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

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>US NRC RG 5.71</td>
<td>Cyber Security Programs for Nuclear Facilities</td>
</tr>
<tr>
<td>IEC 61513</td>
<td>Nuclear Power Plants - I&amp;C important to safety</td>
</tr>
<tr>
<td></td>
<td>- General requirements for systems</td>
</tr>
<tr>
<td>IEC 60880</td>
<td>Nuclear Power Plants - I&amp;C systems important to safety</td>
</tr>
<tr>
<td></td>
<td>- Software aspects for computer-based systems performing category A functions</td>
</tr>
<tr>
<td>IEC 62645 (CD2)</td>
<td>Nuclear Power Plants - I&amp;C systems</td>
</tr>
<tr>
<td></td>
<td>- Requirements for security programmes for computer-based systems</td>
</tr>
</tbody>
</table>
Designers and developers for I&C systems shall have established and verified secure development methodologies in place throughout the development lifecycle of a system.
Programme level

PLAN

5.2 Establish the programme

5.3 Implement and operate the programme

5.4 Monitor and review the programme

5.5 Maintain and improve the programme

ACT

DO

CHECK

Security thematic areas

7.2.1 Security policy
7.2.2. Organizing Information Security
7.2.3. Asset Management
7.2.4. Human Resources Security
7.2.5. Physical and Environmental Security
7.2.6. Communications and Operations Management
7.2.7. Access Control
7.2.8. I&C Systems Acquisition, Development and Maintenance
7.2.9. I&C Security Incident Management
7.2.10. Operation Continuity Management
7.2.11. Compliance

System level

6.2 Requirements

6.3 Planning

6.4 Design

6.5 Implementation

6.6 Test

6.7 Installation, Checkout and Acceptance Testing

6.8 Operation and maintenance

6.9 Change management

6.10 Retirement
This paper focuses on

Our interest!!

This paper focuses on !!!

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

596 rules of 12 categories

Microsoft Visual Studio 2012
A Typical RPS SW Development Process

Development process:
- Requirements Analysis
- Design
- Implementation

- SRS
- FBD / LD Programs
- C Programs
- Executable Code for PLC

Manual Programming
Automatic Translator
COTS Compiler
A Typical RPS SW Development Process

Development process

- Requirements Analysis
- Design
- Implementation

- SRS
- FBD / LD Programs
- C Programs

- Manual Programming
- Automatic Translator
- COTS Compiler

Executable Code for PLC

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

5 critical errors !!!
We found functional correctness (safety) - related errors.

We found no security-related error!
More than 100 errors !!!
- Not categorized
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)