



POWER OF TEN RULES MAPPED TO CODESONAR® 7.4 WARNING CLASSES



TRUSTED LEADERS OF SOFTWARE ASSURANCE AND ADVANCED CYBER-SECURITY SOLUTIONS

WWW.GRAMMATECH.COM

INTRODUCTION

The “Power of Ten” refers to a set of ten rules developed by Gerard Holzmann of the NASA Jet Propulsion Laboratory for use in writing safety-critical software. The rules are simple, but they specify strict limits on the forms code can take. These limits support code clarity and analyzability, which are especially important for safety-critical applications.

CodeSonar 7.4 includes warning classes that support checking for the Power of Ten rules. Every CodeSonar warning report includes the numbers of any Power of Ten rule that are closely mapped to the warning’s class. (The close mapping for a warning class is the set of categories—including Power of Ten rule numbers—that most closely match the class, if any).

You can configure CodeSonar to enable and disable warning classes mapped to specific Power of Ten rule, or use build presets to enable all warning classes that are closely mapped to any Power of Ten rule. In addition, you can use the CodeSonar search function to find warnings related to a specific Power of Ten rule, or to any Power of Ten rule.

For more information on the Power of Ten rules: <http://www.spinroot.com/p10/>

The following table lists the CodeSonar warning classes that are closely mapped to Power of Ten rules.

Note-All CodeSonar Power of Ten mappings are close.

Rule	Rule Name	Supported
POW10:1	Restrict to simple control flow constructs.	Yes
POW10:2	Give all loops a fixed upper-bound.	Yes
POW10:3	Do not use dynamic memory allocation after initialization.	Yes
POW10:4	Limit functions to no more than 60 lines of text.	Yes
POW10:5	Use minimally two assertions per function on average.	Yes
POW10:6	Declare data objects at the smallest possible level of scope.	Yes
POW10:7	Check the return value of non-void functions, and check the validity of function parameters.	Yes
POW10:8	Limit the use of the preprocessor to file inclusion and simple macros.	Yes
POW10:9	Limit the use of pointers. Use no more than two levels of dereferencing per expression.	Yes
POW10:10	Compile with all warnings enabled, and use one or more source code analyzers.	Yes

GrammaTech is a leading global provider of application testing (AST) solutions used by the world’s most security conscious organizations to detect, measure, analyze and resolve vulnerabilities for software they develop or use. The company is also a trusted cybersecurity and artificial intelligence research partner for the nation’s civil, defense, and intelligence agencies.

CodeSonar and CodeSentry are registered trademarks of GrammaTech, Inc.
© GrammaTech, Inc. All rights reserved.

