Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 23-25, 2019

Application of Safety Grade Display System to Accident Monitoring for Nuclear Power Plants

Koh Eun Kim*, Ji Hyeon Kim, Sung Ho Kim
I&C System Engineering Department, NSSS, KEPCO E&C
111, 989 Beon-gil, Daeduck-daero, Daejeon 34057
**Corresponding author: high07@kepco-enc.com*

1. Introduction

Information display systems for the accident monitoring have been developed and applied for domestic nuclear power plants(NPP's) including Inadequate Core Cooling Monitoring System with Important to Safety(ITS) grade software. Research and development for upgrading information display system for accident monitoring to Safety Critical(SC) grade has been performed for high reliability to conform to the recent licensing positions for NPP's. The software Verification and Validation(V&V) process for ITS grade software needs to be enhanced to meet the SC grade software development requirements. Highly reliable software will be provided if the coding process meets strict nuclear and industrial rules by undergoing newly developed test process.

2. Accident Monitoring Systems in Domestic NPP's

Plant variables need to be monitored for the operators to cope with accident conditions by assessing the plant status correctly and promptly for protective actions. The international requirements for accident monitoring have been changed recently and improvements in existing software development process are accordingly necessary.

2.1 Display Requirements for Accident Monitoring

Accident monitoring systems have been developed and applied as Important to Safety(ITS) grade based on the USNRC Regulatory Guides 1.97 for accident monitoring instrumentation and 1.152 for computers in safety systems of nuclear power plants(NPP's). IEEE Standard 1012 is also referred to for the software verification and validation process according to the safety integrity level in the standard. Inadequate Core Cooling Monitoring System has been incorporated in the plant design, as a part of accident monitoring, based on USNRC NUREG-0737, clarifications for Three Mile Island Action Plan.

2.2 Accident Monitoring Systems in Korean NPP's

The features of accident monitoring systems for domestic and overseas Korean NPP's have been summarized as shown in Table 1. Most of the accident monitoring systems have been designed according to the requirements in the revision 3 of the USNRC Regulatory Guide 1.97, whereas revision 4 has been applied for that of Shin Kori NPP Units 5 and 6. Type A variables of Shin Kori 5 and 6 are displayed on the safety grade Operator's Module(OM) with limited verification process for the graphic application software of the accident monitoring display system

2.3 Improvements for the Accident Monitoring Systems

The accident monitoring system software needs to be upgraded from ITS to SC grade to be prepared for the licensing position on Reg. Guide 1.97 for Type A variables since Type A variables should be displayed to the operator reliably during and following accidents. The upgraded display system will increase the reliability of accident monitoring functions.

Stringent V&V activities should be performed for the upgraded software, and a graphic library should be developed for verification tests. Coding rules should also be enhanced to increase the software reliability.

3. Development of Safety Critical Grade Software for Accident Monitoring

For upgrading ITS display software to the SC grade, industrial coding rules for C programming have been surveyed and arranged for the application to NPP's. Customized graphic library has also been developed, inspected, and tested by newly established V&V process.

3.1 Establishment of coding rules

Following industrial standards and regulatory reports provide coding rules for the programming:

- IEC 61508(Reference 1)
- USNRC NUREG/CR-6463(Reference 2)
- KINAC/RS-015(Reference 3)
- MISRA C:2012
- SEI CERT C Coding Standard: Rules for Developing Safe, Reliable, and Secure systems(2016)

Each coding rule above provides recommendations to avoid unwanted functioning of the software and can be applied to the safety-related software for NPP's for secure coding. Total 97 coding rules for the safety critical software have been arranged consisting of 12 from RS-015, 84 from NUREG/CR-6463, and one(1) from IEC 61508. Duplications between coding

standards and those not to be applied for safety critical software have not been included.

3.2 Development of Graphic Library and Display Pages

The functional requirements have been established for SC grade display system. Total of 11 general display functions have been defined based on the requirements and four(4) types of graphic libraries have been identified to be developed. Attributes and functions of the newly identified graphic libraries have been defined, and graphic libraries have been developed for the Safety Critical grade display software as the development process shown in Fig. 1. The graphic support card without any Open-GL(Graphic Library) were used to compose display which is different from usual display system that uses graphic card with Open-GL. Research has been focused in developing the graphic library requirements and new graphic widgets for SC grade software development process.

