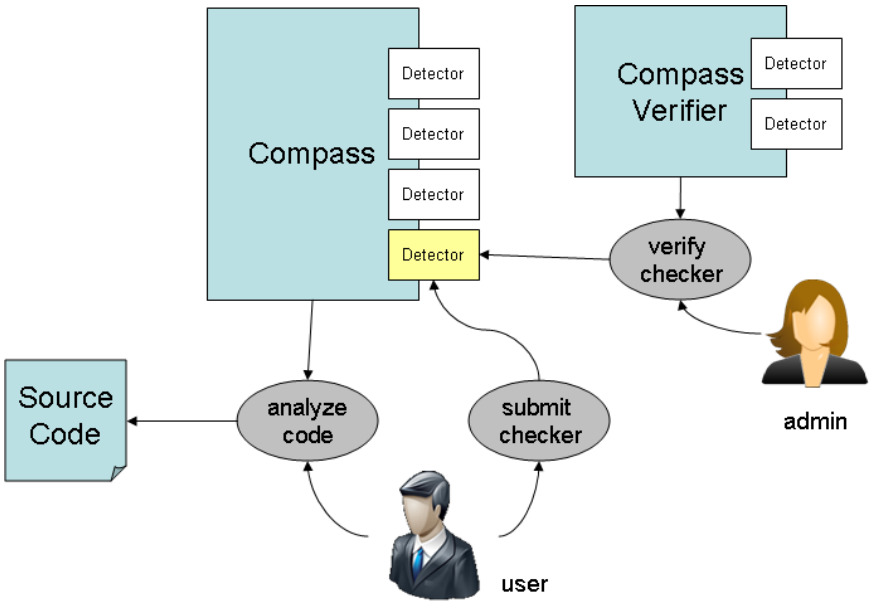

Figure 2.1: Compass Use Case

be robust enough to guarantee an automated proof of security for each checker. Thus, we also assume that someone trusted will also review the checker. *not implemented: We expect that a digital signature is possible to associate a trusted reviewer with a review of the checker together with an MD5 hash that verifies the checker source code.*

2. Since running *Compass Verifier* is an optional part of building the Compass executable, the person running these test is trusted. There are two ways to run the *Compass Verifier* (see section 3.7 for details):

   - Slow: once on each checker (`make verify`). This mechanism tests all the files one checker at a time and thus can not miss a file. Note that even the counter examples are tests which can be a problem when the counter example for the checker is detected as a violation for *Compass Verifier*. Counter examples for checkers have to be carefull written to not represent examples that violate *Compass Verifier*.
   - Fast: once on the union of all the checkers (`make oneBigVerify`). This step forms a single file of all the checkers (and indoing so can miss some files, and so is less secure). It is mostly for testing purposes.

3. The person building the Compass executable is trusted.

4. The environment where the testing using Compass is done is trusted.

5. Compass is designed so that the user running Compass need not be trusted.

It is unclear at present how weak the assumption of trust on the compass checker developer can be and it may ultimately depend directly on the capabilities of the *Compass Verifier*.

2.3 Architecture

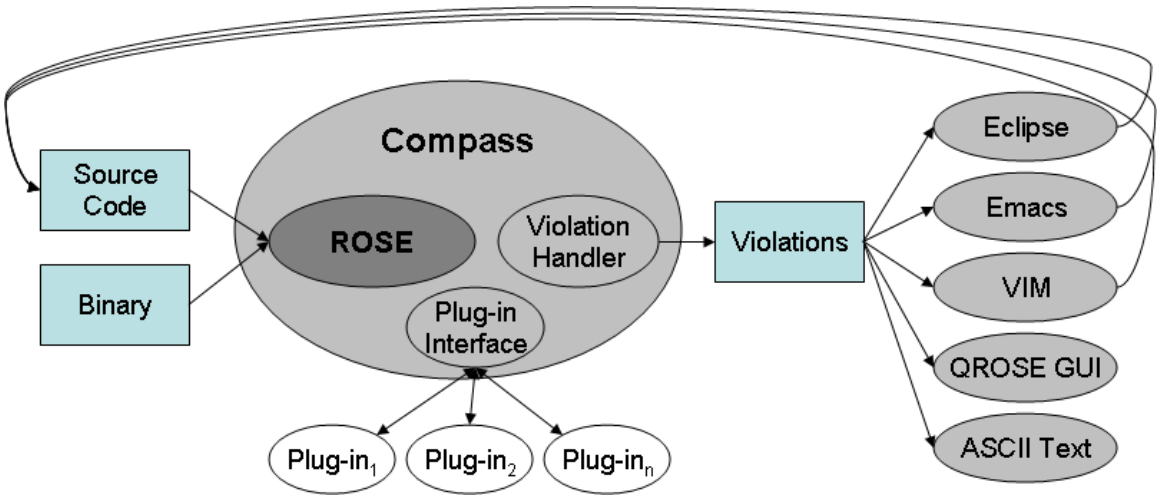

Figure 2.2: Compass Architecture

Compass is a tool that allows users to implement checkers to locate and report software defects. Documentation of various kinds of software defects can be found in sources such as the CERT Secure Coding Rules, Common Weakness Enumeration from MITRE, and other sources. Our focus is not to define new software defects but rather to provide a platform that allows the easy implementation of defect checkers. Compass has been designed to be easy to extend, allowing users to implement their own custom checkers (custom source code analyses for identifying defects), as shown in Figure 2.2. Compass supports the implementation of both simple as well as more advanced defect checkers. For the latter, Compass utilizes the ROSE infrastructure to perform a wide range of general purpose program analyses, such as control flow analysis, data flow analysis, program slicing, etc.

Compass is designed in a way that allows users who do not necessarily have compiler backgrounds to utilize the ROSE infrastructure to build their own analysis tools. Compass is foremost an extensible open source infrastructure for the development of large collections of rules. Our current implementation supports automatic defect checking, programming language restriction, and malware detection in C, C++, and object code. Support for Fortran is a new addition to ROSE and will be supported in Compass in the near future.

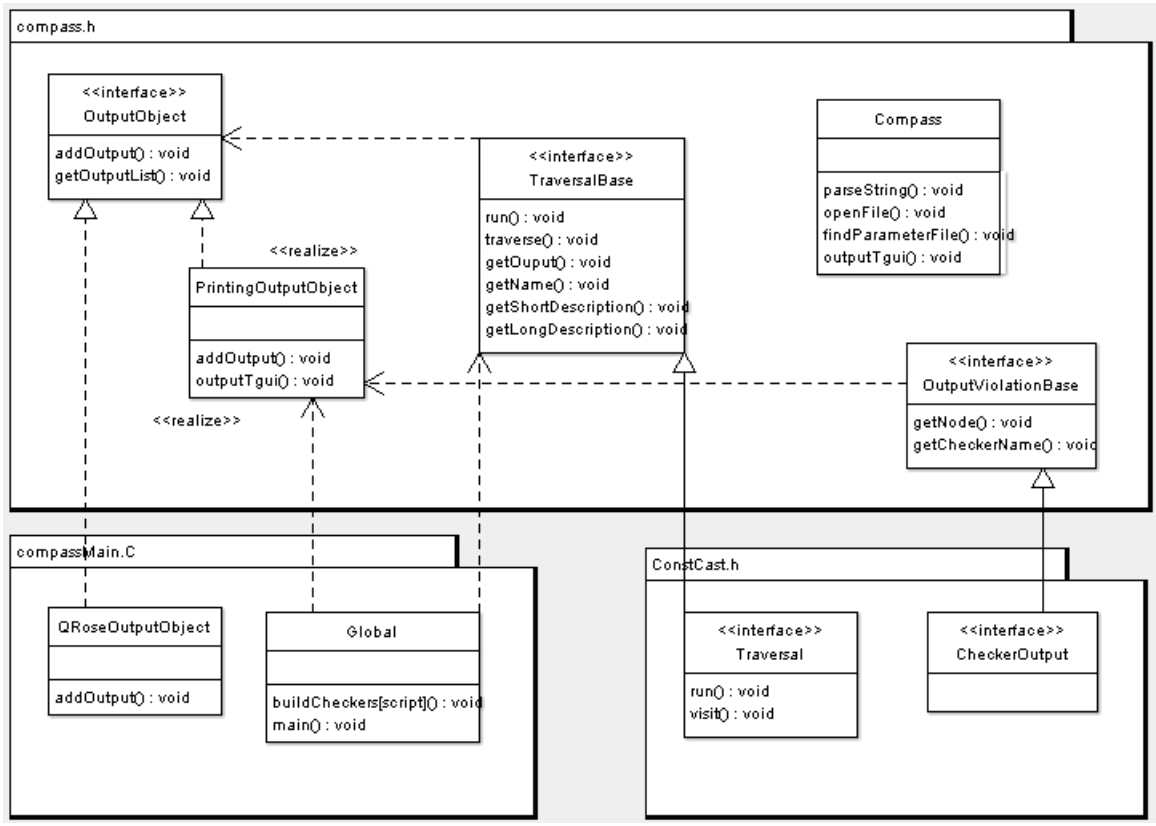

Figure 2.3: Compass Design

2.4 Design

Compass is designed to be easy to extend. Any user may write a checker and add it to Compass. Figure 2.3 illustrates the UML design decisions behind Compass.

Most of the functionality of Compass is in abstract classes hidden in the Compass namespace within compass.h - a file within the compassSupport directory. The figure uses a specific example, *ConstCast*, for illustration; Compass is designed to support a large number of checkers (hundreds). All checkers, such as the *ConstCast* checker (illustrated in figure 2.3), utilize the abstract classes to traverse a program with all its nodes and to output violations found in that code according to the local algorithm.

CompassMain is the main executable that initially calls ROSE to parse a program. Then *buildCheckers* is called to load all checkers that are specified within a configuration file. The configuration file allows users to turn on and turn off specific checkers for their run-time analyses. However, the configuration file only permits checkers to be loaded that were part of Compass at compile-time.

The main interface file compass.h contains the abstract classes *TraversalBase*

and *OutputObject*. TraversalBase is the interface to ROSE, allowing a checker to traverse the ROSE AST (program) and hence perform analysis on that AST. OutputObject aids to output defects found by a specific checker. More functionality to handle e.g. file input and parameters provided to Compass, is provided within the Compass namespace.

2.5 Compass Verifier

Compass must be safe, so that analyses and their results can be trusted. The *Compass Verifier* is used at build time to run a specific set of separate compass rules offer the source code of all the checkers. For simplicity it runs in two modes: fast, for checking specific named checker source files; and slow, for testing *all* checker source files.

2.5.1 Threats

In order to define a complete design for security we outline the threats that understand to be relevant. The main threats to the validity of Compass checkers are:

- *Malicious User*
  A malicious user is an external user of Compass contributing a checker that performs malicious behavior.
- *Malicious Checker*
  Compass is extensible and new checkers can be added externally (users outside the main development group). A checker can be programmed arbitrarily using the C/C++ and assembly programming languages. It is therefore possible for a skilled programmer to hide malicious operations within a checker. Compass must prevent checkers with malicious behavior to be part of the Compass system. Threats are:
  - **exfiltration**
    A checker should act in a secure way with the input files it is given. Securing the inputs to Compass (e.g. the inputs to each checker) from exfiltation is a first priority. Allowing a checker to scan the host machine to exfiltrate arbitrary data (this is a threat that any secure software will have).
  - **modification of filesystem**
    A checker should be side-effect free, or have only well defined side-effects, but a malicious checker could modify or erase parts of the accessible file system (e.g. deleting whole directory structures).
- *Malicious Compass*
  Since Compass is built from ROSE, it is possible to modify compass (or any checker) to generate source code that could be compiled to replace the existing executable (there are some constraints here) or regenerate the source code to replace the existing source code or perhaps just provide an alternative copy of the source code. This indirect transformation of the input code is a threat.

- *Source Code Replacement*
  It should not be possible for users to exchange the source code of checkers within a running system, i.e. Compass cannot implement dynamic loading of checkers. Such a feature would compromise its safety.

- *Binary Replacement*
  Another threat is the replacement of a valid Compass checker with a modified malicious version within a binary release of Compass. Therefore, Compass should be aware if parts of itself were modified and should not execute.

2.5.2 Mitigation of Threats

Compass is designed to be safe. The Compass Verifier is a stable separate copy of Compass that contains only a few checkers to check (external and internal) user delivered checkers for safety. We have hopefully designed Compass in a way that it addresses the threats mentioned above:

- *Malicious User*
  Initially, we permit only trusted individuals to add new checkers to Compass. Once the verification process is matured, we will extend this policy to allow less trusted users to contribute to Compass. A goal will be to allow arbitrary users to contribute checkers, however, a review of the whole Compass design (and the *Compass Verifier* especially) will be required to define required trust levels for user/developers who implement checkers.

FIXME: *We might define trusted and untrusted checkers as a way to have checkers from arbitrary users, but mark them as untrusted.*

- *Malicious Checker*
  To prevent Compass from executing malicious code, the Compass Verifier executes its own checkers on any user defined checker that is being considered to be added to Compass. Currently, the Compass Verifier contains three checkers:

  - *fileReadOnlyAccess* ensures that a user defined checker performs no write or execute operations on files.
  - *allowedFunctions* is a *white list* of function calls permitted in a checker. This list contains functions that are trusted and hence considered safe when integrated to Compass.

FIXME: *This is not yet implemented as a white list and is instead currently a black list; called: forbiddenFunctions.*

  - *noAsmStmtsOps* searches for assembly instructions in a checker and flags and reports all cases as unsafe.
  - To avoid modifications of the AST for the purpose of allowing other checkers to pass, the AST should not be modified (this should extend to all the program analysis graphs generated and used by other checkers). *This is not implemented yet.*

- *Malicious Compass*
  Since Compass does not generate code, it can not be used to modify the input software (source code or binary) or generate an new copy that could be confused with the input. However, future versions of Compass make make transformation to introduce greater levels of security; fix flaws, mitigate specific forms of threats, etc. It will be important to make sure that

such transformation can not change the behavior of an input code to make the modified input code malicious. Current proposed approaches would build a patch which would have to be inspected by a trusted developer before it would be applied to modify the input code.

- *Source Code Replacement*
  Checkers can only be added at compile time to Compass, not at run-time. This means that checkers (meaning the source code) cannot be exchanged against unsafe versions at run-time. Furthermore, we allow only the Compass tool builder (admin) to build versions of Compass that must pass the Compass Verifier.

- *Binary Replacement*
  Our goal is to perform a MD5 checksum on all the checkers part of the binary Compass distribution before Compass is executed. In this way Compass will not run if parts of it were modified. *This is not implemented yet.*

FIXME: *We should describe the policy for allowing MD5 checksums to be verified.*

Chapter 3

Using Compass

3.1 Running Compass

Compass is currently distributed as part of ROSE, and represents one of many tools that can be built using the ROSE open compiler infrastructure. Compass resides in the `ROSE/projects/compass`. As part of building ROSE Compass will be automatically built in the Compass directory. Running compass is a matter if typing `compassMain` and handing in a number of options. The `compassMain` program acts just like a compiler so it is appropriate to hand it the same options required to compile your source file (e.g `-I` directory paths and a source file. Compass will figure out the language from the source file suffix. Using the `--help` option will provide a more complete list of options available to ROSE based tools. See also the section of this chapter on the include/exclude options for path and file names as these will permit the output from header files to be tailored.

3.2 Output from Compass

Output from compass can be generated in a number of forms, the default is ASCII text output of the messages about rule violations with the source code position in *GNU standard source code position format*. This form can be used to interact with external tools (e.g. Emacs) to permit alternative interface to Compass. Mechanisms available include:

- Emacs:
  Detecting errors while you type 3.5 and 3.1.
- Vim 7:
  Compass can work with Vim 7's QuickFix commands to highlight source lines with error messages 3.9.
- CompassGUI:
  There is also a Compass GUI for reviewing Compass output and interactively rerunning compass and sifting through the output while relating them to the source code 3.2. This work uses the QRose library produced

at Imperial College London by Gabriel Coutinho, as part of their development of FPGA tools using ROSE. QRose is based on the Qt library and provides a wide number of ROSE aware components to make the development of GUIs for ROSE based tools easy. The source code for the Compass GUI is provided, but this work is unfinished (and required the QRose library available from Imperial).

- ToolGear post-processing:
  Output in XML permits the use of ToolGear (LLNL tool available on the web) for viewing Compass generated output. This mechanism is particularly useful for reviewing the results of nightly builds (and associated runs of large projects using Compass). See figure 3.3

- ASCII output:
  Output in ASCII format is of the form shown in 3.4. This form permits the connection to multiple external tools (the Emacs interface reads the ASCII output format directly).

3.2.1 Using Compass With Emacs

Compass as a checker is most useful when the user is notified as early as possible when he violates a desired software property. Although for many purposes it is sufficient to run Compass separately; it is possible to use compass seamlessly when developing in emacs. By using an emacs extension called *flymake* together with Compass erroneous lines can be highlighted while programming, and the relevant error messages displayed in a dialog. Syntax errors from ROSE will be displayed as well, see figure 3.1.

Much thanks for David Svoboda at CERT at CMU for first configuring Flymake to work with Compass and demonstrating the idea. It has provided a great way to check code using compass and its use in Emacs has stimulate a number of ideas that have made their way back into Compass.

Emacs .emacs Code Requirement

Figure 3.5 shows the code that is required to be added to the `.emacs` file. A copy of this code is available in the compass source directory in the file `emacs_compass_config.el`.

Emacs Version Requirement

Emacs version 22 or newer is required to take advantage of the emacs integration of Compass. Before using Compass a 3 step process must be followed:

- Add the text in figure 3.5 (in `ROSE/projects/compass/emacs_compass_config.el`) to .emacs

- Change /path/to/makefile in figure 3.5 to the path to the project you are editing in Compass

