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)

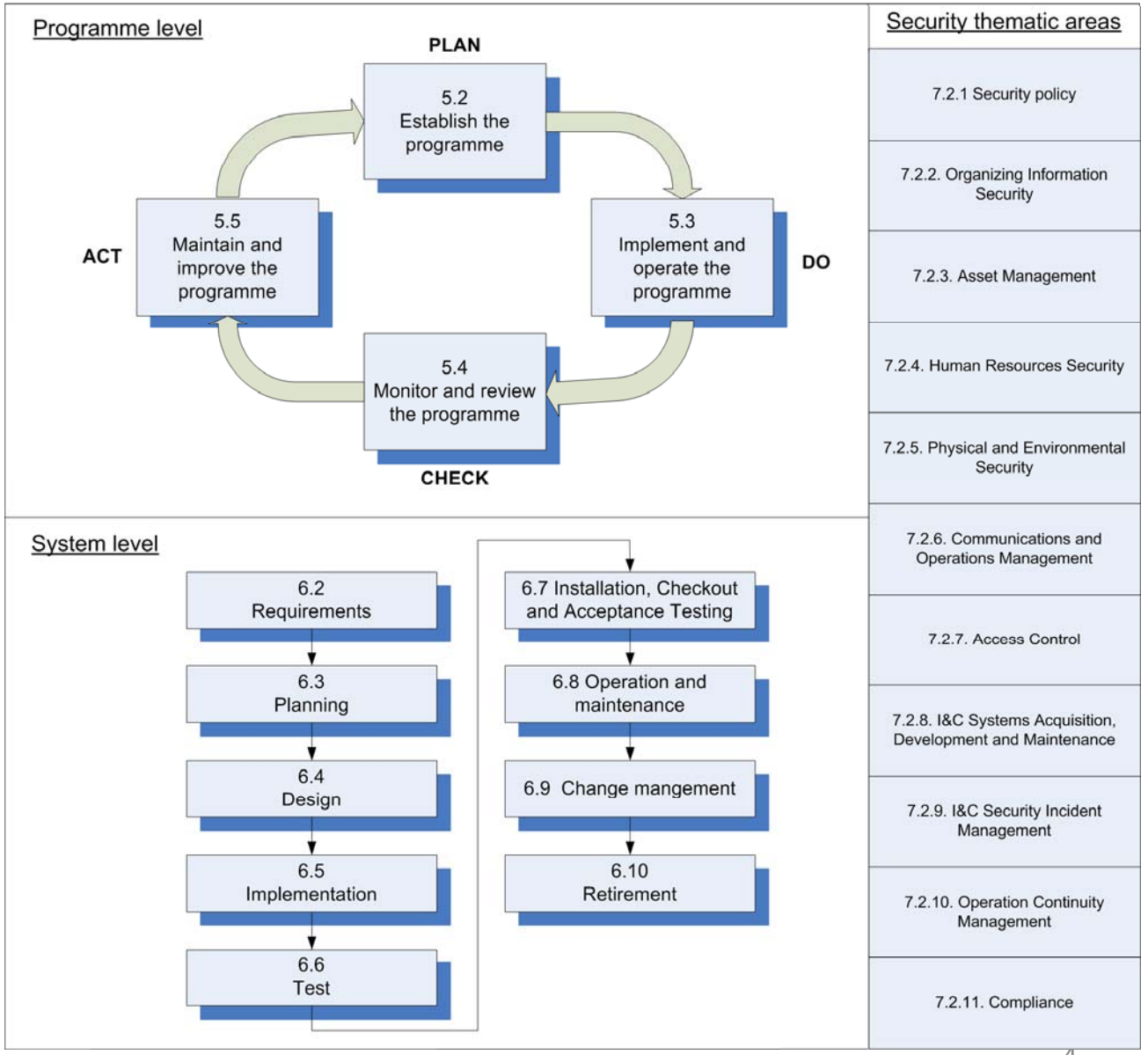
Cyber Security Standards for NPPs

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