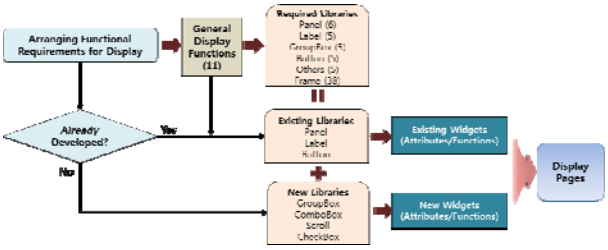

Fig. 1 Development of SC Customized Graphic Library

3.3 Enhancement of V&V Test Process

A unit test is performed for the accident monitoring software according to the ITS grade V&V process as shown in Fig.2. This means that functional testing of the software unit installed on the processor is performed by checking the outputs comparing to the expected results after applying inputs to the software unit. Module test is not generally performed for the ITS grade software, and the source codes of the commercial graphic library cannot be tested since the tool vendors usually do not provide them.

A prototype project has been developed to apply the enhanced coding rules, and module tests have been performed for the developed customized graphic library and display pages including the display software unit during this research.

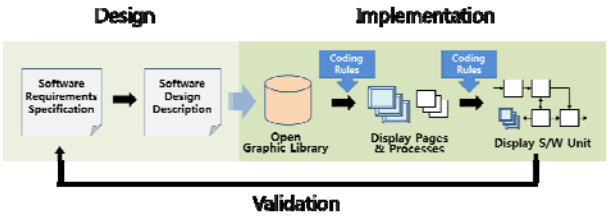

Fig. 2. Development of ITS Grade Display Software

White box tests have been performed for static and dynamic verification of the developed software modules according to the enhanced software V&V process as shown in Fig. 3. Static verification of the software modules has been performed using the Code Inspector® with the violations with respect to the enhanced coding rules as shown in Table 2. Each of the violations has been reviewed and corrected as appropriate based on the guidelines of the coding rules and coding experience.

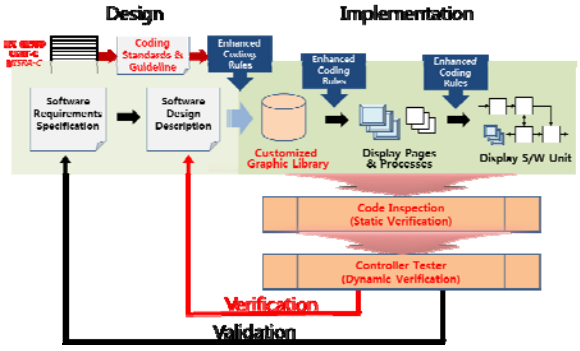

Fig. 3 Development of SC Grade Display Software

Dynamic verification has been performed using Controller Tester® to increase test coverages of the display software modules of the prototype project including statement coverage, branch coverage, function call coverage, and Modified Condition/Decision Coverage(MC/DC) as shown in Table 3. The coverage can be increased up to 100% by generating more test cases manually.

Table 2. Finding Violations by Code Inspection

Coding Rules	No. of Violations	Severity(%)				
		Very High	High	Low	Very Low	Other
IEC 61508	586	3.41	16.04	37.88	42.66	0
MISRA C	1568	17.54	48.72	33.74	0	0
CERT C	3585	36.18	21.37	26.28	0	16.18

Table 3. Coverage by Testing

Coverage Type	Statement	Branch	Call	MC/DC
Coverage(%)	72.29	73.54	72.93	64.46

4. Conclusion

Graphic library has been developed and verified based on the strict coding rules established during this project. The software modules of the prototype project

have been tested for verification using commercial tools for white box tests. Strict V&V process and secure coding steps have been established for Safety Critical grade software development. The display systems for accident monitoring which require the highest level of integrity can be provided using the software development methodology, graphic library, and coding rules developed during this project. Establishing verification process can be completed with additional activities of module tests for in full scope of the application software of the accident monitoring system during the replacement project for the sites.

REFERENCES

[1] IEC-61508, Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-related System, 2010, IEC.
[2] USNRC NUREG/CR-6463, Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems, June 1996.
[3] KINAC/RS-015.01, 원자력시설 등의 컴퓨터 및 정보시스템 보안 기술기준, 2014.