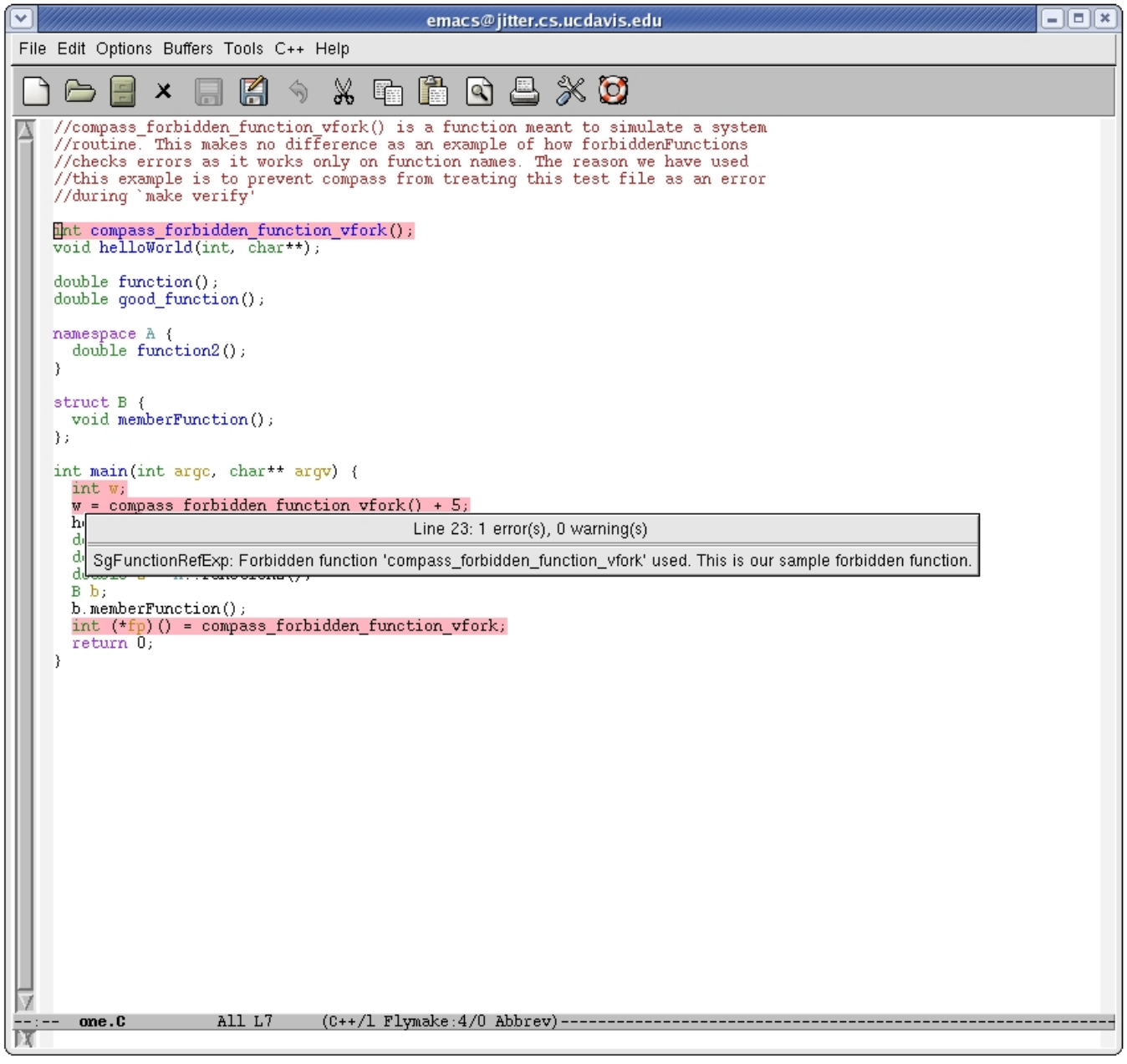

Figure 3.1: Compass error messages integrated into Emacs

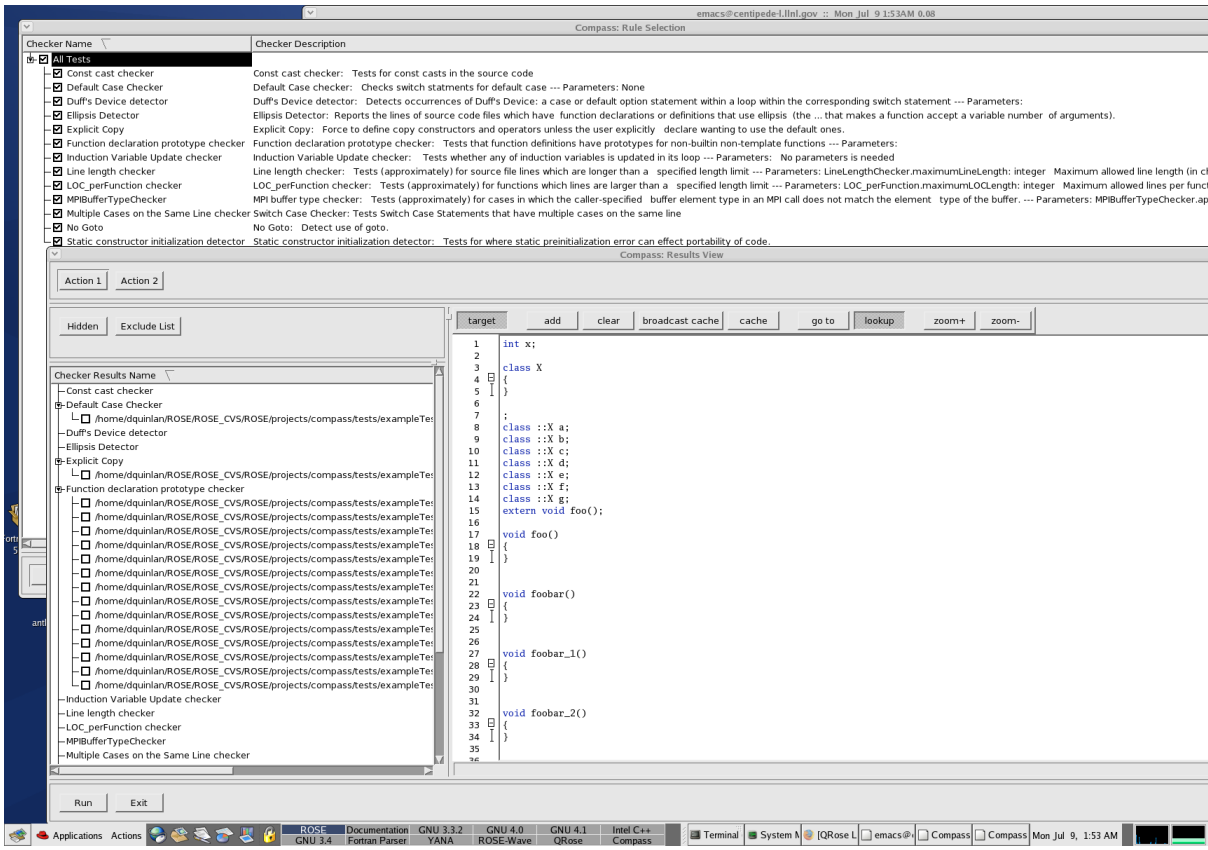

Figure 3.2: Compass GUI for interpretation of rule violations

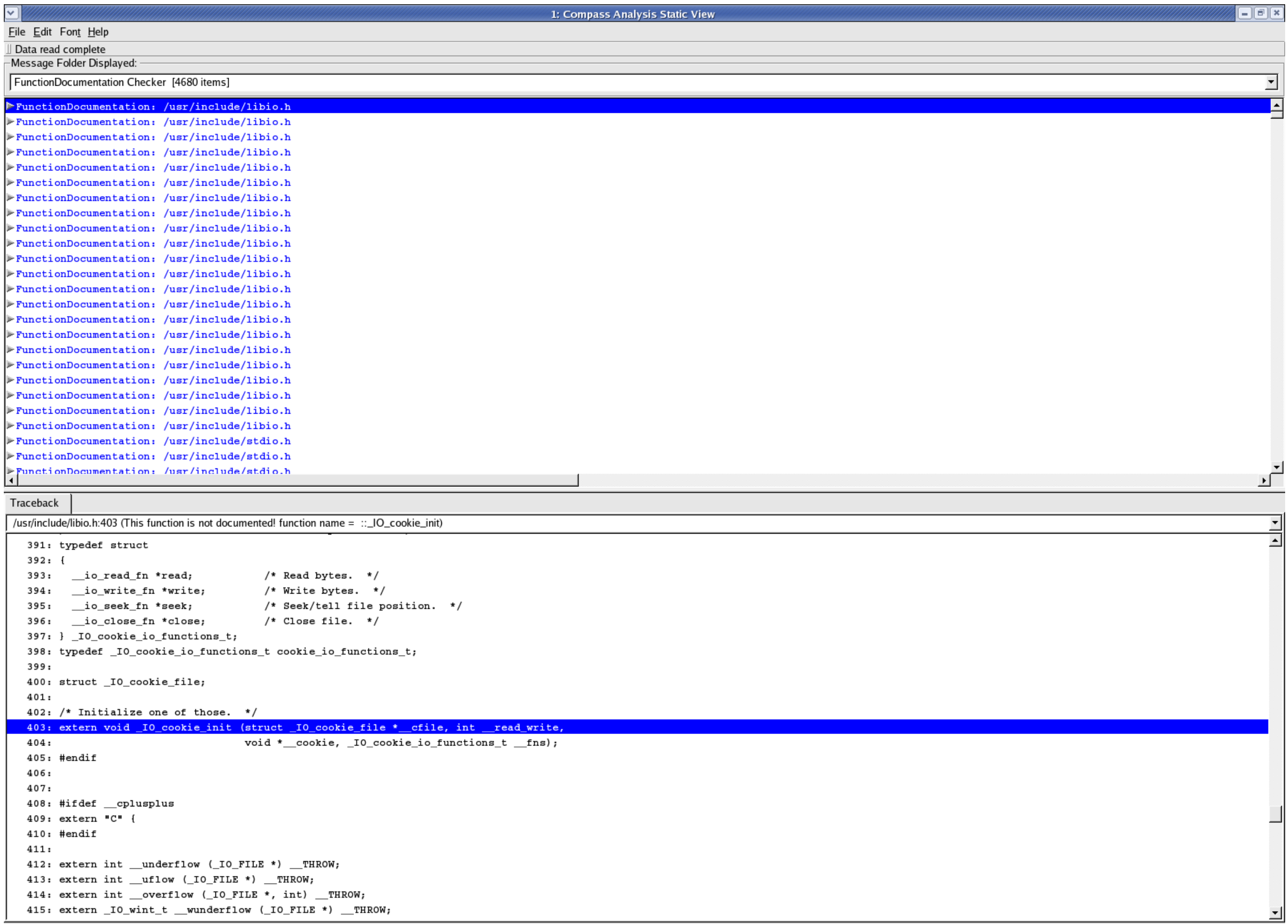

Figure 3.3: Processing of XML Compass output using ToolGear

```
LocalizedVariables: /home/ROSE/projects/compass/tests/Cxx_tests/test2006_117.C:30.5: Variable pmNull does not seem to be used.
FunctionDefinitionPrototype: /home/ROSE/projects/compass/tests/Cxx_tests/test2006_123.C:27.1-10: matching function prototype not availabl
LocPerFunction: /home/ROSE/projects/compass/tests/Cxx_tests/test2006_117.C:23.1-20: This function has too many lines of code :: LOC = 14
MagicNumber: /home/ROSE/projects/compass/tests/Cxx_tests/test2006_117.C:33.14: Occurrence of integer or floating constant.
MagicNumber: /home/ROSE/projects/compass/tests/Cxx_tests/test2006_117.C:36.14: Occurrence of integer or floating constant.
MagicNumber: /home/ROSE/projects/compass/tests/Cxx_tests/test2006_117.C:37.14: Occurrence of integer or floating constant.
FunctionDocumentation: /home/ROSE/projects/compass/tests/Cxx_tests/test2006_123.C:27.1-10: function is not documented: name =  ::main
FunctionDocumentation: /home/ROSE/projects/compass/tests/Cxx_tests/test2006_123.C:9.10: function is not documented: name =  ::X < int , i
FunctionDocumentation: /home/ROSE/projects/compass/tests/Cxx_tests/test2006_123.C:12.10: function is not documented: name =  ::X < int ,
FunctionDocumentation: /home/ROSE/projects/compass/tests/Cxx_tests/test2006_123.C:16.10: function is not documented: name =  ::X < int *
```

Figure 3.4: Example of ASCII output from Compass.

```
; New Compass support for Emacs using version 22 of Emacs and Flymake.
; Comment out these two lines to use older version of emacs.
(require 'flymake)
(setq flymake-allowed-file-name-masks (cons '(".+\\.C\\'" flymake-simple-make-init flymake-simple-cleanup flymake-get-real


(defun flymake-master-make-header-init ()
  (flymake-master-make-init 'flymake-get-include-dirs
    '("\\.C\\'" "\\.c\\'")
    "[ \t]*#[ \t]*include[ \t]*\"\\([[:word:]0-9/\\_.]*%s\\)\""))

(add-hook 'find-file-hook 'flymake-find-file-hook)

(setq flymake-log-level 3)
(setq flymake-no-changes-timeout 0.5)

(defcustom rose-source-tree "/home/dquinlan/ROSE/NEW_ROSE/" "Location of top of ROSE source tree")
(defcustom rose-build-tree "/home/dquinlan/ROSE/ROSE_CompileTree/LINUX-64bit-3.4.6/" "Location of top of ROSE build tree")
(defun add-buildfile-dir-for-rose ()
  (let ((source-dir-name (file-name-directory buffer-file-name)))
    ;(message "%S" `(source dir ,source-dir-name))
    (if
      ; (string-equal rose-source-tree (substring source-dir-name 0 (length rose-source-tree)))
        (string-equal rose-source-tree (substring source-dir-name 0 (min (length source-dir-name) (length rose-source-tree
        (let ((buildfile-dir (concat "../../../../../../../../../../../../../../../../../../../../" rose-build-tree "/" (subs
        ; (message "%S" `(buildfile-dir ,buildfile-dir))
        ; (set-variable 'flymake-buildfile-dirs (cons buildfile-dir flymake-buildfile-dirs) 'local))
          (set-variable 'flymake-buildfile-dirs (append (mapcar (lambda (dir) (concat buildfile-dir "/" dir)) flymake-buil
      (progn
        ;(message "%S" `(bad-prefix))
        source-dir-name))))
(defun set-rose-source-dir (dir) "Set the top of the ROSE source tree to use with Flymake" (interactive "DThe top of the R
  (setq rose-source-tree dir 'local)
  (add-buildfile-dir-for-rose))
(defun set-rose-build-dir (dir) "Set the top of the ROSE build tree to use with Flymake" (interactive "DThe top of the ROS
  (setq rose-build-tree dir 'local)
  (add-buildfile-dir-for-rose))

(add-hook 'find-file-hook 'add-buildfile-dir-for-rose)

;(list "make"
;;  (list "-s" "-C" "/home/dquinlan/ROSE/NEW_ROSE/developersScratchSpace/Dan/EmacsCompass_tests/"
;    (list "-s"
;   (list "-s -C" "`pwd | sed 's@^/home/dquinlan/ROSE/NEW_ROSE/@/home/dquinlan/ROSE/ROSE_CompileTree/LINUX-64bit-3.4.6/@'`
;    (concat "CHK_SOURCES=" source)
;      "SYNTAX_CHECK_MODE=1"
;    "check-syntax"))

(global-set-key [f3] 'flymake-display-err-menu-for-current-line)
(global-set-key [f4] 'flymake-goto-next-error)
```

Figure 3.5: Addition to .emacs when integrating Compass into emacs.

```
one: inc.h one.C
        g++ -c one.C
```

Figure 3.6: Example makefile before the Compass addition

```
one: inc.h one.C
        g++ -c one.C

check-syntax: inc.h one.C
        /path/to/compass/executable/compassMain -c one.C
```

Figure 3.7: Example makefile after addition to support integration of compass

- Add a 'check-syntax' rule to the makefile of the project that you are working on in Compass. This rule should compile all the files you want Compass to check or all files that you are editing with Compass as the compiler.

Figure 3.5 shows the needed changes in .emacs for integrating Compass. The last two lines are the most interesting lines since they introduce two shortkeys. [f3] can be clicked in order to display all errors for the current line while [f4] will move the cursor to the next error.

A short explanation of the code in figure 3.5 is that the first line will require the flymake extension to be available upon loading emacs while the second line will load the find-file-hook and flymake-find-file-hook functions. The "setq" sections that follows runs Compass for all files that are being edited that has the c and C extensions. The "list" section tells flymake to execute the check-syntax rule in the makefile.

Example check-syntax rule

Figure 3.6 shows an example makefile that compiles a file "one.C" using g++. If "one.C" is edited using emacs the addition of the "check-syntax" rule is needed, as shown in figure 3.7.

3.2.2 Using Compass With Vim

Compass can be used with Vim 7's QuickFix commands to display warning messages and highlight the source lines in question. A compass compiler plugin (compass.vim as shown in Figure 3.8) has been provided for Vim to parse the warning messages outputted by Compass.

Steps to make Compass work with Vim 7

- Save compass.vim into .vim/compiler. Create the target directory if it does not exist.
- Download errormarker.vim from http://www.vim.org/scripts/script.php?script_id=1861 and save it into .vim/plugin . Again, create the target directory first when it does not exist.

- Change your Makefile to use an installed compassMain as the compiler to compile your code.
- Use quickfix features of Vim 7 as documented at http://vimdoc.sourceforge.net/htmldoc/quickfix.html. Some frequently used commands are:
  - Specifying the compass plugin to use by typing a command :compiler compass
  - Open your source code using gvim and set the compiler to Compass by
  - Compile you code using compassMain, type :make
  - Display current message, type :cc
  - Display all messages, type :clist
  - Jump to next message, type :cnext

```
" Vim compiler file
" Compiler:     ROSE Compass 0.9.2a
" Maintainer:   Chunhua Liao <liao6@llnl.gov>
" Last Change:  2008 Apr. 3
"
if exists("current_compiler")
  finish
endif
let current_compiler = "compass"

if exists(":CompilerSet") != 2          " older Vim always used :setlocal
  command -nargs=* CompilerSet setlocal <args>
endif

" single line warning
" multiple line warning, %W, %C continue line %Z end of multiple line
CompilerSet errorformat=%s:\ %f:%l%.%c:\ %m,
         \%s:\ %f:%l%.%c-%*\\d:\ %m,
         \%s:\ %f:%l%.%c-%*\\d%.%*\\d:\ %m,
         \\\"%f\"\\,\ line\ %l%*\\D%c%*[^\ ]\ %m
"some notes about the error/warning message format
"Official guide: http://vimdoc.sourceforge.net/htmldoc/quickfix.html#error-file-format
" Each new rule start with a leading \ unless it is the first rule in the
" first line
"  %f: filename %l: line number %c: column number, only one is permitted %m
" actual error/warning message \ :matching a space
"  %*\\d: matching any number
```

Figure 3.8: A compiler plugin for Vim 7 compass.vim

Figure 3.9 shows an example of Compass error messages integrated into Vim 7.

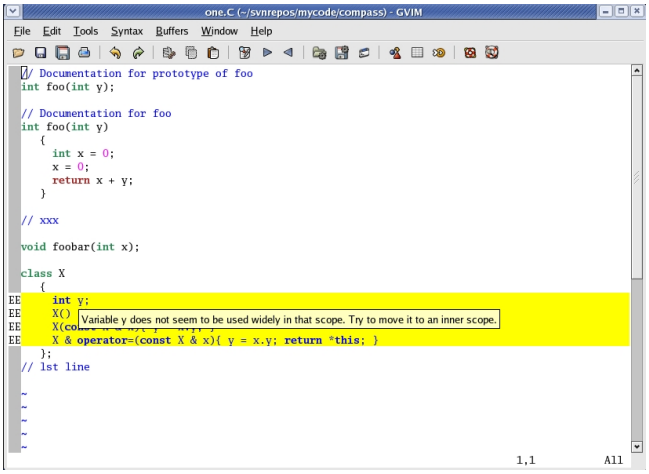

Figure 3.9: Compass error messages integrated into Vim 7

3.3 How To Write A New Checker

3.3.1 Creating A Skeleton

Compass has scripts for creating a skeleton for a new Compass checker. This skeleton can be easily adapted to write all checkers.

Follow these steps to generate a checker skeleton:

1. Enter a directory where you want the directory of your checker to be created
2. Execute `ROSE_SRC_DIR/projects/compass/compass_scripts/gen_checker.sh <name of your checker>`

The results of executing gen_checker.sh script is that a new directory name "multipleCasesOnSameLine" (name of your checker in camel case) is created with the following files:

```
compass.C           multipleCasesOnSameLine.C
compass.h           multipleCasesOnSameLineDocs.tex
compass_parameters  multipleCasesOnSameLine.h
compassTestMain.C   multipleCasesOnSameLine.inc
Makefile            multipleCasesOnSameLineMain.C
Makefile.am         multipleCasesOnSameLineTest1.C
```

Some of these files (compass.[Ch], compass_parameters, and compassTestMain.C) are copied from the compass_template_generator directory; while others are generated (multiple*, Makefile, Makefile.am)

It is suggested that you keep the following in mind when using gen_checker.sh:

- It is advised that you do not invoke the script gen_checker with words like checker, detector, tester, etc. Adding these verbs at the command line means that these words are added as suffixes into the directory-name. Which will make it redundant, as the compass project is about writing style-checkers!
- Some of the files have read-only permissions and are intended only for such use. Please do not change the permissions of these files.
- Advanced: The file 'multipleCasesOnSameLine.inc' is used to pass in custom LDADD lines to the Make environment on a per checker basis. The LDADD line specified in this file will be added verbatim to the compass makefile.

3.3.2 Integrating New Checkers Into Compass

The process for integrating a new checker into Compass has been automated. These directions are meant for checkers generated using gen_checker.sh.

The steps to integrate a new checker is

1. Create a tar file of the directory tar -zcvf <name of your checker>.tar.gz <name of your checker>

2. Add <name of your checker> to CHECKER_LIST
3. Copy <name of your checker>.tar.gz to ROSE_SRC_DIR/projects/compass/compassRepository/
4. Enter ROSE_BUILD_DIR/projects/compass/
5. Execute 'make regenerate'
6. After running 'make regenerate' in the build tree then you may run make as usual.
7. Examine the RULE_SELECTION file in projects/compass such that it reflects your most recent additional checker(s) choice of execution at runtime; the default setting is "on". Please refer to section 3.5.

In the Makefile, the compass_submission_setup.sh handles adding/updating a Compass checker into an existing Compass source tree. "regenerate" is an argument that instructs the script to perform a read-only operation on the file CHECKER_LIST in your projects/compass directory. This file contains a list of checkers that will be integrated by compass_submission_setup.sh.

The file 'CHECKER_LIST' can use the '#' comment delimiter at the beginning of any checker name to remove that checker from compilation. The hash mark may only appear at the beginning of the line. The compass_submission_setup.sh script must be run again with the "regenerate" option if any checkers are commented out. **Note that no space is permitted between the '#' and the name of the checker.**

As stated previously, the compass_submission_setup.sh script handles adding/updating Compass checkers into the compass source tree (usually located at ROSE/projects/compass). It does this by generating the necessary files to compile Compass with the checkers located in <COMPASS SUBMIT DIR>. These files are:

- **CHECKER_LIST**: a file that keeps a running list of all checkers seen by compass_submission_setup.sh.
- **$CHECKER/$CHECKER.makefile**: An individual Make file is generated per checker in its directory such that it may be separated for individual development before being reincorporated with Compass.

The $CHECKER.makefile file is generated such that any checker may be copied out of the source tree projects/compass and worked on separately. This feature speeds up development of single checkers as is removes the requirement to rebuild the entire compassMain tool.

Many automatically generated files required for the build of Compass are generated in the build tree. Rules for the generation of these files are found in the automake Makefile.am file in the Compass source tree directory projects/-compass. These file include:

- **CHECKER_LIST_WITHOUT_COMMENTS**: a version of CHECKER_LIST that expands in two columns those checkers built as part of Compass in camel case starting with a lower-case letter and an upper-case letter respectively.

- **compass_makefile.inc**: a Make include file that sets the Make environment with the information for each checker. This environment specifies the rules needed to compile each checker object, make the documentation, and test all checkers together or separately. **compass_makefile.inc**: provides the following Make rules: (note ${CHECKER} is the name of a checker directory i.e. doNotDeleteThis)
  - **docs**: makes the documentation
  - test${CHECKER}: tests a single checker, a single rule is provided per checker.
  - testAllCheckersSeparately: tests all checkers separately as a batch.
  - archive${CHECKER}: – tar & gzips a single checker directory in projects/compass/${CHECKER} to projects/compass/compassRepository/${CHECKER}.tar.gz
  - archiveCheckers: archives all checkers (uncommented in CHECKER_LIST) projects/compass to projects/compass/compassRepository/${CHECKER}.tar.gz
- **checkers.h**: An automatically generated file needed by compassMain.C that contains a list of #include directives for each checker header .h file.
- **buildCheckers.C**: An automatically generated source file needed by compassMain.C to build the Compass checker traversals.
- **compassCheckerDocs.tex**: A Latex include file that inputs each checker .tex documentation file into the compass.tex document.
- **compass_parameters**: The concatentation of individual checker parameter files to be used with compassMain.

3.4 Including/Excluding Checkers in the Compass Build Process

This section describes how to select which of the checkers to integrate into Compass out of all the checkers available in source form in the Compass source directory. For security reasons Compass uses this static build process since it is a central goal of Compass that it should run as a trusted part of a project's build process. If the integration of checkers had been automatic through a dynamic plugin mechanism it would be hard to ensure that the dynamic list of checkers was secure, but for a static list of trusted checkers this is possible.

In order to integrate a checker into Compass the user must:

- Add the name of the checkers directory in the CHECKER_LIST in the compass source directory
- Run `make regenerate` in the Compass build directory

If a user or developer intends to integrate a new checker into the Compass source tree refer to section 3.3.2.

Usually the CHECKER_LIST is only modified when a user or developer wants to add a new checker or select a subset of trusted checkers. Checkers can be commented out using a `#`, no space is allowed between the `#` and the checker name.

3.5 Including/Excluding Checkers During Compass Execution

This section describes how to execute a subset of the checkers provided in the build process (see section 3.4). This process is significantly more interactive than defining what checkers to include in the Compass build process. Since it is not unheard of that rules implemented by different checkers can be mutually exclusive or even contradicting this mechanism is essential for selecting the subset of checkers that are interesting for a specific program that is checked. Separate projects of developers could easily have their own RULE_SELECTION file to permit high levels of customization in the use of a Compass tool containing a large number of checkers (e.g. for different languages).

When used with the Emacs interface this provides a simple way to turn on and off specific checkers by editing a single file (RULE_SELECTION). The name of this file is specified in the `compass_parameters` file, this name may be changed. The directories searched are: current directory, user home directory, and Compass source tree (respectively).

```
Compass.RuleSelection=RULE_SELECTION
```

In order to select a checker to run the user must:

- Add a line '-:<name of checker>' in a file called RULE_SELECTION.
- If a line '-:<name of checker>' already exist the '-' can be modified into a '+' to enable the checker or into a '-' to disable a checker.

It is required that every checker integrated into the Compass build is mentioned in the RULE_SELECTION.

3.6 Including/Excluding Paths and Filenames with Compass

Compass permits paths and filenames to be specified for inclusion/exclusion in reporting checker rule violations. Run `compassMain --help` to see the commandline options. Numerous other commandline options provided for all tools build using ROSE may also be relevant.

3.7 Checking Security Properties of Checkers

Compass is designed for extensibility while providing the security for the codes being checked. To support this Compass provides a simple mechanism for verifying specific properties of the checkers used in Compass. Compass implements

a specific small number of checkers that are used for checking the checkers in Compass. The directory compassVerify contains the implementation of this subset of Compass that is used on itself. These checkers may not be modified and in the future MD-5 checksums will be provided to ensure the integrity of this subset of Compass. To verify the compass checkers run:

- `make verify`
  This makefile rule runs the compassVerify/compassMain on all the source files in all the checkers directories in Compass. Because it runs compass on so many separate files this step can take a long time.

- Or `make oneBigVerify`
  The makefile rule runs the compassVerify/compassMain on a single generated file built from all the checker source files and is particularly quick to run.

3.8 Testing Compass and its Checkers

The `tests` directory contains directories of tests that are language specific:

- C_tests
  This directory contains a Makefile which will use the ROSE C test codes to test Compass.

- Cxx_tests
  This directory contains a Makefile which will use the ROSE C++ test codes to test Compass.

To run these tests type `make check` at any level on the Compass directory hierarchy of the build tree.

Chapter 4

Compass Checkers

4.1 Allocate And Free Memory In The Same Module At The Same Level Of Abstraction

Allocating and freeing memory in different modules and levels of abstraction burdens the programmer with tracking the lifetime of that block of memory. This may cause confusion regarding when and if a block of memory has been allocated or freed, leading to programming defects such as double-free vulnerabilities, accessing freed memory, or writing to unallocated memory.