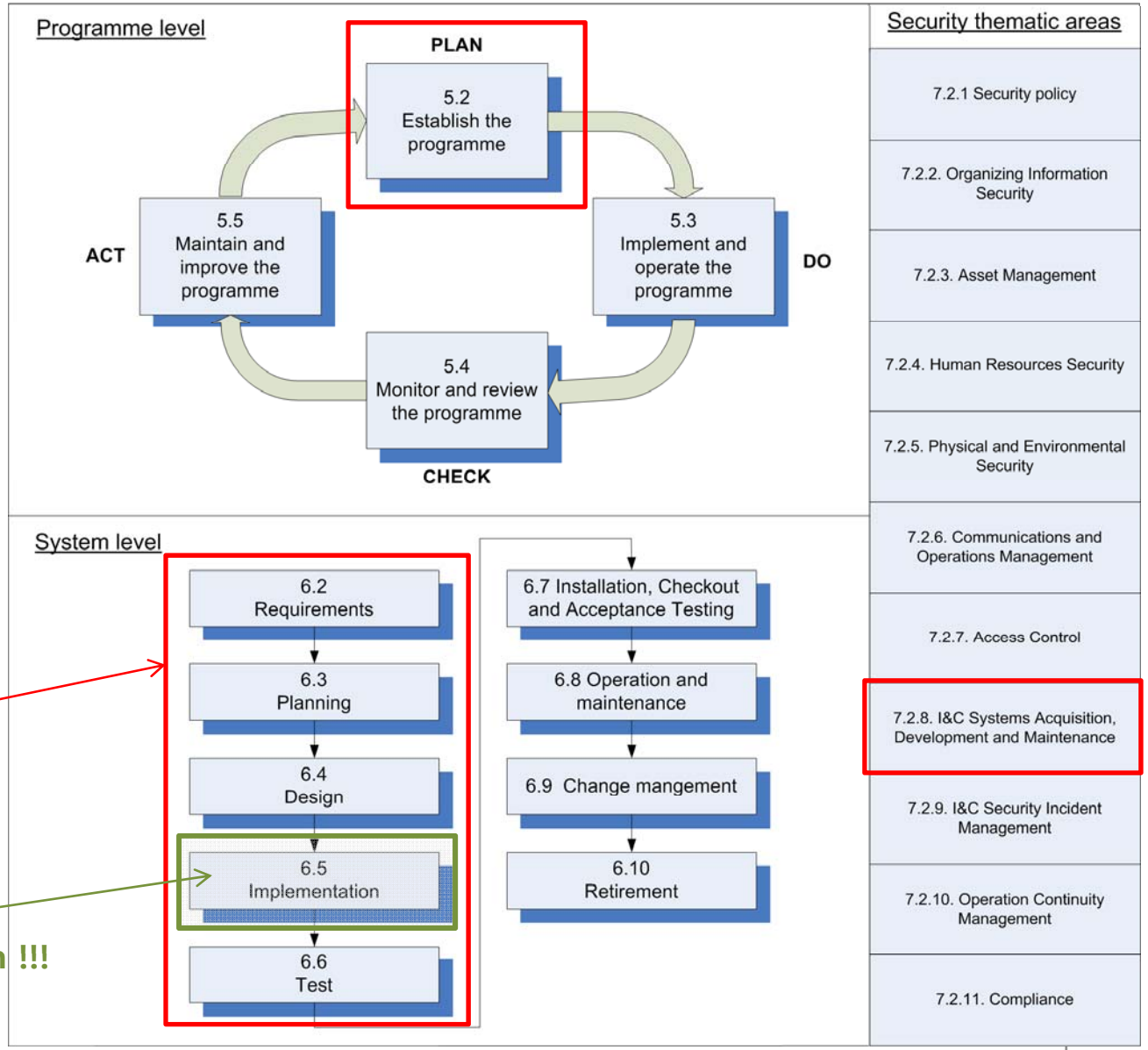
US NRC RG 5.71

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)



IEC 62645 (CD2)



Our interest !!

