MIM 2013 Saint Petersburg, Russia 2013.06.19 ~ 06.21



A Preliminary Report on Static Analysis of C Code for Nuclear Reactor Protection System

Jong-Hoon Lee , Eui-Sub Kim , Junbeom Yoo KONKUK University, South Korea

Jang-Soo Lee

KAERI (Korea Atomic Energy Research Institute)





Cyber Security Standards for NPPs

US NRC RG 5.71	Cyber Security Programs for Nuclear Facilities
IEC 61513	Nuclear Power Plants - I&C important to safety - General requirements for systems
IEC 60880	Nuclear Pow er Plants - I&C systems important to safety - Software aspects for computer-based systems performing category A functions
IEC 62645 (CD2)	Nuclear Power Plants - I&C systems - Requirements for security programmes for computer-based systems





US NRC RG 5.71

Designers and developers for I&C systems shall have established and verified secure development methodologies in place throughout the development lifecycle of a system.







IEC 62645 (CD2)









Secure Software Development Methodologies

SAFECode

Widely-accepted practices should be followed throughout programming.

Use of static and dynamic analysis code analysis tools is highly recommended.

in the implementation phase





C Code Analysis Tool

Analyze - 😳 Search	🔎 - 🗊 🗊 Group by: Category 🕒 🔽 😢 🗗 🏓	Search
-	🐨 🚺 This is a Microsoft rule set and cannot be modified. To create your own rule se	t based on this rule set, make your changes below. Then save your changes to a new file to create the rule s
	ID 🔺 Name	Action
	Microsoft.Security	🖷 Warning
	CA2100 Review SQL queries for security vulnerabilities	🔥 Warning
	CA2102 Catch non-CLSCompliant exceptions in general	I handlers 🔥 Warning
	CA2103 Review imperative security	4 Warning
	CA2104 Do not declare read only mutable reference to	pes 🦺 Warning
	CA2105 Array fields should not be read only	A Warning
	CA2106 Secure asserts	A Warning
	CA2107 Review deny and permit only usage	A Warning
	CA2108 Review declarative security on value types	A Warning
	CA2109 Review visible event handlers	4 Warning
596 rules	CA2111 Pointers should not be visible	A Warning
	CA2112 Secured types should not expose fields	A Warning
2 categories	CA2114 Method security should be a superset of type	A Warning
.2 categones	CA2115 Call GC.KeepAlive when using native resources	4 Warning
	CA2116 APTCA methods should only call APTCA meth	ods 🔥 Warning
	Microsoft V	isual Studio 2012





A Typical RPS SW Development Process







A Typical RPS SW Development Process





Static Analysis Result

FIX_RISING_pSET - Microsoft Visual Studio	Quick Launch (Ctrl+Q)	<mark>ب</mark>	ð
FILE EDIT VIEW PROJECT BUILD DEBUG TE	A <u>M</u> SQL <u>T</u> OOLS TE <u>S</u> T A <u>M</u> ALYZE <u>WI</u> NDOW <u>H</u> ELP		
	Indows Debugger ▼ Auto		
Code Analysis 👻 👎	AllRules.ruleset = iec_sub_dint.c FIX_RISING.c + ×		_
Analyze - 😳 Search	Global Scope) + © FIX_RISING_(FIX_RISING_t * a_)		_
All Projects (3) All Results (3)	96 it(a>EN) { 97		
C6001 Using uninitialized memory	<pre>98 GE_DINT(TRUE, a>PV_OUT, a>PTSP, &(ENO_1_FIX_RISING), &(OUT_1_FIX_RISING));</pre>		
Using uninitialized memory '_tmp'.			
Line Explanation	100 AND2_DODL(1KUE, 001_1_FIX_KISING, :(a ->PIKIP_LOGIC), &(ENU_2_FIX_KISING), &(001_2_FIX_KISING)); 101		
89 '_tmp' is not initialized	102 ADD2 DINT(TRUE, a ->PTRIP CNT, 1, &(ENO 3 FIX RISING), &(OUT 3 FIX RISING));		
113 'tmp' is used, but may not have been initialized	104 SUB DINT(TRUE, a ->PTSP, a ->PHYS, &(ENO 4 FIX RISING), &(OUT 4 FIX RISING));		
More Information	105		
fix_rising.c (Line 113)	<pre>106 SEL_DINT(TRUE, OUT_2_FIX_RISING, 0, OUT_3_FIX_RISING, &(ENO_5_FIX_RISING), &(OUT_5_FIX_RISING));</pre>		
Warning Actions	107 if(ENO_5_FIX_RISING) {		
C6281 Bitwise relation precedence	109tmp[0]tdint = OUT_5_FIX_RISING;		
iec_sub_dint.c (Line 11)	110 a>PTRIP_CNT =tmp[0]tdint;		
C6281 Bitwise relation precedence			
C6281 Bitwise relation precedence	<pre>113 GE_DINT(TRUE, _tmp[0]tdint, a>MAXCNT, &(ENO_6_FIX_RISING), &(OUT_6_FIX_RISING));</pre>		
iec_sub_dint.c (Line 19)	115 if(ENO_6_FIX_RISING) {		
C6281 Bitwise relation precedence	<pre>116tmp[1]tbool = OUT_6_FIX_RISING;</pre>		
iec_sub_dint.c (Line 19)			
	<pre>119 SEL_BOOL(TRUE,tmp[1]tbool, a>PTRIP_LOGIC, TRUE, &(ENO_7_FIX_RISING), &(OUT_7_FIX_RISING));</pre>		
tical errors !!!	122TI		
	123 }		
	124 125 SEL DINT(TRUE, tmp[1]. tbool, a ->PTSP, OUT 4 FIX RISING, &(ENO 8 FIX RISING), &(OUT 8 FIX RISING));		
	126		
	127 if(ENO_8_FIX_RISING) { 128 tmm[3]. tdipt = OUT_8_FIX_RISING:		
	129 }		
	130		
	100 % - 4		
	Output	••••••••••••••••	1
	Show output from: Build - 🖌 🛬 🛬 🚈		
	iec_sub_dint.c(1) warning : 05291 incorrect order of operations: relational operators have higher precedence than bitwise operators.		
	iec.sub.dint.c(19): warning : C6281: Incorrect order of operations: relational operators have higher precedence than bitwise operators.		
	Rebuild XII. I Succeeded, Olalied, Olskipped		
	4		ļ