To avoid these situations, it is recommended that memory be allocated and freed at the same level of abstraction, and ideally in the same code module.

The affects of not following this recommendation are best demonstrated by an actual vulnerability. Freeing memory in different modules resulted in a vulnerability in MIT Kerberos 5 MITKRB5-SA-2004-002 . The problem was that the MIT Kerberos 5 code contained error-handling logic, which freed memory allocated by the ASN.1 decoders if pointers to the allocated memory were non-NULL. However, if a detectable error occured, the ASN.1 decoders freed the memory that they had allocated. When some library functions received errors from the ASN.1 decoders, they also attempted to free, causing a double-free vulnerability.

4.1.1 Parameter Requirements

No Parameter specifications.

4.1.2 Implementation

No implementation yet!

4.1.3 Non-Compliant Code Example

This example demonstrates an error that can occur when memory is freed in different functions. The array, which is referred to by list and its size, number, are then passed to the verify_list() function. If the number of elements in the array is less than the value MIN_SIZE_ALLOWED, list is processed. Otherwise, it is assumed an error has occurred, list is freed, and the function returns. If the error occurs in verify_list(), the dynamic memory referred to by list will be freed twice: once in verify_list() and again at the end of process_list().

```
1
2  int verify_size(char *list, size_t list_size) {
3    if (size < MIN_SIZE_ALLOWED) {
4      /* Handle Error Condition */
5      free(list);
6      return -1;
7    }
8    return 0;
9  }
10
11 void process_list(size_t number) {
12   char *list = malloc(number);
13
14   if (list == NULL) {
15     /* Handle Allocation Error */
16   }
17
18   if (verify_size(list, number) == -1) {
```

```
19      /* Handle Error */
20
21    }
22
23    /* Continue Processing list */
24
25    free(list);
26  }
27
```

4.1.4 Compliant Solution

To correct this problem, the logic in the error handling code in verify_list() should be changed so that it no longer frees list. This change ensures that list is freed only once, in process_list().

```
1
2  int verify_size(char *list, size_t list_size) {
3    if (size < MIN_SIZE_ALLOWED) {
4      /* Handle Error Condition */
5      return -1;
6    }
7    return 0;
8  }
9
10 void process_list(size_t number) {
11   char *list = malloc(number);
12
13   if (list == NULL) {
14     /* Handle Allocation Error */
15   }
16
17   if (verify_size(list, number) == -1) {
18     /* Handle Error */
19   }
20
21   /* Continue Processing list */
22
23   free(list);
24 }
25
```

4.1.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Write your checker algorithm

4.1.6 References

ISO/IEC9899-1999 MEM00-A. Allocate and free memory in the same module, at the same level of abstraction

4.2 Assignment Operator Check Self

This test checks to make sure that the first statement in a assignment operator is a check for self-assignment. As noted in An Abbreviated C++ Code Inspection Checklist 12.1.3 . This will save time allocating new memory and (hopefully) deleting the previous copy. The check for return this; is handled by another checker.

4.2.1 Parameter Requirements

No parameters required.

4.2.2 Implementation

This test checks to make sure that the first statement in a assignment operator is a check for self-assignment. As noted in An Abbreviated C++ Code Inspection Checklist 12.1.3 . This will save time allocating new memory and (hopefully) deleting the previous copy. The check for return this; is handled by another checker.

4.2.3 Non-Compliant Code Example

```
1
2 class bike
3 {
4 public:
5  const bike& operator= (const bike& other);
6 };
7
8 const bike& bike::operator= (const bike& other)
9 {
10 ...
11 return *this;
12 }
13
```

4.2.4 Compliant Solution

```
1
2 const bike& bike::operator= (const bike& other)
3 {
4 if (this == &other)
5     {return *this;
6     }
7 ...
8 return *this;
9 }
10
```

4.2.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Identify member function
2. Check name for operator=
3. Check first statement as If Statement
4. Check arguments to expression to be this and the right hand argument.

4.2.6 References

Abbreviated Code Inspection Checklist Section 12.1.3, Assignment Operator"

4.3 Assignment Return Const This

Here we check to make sure that all assignment operators (operator=) return const classType&. By making the return a reference we can use a = b = c; which is legal C++. By making the reference const we prevent (a = b) = c; which is illegal C++.

4.3.1 Parameter Requirements

No parameters necessary.

4.3.2 Implementation

Every member function is checked to see if the name matches 'operator='. If so we check to make sure the return type is const nameofclass&. All three (const, ref, classname) must be present. We then make sure there is at least one explicit return of *this and no explicit returns of anything else. Note: At this time we do not make sure that all paths must reach an explicit return. This is, however, already a warning in ROSE when there is not an explicit return for a non-void returning function. There is also another checker to ensure explicit returns.

4.3.3 Non-Compliant Code Example

```
1
2 class smallCat
3 {
4 smallCat& operator=(smallCat& other);
5 }
6
7 smallCat& smallCat::operator=(smallCat& other)
8 {
9 ...
10 }
11
```

4.3.4 Compliant Solution

```
1
2 class smallCat
3 {
4 const smallCat& operator=(smallCat& other);
5 }
6
7 const smallCat& smallCat::operator=(smallCat& other)
8 {
9 ...
10 }
```

4.3.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Identify member function
2. Check Name for operator=
3. Get return type
4. check for typename and const
5. find explicit return and check for this.

4.3.6 References

Abbreviated Code Inspection Checklist Section 12.1.4, Assignment Operator"

4.4 Asynchronous Signal Handler

Namespace: `AsynchronousSignalHandler`

4.4.1 Introduction

No introduction yet!

No reference to literature as yet!

4.4.2 Parameter Requirements

No Parameter specifications yet!

4.4.3 Implementation

No implementation yet!

4.4.4 Example of Failing Output Code

See example: asynchronousSignalHandlerTest1.C

```
#include <stdio.h>
#include <stdlib.h>
#include <signal.h>
#include <string.h>

// Included to get sleep() function
#include <unistd.h>

char *err_msg;
volatile sig_atomic_t e_flag = 0;

void nonAsyncSafeFunction();

void handler(int signum) {
  signal(signum, handler);

// This function is NOT on the async-safe list and IS reported (line 19)
  nonAsyncSafeFunction();

// This function is on the async-safe list and is NOT reported (line 22)
  sleep(1);

  e_flag = 1;
}

int main(void) {
  signal(SIGINT, handler);

  err_msg = (char*) malloc(24);
  if (err_msg == NULL) {
    /* handle error condition */
  }

  strcpy(err_msg, "No errors yet.");

  /* main code loop */
  if (e_flag) {
    strcpy(err_msg, "SIGINT received.");
```

```
    }

    return 0;
}
```

4.5 Avoid Using The Same Handler For Multiple Signals

It is possible to safely use the same handler for multiple signals, but doing so increases the likelihood of a security vulnerability. The delivered signal is masked and is not delivered until the registered signal handler exits. However, if this same handler is registered to handle a different signal, execution of the handler may be interrupted by this new signal. If a signal handler is constructed with the expectation that it cannot be interrupted, a vulnerability might exist. To eliminate this attack vector, each signal handler should be registered to handle only one type of signal.

4.5.1 Parameter Requirements

No Parameter specifications.

4.5.2 Implementation

No implementation yet!

4.5.3 Non-Compliant Code Example

This non-compliant program registers a single signal handler to process both SIGUSR1 and SIGUSR2. The variable sig2 should be set to one if one or more SIGUSR1 signals are followed by SIGUSR2.

```
1
2 #include <signal.h>
3 #include <stdlib.h>
4 #include <string.h>
5
6 volatile sig_atomic_t sig1 = 0;
7 volatile sig_atomic_t sig2 = 0;
8
9 void handler(int signum) {
10   if (sig1) {
11      sig2 = 1;
12   }
13   if (signum == SIGUSR1) {
14     sig1 = 1;
15   }
16 }
17
18 int main(void) {
19   signal(SIGUSR1, handler);
20   signal(SIGUSR2, handler);
21
22   while (1) {
23     if (sig2) break;
24     sleep(SLEEP_TIME);
25   }
26
27   /* ... */
28
29   return 0;
30 }
31
```

The problem with this code is that there is a race condition in the implementation of handler(). If handler() is called to handle SIGUSR1 and is interrupted

to handle SIGUSR2, it is possible that sig2 will not be set. This non-compliant code example also violates SIG31-C. Do not access or modify shared objects in signal handlers.

4.5.4 Compliant Solution

This compliant solution registers two separate signal handlers to process SIGUSR1 and SIGUSR2. The sig1_handler() handler waits for SIGUSER1. After this signal occurs, the sig2_handler() is registered to handle SIGUSER2. This solution is fully compliant and accomplishes the goal of detecting whether one or more SIGUSR1 signals are followed by SIGUSR2.

```
1
2 #include <signal.h>
3 #include <stdlib.h>
4 #include <string.h>
5
6 volatile sig_atomic_t sig1 = 0;
7 volatile sig_atomic_t sig2 = 0;
8
9 void sig1_handler(int signum) {
10   sig1 = 1;
11 }
12
13 void sig2_handler(int signum) {
14   sig2 = 1;
15 }
16
17 int main(void) {
18   signal(SIGUSR1, handler);
19
20   while (1) {
21     if (sig1) break;
22     sleep(SLEEP_TIME);
23   }
24
25   signal(SIGUSR2, handler);
26   while (1) {
27     if (sig2) break;
28     sleep(SLEEP_TIME);
29   }
30
31   /* ... */
32
33   return 0;
34 }
35
```

4.5.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Write your checker algorithm

4.5.6 References

ISO/IEC 03 SIG00-A. Avoid using the same handler for multiple signals

4.6 Boolean Is Has

This checker makes sure that all boolean variables and functions that return a boolean are all named following the convention 'is_" or 'has_" per the ALE3D manual.

4.6.1 Parameter Requirements

No parameters required.

4.6.2 Implementation

This implementation checks to see if a function returns a boolean, if so it checks the first 4 characters in the name of the function for 'is_" or 'has_". It also checks all variable declarations, checks for boolean type, then does the same substring match on its name.

4.6.3 Non-Compliant Code Example

```
1
2 bool chosen_poorly ()
3 {
4 return true;
5 }
6
7 int main()
8 {
9 bool badly_named;
10 return 0;
11 }
12
```

4.6.4 Compliant Solution

```
1
2 bool has_chosen_poorly ()
3 {
4 return true;
5 }
6
7 int main()
8 {
9 bool is_badly_named;
10 return 0;
11 }
12
13
14
```

4.6.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. finds bool declarations or bool return function declarations

2. checks name

4.6.6 References

ALE3D Section ??.?, Booleans”

4.7 [No Reference] Buffer Overflow Functions

This analysis detects possible buffer overflows due to the usage of 'unsafe' function calls. The results need to be either inspected by the user or if applicable, unsafe function calls can be exchanged against their safe counterparts.

4.7.1 Non-Compliant Code Examples

```
1 #include <stdio.h>
2 #include <string.h>
3
4 using namespace std;
5
6 void fail() {
7   char string[50];
8   int file_number = 0;
9   sprintf( string, "file.%d", file_number );
10
11  char result[100];
12  float fnum = 3.14159;
13  sprintf( result, "%f", fnum );
14
15
16  char str1[]="Sample string";
17  char str2[40];
18  char str3[40];
19  memcpy (str2,str1,strlen(str1)+1);
20  memcpy (str3,"copy successful",16);
21  printf ("str1: %s\nstr2: %s\nstr3: %s\n",str1,str2,str3);
22
23 }
```

4.7.2 Compliant Solution

Example as above; use snprintf instead of sprintf.

4.7.3 Parameter Requirements

None.

4.7.4 Implementation

The following functions are checked for

- sprintf
- scanf
- sscanf
- gets
- strcpy
- _mbscpy
- lstrcat
- memcpy
- strcat

4.7.5 References

Foster , "James C.Foster, Vitaly Osipov, Nish Bhalla, Niels Heinen, Buffer Overflow Attacks, ISBN 1-932266-67-4, p. 211"

4.8 Secure Coding : EXP04-A. Do not perform byte-by-byte comparisons between structures

Structures may be padded with data to ensure that they are properly aligned in memory. The contents of the padding, and the amount of padding added is implementation defined. This can can lead to incorrect results when attempting a byte-by-byte comparison between structures.

4.8.1 Non-Compliant Code Example

This example uses `memcmp()` to compare two structures. If the structures are determined to be equal, `buf_compare()` should return 1 otherwise, 0 should be returned. However, structure padding may cause `memcmp()` to evaluate the structures to be unequal regardless of the contents of their fields.

```
1 struct my_buf {
2   size_t size;
3   char buffer[50];
4 };
5
6 unsigned int buf_compare(struct my_buf *s1, struct my_buf *s2) {
7   if (!memcmp(s1, s2, sizeof(struct my_struct))) {
8     return 1;
9   }
10  return 0;
11 }
12
```

4.8.2 Compliant Solution

To accurately compare structures it is necessary to perform a field-by-field comparison [Summit 95]. The `buf_compare()` function has been rewritten to do this.

```
1 struct my_buf {
2   size_t size;
3   char buffer[50];
4 };
5
6 unsigned int buf_compare(struct buffer *s1, struct buffer *s2) {
7   if (s1->size != s2->size) return 0;
8   if (strcmp(s1->buffer, s2->buffer) != 0) return 0;
9   return 1;
10 }
11
```

4.8.3 Risk Assessment

Failure to correctly compare structure can lead to unexpected program behavior.

Rule	Severity	Likelihood	Remediation Cost	Priority	Level
EXP04-A	**2** (medium)	**1** (unlikely)	**1** (high)	**P2**	**L3**

Related Vulnerabilities

Search for vulnerabilities resulting from the violation of this rule on the CERT website .

4.8.4 References

[Dowd 06] Chapter 6, "C Language Issues" (Structure Padding 284-287) [ISO/IEC 9899-1999] Section 6.7.2.1, "Structure and union specifiers" [Kerrighan 88] Chapter 6, "Structures" (Structures and Functions 129) [Summit 95] comp.lang.c FAQ list - Question 2.8

4.9 Char Star For String

This checker will report when STL strings are used.

4.9.1 Parameter Requirements

The checker does not take any parameters.

4.9.2 Implementation

The checker finds variables declarations, function arguments and typedefs of string type. The string type may be of pointer type, reference type, array type or it can be modified without any problems.

4.9.3 Non-Compliant Code Example

```
1 #include <string>
2
3 typedef std::string string2;
4 void bar(std::string arg1){
5
6 };
7
8 int main(){
9    std::string  foo1;
10   std::string* foo2;
11   std::string  foo4[4];
12
13 };
```

4.9.4 Compliant Solution

```
1 typedef char* string2;
2 void bar(char* arg1){
3
4 };
5
6 int main(){
7    char*  foo1;
8    char** foo2;
9    char   foo4[4];
10 };
```

4.9.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Traverse the AST
2. If a variable declaration, functions argument or typedef has a string base type report an error.

4.9.6 References

The ALE3D style guide section 16.2 states that C strings must be used instead of STL strings due to portability problems.

4.10 Comma Operator

The comma operator is commonly considered confusing without any redeeming value. This checker makes sure that it is not used. It reports any use of the built-in comma operator and any declaration of an overloaded comma operator.

4.10.1 Parameter Requirements

This checker does not require any parameters.

4.10.2 Non-Compliant Code Example

```
1 int f_noncompliant(int n)
2 {
3     return (n++, n++, n); // not OK (twice): comma operator
4 }
```

4.10.3 Compliant Solution

```
1 int f_compliant(int n)
2 {
3     n++;
4     n++;
5     return n;
6 }
```

4.10.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers identifying any appearance of the built-in comma operator and any declaration of a function overloading the comma operator.

4.10.5 References

A reference to this pattern is: The Programming Research Group: “High-Integrity C++ Coding Standard Manual”, Item 10.19: “Do not use the comma operator.”

4.11 [No Reference] : Loc Per Function

This analysis detects for each function the amount of lines of code (LOC) and checks the value against a user defined max value. If LOC > max value, then an exception is triggered.

4.11.1 Non-Compliant Code Examples

```
1 // if LocPerFunction.Size = 2
2 void fail() {
3   int x;
4   x = 5;
5   x = 5;
6   x = 5;
7 }
```

4.11.2 Compliant Solution

```
1 // if LocPerFunction.Size = 2
2 void pass() {
3   int x;
4   x = 5;
5   x = 5;
6 }
```

4.11.3 Parameter Requirements

LocPerFunction.Size defines the max value for a permissive LOC.

4.11.4 Implementation

The simple implementation of this checker is defined below:

```
1   if (isSgFunctionDeclaration(sgNode)) {
2     SgFunctionDeclaration* funcDecl = isSgFunctionDeclaration(sgNode);
3     SgFunctionDefinition* funcDef = funcDecl->get_definition();
4     if (funcDef) {
5       Sg_File_Info* start = funcDef->get_body()->get_startOfConstruct();
6       Sg_File_Info* end = funcDef->get_body()->get_endOfConstruct();
7       ROSE_ASSERT(start);
8       ROSE_ASSERT(end);
9       int lineS = start->get_line();
10      int lineE = end->get_line();
11      loc_actual = lineE-lineS;
12      if (loc_actual>loc) {
13        output->addOutput(new CheckerOutput(funcDef));
14      }
15    }
16  }
```

4.11.5 References

4.12 [No Reference] Computational Functions

This analysis computes the amount of floating point, integer, floating point pointer and integer pointer operations within each function. If the value is larger than specified, than a warning is triggered. The analysis helps to identify functions with high computatuional value.

4.12.1 Non-Compliant Code Examples

```
1 void fail() {
2   int x=4;
3   int y=x+5+7;
4   int *z = &x;
5   y = *z+*z+6+8+9;
6 }
```

4.12.2 Compliant Solution

```
1 void pass() {
2   int x= 4;
3   int y = x+5+7;
4 }
```

4.12.3 Parameter Requirements

computationalFunctions.maxIntOps defines the maximum of integer operations permitted. computationalFunctions.maxFloatOps defines the maximum of floating point operations permitted.

4.12.4 Implementation

The implementation checks for the following direct types:

- SgAddOp
- SgSubtractOp
- SgDivideOp
- SgMultiplyOp

The implementation checks for the following indirect types:

- SgCastExp - operations hidden behind cast
- SgVarRefExp - variable operations
- SgPointerDerefExp - pointer operations
- SgPntrArrRefExp - array operations

4.12.5 References

4.13 Const Cast

Casting the constness away should never be done.

Casting away constness via const_cast is just plain false advertising. If a member function's signature is void someFunc(const foo& arg); then the function advertises to it's clients that it will not call any non-const member functions on the arg. Casting the constness of arg away to allow the use of non-const member functions can create unexpected results for clients of this function.

4.13.1 Parameter Requirements

No paramaters are needed.

4.13.2 Implementation

The checker inspects every cast in the AST. If the type casted to is equal to the type casted from minus the const-modifier it is an error.

4.13.3 Non-Compliant Code Example

```
1  void foo(){
2     const int x = 2;
3     int y = (int) x;
4  }
```

4.13.4 Compliant Solution

```
1  void foo(){
2     int x = 2;
3     int y = x;
4  }
5
```

4.13.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Traversee the AST
2. If a cast expression casts away constness report an error.

4.13.6 References

ALE3D Style Guide section 14.4.

4.14 Constructor Destructor Calls Virtual Function

C++ Coding Standards, states that:

> Virtual functions only "virtually" always behave virtually: Inside constructors and destructrors, they don't. Worse, any direct or indirect call to an unimplemented *pure virtual* function from a constructor or destructor results in undefined behavior. If your design wants virtual dispatch into a derived class from a base class constructor or destructor, you need other techniques such as post-constructors.

4.14.1 Parameter Requirements

This checker takes no parameters and inputs source file

4.14.2 Implementation

This pattern is checked using a nested AST traversal in which the top level traversal seeks out definitions of constructors and destructors and two nested traversals seek out calls to virtual functions of member functions and non-member functions respectively.

4.14.3 Non-Compliant Code Example

The following code calls a virtual function from a public constructor. This is a contrived trivial example.

```
1  class Class
2  {
3    int n;
4
5    public:
6      Class() { n = Classy(); } //constructor
7      ~Class() {} //Destructor
8
9      virtual int Classy() { return 1; }
10 }; //class Class
11
12 int main()
13 {
14   Class c;
15   return 0;
16 } //main()
```

4.14.4 Compliant Solution

```
1  class Class
2  {
3    int n;
4
5    public:
6      Class() { n = 1; } //constructor
7      ~Class() {} //Destructor
8  }; //class Class
9
10 int main()
11 {
```

```
12   Class c;
13   return 0;
14 } //main()
```

4.14.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform a AST traversal visiting class constructors and destructors.
2. Flag any calls to virtual functions in class constructor or destructor nodes.
3. Report any violations.

4.14.6 References

Alexandrescu A. and Sutter H. *C++ Coding Standards 101 Rules, Guidelines, and Best Practices*. Addison-Wesley 2005.

4.15 Secure Coding : STR05-A. Prefer making string literals const-qualified

String literals are constant and should consequently be protected by the `const` qualification. This recommendation supports rule STR30-C. Do not attempt to modify string literals .

4.15.1 Non-Compliant Code Example

In the following non-compliant code, the `const` keyword has been omitted.

```
1 char *c = "Hello";
2
```

If a statement such as `c[0] = 'C'` were placed following the above declaration, the code would likely still compile cleanly, but the result of the assignment is undefined as string literals are considered constant.

4.15.2 Compliant Solution 1

In this compliant solution, the characters referred to by the pointer `c` are `const`-qualified, meaning that any attempts to assign them to different values is an error.

```
1 char const *c = "Hello";
2
```

4.15.3 Compliant Solution 2

In cases where the string is meant to be modified, use initialization instead of assignment. In this compliant solution, `c` is a modifiable `char` array which has been initialized using the contents of the corresponding string literal.

```
1 char c[] = "Hello";
2
```

Thus, a statement such as `c[0] = 'C'` is valid and will do what is expected.

4.15.4 Non-Compliant Code Example 1

Although this code example is not compliant with the C99 Standard, it executes correctly if the contents of `CMUfullname` are not modified.

```
1 char *CMUfullname = "Carnegie Mellon University";
2 char *school;
3
4 /* Get school from user input and validate */
5
6 if (strcmp(school, "CMU")) {
7     school = CMUfullname;
8 }
9
```

4.15.5 Non-Compliant Code Example 2

Adding in the `const` keyword will likely generate a compiler warning, as the assignment of `CMUfullname` to `school` discards the `const` qualifier. Any modifications to the contents of `school` after this assignment will lead to errors.

```
1 char const *CMUfullname = "Carnegie Mellon University";
2 char *school;
3
4 /* Get school from user input and validate */
5
6 if (strcmp(school, "CMU")) {
7     school = CMUfullname;
8 }
9
```

4.15.6 Compliant Solution

The compliant solution uses the `const` keyword to protect the string literal, as well as using `strcpy()` to copy the value of `CMUfullname` into `school`, allowing future modification of `school`.

```
1 char const *CMUfullname = "Carnegie Mellon University";
2 char *school;
3
4 /* Get school from user input and validate */
5
6 if (strcmp(school, "CMU")) {
7     /* Allocate correct amount of space for copy */
8     strcpy(school, CMUfullname);
9 }
10
```

4.15.7 Risk Assessment

Modifying string literals causes undefined behavior, resulting in abnormal program termination and denial-of-service vulnerabilities.