This paper focuses on !!!

Secure Software Development Methodologies

SAFECode

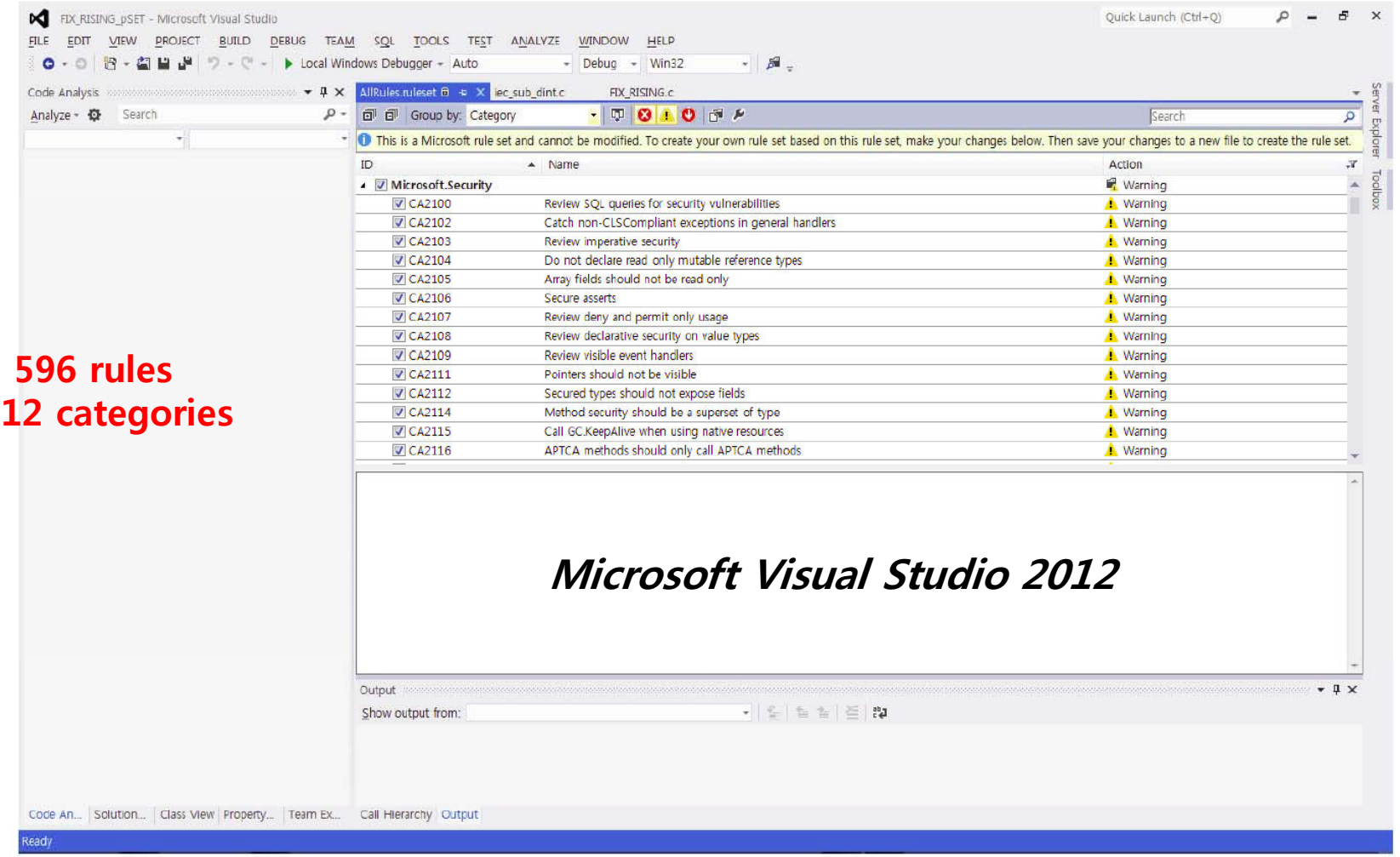
Widely-accepted practices should be followed throughout programming.