C6001 Using uninitialized memory



C6281 Bitwise relation procedure

All Projects (5)		All Results (5)	
C6001 Using uninitializ fix_rising.c (Line 113)	ed m	emory	
C6281 Bitwise relation	prec	edence	
Incorrect order of operat higher precedence than iec_sub_dint.c (Line 11)	tions: bitwis	relational operato se operators.	rs have
Warning			Actions -
C6281 Bitwise relation iec_sub_dint.c (Line 11)	prec	edence	
C6281 Bitwise relation iec_sub_dint.c (Line 19)	prec	edence	
C6281 Bitwise relation iec_sub_dint.c (Line 19)	prec	edence	

We found functional correctness (safety) - related errors.

We found no security-related error!



KU KONKUK UNIVERSITY

Splint

More than 100 errors !!! - Not categorized



<pre>\$ splint FIX_RISING.c</pre>
Splint 3.1.2 28 Mar 2013
<pre>psettype.h:4:22: Type BOOL is probably meant as a boolean</pre>
type, but the boolean
type name is not set. Use -booitype BU
Use the shealtyne shealfalse and shealthyse flags to she
nge the name of the
default boolean type. (Use -likelybool to inhibit warnin
a)
FIX RISING.c: (in function FIX RISING)
FIX RISING.c:96:5: Test expression for if not boolean, typ
e BOOL: a ->EN
Test expression type is not boolean or int. (Use -predbo
olint to inhibit
warning)
FIX_RISING.c:98:2: Return value (type BOOL) ignored: GE_DI
NT(TRUE, a
Result returned by function call is not used. If this is
intended, can cast
result to (void) to eliminate message. (Use -retvalother
to inhibit warning)
•••
ery presses and the second but and and do
FIX_RISING.C:61:6: Variable exported but not used outside
FIX_KIDING:
ETY RISING (:62:6: Variable exported but not used outside
FIX RISING:
END 25 ETX RISING
FIX RISING.c:63:6: Variable exported but not used outside
FIX RISING:
OUT 25 FIX RISING
FIX_RISING.c:64:6: Variable exported but not used outside
FIX_RISING:
END_26_FIX_RISING
FIX_RISING.c:65:6: Variable exported but not used outside
FIX_RISING:
OUT_26_FIX_RISING
Finished checking 103 code warnings



Lesson Learned

Find appropriate static code analysis tools!!

A number of tools are available

Different rules and categories





Lesson Learned

Consider OS and HW as well as safety/security rules!!

Most of tools assume the use of MS Windows and Linux

But, the RPS uses PLCs not PCs

Operating systems and HWs are different





Lesson Learned

Develop a secure development process from requirements!!

A systematic process is required





THANK YOU!!! and Questions?

Jang-Soo Lee

Principal Researcher / Ph.D KAERI (Korea Atomic Energy Research Institute)