Rule	Severity	Likelihood	Remediation Cost	Priority	Level
STR05-A	**1** (low)	**3** (likely)	**2** (medium)	**P6**	**L3**

Related Vulnerabilities

Search for vulnerabilities resulting from the violation of this rule on the CERT website .

http://www.open-std.org/jtc1/sc22/wg21/docs/papers/1993/N0389.asc [ISO/IEC 9899-1999:TC2] Section 6.7.8, "Initialization" [Lockheed Martin 2005] Lockheed Martin. Joint Strike Fighter Air Vehicle C++ Coding Standards for the System Development and Demonstration Program. Document Number 2RDU00001, Rev C. December 2005. AV Rule 151.1

4.16 Control Variable Test Against Function

This checker detects if there exists a for loop that tests its control (induction) variable against a function. One can get better performance by pulling out the function call before the loop and use a constant value for the test. That is,

```
1  for(int i = 0; i < constSize(); ++i)
2  { // do something }
```

The code above can be improved as the following:

```
1  const int size = constSize();
2  for(int i = 0; i < size; ++i)
3  { // do something }
```

4.16.1 Parameter Requirements

None

4.16.2 Implementation

This checker uses a simple traversal. For every `for` statement, the checker examines whether or not there is a function call inside the test expression.

4.16.3 Non-Compliant Code Example

```
1 int bar();
2
3 void foo()
4 {
5   int j=2;
6
7   for(int i = 0; i < bar(), j < 10; ++i)
8   {
9     j += 2;
10  }
11 }
```

4.16.4 Compliant Solution

```
1 int bar();
2
3 void foo()
4 {
5   int j=2;
6
7   for(int i = 0; i < 10; ++i)
8   {
9     j += 3;
10  }
11 }
```

4.16.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Check if a node is a for statement
2. Check if the test expression for the for statement contains a function call

4.16.6 References

The Programming Research Group, High-Integrity C++ Coding Standard Manual, Item 5.7: "The control variable in a for loop should be tested against a constant value, not a function"

4.17 Copy Constructor Const Arg

This checks whether the copy constructor for a class uses a const reference as an argument. This should always be the case as a copy constructor should never change its input argument and a reference is necessary to avoid needing a copy operator.

4.17.1 Parameter Requirements

No Parameter necessary.

4.17.2 Implementation

This checker begins by finding class declarations and getting the class name. It then runs through each member of the class until finding a constructor. It checks if the constructor has one argument and that argument is a member of the same class. If it is and it is not const a message is returned.

4.17.3 Non-Compliant Code Example

```
1
2 class interviewer
3 {
4 interviewer(interviewer other) {return;}
5 }
6
```

4.17.4 Compliant Solution

```
1
2 class interviewer
3 {
4 interviewer(const interviewer& other) {return;}
5 }
6
```

4.17.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Identify member function
2. check args for copy constructor
3. ensure type and const
4. if not both, return notification

4.17.6 References

Abbreviated Code Inspection Checklist Section 12.1.2, Copy Constructor"

4.18 Cpp Calls Setjmp Longjmp

The Elements of C++ Style state that:

> [The setjmp() and longjmp()] functions provide exception handling for C programs. You cannot safely use these functions in C++ code because the exception-handling mechanism they implement does not respect normal object lifecycle semantics–a jump will not result in destruction of scoped, automatically allocated objects.

4.18.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.18.2 Implementation

This pattern is checked using a simple AST traversal that seeks out calls to setjmp() and longjmp() in source files without the ".c" extension. These nodes are flagged as violations.

4.18.3 Non-Compliant Code Example

This contrived trivial example calls setjmp() and longjmp() in C++ code

```
1 #include <setjmp.h>
2
3 int main()
4 {
5   jmp_buf env;
6   my_container c1;
7   int i = setjmp(env);
8
9   if( i != 0 ) exit( 1 );
10
11  int err = c1.clear();
12
13  if( err != 0 ) longjmp( env, 1 );
14
15  return 0;
16 }
```

4.18.4 Compliant Solution

The compliant solution uses C++ exception handling.

```
1 int main()
2 {
3   my_container c1;
4
5   try
6   {
7     c1.clear();
8   }
9   catch(...)
10  {
11    exit( 1 );
12  }
13
14  return 0;
15 }
```

4.18.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform simple AST traversal visiting function reference codes.
2. Flag all function references named `setjmp()` or `longjmp()` as violations.
3. Report all violations.

4.18.6 References

Bumgardner G., Gray A., and Misfeldt T. *The Elements of C++ Style*. Cambridge University Press 2004.

4.19 Paper: Cyclomatic Complexity

This is a checker to detect functions with high complexity. High complexity is defined by Mc Cabe's cyclomatic complexity metric. This metric measures the amount of branches in a function, i.e. through if and switch conditions.

4.19.1 Non-Compliant Code Examples

```
1 void fail() {
2   int x;
3   x=5;
4   if (x>3) {
5   }
6   if (x>3) {
7   }
8   if (x>3) {
9   }
10 }
```

4.19.2 Compliant Solution

```
1 void pass() {
2   int x;
3   x=5;
4   if (x>3) {
5   }
6 }
```

4.19.3 Parameter Requirements

CyclomaticComplexity.maxComplexity defines the max value for the complexity analysis.

4.19.4 Implementation

The algorithm searches for each function the number of occurances of:

```
1   if          (isSgIfStmt(node) || isSgCaseOptionStmt(node) || isSgForStatement(node) ||
isSgDoWhileStmt(node) || isSgWhileStmt(node)) {
2     complexity++;
3   }
```

4.19.5 References

McCabe , "Thomas McCabe, A Complexity Measure - IEEE Transactions on Software Engineering, Vol SE-2, No.4, December 1976."

4.20 Data Member Access

Following the spirit of data hiding in object-oriented programming, classes should in general not have public data members as these might give away details of the underlying implementation, making a change of implementation more difficult and possibly giving users a way to mess up the internal state of objects of the class. It is, however, sometimes useful to have 'behaviorless aggregates', i. e. C-style structs where all data members are public (and no member functions are present).

This checker warns about class definitions that fit into neither of the above patterns. Specifically, it warns about class definitions that contain both public and nonpublic data members.

4.20.1 Parameter Requirements

This checker does not require any parameters.

4.20.2 Non-Compliant Code Example

```
1 class NoNo { // not acceptable, contains both public and nonpublic data members
2 public:
3     int get_a() const;
4     void set_a(int);
5
6     double d;
7
8 protected:
9     int a;
10 };
```

4.20.3 Compliant Solution

```
1 struct C_style { // acceptable, all data members are public
2     int a, b;
3     double d;
4 };
5
6 class WellProtected { // acceptable, no data members are public
7 public:
8     int get_a() const;
9     void set_a(int);
10
11    double get_d() const;
12    void set_d(double);
13
14 protected:
15    int a;
16
17 private:
18    double d;
19 };
```

4.20.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For each class definition, count the numbers of public and nonpublic data members.
2. If both of the counts for a given class definition are greater than zero, a mix of public and nonpublic data members is present; emit a diagnostic.

4.20.5 References

A literature reference for this checker is: H. Sutter, A. Alexandrescu: "C++ Coding Standards"", Item 41: "Make data members private, except in behaviorless aggregates (C-style structs)". Note that the authors advise not only against public, but also against protected data members; this checker does not report protected data.

4.21 Deep Nesting

It is widely agreed that functions should not be 'too big' (without a good reason, at least). Various size measures exist, including source code lines and cyclomatic complexity. This checker adds one more: It tests if function definitions contain more nested scopes than allowed by the user.

4.21.1 Parameter Requirements

This checker requires an integer entry DeepNestingChecker.maximumNestedScopes in the Compass parameters specifying the maximum allowed number of nested scopes.

4.21.2 Non-Compliant Code Example

```
1 /* The innermost scope (the if statement) in this toy function will be
2  * reported by the DeepNestingChecker if maximumNestedScopes is set to 2. */
3 void matrix_abs(int n, int m, int **matrix)
4 {
5     for (int i = 0; i < n; i++)
6     {
7         for (int j = 0; j < m; j++)
8         {
9             if (matrix[i][j] < 0)
10            {
11                matrix[i][j] = -matrix[i][j];
12            }
13        }
14    }
15 }
```

4.21.3 Compliant Solution

```
1 /* The nesting in each function is not greater than 2; the if statement has
2  * been pulled out into its own function. */
3 void abs_if_necessary(int *p)
4 {
5     if (*p < 0)
6     {
7         *p = -*p;
8     }
9 }
10
11 void matrix_abs2(int n, int m, int **matrix)
12 {
13     for (int i = 0; i < n; i++)
14     {
15         for (int j = 0; j < m; j++)
16         {
17             abs_if_necessary(&matrix[i][j]);
18         }
19     }
20 }
```

4.21.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For each 'scope statement' (loops, if, basic blocks) count the number of enclosing scopes until a function definition is reached (if at all).
2. If the count is greater than the specified limit, emit a diagnostic.

4.21.5 References

A reference for this checker is: H. Sutter, A. Alexandrescu: "C++ Coding Standards", Item 20: "Avoid long functions. Avoid deep nesting".

4.22 Default Case

This test checks to ensure each switch statement has a default option. It has been noted that unexpected cases 'falling through" can be a cause of difficult to detect bugs. A default case will catch those cases.

4.22.1 Parameter Requirements

No parameters required.

4.22.2 Implementation

This implementation checks all statements in the basic block of the switch statement, searching for defaults. Currently this implementation may have false positives (ie. A switch with a default will raise an alert) on duff's device. In general Duff's device does not use a default.

4.22.3 Non-Compliant Code Example

```
1
2 switch(x)
3 {
4 case 1:
5 ...
6 case 2:
7 ...
8 }
9
```

4.22.4 Compliant Solution

```
1 switch(x)
2 {
3 case 1:
4 ...
5 case 2:
6 ...
7 default:
8 //handle unexpected cases
9 }
10
```

4.22.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Identifies switch statement
2. Reads all statements in it's basic block searching for default
3. if none found, notify message.

4.22.6 References

Abbreviated Code Inspection Checklist Section 11.2.2, Branching"

4.23 Default Constructor

The Elements of C++ Style item #97 states that

> Declare a default constructor for every class you create. Although some compilers may be able to automatically generate a more efficient implementation in some situations, choose an explicit default constructor for added clarity.

4.23.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.23.2 Implementation

This pattern is checked using a simple AST traversal that seeks out instances of SgClassDefinition. The children of these instances are stored in a successor container and looped over to find a default constructor. If no such default constructor exists then a violation is flagged.

4.23.3 Non-Compliant Code Example

The following trivial example does not declare a default constructor.

```
1 class Class
2 {
3   public:
4     ~Class(){}
5 }; //class Class
```

4.23.4 Compliant Solution

The compliant solution simply adds a default constructor to the class definition.

```
1 class Class
2 {
3   public:
4     Class(){}
5     ~Class(){}
6 }; //class bad
```

4.23.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform AST traversal visiting the member functions of class definitions.
2. If no constructor is found for a single class definition then flag violation.
3. Report any violations.

4.23.6 References

Bumgardner G., Gray A., and Misfeldt T. *The Elements of C++ Style*. Cambridge University Press 2004

4.24 Discard Assignment

According to some coding standards, the assignment operator should not be used within larger constructs, but only as a stand-alone expression statement; in particular, it should not be used as the controlling expression in a branch because it might be confused with the equality operator. This checker reports any use of the assignment operator (built-in or overloaded) that is not the sole expression in an expression statement.

4.24.1 Parameter Requirements

This checker does not require any parameters.

4.24.2 Non-Compliant Code Example

```
1 void strcpy_noncompliant(char *dest, const char *source)
2 {
3     while (*dest++ = *source++)
4         ;
5 }
```

4.24.3 Compliant Solution

```
1 void strcpy_compliant(char *dest, const char *source)
2 {
3     char last = *source;
4     do {
5         last = *source;
6         *dest++ = *source++;
7     } while (last != '\0');
8 }
```

4.24.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For each assignment, geneate a diagnostic if its parent is not an expression statement.
2. For each assignment that has an expression statement as its parent, generate a diagnostic if that expression statement is the controlling expression statement of a loop, if, or switch.

4.24.5 References

A reference to this pattern is: The Programming Research Group: "High-Integrity C++ Coding Standard Manual", Item 10.5: "Always discard the result of an assignment operator."

4.25 Do Not Call Putenv With Auto Var

The POSIX function putenv() is used to set environment variable values. The putenv() function does not create a copy of the string supplied to it as an argument, rather it inserts a pointer to the string into the environment array. If a pointer to a buffer of automatic storage duration is supplied as an argument to putenv(), the memory allocated for that buffer may be overwritten when the containing function returns and stack memory is recycled. This behavior is noted in the Open Group Base Specifications Issue 6 [Open Group 04]:

A potential error is to call putenv() with an automatic variable as the argument, then return from the calling function while string is still part of the environment.

The actual problem occurs when passing a pointer to an automatic variable to putenv(). An automatic pointer to a static buffer would work as intended.

4.25.1 Parameter Requirements

No Parameter specifications.

4.25.2 Implementation

The putenv() function is not required to be thread-safe, and the one in libc4, libc5 and glibc2.0 is not, but the glibc2.1 version is.

Description for libc4, libc5, glibc: If the argument string is of the form name, and does not contain an '=' character, then the variable name is removed from the environment. If putenv() has to allocate a new array environ, and the previous array was also allocated by putenv(), then it will be freed. In no case will the old storage associated to the environment variable itself be freed.

The libc4 and libc5 and glibc 2.1.2 versions conform to SUSv2: the pointer argument given to putenv() is used. In particular, this string becomes part of the environment; changing it later will change the environment. (Thus, it is an error to call putenv() with a pointer to a buffer of automatic storage duration as the argument, then return from the calling function while the string is still part of the environment.) However, glibc 2.0-2.1.1 differs: a copy of the string is used. On the one hand this causes a memory leak, and on the other hand it violates SUSv2. This has been fixed in glibc2.1.2.

The BSD4.4 version, like glibc 2.0, uses a copy.

SUSv2 removes the 'const' from the prototype, and so does glibc 2.1.3.

The FreeBSD implementation of putenv() copies the value of the provided string, and the old values remain accessible indefinitely. As a result, a second call to putenv() assigning a differently sized value to the same name results in a memory leak.

4.25.3 Non-Compliant Code Example

In this non-compliant coding example, a pointer to a buffer of automatic storage duration is used as an argument to putenv() [Dowd 06]. The TEST environment variable may take on an unintended value if it is accessed once func() has returned and the stack frame containing env has been recycled.

Note that this example also violates rule [DCL30-C. Declare objects with appropriate storage durations].

```
1
2 int func(char *var) {
3   char env[1024];
4
5   if (snprintf(env, sizeof(env),"TEST=%s", var) < 0) {
6     /* Handle Error */
7   }
8
9   return putenv(env);
10 }
11
```

4.25.4 Compliant Solution

The setenv() function allocates heap memory for environment variables. This eliminates the possibility of accessing volatile, stack memory.

```
1
2 int func(char *var) {
3   return setenv("TEST", var, 1);
4 }
5
```

4.25.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Checks to see if the variable being passed to putenv() is declared in the global scope. If it is not, the checker creates new output.

4.25.6 References

Open Group 04 The putenv() function

ISO/IEC9899-1999Section 6.2.4, "Storage durations of objects," and Section 7.20.3, "Memory management functions"

Dowd 06 Chapter 10, "UNIX Processes" (Confusing putenv() and setenv())

4.26 Do Not Delete This

"CERT Secure Coding C++ DAN32-C." states that

> Deleting this leaves it as a "dangling" pointer, which leads to undefined behavior if it is accessed.

4.26.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.26.2 Implementation

This pattern is checked using a simple AST traversal visiting all `delete` expressions and checking its argument to be a `this` expression; if so, flag a violation.

4.26.3 Non-Compliant Code Example

```
1  class SomeClass {
2      public:
3          SomeClass();
4          void doSomething();
5          void destroy();
6          // ...
7  };
8
9  void SomeClass::destroy() {
10     delete this;  // Dangerous!!
11 }
12
13 SomeClass sc = new SomeClass;
14 // ...
15 sc->destroy();
16 // ...
17 sc->soSomething();  // Undefined behavior
```

4.26.4 Compliant Solution

```
1  class SomeClass {
2      public:
3          SomeClass();
4          void doSomething();
5          // ...
6          ~SomeClass();
7  };
8
9  SomeClass sc = new SomeClass;
10 // ...
11 delete sc;
```

4.26.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform simple AST traversal visiting all `delete` expression nodes.

2. For each `delete` expression node, check its argument node to be `this` expression; if so, flag violation.
3. Report any violations.

4.26.6 References

DAN32-C. Do not delete this

4.27 Do Not Use C-style Casts

C++ allows C-style casts, although it has introduced its own casts:

- static_cast¡type¿(expression)
- const_cast¡type¿(expression)
- dynamic_cast¡type¿(expression)
- reinterpret_cast¡type¿(expression)

C++ casts allow for more compiler checking and are easier to find in source code (either by tools or by human readers).

4.27.1 Parameter Requirements

No Parameter specifications.

4.27.2 Implementation

4.27.3 Non-Compliant Code Example

In this example, a C-style cast is used to convert an int to a double:

```
1
2 int dividend, divisor;
3 // ...
4 double result = ((double)dividend)/divisor;
5
```

4.27.4 Compliant Solution

Using the new cast, the division should be written as:

```
1
2 double result = static_cast<double>(dividend)/divisor;
3
```

4.27.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Check to see if the SgCastExp node is of type SgCastExp::e_C_style_cast, and if it is, add ouput.

4.27.6 References

Dewhurst 03 Gotcha 40: Old-Style Casts

ISO/IEC 14882-2003 Sections 5.2.9, 5.2.11, 5.2.7, 5.2.10.

Meyers 96 Item 2: Prefer C++-style casts.

Lockheed Martin 05 AV Rule 185 C++ style casts (const_cast, reinterpret_cast, and static_cast) shall be used instead of the traditional C-style casts.

4.28 Duffs Device

This test checks for the presence of Duff's Device in the source code. Duff's Device is a switch statement containing a loop (for, while or do-while; we do not check for goto loops) that contains one of the switch's case or default labels. If such a construct is found, the position of the switch statement is reported.

4.28.1 Parameter Requirements

This checker does not require any parameters.

4.28.2 Non-Compliant Code Example

```
1 // Duff's Device in its almost original form.
2 void send(int *to, int *from, int count)
3 {
4   int n = (count+7) / 8;
5   switch(count%8) {
6   case 0: do { *to++ = *from++;
7   case 7:      *to++ = *from++;
8   case 6:      *to++ = *from++;
9   case 5:      *to++ = *from++;
10  case 4:      *to++ = *from++;
11  case 3:      *to++ = *from++;
12  case 2:      *to++ = *from++;
13  case 1:      *to++ = *from++;
14             } while (--n>0);
15  }
16 }
```

4.28.3 Compliant Solution

```
1 // An equivalent function without optimization.
2 void send2(int *to, int *from, int count)
3 {
4     for (int i = 0; i < count; i++)
5         *to++ = *from++;
6 }
```

4.28.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For each case or default statement, examine the enclosing scopes, smallest first (i.e. go upward in the AST).
2. If there is a loop statement that is closer than a switch statement, Duff's Device has been found; emit a diagnostic.

4.28.5 References

Duff's Device ist mostly folklore, but one reference in the literature is: B. Stroustrup: "The C++ Programming Language, Third Edition", Exercise §6.6[15].

4.29 Dynamic Cast

The rule is that dynamic_cast¡¿ should always be used when a downcast is needed (ALE3D 14.5). Downcasting is a term for casting a pointer to a base class to a derived class, and should only be done with extreme care. Using dynamic_cast¡¿ will ensure that the object pointed to by the base class pointer is really of the derived class. It will return a nill pointer if it is not. Any other type of cast is unsafe.

4.29.1 Parameter Requirements

This checker does not take any paramaters.

4.29.2 Implementation

This pattern is detected using a simple traversal without inherited or synthesized attributes.

4.29.3 Non-Compliant Code Example

```
1
2   class A//not polymorphic
3    {
4      public:
5        ~A(){}
6        virtual void foo(){};
7    };
8
9   class B: public A
10   {
11   };
12
13  int main()
14    {
15      A * p  = new B;
16      B * p2 = (B*) p;
17    }
18
```

4.29.4 Compliant Solution

```
1
2   class A//not polymorphic
3    {
4      public:
5        ~A(){}
6        virtual void foo(){};
7    };
8
9   class B: public A
10   {
11   };
12
13  int main()
14    {
15      A * p = new B;
16      B * p2 = dynamic_cast<B* > (p);
17    }
18
```

4.29.5 Mitigation Strategies

Static Analysis

1. traverse AST
2. for each cast expression that is a downcast if dynamic cast is not used report an error.

4.29.6 References

4.30 Empty Instead Of Size

While comparing the result of the size() member function on STL containers against 0 is functionally equivalent to calling the empty() member function, empty() is to be preferred as it is always a constant-time operation, while size() on std::list may take linear time. This checker detects cases where the result of size() is compared against the constant 0.

4.30.1 Parameter Requirements

This checker does not require any parameters.

4.30.2 Non-Compliant Code Example

```
#include <vector>

bool f(const std::vector<int> &v)
{
    if (v.size() > 0) // not OK: use !v.empty() instead
        return true;
    if (0 == v.size()) // not OK: use v.empty() instead
        return false;
    return false;
}
```

4.30.3 Compliant Solution

```
#include <vector>
bool f2(const std::vector<int> &v)
{
    if (!v.empty())
        return true;
    if (v.empty())
        return false;
    return false;
}
```

4.30.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For each member function call, see if the called member function is named 'size' and if the call is embedded in an expression that compares its return value against the constant 0.
2. If the above check evaluates to true, emit a diagnostic.

There are numerous ways to defeat this simple analysis, for instance by assigning the return value from size() to a variable, by comparing the return value against a variable that is always 0, or by calling size() through a member function pointer. Further, the analysis only looks for member functions named 'size' but does not try to ascertain that it belongs to a 'container' (as that is not something that can be checked reliably).

4.30.5 References

The reference for this checker is: S. Meyers: "Effective STL", Item 3: "Call `empty` instead of checking `size()` against zero."

4.31 Enum Declaration Namespace Class Scope

The Elements of C++ Style item #79 states that

> To avoid symbolic name conflicts between enumerators and other global names, nest enum declarations within the most closely related class or common namespace.

4.31.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.31.2 Implementation

This pattern is checked using a simple AST traversal that locates nodes that are enumeration declarations. If a enumeration declaration is found then its parent nodes are traversed until a class or namespace declaration is found. If no namespace or class declaration(s) are found then a violation is flagged by this checker.

4.31.3 Non-Compliant Code Example

This non-compliant code contains an enum declaration at the global scope.

```
1 enum violation{ E1=0, E2, E3 }; // This is a violation
```

4.31.4 Compliant Solution

The compliant solution simply nests the violation enum declaration in a unique namespace.

```
1 namespace Namespace
2 {
3   enum violation{ E1=0, E2, E3 }; // This is OK
4 } //namespace Namespace
```

4.31.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform an AST traversal visiting enum declaration nodes.
2. For each enum declaration node visit its parents checking them to be either namespace declarations or class declarations. If no class or namespace declaration parent node is found, then flag violation.
3. Report any violations.

4.31.6 References

Bumgardner G., Gray A., and Misfeldt T. *The Elements of C++ Style*. Cambridge University Press 2004.

4.32 CERT-DCL04-A: Explicit Char Sign

"CERT Secure Coding INT07-A" states

> The three types `char`, `signed char`, and `unsigned char` are collectively called the character types. Compilers have the latitude to define `char` to have the same range, representation, and behavior as either `signed char` or `unsigned char`. Irrespective of the choice made, `char` is a separate type from the other two and is **not** compatible with either.