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

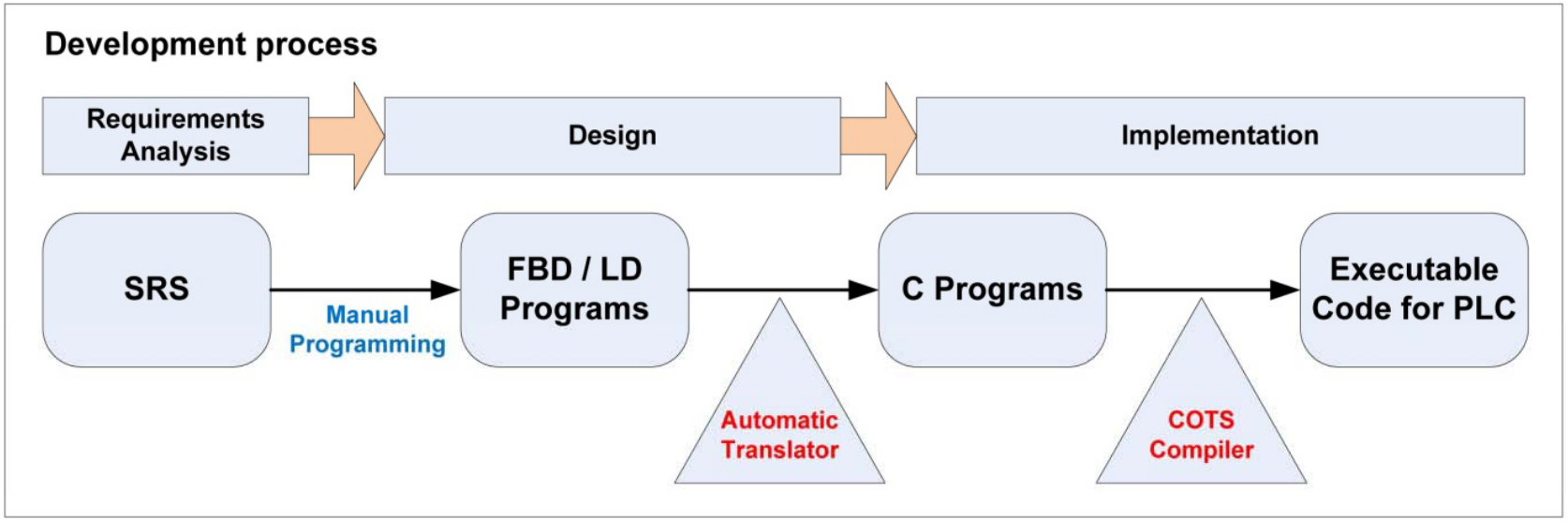
in the implementation phase

C Code Analysis Tool

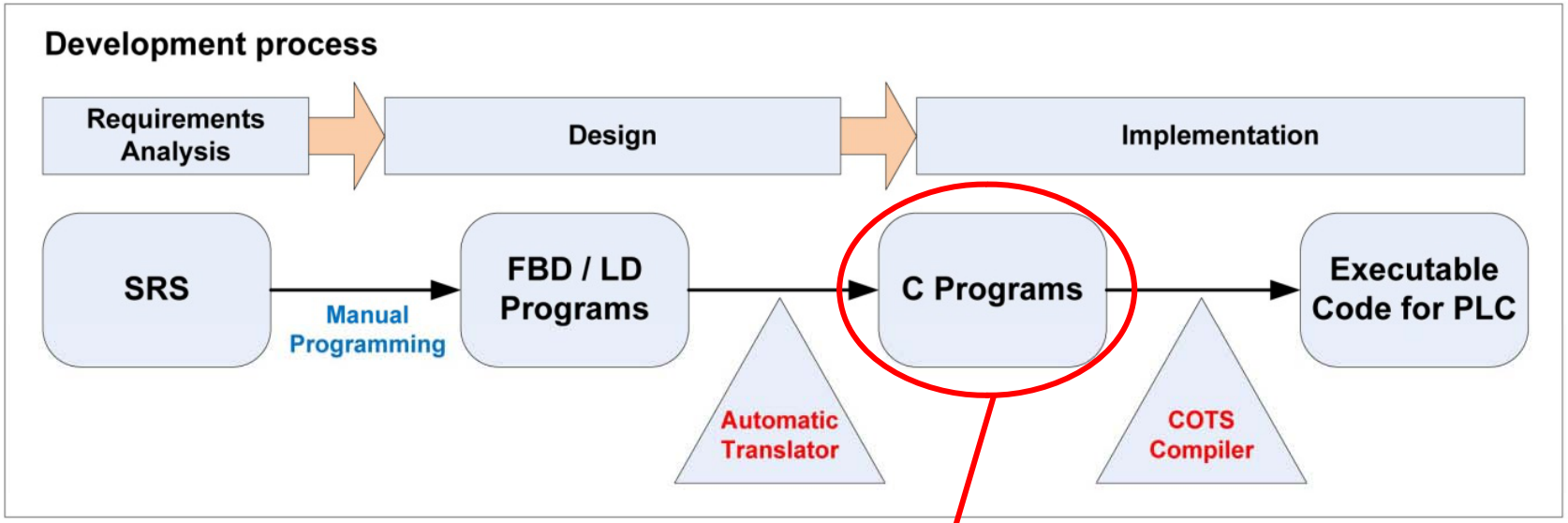
596 rules
of 12 categories



A Typical RPS SW Development Process



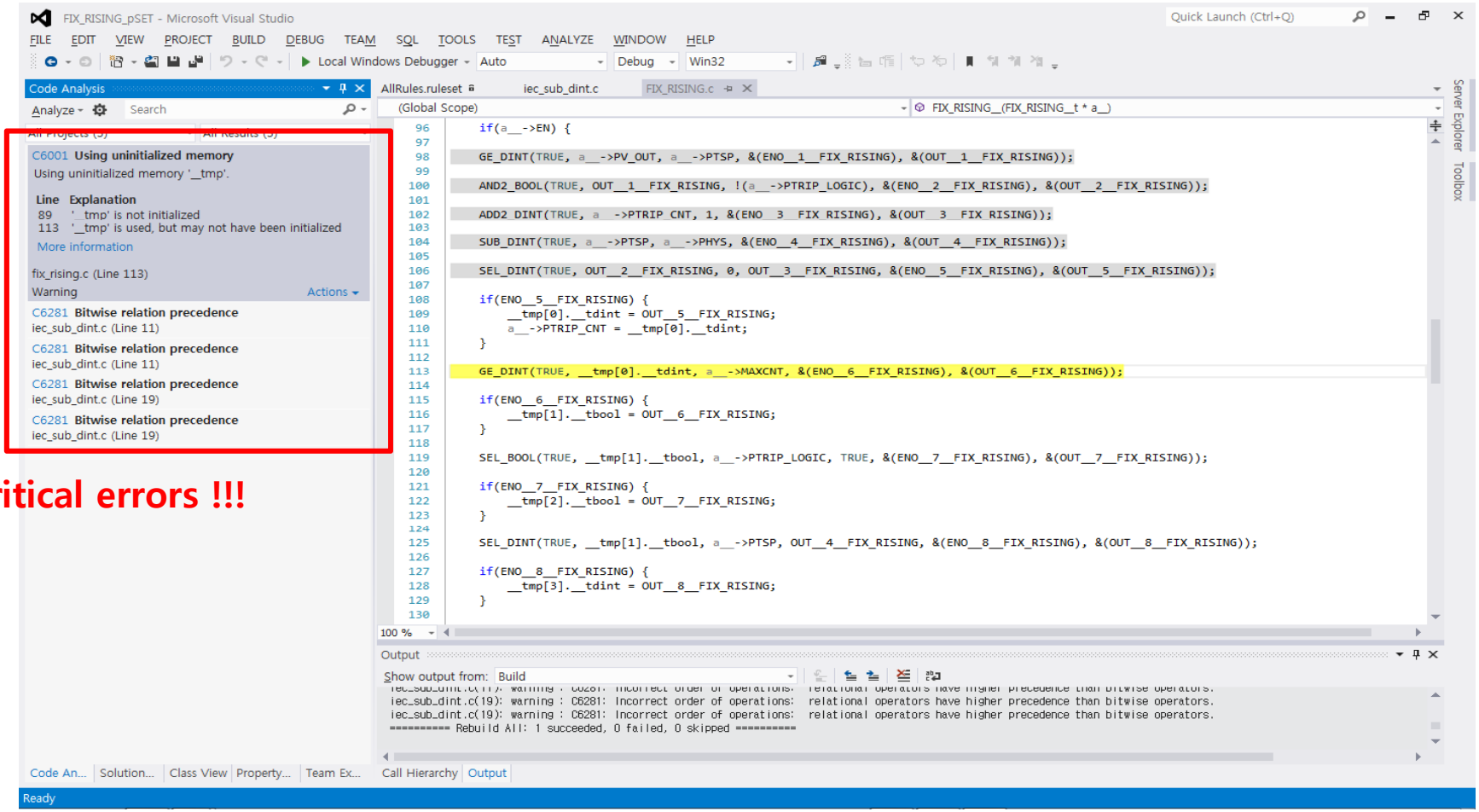
A Typical RPS SW Development Process



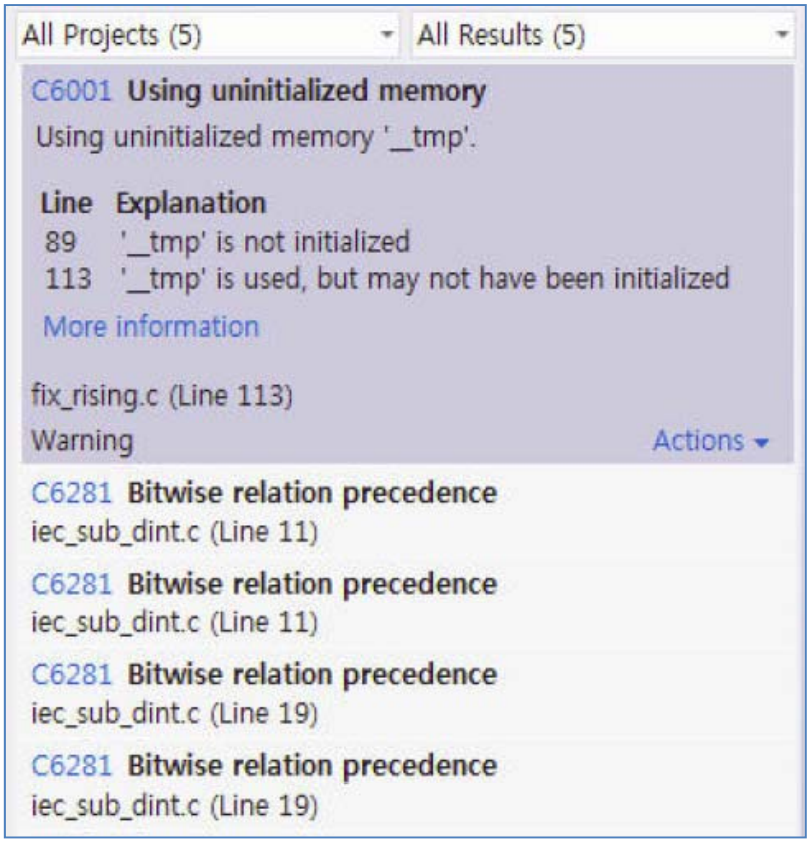
Our target of static code analysis

- A preliminary version of KNICS APR-1400 RPS BP
