secureC Standards Model Summary for C

The LDRA tool suite® is developed and certified to BS EN ISO 9001:2000 and SGS-TÜV Saar.

This information is applicable to version 9.7.1 of the LDRA tool suite®.
It is correct as of 25th September 2017.

Compliance is measured against
"Information Technology-Programming languages, their environments and system software interfaces-C Secure Coding Rules"
2013
Copyright © ISO

Further information is available at http://www.iso.org

Classification	Enhanced Enforcement	Fully Implemented	Partially Implemented	Not yet Implemented	Not statically Checkable	Total
Mandatory	9	17	19	1	0	**46**
Total	**9**	**17**	**19**	**1**	**0**	**46**

secureC Standards Model Compliance for C

Rule	Classification	Rule Description	LDRA Standard	LDRA Standard Description
1	Mandatory	Accessing an object through a pointer to an incompatible type [ptrcomp]	94 S	Casting operation on a pointer.
			95 S	Casting operation to a pointer.
			615 S	Conditional operator has incompatible types.
2	Mandatory	Accessing freed memory [accfree]	51 D	Attempt to read from freed memory.
			484 S	Attempt to use already freed object.
3	Mandatory	Accessing shared objects in signal handlers [accsig]	87 D	Illegal shared object in signal handler.
4	Mandatory	No assignment in conditional expressions [boolasgn]	114 S	Expression is not Boolean.
5	Mandatory	Calling functions in the C standard library other than abort, _Exit, and signal from within a signal handler [asyncsig]	87 D	Illegal shared object in signal handler.
			88 D	Illegal use of longjmp in signal handler.
			89 D	Illegal use of raise in signal handler.
6	Mandatory	Calling functions with incorrect arguments [argcomp]	21 S	Number of parameters does not match.
			102 S	Function and prototype return inconsistent (MR).
			103 S	Function and prototype param inconsistent (MR).
			458 S	Implicit conversion: actual to formal param (MR).
			496 S	Function call with no prior declaration.
7	Mandatory	Calling signal from interruptible signal handlers [sigcall]	97 D	Signal called from within signal handler.
8	Mandatory	Calling system [syscall]	588 S	Use of system function.
9	Mandatory	Comparison of padding data [padcomp]	618 S	Use of memcmp between structures.
10	Mandatory	Converting a pointer to integer or integer to pointer [intptrconv]	439 S	Cast from pointer to integral type.
			440 S	Cast from integral type to pointer.
11	Mandatory	Converting pointer values to more strictly aligned pointer types [alignconv]	94 S	Casting operation on a pointer.
			606 S	Cast involving function pointer.
12	Mandatory	Copying a FILE object [filecpy]	591 S	Inappropriate use of file pointer.
13	Mandatory	Declaring the same function or object in incompatible ways [funcdecl]	17 D	Identifier not unique within *** characters.
			1 X	Declaration types do not match across a system.
			61 X	Identifier match in *** chars.
			62 X	Function prototype/defn return type mismatch (MR).

secureC Standards Model Compliance for C

Rule	Classification	Rule Description	LDRA Standard	LDRA Standard Description
			63 X	Function prototype/defn param type mismatch (MR).
14	Mandatory	Dereferencing an out-of-domain pointer [nullref]	45 D	Pointer not checked for null before use.
			123 D	File pointer not checked for null before use.
			128 D	Global pointer not checked within this procedure.
			129 D	Global file pointer not checked within this procedure.
			135 D	Pointer assigned to NULL may be dereferenced.
			136 D	Global pointer assigned to NULL may be dereferenced.
15	Mandatory	Escaping of the address of an automatic object [addrescape]	42 D	Local pointer returned in function result.
			77 D	Local structure returned in function result.
			71 S	Pointer assignment to wider scope.
			565 S	Assignment to wider scope.
16	Mandatory	Conversion of signed characters to wider integer types before a check for EOF [signconv]	433 S	Type conversion without cast.
17	Mandatory	Use of an implied default in a switch statement [swtchdflt]	48 S	No default case in switch statement.
18	Mandatory	Failing to close files or free dynamic memory when they are no longer needed [fileclose]	49 D	File pointer not closed on exit.
			50 D	Memory not freed after last reference.
			75 D	Attempt to open file pointer more than once.
19	Mandatory	Failing to detect and handle standard library errors [liberr]	80 D	Potentially unused function-modified value.
			124 D	Var set by std lib func return not checked before use.
			130 D	Global set by std lib func return not checked before use.
			382 S	(void) missing for discarded return value.
20	Mandatory	Forming invalid pointers by library function [libptr]	489 S	Insufficient space for operation.
			66 X	Insufficient array space at call.
			70 X	Array has insufficient space.
			71 X	Insufficient space for copy.
			79 X	Size mismatch in memcpy/memset.