4.32.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.32.2 Implementation

This pattern is checked using a simple AST traversal visiting all SgAssignInitializer nodes. If the SgAssignInitializer node is of type `char` and the operand of the node is a SgCastExp of type `int` or is a SgCharVal whose value is negative then flag an error.

4.32.3 Non-Compliant Code Example

This non-compliant example declares a simple `char` type variable.

```
1 #include <stdio.h>
2
3 int main()
4 {
5   int n = 200;
6   char c1 = 'i';
7   char c2 = n;
8   char c3 = 200;
9   int i = 1000;
10
11  printf( "%c/c2 = %d\n%c/c3 = %d\n", c1, i/c2, c1, i/c3);
12
13  return 0;
14 }
```

4.32.4 Compliant Solution

The compliant solution explicitly declares the `char` variables as `unsigned`.

```
1 #include <stdio.h>
2
3 int main()
4 {
5   int n = 200;
6   char c1 = 'i';
7   unsigned char c2 = n;
8   unsigned char c3 = 200;
9   int i = 1000;
10
11  printf( "%c/c2 = %d\n%c/c3 = %d\n", c1, i/c2, c1, i/c3);
12
13  return 0;
14 }
```

4.32.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform simple AST traversal visiting all SgAssignInitializer nodes.
2. For each SgAssignInitializer node of type `char`, if the rhs operand is either a cast expression with operand of type int or a negative character value then flag an error.
3. Report any violations.

4.32.6 References

Secure Coding : INT07-A. Explicitly specify signed or unsigned for character types

4.33 Explicit Copy

This test detects missing copy constructors and operators. In case the user wants to use the default ones then the class has to be annotated with a special comment. These comments should contain "`use default copy constructor`" or "`use default copy operator`".

This checker enforces the rule 53 from H. Sutter, A. Alexandrescu *C++ Coding Standards*: "Explicitly enable or disable copying".

4.33.1 Parameter Requirements

No parameter is required.

4.33.2 Non-Compliant Code Example

```
1 class A {
2 };
```

4.33.3 Compliant Solution

```
1 class A {
2 public:
3   A(const A& other) {
4
5   }
6   A& operator=(const A& other) {
7     return this;
8   }
9 };
```

4.33.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For all class definitions, try to find a copy constructor and a copy operator, or user comments describing that the class should use the default ones.

4.33.5 References

Alexandrescu A. and Sutter H. *C++ Coding Standards 101 Rules, Guidelines, and Best Practices*. Addison-Wesley 2005.

4.34 Explicit Test For Non Boolean Value

This test examines all the test statements whether there is a statement that calls a function call returning a non-boolean value and that does not compare the return value to an explicit value. For example, if a function `foo()` returns an integer value and the function is used in a conditional statement, such as `"if", "while", "do-while", "for"`, or the first operand of "?" operator, the boolean expressions in the conditional statement should always use an explicit test of equality or non-equality. Therefore the following code can pass this checker:

```
1 if(foo()!=0)
2 {// do something}
```

whereas,

```
1 if(foo())
2 {// do something}
```

will be caught by this checker because `foo()` returns an integer, non-boolean value.

4.34.1 Parameter Requirements

None

4.34.2 Implementation

This pattern is detected using a simple traversal. It traverses AST to search conditional statements and if an implicit expression is used in the test, AST contains a casting expression node underneath the conditional statement to convert from a non-boolean values to a boolean value. The checker captures this structure.

4.34.3 Non-Compliant Code Example

```
1  int bar();
2
3  void foo()
4  {
5    int i;
6    if(bar())
7      i = 2;
8
9    while(bar())
10     i = 3;
11
12   do {
13     i = 4;
14   } while(bar());
15
16   for(i=0; bar(); i++)
17     i =5;
18
19   i = (bar() ? 6 : 7);
20
21   for(i = (bar() ? 8 : 9); bar(); i++)
22     i = 10;
23 }
```

4.34.4 Compliant Solution

```
1 if(foo()!=0)
2 {// do something}
```

4.34.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Check if a node is a conditional statement
2. Check further if the conditional statement contains an implicit expression.

4.34.6 References

The Programming Research Group, High-Integrity C++ Coding Standard Manual, Item 5.2: "For boolean epressions('if', 'for', 'while', 'do' and the first operand of the ternary operator '?:') involving non-boolean values, always use an explicit test of equality or non-equality."

4.35 Float For Loop Counter

"CERT Secure Coding" states

> Floating point arithmetic is inexact and is subject to rounding errors. Hence, floating point variables should not be used as loop counters.

4.35.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.35.2 Implementation

This pattern is checked using a simple AST traversal that visits all for loop init statement nodes and checks the type of its counter variable declaration. If that type is `float` or `double` then flag a violation.

4.35.3 Non-Compliant Code Example

```
1 for (float count = 0.1f; count <= 1; count += 0.1f)
2 {
3 }
```

4.35.4 Compliant Solution

The compliant solution uses an `int` type loop counter.

```
1 for (int count = 1; count <= 10; count += 1)
2 {
3 }
```

4.35.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform simple AST traversal visiting all for loop initialization statement nodes.
2. For each node check the type of its variable declaration. If type is `float` or `double` then flag violation.
3. Report any violations.

4.35.6 References

FLP31-C. Do not use floating point variables as loop counters

4.36 Floating Point Exact Comparison

This checker detects a test clause that compares a variable to a floating point value. The rationale for this checker is, floating point representations are platform dependent, so it is necessary to avoid exact comparisons.

4.36.1 Parameter Requirements

None.

4.36.2 Implementation

This checker is implemented with a simple AST traversal. It traverses AST and finds a test clause. If the test clause has a double value on either left-hand-side or right-hand-side, and if the operator used for the test is "==" or "!=", then the checker reports this clause.

4.36.3 Non-Compliant Code Example

```
1 void foo( double f )
2 {
3 if ( f == (float)3)
4 {
5 f = 1.234;
6 }
7
8 while(f != 1.23456)
9 {
10 f += 0.00001;
11 }
12
13 do
14 {
15 f += 0.000001;
16 } while ( f != 1.234567);
17
18 for(f = 1.234567; f != 1.2345678; f += 0.0000001)
19 {
20 int i = f + 1;
21 }
22 }
```

4.36.4 Compliant Solution

```
1 bool double_equal(const double a, const double b)
2 {
3 const bool equal = fabs(a-b) < numeric_limits<double>::epsilon;
4 return equal;
5 }
6
7 void foo(double f)
8 {
9 if(double_equal(f, 3.142))
10 {
11 // do something
12 }
13 }
```

4.36.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Check if a node is a test clause
2. Check further if the clause has a double value and if the test is for (in)equality.

4.36.6 References

The Programming Research Group, High-Integrity C++ Coding Standard Manual, "Item 10.15: Do not write code that expects floating point calculations to yield exact results".

4.37 Fopen Format Parameter

"CERT Secure Coding FIO11-A" states

> The C standard specifies specific strings to use for the `mode` for the function `fopen()`. An implementation may define extra strings that define additional modes, but only the modes in the following table (adapted from the C99 standard) are fully portable and C99 compliant:

1. r
2. w
3. a
4. rb
5. wb
6. ab
7. r+
8. w+
9. a+
10. r+b or rb+
11. w+b or wb+
12. a+b or ab+

4.37.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.37.2 Implementation

This pattern is checked using a simple AST traversal that visits all function call expressions. For each function call expression the function name is confirmed to be `fopen()` then the format parameter is checked against the list of specified strings. If the given parameter is not a standard format string then a violation is flagged.

4.37.3 Non-Compliant Code Example

```
1 #include <stdio.h>
2
3 int main()
4 {
5   FILE *f = fopen( "/tmp/tmp.txt", "wr" );
6
7   fclose( f );
8
9   return 0;
10 }
```

4.37.4 Compliant Solution

The compliant solution uses the "r+" specified parameter string instead.

```
1 #include <stdio.h>
2
3 int main()
4 {
5   FILE *f = fopen( "/tmp/tmp.txt", "r+" );
6
7   fclose( f );
8
9   return 0;
10 }
```

4.37.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform simple AST traversal visiting all function call expression nodes.
2. For each function call expression node, unparse node string then to determine the function name and parse the format parameter.
3. Check the format parameter against list of standard values. If given format parameter does not conform to list of specified values, then flag violation.
4. Report any violations.

4.37.6 References

Secure Coding : FIO11-A. Take care when specifying the mode parameter of fopen()

4.38 Forbidden Functions

Many checks common to Compass center around the forbidden use of certain "dangerous" functions. This checker provides a way to forbid the use of those functions through the simple use of their name.

4.38.1 Parameter Requirements

The forbidden function checker can simultaneously look for any number of functions, either member or non-member. A set of parameters is used, named using a counter. Thus, the parameters of this checker have names of the form `ForbiddenFunctions.Function`*n*, for *n* from zero to some limit. The forbidden function analysis checks each name in turn until one is missing. Thus, if you have parameters named `ForbiddenFunctions.Function0` and `ForbiddenFunctions.Function1` but no parameter named `ForbiddenFunctions.Function2`, the analysis will search for two functions. As a caution, if you skip a number, including zero, no larger numbers will be scanned: any functions specified after a skipped number will be ignored.

The format of a parameter is `white space, function name, white space, comma, reason`. Leading and trailing white space is allowed next to the function name, but any white space after the first comma will become part of the reason string. The function name is a fully qualified name, but the leading `::` to indicate the global scope may be omitted. Member functions are given with their class qualifications, just as they would be referred to when accessing a pointer to them. Choosing one overload from an overload set sharing the same name is not supported. The reason field is used to indicate why a particular function is forbidden; it may be any string (not containing a newline), and is printed out as part of the error message when the corresponding function is found. It is also possible to omit the comma and the reason field, leaving just the function name as the parameter; in this case, no reason will be given for the function's prohibition.

4.38.2 Implementation

This pattern is checked using a simple AST traversal visiting all SgFunctionCallExp nodes. For each node the name of the function being called is compared to those listed as forbidden functions. If a match is found between the function call name and the forbidden function name then flag an error.

4.38.3 Non-Compliant Code Example

In this example, it is assumed that the function `compass_forbidden_function_vfork` is forbidden by the parameter file.

```
1 //compass_forbidden_function_vfork() is a function meant to simulate a system
2 //routine. This makes no difference as an example of how forbiddenFunctions
3 //checks errors as it works only on function names. The reason we have used
4 //this example is to prevent compass from treating this test file as an error
5 //during 'make verify' in which compass checks its own source code.
6
7 int compass_forbidden_function_vfork();
8 void helloWorld(int, char**);
```

```
 9
10 double function();
11 double good_function();
12
13 namespace A {
14   double function2();
15 }
16
17 struct B {
18   void memberFunction();
19 };
20
21 int main(int argc, char** argv) {
22   int w;
23   w = compass_forbidden_function_vfork() + 5;
24   helloWorld(argc, argv);
25   double x = 3.0 * function();
26   double y = 5.0 * good_function();
27   double z = A::function2();
28   B b;
29   b.memberFunction();
30   int (*fp)() = compass_forbidden_function_vfork;
31   return 0;
32 }
```

4.38.4 Compliant Solution

The compliant example would use a function not listed in the parameter file.

4.38.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For each SgFunctionCallExp node if the name of the function being called is forbidden by the parameter file then report error.

4.38.6 References

Foster , "James C.Foster, Vitaly Osipov, Nish Bhalla, Niels Heinen, Buffer Overflow Attacks, ISBN 1-932266-67-4, p. 211"

Secure Coding : MSC30-C. Do not use the rand function

Secure Coding : POS33-C. Do not use vfork()

[ISO/IEC 9899-1999:TC2] Section 7.19.9.2, "The `fseek` function"; 7.19.9.5, "The `rewind` function"

[Klein 02] [
ISO/IEC 9899-1999] Section 7.20.1.4, "The strtol, strtoll, strtoul, and strtoull functions," Section 7.20.1.2, "The atoi, atol, and atoll functions," and Section 7.19.6.7, "The sscanf function"

4.39 For Loop Construction Control Stmt

"ALE3D Coding Standards & Style Guide" item #6.1 states that

> for() construction loops must only include statements that control the loop. In particular, for() loops must not initialize or increment/decrement variables not directly related to the loop control.

4.39.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.39.2 Implementation

This pattern is checked using a simple AST traversal that seeks out for loop statement constructs. Once a for loop is found the for loop construction block, e.g. for(; ;) is string searched for instances of the comma operator that indicates the use of non-control expressions in for loop construction code.

4.39.3 Non-Compliant Code Example

This non-compliant code initializes the array inside the for() control statement.

```
1 #include <stdlib.h>
2
3 int main()
4 {
5   int *array = (int*)malloc( 100*sizeof(int) );
6   for( int i = 0; i < 100; i++, array[i] = i ){}
7
8   free(array);
9   return 0;
10 } //main()
```

4.39.4 Compliant Solution

The compliant solution simply moves the array initialization inside the for() loop body.

```
1 #include <stdlib.h>
2
3 int main()
4 {
5   int *array = (int*)malloc( 100*sizeof(int) );
6   for( int i = 0; i < 100; i++ ){ array[i] = i; }
7
8   free(array);
9   return 0;
10 } //main()
```

4.39.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform simple AST traversal visiting all comma operator expressions.
2. For each comma operator expression node, if parent node is for loop statement then flag violation.
3. Report any violations.

4.39.6 References

Arrighi B., Neely R., Reus J. "ALE3D Coding Standards & Style Guide", 2005.

4.40 For Loop Cpp Index Variable Declaration

"ALE3D Coding Standards & Style Guide" Item #6.2 states that

> C++ loop index variables should be declared in the loop statement. Declaration of a loop index variable in the first clause of the for() statement ensures that its scope is limited to the loop body.

4.40.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.40.2 Implementation

This pattern is checked using a simple AST traversal that seeks SgForInitStatements that have NULL declaration statements. These nodes are flagged as violations.

4.40.3 Non-Compliant Code Example

This non-compliant code declares the loop control variable outside the loop statement.

```
1 int main()
2 {
3   int i = 0;
4   for( i = 0; i < 100; i++ ){}
5
6   return 0;
7 } //main()
```

4.40.4 Compliant Solution

The compliant solution declares the index variable inside the loop statement.

```
1 int main()
2 {
3   for( int i = 0; i < 100; i++ ){}
4
5   return 0;
6 } //main()
```

4.40.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform simple AST traversal visiting all declaration statement nodes.
2. For each declaration statement node, if parent node is for loop initialization statement then flag violation.
3. Report any violations.

4.40.6 References

Arrighi B., Neely R., Reus J. “ALE3D Coding Standards & Style Guide”, 2005.

4.41 Friend Declaration Modifier

The Elements of C++ Style item #96 states that

> Friend declarations are often indicative of poor design because they bypass access restrictions and hide dependencies between classes and functions.

4.41.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.41.2 Implementation

This pattern is checked with a simple AST traversal that seeks declaration statements and determines if any use the "friend" modifier keyword. Any declaration statements found with the "friend" modifier are flagged as violations.

4.41.3 Non-Compliant Code Example

This non-compliant example uses "friend" to access private data.

```
1  class Class
2  {
3    int privateData;
4    friend int foo( Class & c );
5
6    public:
7      Class(){ privateData=0; }
8  }; //class Class
9
10 int foo( Class & c )
11 {
12   return c.privateData + 1;
13 } //foo( Class & c )
```

4.41.4 Compliant Solution

The compliant solution simply uses an accessor function instead.

```
1  class Class
2  {
3    int privateData;
4
5    public:
6      Class(){ privateData=0; }
7      int getPrivateData(){ return privateData; }
8  }; //class Class
9
10 int foo( Class & c )
11 {
12   return c.getPrivateData() + 1;
13 } //foo( Class & c )
```

4.41.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform simple AST traversal and visit all declaration statement nodes
2. For each declaration statement check the "friend" modifier. If "friend" modifier is set then flag violation.
3. Report any violations.

4.41.6 References

Bumgardner G., Gray A., and Misfeldt T. *The Elements of C++ Style*. Cambridge University Press 2004.

4.42 Function Call Allocates Multiple Resources

"CERT Secure Coding RES30-C" states

> Allocating more than one resource in a single statement could result in a memory leak, and this could lead to a denial-of-service attack.

4.42.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.42.2 Implementation

This pattern is checked using a simple AST traversal on each SgFunctionCallExp node. For each node get the expression list of its arguments and check if any such argument expressions are the `new` keyword. If the number of `new` expressions exceeds one then flag an error.

4.42.3 Non-Compliant Code Example

```
1  class A
2  {
3  };
4
5  class B
6  {
7  };
8
9  int foo( A *a, B *b )
10 {
11   return 0;
12 }
13
14 int main()
15 {
16   A *a = new A;
17   B *b = new B;
18   int i = foo( a, b ); //ok...
19
20   return foo( new A, new B ); //bad
21 }
```

4.42.4 Compliant Solution

See the call to `foo` above.

4.42.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Traverse all SgFunctionCallExp nodes
2. For each node get the list of argument expressions

3. Count the number of `new` keyword argument expressions
4. If the number of `new` keyword argument expressions exceeds one then flag an error.
5. Report all violations.

4.42.6 References

RES30-C. Never allocate more than one resource in a single statement

4.43 CERT-DCL31-C: Function Definition Prototype

"CERT Secure Coding DCL31-C" states

> Functions should always be declared with the appropriate function prototype. If a function prototype is not available, the compiler cannot perform checks on the number and type of arguments being passed to functions. Argument type checking in C is only performed during compilation, and does not occur during linking, or dynamic loading.

4.43.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.43.2 Implementation

This pattern is checked using a simple AST traversal of function declaration nodes. For each function declaration node find the first non-defining function declaration; if none is found, then flag violation.

4.43.3 Non-Compliant Code Example

This example `foo()` has no prototype.

```
1 int foo( int i )
2 {
3   return i;
4 }
5
6 int main()
7 {
8   return foo(0);
9 }
```

4.43.4 Compliant Solution

The compliant solution simply adds a function prototype for `foo()`

```
1 int foo(int);
2
3 int foo( int i )
4 {
5   return i;
6 }
7
8 int main()
9 {
10   return foo(0);
11 }
```

4.43.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform a simple AST traversal of code visiting all function declaration nodes.
2. For each function declaration node, find first non-defining declaration. If no non-defining declaration is found, then flag violation.
3. Report any violations detected.

4.43.6 References

Secure Coding : DCL31-C. Ensure every function has a function prototype

4.44 Paper: Function Documentation

This analysis detects all non-compiler generated functions and checks whether they are documented. The documentation must be in front of the function.

4.44.1 Non-Compliant Code Examples

```
1 void fail() {
2   //  this function has no comment in front of it
3 }
```

4.44.2 Compliant Solution

```
1 //Your test file code goes here.
2 void succeed() {
3 }
```

4.44.3 Parameter Requirements

None.

4.44.4 Implementation

This analysis checks for both '//' and '/*' documentation.

4.44.5 References

Panas05 , "Thomas Panas, Rudiger Lincke, Jonas Lundberg, Welf Lowe, A Qualitative Evaluation of a Software Development and Re-Engineering Project, NASA/IEEE Software Engineering Workshop, Washington DC, USA, April 2005"

4.45 Induction Variable Update

This test finds the location in loops (for, do-while, while) where induction variables is updated (through arithmetic operations).

4.45.1 Parameter Requirements

None.

4.45.2 Implementation

This pattern is detected using a simple traversal. It traverses AST to obtain information about induction variables and to locate statements that assign a new value to the induction variables. However, this checker does not track pointers whether or not the pointers actually update induction variables. In addition, function calls that may update induction variables are not considered here, either.

4.45.3 Non-Compliant Code Example

```
1 void foo(){
2   int i;
3   int j = 0;
4   int k = 0;
5
6   for(i = 0; i != 10; ++i)
7   {
8     if( 0 == i % 3)
9     {
10      i = 3;
11      ++i;
12      i++;
13    }
14  }
15
16  while(j < 10)
17  {
18    if(1 == j %3)
19    {
20      j = j + 2;
21    }
22    j++;
23  }
24
25  do {
26    if(2 == k % 3)
27    {
28      k +=1;
29    }
30  } while(++k < 10);
31 }
```

4.45.4 Compliant Solution

```
1
2
```

4.45.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Find a loop and detect its induction variable
2. Check if the variable is updated inside the loop, by examining its loop body.

4.45.6 References

The Programming Research Group, High-Integrity C++ Coding Standard Manual, Item 5.6: "Do not alter a control variable more than once in a for, do or while statement."

4.46 Internal Data Sharing

Classes should usually not return handles to internal data from methods. A 'handle' in this sense is a non-const reference to a member or copy of a pointer member, as the caller could change internal state through such an object. This checker reports such cases. One possible exception to this rule are overloaded operators, which often return such handles (so they can be combined with other operators to bigger expressions), and this checker provides a parameter to define whether operators should be allowed to return internals.

4.46.1 Parameter Requirements

The bool flag **InternalDataSharing.operatorsExcepted** states whether overloaded operators are excepted from this checker's rules, i.e. whether they are allowed to return internal data.

4.46.2 Non-Compliant Code Example

```
1  class A
2  {
3  public:
4      // not OK: returning non-const pointer member
5      int *retptr() { return p; }
6      // not OK: returning non-const reference to data pointed to by member
7      int &retref() { return *p; }
8      // not OK: returning non-const reference to member
9      int *&retptrref() { return p; }
10
11 private:
12     int *p;
13 };
```

4.46.3 Compliant Solution

```
1  class B
2  {
3  public:
4      // OK: returning copy of pointed-to data
5      int retint() { return *p; }
6      // OK: const ptr
7      const int *retcptr() { return p; }
8      // OK: const ref
9      const int &retcref() { return *p; }
10
11     // maybe OK, depending on "operatorsExcepted" parameter
12     int &operator*() { return *p; }
13
14 private:
15     int *p;
16 };
```

4.46.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. While traversing the program representation, set a flag upon entering a member function definition that has a non-const pointer or reference return type.
2. Report any return statement within such a flagged function that returns a (possibly dereferenced) member variable.

4.46.5 References

A reference in the literature is: H. Sutter, A. Alexandrescu: "C++ Coding Standards", Item 42: "Don't give away your internals". Their notion of a handle is more general, however, as it also includes basic types that are used as handles, such as ints that are used as file descriptors.

4.47 Localized Variables

This checker looks for variable declarations and try to determine if the first use is far far the declaration. There can be two ways where the use is far. Either it is used only in an inner scope. Then the declaration can be moved in that scope. Or the it is used not directly after the block of declaration the variables is from. Then the declaration should be moved down.

This checker try to check for item 18 of *C++ Coding Standards* (Sutter and al., 2005).

4.47.1 Parameter Requirements

No parameter is needed.

4.47.2 Non-Compliant Code Example

```
1 void print(int);
2
3 void f()
4 {
5   int i; //i should be declared at the for loop.
6   int sum = 0; //sum is OK.
7
8   //i is only used in the for scope.
9   for (i = 0; i < 10; ++i) {
10    //sum is used right after the block of declaration it belongs.
11    sum += i;
12  }
13
14  //sum is used in the scope of definition.
15  print(sum);
16 }
```

4.47.3 Compliant Solution

```
1 void print(int);
2
3 void f()
4 {
5   int sum = 0;
6
7   for (int i = 0; i < 10; ++i) {
8     sum += i;
9   }
10
11  print(sum);
12 }
```

4.47.4 Mitigation Strategies

Static Analysis

The checker uses a scoped symbol table to track some properties about variable: Was the variable used? Was the variable in the same scope as its declaration? Was the variable used right after the the declaration? Is the declaration right before the current point of the traversal? The traversal updates these flags.