- PLC : *POSAFE-Q* PLC of POSCO ICT
- SW engineering tool : *pSET*
- Shutdown logic : fixed-setpoint rising trip

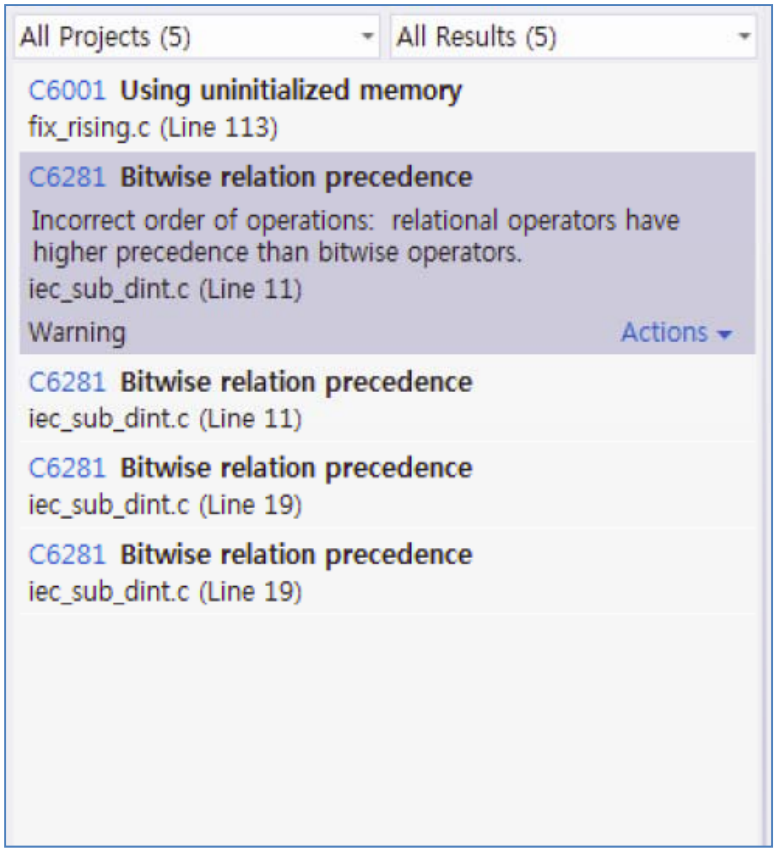
Static Analysis Result



C6001 Using uninitialized memory



C6281 Bitwise relation procedure



We found functional correctness (safety) - related errors.

We found no security-related error!

Splint

More than 100 errors !!!
- Not categorized

```
$ splint FIX_RISING.c
Splint 3.1.2 --- 28 Mar 2013

psettype.h:4:22: Type BOOL is probably meant as a boolean
type, but the boolean
                    type name is not set. Use -booltype BO
OL to set it.
  Use the -booltype, -boolfalse and -booltrue flags to cha
nge the name of the
  default boolean type. (Use -likelybool to inhibit warnin
g)
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)
                          ...

FIX_RISING.c:61:6: Variable exported but not used outside
FIX_RISING:
                       OUT__24__FIX_RISING
FIX_RISING.c:62:6: Variable exported but not used outside
FIX_RISING:
                       ENO__25__FIX_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:
                       ENO__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

KU KONKUK UNIVERSITY

THANK YOU!!!

and Questions?

Jang-Soo Lee

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