secureC Standards Model Compliance for C

Rule	Classification	Rule Description	LDRA Standard	LDRA Standard Description
21	Mandatory	Allocating insufficient memory [insufmem]	487 S	Insufficient space allocated.
			577 S	Sizeof argument is a pointer.
			638 S	Memory allocation non-conformant with type.
			115 D	Copy length parameter not checked before use.
22	Mandatory	Forming or using out-of-bounds pointers or array subscripts [invptr]	47 S	Array bound exceeded.
			64 X	Array bound exceeded at call.
			68 X	Parameter indexing array too big at call.
			69 X	Global array bound exceeded at use.
			72 X	Parameter indexing array too small at call.
23	Mandatory	Freeing memory multiple times [dblfree]	112 D	Free called twice on same variable.
			484 S	Attempt to use already freed object.
24	Mandatory	Including tainted or out-of-domain input in a format string [usrfmt]	86 D	User input not checked before use.
25	Mandatory	Incorrectly setting and using errno [inverrno]	111 D	errno checked without having been set for errno setting fn.
			121 D	errno neither set nor checked for errno setting function.
			122 D	errno not checked after being set for errno setting fn.
			132 D	errno checked after call to non-errno setting function.
			134 D	errno not checked before subsequent function call.
26	Mandatory	Integer division errors [diverr]	43 D	Divide by zero found.
			127 D	Local or member denominator not checked before use.
			131 D	Global denominator not checked within this procedure.
			137 D	Parameter used as denominator not checked before use.
			248 S	Divide by zero in preprocessor directive.
			629 S	Divide by zero found.

secureC Standards Model Compliance for C

Rule	Classification	Rule Description	LDRA Standard	LDRA Standard Description
			80 X	Divide by zero found.
27	Mandatory	Interleaving stream inputs and outputs without a flush or positioning call [ioileave]	84 D	No fseek or flush before I/O.
28	Mandatory	Modifying string literals [strmod]	157 S	Modification of string literal.
29	Mandatory	Modifying the string returned by getenv, localeconv, setlocale, and strerror [libmod]	107 D	Attempt to change system call capture string.
30	Mandatory	Overflowing signed integers [intoflow]	488 S	Value outside range of underlying type.
			493 S	Numeric overflow.
			494 S	Numeric underflow.
31	Mandatory	Passing a non-null-terminated string to a library function that expects a string [nonnullcs]	404 S	Array initialisation has too many items.
			600 S	Argument of strlen is unterminated.
32	Mandatory	Passing arguments to character-handling functions that are not representable as unsigned char [chrsgnext]	431 S	Char used instead of (un)signed char.
			432 S	Inappropriate type - should be plain char.
			433 S	Type conversion without cast.
			663 S	Invalid value may be passed to function in <ctype.h>.
33	Mandatory	Passing pointers into the same object as arguments to different restrict-qualified parameters [restrict]	480 S	String function params access same variable.
			613 S	Use of restrict keyword.
			16 D	Identical actual parameters in call.
34	Mandatory	Reallocating or freeing memory that was not dynamically allocated [xfree]	407 S	free used on string.
			483 S	Freed parameter is not heap item.
			644 S	realloc ptr does not originate from allocation function.
			645 S	realloc ptr type does not match target type.
			125 D	free called on variable with no allocated space.
35	Mandatory	Referencing uninitialized memory [uninitref]	53 D	Attempt to use uninitialised pointer.
			69 D	UR anomaly, variable used before assignment.
			631 S	Declaration not reachable.
			652 S	Object created by malloc used before initialisation.
36	Mandatory	Subtracting or comparing two pointers that do not refer to the same array [ptrobj]	438 S	Pointer subtraction not addressing one array.

secureC Standards Model Compliance for C

Rule	Classification	Rule Description	LDRA Standard	LDRA Standard Description
37	Mandatory	Tainted strings are passed to a string copying function [taintstrcpy]	68 D	Void function has persistent local side effects.
38	Mandatory	Taking the size of a pointer to determine the size of the pointed-to type [sizeofptr]	401 S	Use of sizeof on an array parameter.
			577 S	Sizeof argument is a pointer.
39	Mandatory	Using a tainted value as an argument to an unprototyped function pointer [taintnoproto]	108 D	Tainted argument to unprototyped func ptr.
40	Mandatory	Using a tainted value to write to an object using a formatted input or output function [taintformatio]	109 D	Tainted argument to formatted i/o function.
41	Mandatory	Using a value for fsetpos other than a value returned from fgetpos [xfilepos]	82 D	fsetpos values not generated by fgetpos.
42	Mandatory	Using an object overwritten by getenv, localeconv, setlocale, and strerror [libuse]	133 D	Pointer from system function used after subsequent call.
43	Mandatory	Using character values that are indistinguishable from EOF [chreof]	431 S	Char used instead of (un)signed char.
			432 S	Inappropriate type - should be plain char.
			433 S	Type conversion without cast.
			662 S	EOF compared with char.
44	Mandatory	Using identifiers that are reserved for the implementation [resident]	86 S	Attempt to define reserved word.
			218 S	Name is used in standard libraries.
			219 S	User name starts with underscore.
45	Mandatory	Using invalid format strings [invfmtstr]	486 S	Incorrect number of formats in output function.
			589 S	Format is not appropriate type.
46	Mandatory	Tainted, potentially mutilated, or out-of-domain integer values are used in a restricted sink [taintsink]		

General Compliance Notes

Enhanced Enforcement: LDRA checks additional cases to those specified by the mapped rule for enhanced safety and security.
Fully Implemented: LDRA checks all statically checkable aspects of the mapped rule.
Partially Implemented: LDRA checks certain aspects of the rule.

The assessment of whether a rule is fully or partially implemented is based on whether the mapped LDRA standards cover all statically checkable aspects of the rule with a high level of coverage or only cover certain statically checkable aspects of the rule. If a rule is undecidable then this assessment is based on what it is deemed reasonable for a static analysis tool to check.