Once a scope finished to be traversed, since the variables declared in the scope cannot be used any further, they are checked for the flags: used, used in the same scope and used right after its declaration.

There is another flag saying if the variable is a constant. In this case only check that the variable have been used, whereever it is.

This implementation does not care about aliasing. For more informations see subsection 4.47.6.

4.47.5 References

Alexandrescu A. and Sutter H. *C++ Coding Standards 101 Rules, Guidelines, and Best Practices*. Addison-Wesley 2005.

4.47.6 Limitations

This checker does not do alias analyzing. In the case you use a reference of a variable in an inner scope and re-use in the scope of declaration, the checker will not see the use and propose to move the variable in the inner scope. The effort for supporting the problem is very big, and the result is to handle programs with weird behavior that should have been written differently.

4.48 [No Reference] : Loc Per Function

This analysis detects for each function the amount of lines of code (LOC) and checks the value against a user defined max value. If LOC > max value, then an exception is triggered.

4.48.1 Non-Compliant Code Examples

```
1 // if LocPerFunction.Size = 2
2 void fail() {
3   int x;
4   x = 5;
5   x = 5;
6   x = 5;
7 }
```

4.48.2 Compliant Solution

```
1 // if LocPerFunction.Size = 2
2 void pass() {
3   int x;
4   x = 5;
5   x = 5;
6 }
```

4.48.3 Parameter Requirements

LocPerFunction.Size defines the max value for a permissive LOC.

4.48.4 Implementation

The simple implementation of this checker is defined below:

```
1   if (isSgFunctionDeclaration(sgNode)) {
2     SgFunctionDeclaration* funcDecl = isSgFunctionDeclaration(sgNode);
3     SgFunctionDefinition* funcDef = funcDecl->get_definition();
4     if (funcDef) {
5       Sg_File_Info* start = funcDef->get_body()->get_startOfConstruct();
6       Sg_File_Info* end = funcDef->get_body()->get_endOfConstruct();
7       ROSE_ASSERT(start);
8       ROSE_ASSERT(end);
9       int lineS = start->get_line();
10      int lineE = end->get_line();
11      loc_actual = lineE-lineS;
12      if (loc_actual>loc) {
13        output->addOutput(new CheckerOutput(funcDef));
14      }
15    }
16  }
```

4.48.5 References

4.49 Lower Range Limit

By always using inclusive lower limits and exclusive upper limits, a whole class of off- by-one errors is eliminated. Furthermore, the following assumptions always apply: 1)the size of the interval equals the difference of the two
2) the limits are equal if the interval is empty
3) the upper limit is never less than the lower limit

Examples: instead of saying x¿=23 and x¡=42, use x¿=23 and x¡43.

4.49.1 Parameter Requirements

No parameters required.

4.49.2 Implementation

In a fairly straight-forward implementation we search the strictly lower than operator.

4.49.3 Non-Compliant Code Example

```
1 int x = 5;
2 if (x < 5)
3 {
4 x++;
5 }
6
```

4.49.4 Compliant Solution

```
1 int x = 5;
2 if (x <= 4)
3 {
4 x++;
5 }
6
```

4.49.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. find less than operator
2. raise alert

4.49.6 References

Abbreviated Code Inspection Checklist Section 11.1.1, Control Variables”

4.50 Magic Number

This test checks for the presence of 'magic numbers' in the source code. Magic numbers are all constants of integer or floating point type that occur outside of initializer expressions. The user may configure the checker to ignore certain common constants such as 0 or 1. This detector reports not only hand-written constants but also those that were created by macro expansion.

Note that C++ does not have negative constants; `-1` is not an integer constant but rather the unary minus operator applied to the constant `1`. To ignore occurrences of `-1`, you must therefore instruct the checker to ignore the constant `1`, but this will also ignore all 'positive' occurrences.

4.50.1 Parameter Requirements

The magic number detector requires two entries in the parameter file, one of which is the list of integer constants to ignore, the other the list of floating point constants to ignore. Constants in both lists are separated by whitespace; as explained above, it does not make sense to specify negative values.

An example of parameter entries is:

MagicNumberDetector.allowedIntegers =
MagicNumberDetector.allowedFloats = 42.0 3.14159

This specification has an empty list of integers, so every integer constant (of any type) will be flagged as a magic number; the floating point constants 42.0 and 3.14159 are allowed to appear in the source code, but all others are treated as magic numbers. Note that floating point numbers are compared by numeric value, which may result in strange effects due to inexact representation.

4.50.2 Non-Compliant Code Example

```
1 int f_noncompliant(int n)
2 {
3     int x;
4     x = 42; // not OK: magic number
5     return x + n;
6 }
```

4.50.3 Compliant Solution

```
1 int f_compliant(int n)
2 {
3     int x = 42; // OK: constant only used in initializer
4     return x + n;
5 }
```

4.50.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For every integer or floating point literal, examine the enclosing statement to find out whether it occurs as part of the initializer in a variable declaration. If not, emit a diagnostic.

4.50.5 References

A reference for this pattern is: H. Sutter, A. Alexandrescu: "C++ Coding Standards", Item 17: "Avoid magic numbers".

4.51 Malloc Return Value Used In If Stmt

"ALE3D Coding Standards & Style Guide" item #4.5 states that

> When using raw `malloc()` and `new`, developers should check the return value for `NULL`. This is especially important when allocating large blocks of memory, which may exhaust heap resources.

4.51.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.51.2 Implementation

This pattern is checked using a simple AST traversal that seeks out function references to malloc. Then the parent nodes are traversed up until a basic scope block is found at which point a nested AST traversal seeks If-statement conditional expressions containing the memory block returned from malloc. If no such If-statement conditional is found in the immediate basic containing block scope then an error is flagged.

4.51.3 Non-Compliant Code Example

The non-compliant code fails to check the return value of `malloc()`.

```
1 #include <stdlib.h>
2
3 int main()
4 {
5   int *iptr = (int*)malloc( 256*sizeof(int) );
6
7   return 0;
8 } //main()
```

4.51.4 Compliant Solution

The compliant solution uses an if statement to check the return value of `malloc()` for `NULL`.

```
1 #include <stdlib.h>
2
3 int main()
4 {
5   int *iptr = (int*)malloc( 256*sizeof(int) );
6
7   if( iptr == NULL )
8     return 1;
9
10  return 0;
11 } //main()
```

4.51.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform AST traversal visiting function call nodes corresponding to `malloc()`.
2. For each call to `malloc()` traverse its parent nodes until an if statement or the end of a basic block is reached.
3. If an if statement is encountered, check that the if statement performs a comparison involving the return value from `malloc()`; if this is not the case then flag a violation.
4. If a basic block is reached, then flag a violation as the return value of `malloc()` may be out of scope.
5. Report any violations.

4.51.6 References

Arrighi B., Neely R., Reus J. "ALE3D Coding Standards & Style Guide", 2005.

4.52 Multiple Public Inheritance

Multiple inheritance in C++ can give rise to very complicated issues, in particular when a class has several public superclasses; in contrast, having a single public superclass and several private ones (only inheriting code from these, but not public interfaces) can be much more controllable. This checker ensures that no class has more than one public superclass, while not prohibiting multiple inheritance in general.

4.52.1 Parameter Requirements

This checker does not require any parameters.

4.52.2 Non-Compliant Code Example

```
1 // Dummy classes, the first of which is designed to be used as a base class
2 // from which one inherits an interface, the second designed to be used as a
3 // base class from which one only inherits an implementation.
4 class Interface { /* ... */ };
5 class Implementation { /* ... */ };
6
7 // not OK: multiple public base classes
8 class A: public Interface, public Implementation
9 {
10     /* ... */
11 };
```

4.52.3 Compliant Solution

```
1 class Interface { /* ... */ };
2 class Implementation { /* ... */ };
3
4 // OK: only one public base class, others may be non-public
5 class B: public Interface, private Implementation
6 {
7     /* ... */
8 };
```

4.52.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For each class definition, inspect the list of inheritances. If more than one base class is listed as public, emit a diagnostic.

4.52.5 References

This checker is a small part of the excellent discussion in: S. Meyers: “Effective C++ Second Edition”, Item 43: “Use multiple inheritance judiciously”.

4.53 Name All Parameters

This checker warn for anonymous parameters in function declarations and definitions. For definitions, if the argument is not used, a `static_cast<void>` should be used instead of not naming the parameter.

This checker check for the rule 22 from *The Elements of C++ Style* (Misfeldt and al., 2004).

4.53.1 Parameter Requirements

There is no parameter requirement.

4.53.2 Non-Compliant Code Example

```
1 void f(int)
2 {
3 }
```

4.53.3 Compliant Solution

To avoid warning messages from the compiler about unused variables, you can use a `static_cast<void>` to mark unused parameters.

```
1 void f(int i)
2 {
3   static_cast<void>(i);
4 }
```

4.53.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For all function declarations, check that all parameter has a name.

4.53.5 References

Bumgardner G., Gray A., and Misfeldt T. *The Elements of C++ Style*. Cambridge University Press 2004.

4.54 [No Reference] : New Delete

This analysis checks for the validity of all delete operations in a specific source code. It checks for violations of:

a) Deleting an array with a simple delete operator instead of an delete array operator.

b) Deleting a NULL pointer.

c) Checks for the deletion of uninitialized pointers.

4.54.1 Non-Compliant Code Examples

In the following examples, a) b) and c) from above are demonstrated.

```
1 class Y {
2   int y;
3 };
4
5 void fail() {
6   int x=2;
7   // deleting array
8   Y* m = new Y[5];
9   delete m;
10
11  // deleting NULL
12  Y* n = 0;
13  delete n;
14
15  // deleting NULL
16  Y* c ;
17  if (x==5) {
18    x=7;
19    delete c;
20  }
21 }
```

4.54.2 Compliant Solution

Use assert statements to make sure that a pointer cannot be null, or use the delete[] operator if a new[] operator precedes on that pointer.

4.54.3 Parameter Requirements

None.

4.54.4 Implementation

This analysis uses the BOOST library in order to utilize the breadth first search (BFS) algorithm. Together with the control flow graph and the BFS, the implementation backtracks the code from the delete operation to its definition. On violations of the described cases, the analysis results in warnings.

The algorithm searches first for each occurance of a SgDeleteExp and backtracks this Node to its definition. If we find a SgNew operation, we need to see if the delete and new operations match, i.e. whether they are both operations on pointers or arrays.

The following cases are checked for and handled during the backwards dataflow analysis:

```
1  case V_SgNewExp:
2  case V_SgVarRefExp:
3  case V_SgAddressOfOp:
4  case V_SgCastExp:
5  case V_SgIntVal:
```

The above indicates a recursive algorithm.

4.54.5 References

4.55 No Exceptions

This checker detects all usages of C++ exception handling.

4.55.1 Parameter Requirements

No parameters are required.

4.55.2 Implementation

The checker detects try statements, throw operations and catch statements.

4.55.3 Non-Compliant Code Example

```
1 class Exception{};
2
3 int main(){
4  try {
5     throw Exception();
6  } catch( Exception e )
7     { }
8 };
```

4.55.4 Compliant Solution

```
1 int main(){
2 };
```

4.55.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Traverse the AST
2. For each try statements, throw operations and catch statements report and error.

4.55.6 References

The ALE3D style guide section 17.1 forbids usage of C++ exceptions.

4.56 No Exit In Mpi Code

"ALE3D Coding Standards & Style Guide" item #19.1 states that

> `exit()` must never be called from a parallel code. Calling `exit()` from a parallel code will cause the code to deadlock. Even if you can guarantee that every processor will call `exit()` collectively, this can leave some parallel environments in a hung state because MPI resources are not properly cleaned up.

4.56.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.56.2 Implementation

This pattern is checked using a simple AST traversal seeking function reference expressions. These function reference expressions matching a call to the exit() function between blocks of MPI code (as delimited between MPI Init and MPI Finalize) are flagged as checker violations.

4.56.3 Non-Compliant Code Example

This trivial non-compliant code calls `exit()` from an MPI block.

```
1 #include <stdlib.h>
2 #include "mpi.h"
3
4 int main( int argc, char **argv )
5 {
6   MPI_Init( &argc, &argv );
7     exit(1);
8   MPI_Finalize();
9
10   return 0;
11 } //main()
```

4.56.4 Compliant Solution

The compliant solution uses `MPI_Abort()` instead.

```
1 #include <stdlib.h>
2 #include "mpi.h"
3
4 int main( int argc, char **argv )
5 {
6   MPI_Init( &argc, &argv );
7     MPI_Abort( MPI_COMM_WORLD, 1 );
8   MPI_Finalize();
9
10   return 0;
11 } //main()
```

4.56.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform a simple AST traversal of nodes that occur between `MPI_Init()` and `MPI_Finalize()` blocks.
2. For each node between MPI blocks, if node is call to `exit()` then flag violation.
3. Report any violations.

4.56.6 References

Arrighi B., Neely R., Reus J. "ALE3D Coding Standards & Style Guide", 2005.

4.57 No Goto

This checker detects uses of `goto` statements conforming with *High-Integrity C++ Coding Standard Manual*, rule 5.8: "Do not use `goto`"

4.57.1 Parameter Requirements

No parameter is needed

4.57.2 Non-Compliant Code Example

```
1 void foo() {
2   tryAgain:
3   try {
4     doSomething();
5   }
6   catch (...) {
7     goto tryAgain;
8   }
9 }
```

4.57.3 Compliant Solution

```
1 void foo() {
2   do {
3     try {
4       doSomething();
5     }
6     catch (...) {
7       continue ;
8     }
9     break ;
10  } while (true);
11 }
```

4.57.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Look for goto expressions.

4.57.5 References

The Programming Research Group, *High-Integrity C++ Coding Standard Manual*, rule 5.8: "Do not use `goto`".

4.58 Non Associative Relational Operators

C++ Secure Coding Practices states that:

> The relational and equality operators are left-associative, not non-associative as they often are in other languages. This allows a C++ programmer to write an expression (particularly an expression used as a condition) that can be easily misinterpreted.

This checker checks that relational binary operators ($==, !=, <, >, <=, >=$) are not treated as if they were non-associative.

4.58.1 Parameter Requirements

This checker takes no parameters and inputs source file

4.58.2 Implementation

This pattern is checked using a nested AST traversal on the parent nodes of the operand of a binary operator expression. Any such parent node that treats relational binary operators as non-associative will use more than one binary relational operator. Flag these expressions as violations.

4.58.3 Non-Compliant Code Example

```
1 #include <stdio.h>
2
3 int main()
4 {
5   int a = 2;
6   int b = 2;
7   int c = 2;
8
9   if ( a < b < c ) // condition #1, misleading, likely bug
10    printf( "a < b < c\n" );
11  if ( a == b == c ) // condition #2, misleading, likely bug
12    printf( "a == b == c\n" );
13
14  return 0;
15 }
```

4.58.4 Compliant Solution

```
1 #include <stdio.h>
2
3 int main()
4 {
5   int a = 2;
6   int b = 2;
7   int c = 2;
8
9   if ( a < b && b < c ) // clearer, and probably what was intended
10    printf( "a < b && b < c\n" );
11  if ( a == b && a == c ) // ditto
12    printf( "a == b && a == c\n" );
13
14  return 0;
15 }
```

4.58.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform simple AST traversal and locate SgBinaryOp nodes.
2. At each SgBinaryOp node perform a nested traversal of the operands parent node and count the number of relational binary operators used.
3. If said count is greater than one then flag error.
4. Report all errors.

4.58.6 References

EXP09-A. Treat relational and equality operators as if they were nonassociative

4.59 Nonmember Function Interface Namespace

User-defined classes should typically reside in the same namespace as their nonmember function interface, i.e. friend functions and operators for that class. The reasons are uniform lookup of overloaded functions and that the interface of a class consists not only of its member functions. This checker enforces this guideline. It reports friend function declarations that refer to functions from a different namespace. Further, it makes sure that every class mentioned in a nonmember operator's signature (return and argument types) is in the same namespace as the operator, or in the global std namespace.

4.59.1 Parameter Requirements

No parameters are required.

4.59.2 Non-Compliant Code Example

```
1 void f(); // not OK: used as friend in class N::A, not in same namespace
2 namespace N
3 {
4     class A
5     {
6     public:
7         friend void ::f();
8     };
9 }
```

4.59.3 Compliant Solution

```
1 namespace M
2 {
3     void f(); // OK: used as friend in M::B, same namespace
4
5     class B
6     {
7     public:
8         friend void f();
9     };
10 }
```

4.59.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For each friend function or operator for a class, look up the namespace it is declared in and compare to the namespace of the class.

4.59.5 References

The reference for this checker is: H. Sutter, A. Alexandrescu: "C++ Coding Standards", Item 57: "Keep a type and its nonmenber function interface in the same namespace".

4.60 Non Standard Type Ref Args

Per the Abbreviated C++ Code Inspection Checklist "While it is cheaper to pass ints, longs, and such by value, passing objects this way incurs significant expense due to the construction of temporary objects. The problem becomes more severe when inheritance is involved. Simulate pass-by-value by passing const references."

4.60.1 Parameter Requirements

No parameters necessary

4.60.2 Implementation

The arguments to all functions are checked for base type in the declaration. If the base type is found to be a struct or a class, it is then checked to ensure it is a reference. If it is not, a notification is raised.

4.60.3 Non-Compliant Code Example

```
1
2 class incrediblyComplex
3 {
4 private:
5 //loads of members
6 }
7
8 bool justLooking(incrediblyComplex fullCopy)
9 {
10 return (! &fullCopy);
11 }
12
```

4.60.4 Compliant Solution

```
1
2 class incrediblyComplex
3 {
4 private:
5 //loads of members
6 }
7
8 bool justLooking(incrediblyComplex& fullCopy)
9 {
10 return (! &fullCopy);
11 }
12
13
```

4.60.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Identify function declaration
2. Check arguments for base type
3. if non-intrinsic type and not a reference, notify

4.60.6 References

Abbreviated Code Inspection Checklist Section 13.1, Argument Passing"

4.61 Non Standard Type Ref Returns

While it is cheaper to pass ints, longs, and such by value, passing objects this way incurs significant expense due to the construction of temporary objects. The problem becomes more severe when inheritance is involved. Simulate pass-by-value by passing const references.

4.61.1 Parameter Requirements

No parameters necessary.

4.61.2 Implementation

The return types to all functions are checked for base type in the declaration. If the base type is found to be a struct or a class, it is then checked to ensure it is a reference. If it is not, a notification is raised.

4.61.3 Non-Compliant Code Example

```
1
2
3 class incrediblyComplex
4 {
5 private:
6 //loads of members
7 }
8
9 incrediblyComplex justLooking()
10 {
11 incrediblyComplex *fullCopy = new incrediblyComplex();
12 return (*fullCopy);
13 }
14
15
```

4.61.4 Compliant Solution

```
1
2 class incrediblyComplex
3 {
4 private:
5 //loads of members
6 }
7
8 incrediblyComplex& justLooking()
9 {
10 incrediblyComplex *fullCopy = new incrediblyComplex();
11 return (*fullCopy);
12 }
13
```

4.61.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Identify function declaration
2. Check return for base type
3. if non-intrinsic type and not a reference, notify

4.61.6 References

Abbreviated Code Inspection Checklist Section 14.5, Return Values"

4.62 Non Virtual Redefinition

Calls of nonvirtual member functions are resolved at compile time, not run time. Redefinition of an inherited nonvirtual function in a derived class has different semantics that can result in surprising behavior and should therefore be avoided. This checker reports cases where a class redefines a function that was declared nonvirtual in one of its superclasses.

4.62.1 Parameter Requirements

This checker does not require any parameters.

4.62.2 Non-Compliant Code Example

```
1  namespace NonCompliant {
2      class Base {
3      public:
4          virtual void overrideIfYouWish(int);
5          void doNotOverride(int);
6      };
7
8      class Inherited: public Base {
9      public:
10         void doNotOverride(int); // trying to override nonvirtual function
11     };
12 }
```

4.62.3 Compliant Solution

```
1  namespace Compliant {
2      class Base {
3      public:
4          virtual void overrideIfYouWish(int);
5          void doNotOverride(int);
6      };
7
8      class Inherited: public Base {
9      public:
10         void overrideIfYouWish(int); // overriding virtual function
11     };
12 }
```

4.62.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For every member function declaration, traverse the inheritance DAG of the enclosing class.
2. Identify any functions that may be overridden by the current one (by checking name and type).
3. Issue a diagnostic if the overridden function is not declared virtual.

4.62.5 References

A reference for this checker is: S. Meyers: "Effective C++ Second Edition", Item 37: "Never redefine an inherited nonvirtual function."

4.63 No Overload Ampersand

The C++ standard [ISO/IEC 14882-2003] says in Section 5.3.1 paragraph 4 that

The address of an object of incomplete type can be taken, but if the complete type of that object is a class type that declares operator&() as a member function, then the behavior is undefined (and no diagnostic is required).

Therefore, to avoid possible undefined behavior, the operator & should not be overloaded.

4.63.1 Parameter Requirements

No Parameters Required.

4.63.2 Implementation

We check any member function then compare the name to 'operator&'. If this combination is found an alert is raised.

4.63.3 Non-Compliant Code Example

```
1
2 class peanutButter
3 {
4   string name;
5   void operator&()
6   {
7     name += '&jelly';
8   }
9 }
10
```

4.63.4 Compliant Solution

```
1
2 class peanutButter
3 {
4   string name;
5   void addJelly()
6   {
7     name += '&jelly';
8   }
9 }
10
```

4.63.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Find member function
2. Check name

3. raise alert

4.63.6 References

ISO/IEC 9899-1999:TC2 ISO/IEC 14882-2003 Section 5.3.1, “Unary operators” Lockheed Martin 05 AV Rule 159, “Operators ||, &&, and unary & shall not be overloaded”

4.64 CERT-MSC30-C: No Rand

"CERT Secure Coding MSC30-C" states

> The C Standard function `rand` (available in `stdlib.h`) does not have good random number properties. The numbers generated by `rand` have a comparatively short cycle, and the numbers may be predictable. To achieve the best random numbers possible, an implementation-specific function needs to be used.

4.64.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.64.2 Implementation

This pattern is checked using a simple AST traversal that visits all function reference expressions. If a functino reference expression node corresponds to the `rand()` function, then a violation is flagged.

4.64.3 Non-Compliant Code Example

The following code calls `rand()`.

```
1 #include <stdlib.h>
2
3 int main()
4 {
5   int r = rand();  /* generate a random integer */
6
7   return 0;
8 }
```

4.64.4 Compliant Solution

The compliant solution is to use a implementation-specific random number generator.

```
1 int main()
2 {
3   int r = my_rand();  /* generate a random integer */
4
5   return 0;
6 }
```

4.64.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform a simple AST traversal visiting all function reference expression nodes.

2. For each node visited, if the function reference expression corresponds to `rand()` then flag violation.
3. Report any violations.

4.64.6 References

Secure Coding : MSC30-C. Do not use the rand function

4.65 No Second Term Side Effects

The logical AND and logical OR operators (&&, ||) exhibit "short circuit" operation. That is, the second operand is not evaluated if the result can be deduced solely by evaluating the first operand. Consequently, the second operand should not contain side effects because, if it does, it is not apparent if the side effect occurs

4.65.1 Parameter Requirements

No parameters required.

4.65.2 Implementation

We check for And or Or. We then query for any of a set of operators known to have side effects. This checker has the known deficiency of not checking function calls for side-effects. To avoid false positives, it does not notify of functions at all.

4.65.3 Non-Compliant Code Example

```
1 int i;
2 int max;
3
4 if ( (i >= 0 && (i++) <= max) ) {
5   /* code */
6 }
```

It is unclear whether the value of i will be incremented as a result of evaluating the condition.

4.65.4 Compliant Solution

In this compliant solution, the behavior is much clearer.

```
1 int i;
2 int max;
3
4 if ( (i >= 0 && (i + 1) <= max) ) {
5   i++;
6   /* code */
7 }
```

4.65.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Find the And or Or operator
2. query the right-hand child for known side-effect having operators

4.65.6 References

ISO/IEC 9899-1999:TC2 [ISO/IEC 9899-1999] Section 6.5.13, “Logical AND operator,” and Section 6.5.14, “Logical OR operator”

4.66 Secure Coding : EXP06-A. Operands to the sizeof operator should not contain side effects

The `sizeof` operator yields the size (in bytes) of its operand, which may be an expression or the parenthesized name of a type. If the type of the operand is not a variable length array type the operand is **not** evaluated.

Providing an expression that appears to produce side effects may be misleading to programmers who are not aware that these expressions are not evaluated. As a result, programmers may make invalid assumptions about program state leading to errors and possible software vulnerabilities.

4.66.1 Non-Compliant Code Example

In this example, the variable `a` will still have a value 14 after `b` has been initialized.

```
1 int a = 14;
2 int b = sizeof(a++);
3
```

The expression `a++` is not evaluated. Consequently, side effects in the expression are not executed.

Implementation Specific Details

This example compiles cleanly under Microsoft Visual Studio 2005 Version 8.0, with the /W4 option.

4.66.2 Compliant Solution

In this compliant solution, the variable `a` is incremented.

```
1 int a = 14;
2 int b = sizeof(a);
3 a++;
4
```

Implementation Specific Details

This example compiles cleanly under Microsoft Visual Studio 2005 Version 8.0, with the /W4 option.

4.66.3 Risk Assessment

If expressions that appear to produce side effects are supplied to the `sizeof` operator, the returned result may be different then expected. Depending on how this result is used, this could lead to unintended program behavior.

Rule	Severity	Likelihood	Remediation Cost	Priority	Level
EXP06-A	**1** (low)	**1** (unlikely)	**3** (low)	**P3**	**L3**

Related Vulnerabilities

Search for vulnerabilities resulting from the violation of this rule on the CERT website .

4.66.4 References

[ISO/IEC 9899-1999] Section 6.5.3.4, "The sizeof operator"

4.67 No Template Usage

Finds all usages of C++ templates. It will not detect C++ template declarations that are not instantiated.

4.67.1 Parameter Requirements

No parameters are required.

4.67.2 Implementation

The checker finds all template instatiation declaration, template instatiation definitions, template instantiation member function declarations and template instatiation function declarations.

4.67.3 Non-Compliant Code Example

```
1 template<typename t>
2 class Foo
3 {
4    public:
5       Foo(){};
6       ~Foo(){};
7 };
8
9 void main()
10 {
11  Foo<int>    fi;
12  Foo<float> ff;
13 }
```

4.67.4 Compliant Solution

```
1 class Foo
2 {
3    public:
4       Foo(){};
5       ~Foo(){};
6 };
7
8 void main()
9 {
10  Foo    fi;
11  Foo    ff;
12 }
```

4.67.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Traverse the AST
2. For each template instantiations and template declaration report an error

4.67.6 References

The ALE3D style guide section 16.1 states that templates must not be used.

4.68 CERT-POS33-C: No Vfork

"CERT Secure Coding POS33-C" states

> Using the `vfork` function introduces many portability and security issues. There are many cases in which undefined and implementation specific behavior can occur, leading to a denial of service vulnerability.

4.68.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.68.2 Implementation

This pattern is checked using a simple AST traversal that visits all function reference expressions. If a functino reference expression node corresponds to the `vfork()` function, then a violation is flagged.

4.68.3 Non-Compliant Code Example

This non-compliant example calls `vfork()`.

```
1  #include <stdlib.h>
2  #include <unistd.h>
3
4  int main()
5  {
6    pid_t pid = vfork();
7
8    if ( pid == 0 )  /* child */
9    {
10     system( "echo \"Hello World\"" );
11   }
12
13   return 0;
14 }
```

4.68.4 Compliant Solution

The compliant solution calls `fork()` instead.

```
1  #include <stdlib.h>
2  #include <unistd.h>
3
4  int main()
5  {
6    pid_t pid = fork();
7
8    if ( pid == 0 )  /* child */
9    {
10     system( "echo \"Hello World\"" );
11   }
12
13   return 0;
14 }
```

4.68.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform a simple AST traversal visiting all function reference expressions.
2. For each node visited, if the function reference expression corresponds to `vfork()` then flag violation.
3. Report any violations.

4.68.6 References

Secure Coding : POS33-C. Do not use vfork()

4.69 CERT EXP33-C and EXP34-C : Null Dereference

NULL Dereference checker. If any variable that could be NULL is dereferenced, a warning is issued. This is an implementation of US-CERT rules: EXP33-C - Do not reference uninitialized variables and EXP34-C - Ensure a pointer is valid before dereferencing it.

EXP33-C - Do not reference uninitialized variables

Local, automatic variables can assume unexpected values if they are used before they are initialized. C99 specifies *If an object that has automatic storage duration is not initialized explicitly, its value is indeterminate* [ISO/IEC 9899-1999]. In practice, this value defaults to whichever values are currently stored in stack memory. While uninitialized memory often contains zero, this is not guaranteed. Consequently, uninitialized memory can cause a program to behave in an unpredictable or unplanned manner and may provide an avenue for attack.

4.69.1 EXP34-C - Ensure a pointer is valid before dereferencing it

Attempting to dereference an invalid pointer results in undefined behavior, typically abnormal program termination. Given this, pointers should be checked to make sure they are valid before they are dereferenced.

4.69.2 Non-Compliant Code Examples

EXP33-C - Do not reference uninitialized variables

In this example, the set_flag() function is supposed to set a the variable sign to 1 if number is positive and -1 if number is negative. However, the programmer forgot to account for number being 0. If number is 0, then sign will remain uninitialized. Because sign is uninitialized, it assumes whatever value is at that location in the program stack. This may lead to unexpected, incorrect program behavior.

```
1 void set_flag(int number, int *sign_flag) {
2   if (number > 0) {
3     *sign_flag = 1;
4   }
5   else if (number <0) {
6     *sign_flag = -1;
7   }
8   int x = *sign_flag;
9 }
10
11 int main(int argc, char** argv) {
12   int sign;
13   set_flag(0,&sign);
14   return 0;
15 }
```

EXP34-C - Ensure a pointer is valid before dereferencing it

In this example, input_str is copied into dynamically allocated memory referenced by str. If malloc() fails, it returns a NULL pointer that is assigned to str. When str is dereferenced in strcpy(), the program behaves in an unpredictable manner.

```
1 #include "assert.h"
2 #include <stdlib.h>
3
4 void testme() {
5   // case 1
6   int size = 5;
7   char* str = (char*) malloc(size+1);
8   char z = *str;
9
10  // case 2
11  int *p = 0;
12  int l = *p;
13
14  // case 3
15  char *k=0;
16  free(k);
17
18 }
```

4.69.3 Compliant Solution

EXP33-C - Do not reference uninitialized variables

We do not check the expressions in if conditions, and hence it is irrelevant what the if conditions state. However, because an if condition occurs, there might be a path that leaves sign_flag uninitialized. In this case a simple assert helps to avoid the warning caused by this analysis.

```
1 #include "assert.h"
2
3 void set_flag(int number, int *sign_flag) {
4   assert(sign_flag);
5   if (number > 0) {
6     *sign_flag = 1;
7   }
8   else if (number <0) {
9     *sign_flag = -1;
10  }
11  int x = *sign_flag;
12 }
13
14 int main(int argc, char** argv) {
15   int sign;
16   set_flag(0,&sign);
17   return 0;
18 }
```

4.69.4 EXP34-C - Ensure a pointer is valid before dereferencing it

```
1 #include "assert.h"
2 #include <stdlib.h>
3
4 void testme() {
5   // case 1
6   int size = 5;
```

```
 7   char* str = (char*) malloc(size+1);
 8   if (str==NULL) {
 9     *str = '5';
10   }
11   char z = *str;
12
13   // case 2
14   int *p = 0;
15   assert(p);
16   int l = *p;
17
18   // case 3
19   char *k=0;
20   assert(k);
21   free(k);
22
23 }
```

4.69.5 Parameter Requirements

None.

4.69.6 Implementation

We use a dataflow analysis to determine null dereference. The dataflow analysis is based on an *breadth first search* (bfs) algorithm, implemented in BOOST. The implementation does a bfs backwards traversal for each:

a) SgArrowExp
b) SgPointerDerefExp
c) SgAssignInitializer
d) SgFunctionCallExp (free)

The above are the points that need to be validated by the algorithm. At each such point the program might be invalid due to NULL pointer dereferences. Therefore, the variable at that point must be determined and the programmed is tracked back (dataflow).

If at any point an assertion is found, the analysis is aborted for that run, i.e. no null pointer dereference is present.

4.69.7 References

EXP33C , "Do not reference uninitialized variables"
EXP34C , "Ensure a pointer is valid before dereferencing it"

4.70 CERT-DCL04-A: One Line Per Declaration

"CERT Secure Coding DCL04-A" states

> Declaring multiple variables on a single line of code can cause confusion regarding the types of the variables and their initial values. If more than one variable is declared on a line, care must be taken that the actual type and initialized value of the variable is known. To avoid confusion, more than one type of variable should not be declared on the same line.

4.70.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.70.2 Implementation

This pattern is checked using a simple AST traversal, visiting all variable declaration statements. The line number of each variable declaration statement node is saved to a std set unique to each file. If any line number is added to this set more than once then a violation is flagged.

4.70.3 Non-Compliant Code Example

The non-compliant code declares multiple `int` variables on the same line.

```
1 int main()
2 {
3   int i1 = 0, i2 = 0, i3 = 0;
4
5   return 0;
6 }
```

4.70.4 Compliant Solution

The compliant solution is to give each `int` declaration its own line.

```
1 int main()
2 {
3   int i1 = 0;
4   int i2 = 0;
5   int i3 = 0;
6
7   return 0;
8 }
```

4.70.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform a simple AST traversal visiting all variable declaration nodes.

2. For each line number associated with a variable declaration node, add the line number to a set of line numbers unique to its source file.
3. If any line number is added more than once per source file set of line numbers then flag a violation.
4. Report any violations.

4.70.6 References

Secure Coding : DCL04-A. Take care when declaring more than one variable per line

4.71 Operator Overloading

This test detects function declaration that overloads operators that can cause subtle bugs, such as "`&&`", "`||`", or "`,`". That is, one can not ensure that the overloaded operators will be evaluated in left-to-right order. This is based on the following rules:

- Function calls always evaluate all arguments before execution.
- The order of evaluation of function arguments is unspecified.

For example,

```
1 auto_ptr<Employee> e = GetEmployee();
2 if(e && e->Manager())
```

The usual evaluation order (left to right) prevents the test from executing `e->Manager()` and the code above looks fine. However, the code above can invoke an overloaded `operator&&` and it will potentially call `e->Manager()` before checking if `e` is `NULL`.

4.71.1 Parameter Requirements

None.

4.71.2 Implementation

This pattern is detected using a simple traversal. It traverses AST to find function declarations and check whether or not the name of the functions is "`operator&&`", "`operator||`", or "`operator,`".

4.71.3 Non-Compliant Code Example

```
1 class Test
2 {
3   public:
4     Test();
5     ~Test();
6     Test operator&&(const Test &);
7     Test operator||(const Test &);
8     Test operator,(const Test &);
9 };
```

4.71.4 Compliant Solution

```
1 N/A
```

4.71.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Check if a node is a function declaration

2. Check if the name of the function contains "`operator&&`", "`operator||`", or "`operator,`".

4.71.6 References

T. Misfeldt, G. Bumgardner, A. Gray, "The Elements of C++ Style", Item 111: "Do not overload `operator &&` or `operator ||`".

4.72 Other Argument

This checker enforce the name convention of the first argument in copy constructors and copy operators. This is taken from rule 23 from *the Elements of C++ Style* (Misfeldt and al., 2004). The parameter should be called `other`. This checker also accept two other naming conventions: `that` and the class name in lower camel case.

4.72.1 Parameter Requirements

There is no parameter requirement.

4.72.2 Non-Compliant Code Example

```
1 A::A(const A& foo)
2 {
3   //...
4 }
```

4.72.3 Compliant Solution

```
1 A::A(const A& other)
2 {
3   //...
4 }
```

4.72.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For all constructors and operator fulfilling the copy requirement of the C++ standard, check that the first parameter is of the three possible name.

4.72.5 References

Bumgardner G., Gray A., and Misfeldt T. *The Elements of C++ Style*. Cambridge University Press 2004.

4.73 Place Constant On The Lhs

This checker detects a test clause whether or not it contains a constant on the left hand side when comparing a varialbe and the constant for equality. By putting the constant on the left hand side, the compiler can prevent programmers from making mistake to write '=' for '=='.

4.73.1 Parameter Requirements

None

4.73.2 Implementation

This checker is implemented with a simple traversal. It traverses AST and finds a test clause. If the test clause has a variable on its left hand side, then, then the checker report this clause to the standard output.

4.73.3 Non-Compliant Code Example

```
1 void foo()
2 {
3 int a = 0;
4
5 if(a == 10) // a is on the LHS
6 {
7 a = 1;
8 }
9
10 while(a == 10) // a is on the LHS
11 {
12 a++;
13 }
14
15 do
16 {
17 a++;
18 }while(a == 12); // a is on the LHS
19
20 for(int i = 0; i == 0; i++) // i is on the LHS
21 {
22 a = 12;
23 }
24 }
```

4.73.4 Compliant Solution

```
1 void foo()
2 {
3 int a = 0;
4
5 if(1 == a) // fine
6 {
7 a = 2;
8 }
9 }
```

4.73.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Check if the node visiting is an if statement.
2. If yes, find its test clause to see if it contains a constant on the left hand side.
3. Check also if the if statement compares a variable and the constant for equality

4.73.6 References

The Programming Research Group: High-Integrity C++ Coding Standard Manual, Item 10.6: "When comparing variables and constants for equality always place place the constnat on the left hand side."

4.74 Prefer Algorithms

Many people consider hand-written loops over STL containers inferior to calls to STL algorithms for reasons of efficiency, correctness, and maintainability.

This checker is meant to highlight cases where a loop might be replaced by an equivalent STL algorithm call. It reports for loops where the loop head fulfills the following properties:

- The initialization part contains an assignment or variable declaration with an initializer,
- the condition part consists of an inequality comparison, and
- the increment part consists of an increment or decrement operation.

For loops on integer or floating-point types are not reported as those cannot be replaced by STL algorithms.

4.74.1 Parameter Requirements

This checker does not require any parameters.

4.74.2 Non-Compliant Code Example

```
1 #include <vector>
2
3 void add_x_to_each_element_noncompliant(int x, std::vector<int> &v)
4 {
5     // not OK: loop to add x to each element
6     std::vector<int>::iterator v_itr;
7     for (v_itr = v.begin(); v_itr != v.end(); ++v_itr)
8         *v_itr += x;
9 }
```

4.74.3 Compliant Solution

```
1 #include <vector>
2 #include <algorithm>
3 #include <functional>
4
5 void add_x_to_each_element_compliant(int x, std::vector<int> &v)
6 {
7     // OK: using an algorithm to add x to each element
8     transform(v.begin(), v.end(), v.begin(),
9               std::bind2nd(std::plus<int>(), x));
10 }
```

4.74.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For each for loop, check the criteria explained above, taking both built-in and overloaded operators.
2. If the loop fulfills all criteria, generate a diagnostic.

4.74.5 References

A reference for this checker is: S. Meyers: “Effective STL”, Item 43: “Prefer algorithm calls to hand-written loops”.

4.75 Secure Coding : FIO07-A. Prefer fseek() to rewind()

`rewind()` sets the file position indicator for a stream to the beginning of that stream. However, `rewind()` is equivalent to `fseek()` with `0L` for the offset and `SEEK_SET` for the mode with the error return value suppressed. Therefore, to validate that moving back to the beginning of a stream actually succeeded, `fseek()` should be used instead of `rewind()`.

4.75.1 Non-Compliant Code Example

The following non-compliant code sets the file position indicator of an input stream back to the beginning using `rewind()`.

```
1 FILE* fptr = fopen("file.ext", "r");
2 if (fptr == NULL) {
3   /* handle open error */
4 }
5
6 /* read data */
7
8 rewind(fptr);
9
10 /* continue */
11
```

However, there is no way of knowing if `rewind()` succeeded or not.

4.75.2 Compliant Solution

This compliant solution instead using `fseek()` and checks to see if the operation actually succeeded.

```
1 FILE* fptr = fopen("file.ext", "r");
2 if (fptr == NULL) {
3   /* handle open error */
4 }
5
6 /* read data */
7
8 if (fseek(fptr, 0L, SEEK_SET) != 0) {
9   /* handle repositioning error */
10 }
11
12 /* continue */
13
```

4.75.3 Risk Assessment

Using `rewind()` makes it impossible to know whether the file position indicator was actually set back to the beginning of the file. If the call does fail, the result may be incorrect program flow.

Rule	Severity	Likelihood	Remediation Cost	Priority	Level
FIO07-A	**1** (low)	**1** (unlikely)	**2** (medium)	**P2**	**L3**

Related Vulnerabilities

Search for vulnerabilities resulting from the violation of this rule on the CERT website .

4.75.4 References

[ISO/IEC 9899-1999:TC2] Section 7.19.9.2, "The `fseek` function"; 7.19.9.5, "The `rewind` function"

4.76 Prefer Setvbuf To Setbuf

The functions setvbuf() and setbuf() are defined as follows:

void setbuf(FILE * restrict stream, char * restrict buf); int setvbuf(FILE * restrict stream, char * restrict buf, int mode, size_t size);

setvbuf() is equivalent to setbuf() with _IOFBF for mode and BUFSIZE for size (if buf is not NULL) or _IONBF for mode (if buf is NULL), except that it returns a nonzero value if the request could not be honored. For added error checking, prefer using setvbuf() over setbuf().

4.76.1 Parameter Requirements

No Parameter specifications.

4.76.2 Implementation

No implementation yet!

4.76.3 Non-Compliant Code Example

The following non-compliant code makes a call to setbuf() with an argument of NULL to ensure an optimal buffer size.

```
1
2 FILE* file;
3 char *buf = NULL;
4 /* Setup file */
5 setbuf(file, buf);
6 /* ... */
7
```

However, there is no way of knowing whether the operation succeeded or not.

4.76.4 Compliant Solution

This compliant solution instead calls setvbuf(), which returns nonzero if the operation failed.

```
1
2 FILE* file;
3 char *buf = NULL;
4 /* Setup file */
5 if (setvbuf(file, buf, buf ? _IOFBF : _IONBF, BUFSIZ) != 0) {
6   /* Handle error */
7 }
8 /* ... */
9
```

4.76.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Write your checker algorithm

4.76.6 References

ISO/IEC9899-1999:TC2 FIO12-A. Prefer setvbuf() to setbuf()

4.77 Protect Virtual Methods

The Elements of C++ Style item #107 states

> Do not expose virtual methods in the public interface of a class. Use a public methods with a similar name to call the protected virtual method.

4.77.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.77.2 Implementation

This pattern is checked using a simple AST traversal that seeks instances of SgMemberFunctionDeclaration that have the public access modifier and the virtual function modifier boolean values set to true. Member functions that match this pattern are flagged as violations.

4.77.3 Non-Compliant Code Example

This non-compliant code contains a virtual function in the public interface of a class.

```
1 class Class
2 {
3   int n;
4
5   public:
6     Class() { n = publicVirtualFunction(); } //constructor
7     ~Class() {} //Destructor
8
9     virtual int publicVirtualFunction() { return 1; }
10 }; //class Class
```

4.77.4 Compliant Solution

The compliant solution protects the virtual function and adds a public accessor to the virtual function.

```
1 class Class
2 {
3   int n;
4
5   protected:
6     virtual int protectedVirtualFunction() { return 1; }
7   public:
8     Class() { n = publicVirtualFunction(); } //constructor
9     ~Class() {} //Destructor
10    int publicVirtualFunction(){ return protectedVirtualFunction(); }
11 }; //class Class
```

4.77.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform a simple AST traversal visiting all function declaration nodes.
2. For each function declaration check the "public" and "virtual" modifiers. If both "public" and "virtual" modifiers are set then flag violation.
3. Report any violations.

4.77.6 References

Bumgardner G., Gray A., and Misfeldt T. *The Elements of C++ Style*. Cambridge University Press 2004.

4.78 Push Back

Tests if the source uses front or back insertion in sequences using insert or resize where a `push_front` or `push_back` could be used. The patterns are very simple and matches simple calls like `vector.insert(vector.end(), ...)`.

In these case, `push_back` and `push_front` only are insured to be efficient. All other calls may be quadratic.

This test is inspired by the rule 80 of C++ Coding Standards: "Use the accepted idioms to really shrink capacity and really erase elements".

4.78.1 Parameter Requirements

There is no parameter required.

4.78.2 Implementation

No implementation yet!

4.78.3 Non-Compliant Code Example

```
1 #include <vector>
2 #include <list>
3
4 void g()
5 {
6   std::vector<int> v;
7   v.insert(v.end(), 1);
8
9   v.resize(v.size() + 1, 1);
10
11  std::list<int>* vv = new std::list<int>();
12  vv->insert(vv->begin(), 1);
13
14 }
```

4.78.4 Compliant Solution

```
1 #include <vector>
2 #include <list>
3
4 void g()
5 {
6   std::vector<int> v;
7   v.push_back(1);
8   v.push_back(1);
9
10  std::list<int>* vv = new std::list<int>();
11  vv->push_front(1);
12
13 }
```

4.78.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers looking for these patterns:

For all types `T`,
where `V` variable of type `vector<T>`,
where `Vp` variable of type `vector<T>*`,
where `L` variable of type `list<T>`,
where `Lp` variable of type `list<T>*`,
where `S` variable of type `slist<T>`,
where `Sp` variable of type `slist<T>*`,
where `D` variable of type `deque<T>`,
where `Dp` variable of type `deque<T>*`,
where `Value` expression of type `T`,
the check will look for these patterns in the source code.

```
1  V.resize(V.size() + 1, Value)
2  Vp->resize(Vp->size() + 1, Value)
3  D.resize(D.size() + 1, Value)
4  Dp->resize(Dp->size() + 1, Value)
5  L.resize(L.size() + 1, Value)
6  Lp->resize(Lp->size() + 1, Value)
7  V.resize(1 + V.size(), Value)
8  Vp->resize(1 + Vp->size(), Value)
9  D.resize(1 + D.size(), Value)
10 Dp->resize(1 + Dp->size(), Value)
11 L.resize(1 + L.size(), Value)
12 Lp->resize(1 + Lp->size(), Value)
13 V.insert(V.end(), Value)
14 Vp->insert(Vp->end(), Value)
15 D.insert(D.end(), Value)
16 Dp->insert(Dp->end(), Value)
17 L.insert(L.end(), Value)
18 Lp->insert(Lp->end(), Value)
19 S.insert(S.begin(), Value)
20 Sp->insert(Sp->begin(), Value)
21 D.insert(D.begin(), Value)
22 Dp->insert(Dp->begin(), Value)
23 L.insert(L.begin(), Value)
24 Lp->insert(Lp->begin(), Value)
```

For all `resize` and back `insert` patterns, `push_back` could be used. For front `insert` patterns, `push_front` could be used instead.

4.78.6 References

Alexandrescu A. and Sutter H. *C++ Coding Standards 101 Rules, Guidelines, and Best Practices*. Addison-Wesley 2005.

4.79 Right Shift Mask

Do not assume that a right shift operation is implemented as either an arithmetic (signed) shift or a logical (unsigned) shift. If E1 in the expression E1 ¿¿ E2 has a signed type and a negative value, the resulting value is implementation defined and may be either an arithmetic shift or a logical shift. Also, be careful to avoid undefined behavior while performing a bitwise shift.

4.79.1 Parameter Requirements

No Parameter Required.

4.79.2 Implementation

Upon finding a right shift we trace parent pointers up until we find a bit and operator. If we find this bitwise and then we return. If we make it to the basic block node of the statement we raise an alert.

4.79.3 Non-Compliant Code Example

For implementations in which an arithmetic shift is performed and the sign bit can be propagated as the number is shifted.

```
1 int stringify;
2 char buf[sizeof("256")];
3 sprintf(buf, "%u", stringify >> 24);
4
```

If stringify has the value 0x80000000, stringify ¿¿ 24 evaluates to 0xFFFFFF80 and the subsequent call to sprintf() results in a buffer overflow.

4.79.4 Compliant Solution

For bit extraction, make sure to mask off the bits you are not interested in.

```
1 int stringify;
2 char buf[sizeof("256")];
3 sprintf(buf, "%u", ((number >> 24) & 0xff));
4
```

4.79.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Find the bitwise and
2. climb parent tree
3. alert if parent null or basicblock found.

4.79.6 References

ISO/IEC 9899-1999:TC2 [Dowd 06] Chapter 6, "C Language Issues" [ISO/IEC 9899-1999] Section 6.5.7, "Bitwise shift operators" [ISO/IEC 03] Section 6.5.7, "Bitwise shift operators"

4.80 Set Pointers To Null

Dangling pointers can lead to exploitable double-free and access-freed-memory vulnerabilities. A simple yet effective way to eliminate dangling pointers and avoid many memory related vulnerabilities is to set pointers to NULL after they have been freed. Calling free() on a NULL pointer results in no action being taken by free().

4.80.1 Parameter Requirements

No Parameter specifications.

4.80.2 Implementation

4.80.3 Non-Compliant Code Example

In this example, the type of a message is used to determine how to process the message itself. It is assumed that message_type is an integer and message is a pointer to an array of characters that were allocated dynamically. If message_type equals value_1, the message is processed accordingly. A similar operation occurs when message_type equals value_2. However, if message_type == value_1 evaluates to true and message_type == value_2 also evaluates to true, then message will be freed twice, resulting in an error.

```
1
2 if (message\_type == value\_1) {
3   /* Process message type 1 */
4   free(message);
5 }
6 /* ...*/
7 if (message\_type == value\_2) {
8    /* Process message type 2 */
9   free(message);
10 }
11
```

4.80.4 Compliant Solution

As stated above, calling free() on a NULL pointer results in no action being taken by free(). By setting message equal to NULL after it has been freed, the double-free vulnerability has been eliminated.

```
1
2 if (message_type == value_1) {
3   /* Process message type 1 */
4   free(message);
5   message = NULL;
6 }
7 /* ...*/
8 if (message_type == value_2) {
9   /* Process message type 2 */
10  free(message);
11  message = NULL;
12 }
13
```

4.80.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Write your checker algorithm

4.80.6 References

ISO/IEC 9899-1999 MEM01-A. Eliminate dangling pointers

4.81 Single Parameter Constructor Explicit Modifier

The Elements of C++ Style item #104 states that

> A compiler can use a single parameter constructor for type conversions. While this is natural in some situations, it might be unexpected in others... you can avoid this behavior by declaring a constructor with the `explicit` keyword.

4.81.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.81.2 Implementation

This pattern is checked using a simple AST traversal that finds instances of SgFunctionDeclaration that are constructors with a single parameter. If these SgFunctionDeclaration are not modified with the "explicit" keyword then a violation is flagged.

4.81.3 Non-Compliant Code Example

This non-compliant code has a single parameter constructor that is not declared with the `explicit` keyword.

```
1 class Class
2 {
3   int num;
4   public:
5     Class( int n ){ num = n; }
6     int getNum() const { return num; }
7 }; //class Class
```

4.81.4 Compliant Solution

The compliant solution declares the single parameter constructor with the `explicit` keyword modifier.

```
1 class Class
2 {
3   int num;
4   public:
5     explicit Class( int n ){ num = n; }
6     int getNum() const { return num; }
7 }; //class Class
```

4.81.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform a simple AST traversal visiting all function declaration nodes.

2. For each function declaration, if node is constructor then check the size of its parameter list.
3. If the parameter list size of constructor is 1 and is not declared with the `explicit` modifier then flag violation.
4. Report any violations.

4.81.6 References

Bumgardner G., Gray A., and Misfeldt T. *The Elements of C++ Style*. Cambridge University Press 2004.

4.82 Size Of Pointer

Do not take the size of a pointer to a type when you are trying to determine the size of the type. Taking the size of a pointer to a type always returns the size of the pointer and not the size of the type.

This can be particularly problematic when tyring to determine the size of an array.

4.82.1 Parameter Requirements

No Parameter specifications yet!

4.82.2 Implementation

Finds calls to the sizeof function. Checks argument for level of pointer (ie pointer to pointer etc...) then checks the number of dereference levels. If these do not match an alert is raised.

4.82.3 Non-Compliant Code Example

This non-compliant code example mistakenly calls the sizeof() operator on the variable d_array which is declared as a pointer to double instead of the variable d which is declared as a double.

```
1 double *d_array;
2 size_t num_elems;
3 /* ... */
4
5 if (num_elems > SIZE_MAX/sizeof(d_array)){
6   /* handle error condition */
7 }
8 else {
9   d_array = malloc(sizeof(d_array) * num_elems);
10 }
```

The test of num_elems is to ensure that the multiplication of sizeof(d_array) * num_elems does not result in an integer overflow

For many implementaion, the size of a pointer and the size of double (or other type) is likely to be different. On IA-32 implementations, for example, the sizeof(d_array) is four, while the sizeof(d) is eight. In this case, insufficient space is allocated to contain an array of 100 values of type double.

4.82.4 Compliant Solution

Make sure you correctly calculate the size of the element to be contained in the aggregate data structure. The expression sizeof (*d_array) returns the size of the data structure referenced by d_array and not the size of the pointer.

```
1
2 double *d_array;
3 size_t num_elems;
4 /* ... */
5
6 if (num_elems > SIZE_MAX/sizeof(*d_array)){
7   /* handle error condition */
8 }
9 else {
10   d_array = malloc(sizeof(*d_array) * num_elems);
11
```

```
12
```

4.82.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Write your checker algorithm

4.82.6 References

ISO/IEC 9899-1999:TC2 [Viega 05] Section 5.6.8, "Use of sizeof() on a pointer type" [ISO/IEC 9899-1999] Section 6.5.3.4, "The sizeof operator" [Drepper 06] Section 2.1.1, "Respecting Memory Bounds"

4.83 Secure Coding : INT06-A. Use strtol() to convert a string token to an integer

Use `strtol()` or a related function to convert a string token to an integer. The `strtol()`, `strtoll()`, `strtoul()`, and `strtoull()` functions convert the initial portion of a string token to `long int`, `long long int`, `unsigned long int`, and `unsigned long long int` representation, respectively. These functions provide more robust error handling than alternative solutions.

4.83.1 Non-Compliant Example

This non-compliant code example converts the string token stored in the static array `buff` to a signed integer value using the `atoi()` function.

```
1 int si;
2
3 if (argc > 1) {
4   si = atoi(argv[1]);
5 }
6
```

The `atoi()`, `atol()`, and `atoll()` functions convert the initial portion of a string token to `int`, `long int`, and `long long int` representation, respectively. Except for the behavior on error, they are equivalent to

```
1 atoi: (int)strtol(nptr, (char **)NULL, 10)
2 atol: strtol(nptr, (char **)NULL, 10)
3 atoll: strtoll(nptr, (char **)NULL, 10)
4
```

Unfortunately, `atoi()` and related functions lack a mechanism for reporting errors for invalid values. Specifically, the `atoi()`, `atol()`, and `atoll()` functions:

4.83.2 Non-Compliant Example

This non-compliant example uses the `sscanf()` function to convert a string token to an integer. The `sscanf()` function has the same problems as `atoi()`.

```
1 int si;
2
3 if (argc > 1) {
4   sscanf(argv[1], "%d", &si);
5 }
6
```

4.83.3 Compliant Solution

This compliant example uses `strtol()` to convert a string token to an integer value and provides error checking to make sure that the value is in the range of `int`.

```
1 long sl;
2 int si;
3 char *end_ptr;
4
5 if (argc > 1) {
6
7   errno = 0;
8
9   sl = strtol(argv[1], &end_ptr, 10);
```

```
10
11   if (ERANGE == errno) {
12     puts("number out of range\n");
13   }
14   else if (sl > INT_MAX) {
15     printf("%ld too large!\n", sl);
16   }
17   else if (sl < INT_MIN) {
18     printf("%ld too small!\n", sl);
19   }
20   else if (end_ptr == argv[1]) {
21     puts("invalid numeric input\n");
22   }
23   else if ('\0' != *end_ptr) {
24     puts("extra characters on input line\n");
25   }
26   else {
27     si = (int)sl;
28   }
29 }
30
```

If you are attempting to convert a string token to a smaller integer type (`int`, `short`, or `signed char`), then you only need test the result against the limits for that type. The tests do nothing if the smaller type happens to have the same size and representation on a particular compiler.

4.83.4 Risk Assessment

While it is relatively rare for a violation of this rule to result in a security vulnerability, it could more easily result in loss or misinterpreted data.

Rule	Severity	Likelihood	Remediation Cost	Priority	Level
INT06-A	**2** (medium)	**2** (probable)	**2** (medium)	**P8**	**L2**

Related Vulnerabilities

Search for vulnerabilities resulting from the violation of this rule on the CERT website .

4.83.5 References

[Klein 02] [
ISO/IEC 9899-1999] Section 7.20.1.4, "The strtol, strtoll, strtoul, and strtoull functions," Section 7.20.1.2, "The atoi, atol, and atoll functions," and Section 7.19.6.7, "The sscanf function"

4.84 Sub Expression Evaluation Order

This checker detects if there exist, within an expression, sub-expressions that update the same variable. As the order of evaluation of such expressions is not guaranteed to be left-to-right, any of the sub-expressions can be taken place first.

4.84.1 Parameter Requirements

None.

4.84.2 Implementation

This checker uses a simple traversal. For every function call statement, the checker examines 1) whether the function call has sub-expressions that update variables and 2) the variables updated are identical.

4.84.3 Non-Compliant Code Example

```
1 int bar(int a, int b);
2
3 void foo()
4 {
5   int i = 0;
6
7   i = bar(++i, ++i); // either ++i could be evaluated first
8   i = bar((i=3), (i=4)); // no particular order is guaranteed.
9 }
```

4.84.4 Compliant Solution

```
1
2 int bar(int a, int b);
3
4 void foo()
5 {
6   int i = 0;
7
8   i = bar(2, 3); // fine
9   i = bar((i=2), 3); //fine
10 }
```

4.84.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For each node, check if the node is a function call statement.
2. Examine if the function call has sub-expressions that update variables.
3. If yes, examine further if the variables updated are identical.

4.84.6 References

The Programming Research Group, High-Integrity C++ Coding Standard Manual, Item 10.3: "Do not assume the order of evaluation of operands in an expression."

4.85 Ternary Operator

This checker detects a expression that uses the ternary operator. The rationale for this checker is, according to "High-Integrity C++ Coding Standard Manual", because evaluation of a complex condition is best achieved through explicit conditional statements.

4.85.1 Parameter Requirements

None.

4.85.2 Implementation

This checker is implemented with a simple traversal. It traverses AST, checks if a statement uses a ternary operator, and reports it if yes.

4.85.3 Non-Compliant Code Example

```
1
2 void foo()
3 {
4 int i = 0;
5 int j;
6
7 (i==3) ? (j=1) : (j=2);
8 }
```

4.85.4 Compliant Solution

```
1 void foo()
2 {
3 int i = 0;
4 int j;
5
6 if(i == 4)
7 j = 1;
8 else
9 j = 2;
10 }
```

4.85.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For each node, check if a node represents a ternary operator.
2. If yes, report it

4.85.6 References

The Programming Research Group, High-Integrity C++ Coding Standard Manual, Item 10.20: "Do not use the thernary operator(?:) in expressions."

4.86 Time_t Direct Manipulation

"CERT Secure Coding MSC05-A" states

> `time_t` is specified as an "arithmetic type capable of representing times." However, how time is encoded within this arithmetic type is unspecified. Because the encoding is unspecified, there is no safe way to manually perform arithmetic on the type, and, as a result, the values should not be modified directly.

4.86.1 Parameter Requirements

This checker takes no parameters and inputs source file.

4.86.2 Implementation

This pattern is checked using a simple AST traversal that visits all binary operation nodes. For each binary operation node, if the node is a arithmetic expression then check the type of its left and right hand side operands. If either operand type is `time_t` then flag violation.

4.86.3 Non-Compliant Code Example

This code attempts to execute `do_some_work()` multiple times until at least `seconds_to_work` has passed. However, because the encoding is not defined, there is no guarantee that adding `start` to `seconds_to_work` will result adding `seconds_to_work` seconds.

```
1  #include <time.h>
2
3  int do_work(int seconds_to_work)
4  {
5    time_t start;
6    start = time( NULL );
7
8    if (start == (time_t)(-1)) {
9      /* Handle error */
10   }
11   while (time(NULL) < start + seconds_to_work)
12   {
13     //do_some_work();
14   }
15
16   return 0;
17 }
```

4.86.4 Compliant Solution

This compliant solution uses `difftime()` to determine the difference between two `time_t` values. `difftime()` returns the number of seconds from the second parameter until the first parameter and returns the result as a `double`.

```
1  #include <time.h>
2
3  int do_work(int seconds_to_work) {
4    time_t start;
5    time_t current;
6    start = time(NULL);
7    current = start;
```

```
 8
 9   if (start == (time_t)(-1)) {
10     /* Handle error */
11   }
12   while (difftime(current, start) < seconds_to_work) {
13     current = time(NULL);
14     if (current == (time_t)(-1)) {
15       /* Handle error */
16     }
17     //do_some_work();
18   }
19
20   return 0;
21 }
```

4.86.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Perform simple AST traversal on all binary operation nodes.
2. For each binary operation node, if node is arithmetic expression then determine the type of its left and right hand side operands.
3. If either the left or right hand side is type `time_t` then flag violation.
4. Report any violations.

4.86.6 References

Secure Coding : MSC05-A. Do not manipulate time_t typed values directly

4.87 Type Typedef

Typedefs can be used instead of a type in the cases where it would increase maintainability or ensure cross-platform compatilibily.

For instance the ALE3D style guide section 3.5 says that the typedef 'Real8' should be used instead of 'double'. The introduction of Real8 is due to the days when a 'double' on CRAY Y-MP meant 16-bytes for that particular compiler. Although virtually all compilers now interprets 'double' as 8-byte ALE3D use the typedef for consistency.

4.87.1 Parameter Requirements

Through the 'TypeTypedef.RulesFile' paramaters a filename is provided, like e.g 'TypeTypedef.RulesFile=/path/to/file/exampleRules.sn'.

The rules are provided through a file where each word is a rule except everything on the line after a '#' which is considered a comment. Comments can be placed anywhere. There are two types of rules; 'typedefName1', 'c:typedefName2'. The type of the typedef is found in the AST so the user does not have to type it in. Only declarations with the exact type of the typedef which does not used the typedef is flagged as an error. When a typedef rule is prefixed with 'c:' exact type matches with and without const modifiers are both allowed.

4.87.2 Implementation

The implementation checks the type of all typed constructs that has the same type as the typedef and if the typedef is not used it reports an error.

4.87.3 Non-Compliant Code Example

```
1 typedef double Real8;
2 void foo(){
3    double bar; //A violation
4 };
```

4.87.4 Compliant Solution

```
1 typedef double Real8;
2 void foo(){
3    Real8 bar; //A violation
4 };
```

4.87.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Traverse the AST

2. For each typed contruct of the same type as the typedef it reports an error if the typedef is not used.

4.87.6 References

ALE3D style guide section 3.5.

4.88 Unary Minus

The unary minus operator should only be used with signed types, as its use with unsigned types will never result in a negative value. This checker reports any uses of the built-in unary minus operator on an unsigned type.

4.88.1 Parameter Requirements

This checker does not require any parameters.

4.88.2 Non-Compliant Code Example

```
1 unsigned int f_noncompliant(unsigned int u)
2 {
3     return -u;
4 }
```

4.88.3 Compliant Solution

```
1 int f_compliant(int n)
2 {
3     return -n;
4 }
```

4.88.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Check the type of the operand of any unary minus expression; emit a diagnostic if it is an unsigned integer type.

4.88.5 References

A reference for this rule is: The Programming Research Group: “High-Integrity C++ Coding Standard Manual”, Item 10.21: “Apply unary minus to operands of signed type only.”

4.89 Uninitialized Definition

This test ensures that all variables are initialized at their point of definition. The detector will report all variable declarations without initializer expressions, except for some special cases:

- Variables declared extern: Such declarations refer to variables defined elsewhere, initializers are therefore not required at this point.
- Variables declared static: These variables are automatically initialized to 0 (of the appropriate type) if no explicit initializer is present.
- Class member variables: The class constructor is responsible for initializing such variables.
- Variables of class type: Class objects are default-initialized if no explicit initializer expression is present.
- Variables declared at file ('global') scope: File scope declarations are implicitly static; they can be changed to extern by an explicit modifier. One of the above cases will always apply.

4.89.1 Parameter Requirements

This checker does not require any parameters.

4.89.2 Non-Compliant Code Example

```
1 void f_noncompliant()
2 {
3     int x; // not OK, no initializer
4 }
```

4.89.3 Compliant Solution

```
1 struct foo {
2     int member; // OK, class member
3 };
4
5 void f_compliant(int n)
6 {
7     int x = n; // OK, initializer present
8     static int y; // OK, static
9     struct foo st; // OK, class type (has constructor)
10    extern int not_here; // OK, extern
11 }
```

4.89.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For each variable declaration without an initializer expression, check the above criteria.
2. If none of the exceptions apply, generate a diagnostic.

4.89.5 References

A reference for this rule is: H. Sutter, A. Alexandrescu: "C++ Coding Standards", Item 19: "Always initialize variables".

4.90 Upper Range Limit

By always using inclusive lower limits and exclusive upper limits, a whole class of off- by-one errors is eliminated. Furthermore, the following assumptions always apply: 1)the size of the interval equals the difference of the two
2) the limits are equal if the interval is empty
3) the upper limit is never less than the lower limit

Examples: instead of saying x¿=23 and x¡=42, use x¿=23 and x¡43.

4.90.1 Parameter Requirements

No parameters required.

4.90.2 Implementation

In a fairly straight-forward implementation we search for the greater than or equal to operator.

4.90.3 Non-Compliant Code Example

```
1 int x = 5;
2 if (x >= 5)
3 {
4 x++;
5 }
6
7
```

4.90.4 Compliant Solution

```
1 int x = 5;
2 if (x > 4)
3 {
4 x++;
5 }
6
7
```

4.90.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. find greater than or equal to operator
2. raise alert

4.90.6 References

Abbreviated Code Inspection Checklist Section 11.1.2, Control Variables”

4.91 Variable Name Equals Database Name

For some member function accesses the name of the local variable that gets assigned the result of the function call should have a name equal to the first argument. [ALE3D] E.g:

```
1       real8 *sx = regM->fieldReal("sx") ;
2       real8 *syy = regM->fieldReal("sy") ;
```

Where the name of the local variable is not the same as the name in the database for "syy", but it is the same for "sx".

This checker will only report the locations of the assign expressions where this rule is not followed.

4.91.1 Parameter Requirements

The checker takes the name of the class and member function that on call should assign it's result to a variable with the same name as the first argument. The arguments are "VariableNameEqualsDatabaseName.ClassName=CLASSNAME" and "VariableNameEqualsDatabaseName.MemberFunctionName=MEMFUNCNAME".

4.91.2 Implementation

The checker will look for a function call to the member function within the class that we are looking for. When such a call is found it assumes that the lhs of the last assign expression is the variable access that we are interested in. If the name of that variable does not satisfy the rule we report an error.

4.91.3 Non-Compliant Code Example

```
1 #include <string>
2 class MixMatmodel{
3
4   public:
5     double fieldReal(std::string str){ return 1; };
6
7 };
8
9 int main(){
10    MixMatmodel x;
11
12    int y     = x.fieldReal("test1");
13    int z     = x.fieldReal("test1:test2");
14    int test2 = x.fieldReal("test1:test2:test3");
15
16 };
```

4.91.4 Compliant Solution

```
1 #include <string>
2 class MixMatmodel{
3
4   public:
5     double fieldReal(std::string str){ return 1; };
6
7 };
8
```

```
 9 int main(){
10     MixMatmodel x;
11
12     int test1 = x.fieldReal("test1");
13     int test2 = x.fieldReal("test1:test2");
14     int test3 = x.fieldReal("test1:test2:test3");
15
16 };
```

4.91.5 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. Travese the AST
2. For each call to the member function we are interested in make sure field name is equal to the string provided as an argument.

4.91.6 References

4.92 Void Star

This checker enforces the guideline of section 87 of *the Elements of C++ Style* (Misfeldt and al., 2004). No public method should be using `void*` type for arguments or return type. If needed, it can be wrapped.

4.92.1 Parameter Requirements

There is not parameter requirement.

4.92.2 Non-Compliant Code Example

```
1 class A {
2 public:
3   const void* getData();
4 };
```

4.92.3 Compliant Solution

```
1 class A {
2 public:
3   const Data getData();
4 };
```

4.92.4 Mitigation Strategies

Static Analysis

Compliance with this rule can be checked using structural static analysis checkers using the following algorithm:

1. For each public member function declaration, check all argument types and the return type are not `void*`.

4.92.5 References

Bumgardner G., Gray A., and Misfeldt T. *The Elements of C++ Style*. Cambridge University Press 2004.

Chapter 5

Appendix

5.1 Design And Extensibility of Compass Detectors

The design of the detectors is intended to be simple and with little required to be specified to build individual detectors. Of course some detectors may be non-trivial (e.g. null pointer analysis, buffer overflow detectors, etc. (not yet provided in Compass)) the majority are simple. All detectors are meant to be side-effect free and are the subject of separate research to independently provide automated combining (evaluation of multiple patterns in a single AST traversal) and parallelization of the pattern evaluations on the AST.

5.1.1 Input Parameter Specification

Parameters to all detectors are specified in an input parameter file (if required). This permits numerous knobs associated with different pattern detectors and separate input files be specified for different software projects.

5.1.2 Pattern Detection

Currently it is assumed that patterns will be detected as part of a traversal of the AST. See the ROSE Tutorial for example and general documentation on the different sorts of traversals possible within ROSE.

5.1.3 Output Specification

Output of source position information specific to detected patterns are output in GNU standard source position formats. See **http://www.gnu.org/prep/standards/html_node/Errors.html** for more details on this format specification and now it is used by external tools (e.g. emacs, etc.).