Development of Digital MMIS for Research Reactors: Graded Approaches

Rahman Khalil ur [a], Jinsoo Shin [a], Gyunyoung Heo [a*], Hanseong Son [b],
Youngki Kim [c], Jaekwan Park [c], Sangmun Seo [c], Yongjun Kim [c]
[a]*Kyung Hee Univ., Yongin-si, Gyeonggi-do, 446-701, Korea*
[b]*Joongbu Univ., Chubu-myeon, Geumsan-gun, Chungnam, 312-702, Korea*
[c]*Korea Atomic Energy Research Institute, Deokjin-dong, Daejeon, 305-353, Korea*
[*]*Corresponding author: gheo@khu.ac.kr*

1. Introduction

Though research reactors are small in size yet they are important in terms of industrial applications and R&D, educational purposes. Keeping the eye on its importance, Korean government has intention to upgrade and extend this industry. Presently, Korea is operating only HANARO at Korea Atomic Energy Research Institute (KAERI) and AGN-201K at Kyung Hee University (KHU), which are not sufficient to meet the current requirements of research and education. In addition, we need self-sufficiency in design and self-reliance in design and operation, as we are installing research reactors in domestic as well as foreign territories for instance Jordan. Based on these demands, KAERI and universities initiated a 5 year research project since December 2011 collaboratly, for the deep study of reactor core, thermal hydraulics, materials and instrumentation and control (I&C).

This particular study is being carried out to develop highly reliable advanced digital I&C systems using a grading approach. It is worth mentioning that next generation research reactor should be equipped with advance state of the art digital I&C for safe and reliable operation and impermeable cyber security system that is needed to be devised. Moreover, human error is one of important area which should be linked with I&C in terms of Man Machine Interface System (MMIS) and development of I&C should cover human factor engineering.

Presently, the digital I&C and MMIS are well developed for commercial power stations whereas such level of development does not exist for research reactors in Korea. Since the functional and safety requirements of research reactors are not so strict as commercial power plants, the design of digital I&C systems for research reactors seems to be graded based on the stringency of regulatory requirements.

This paper was motivated for the introduction of those missions, so it is going to describe the general overview of digital I&C systems, the graded approaches, and future plans of the project.

2. Methods and Results

2.1 Overview of Digital I&C and MMIS

In case of large-scale commercial Nuclear Power Plants (NPPs), analogue I&C for effective monitoring and control has been almost replaced with digital ones. As well as reliability, flexibility of design and modification has been enhanced through digitalization of safety system such as safety grade programming logic circuits. Plant monitoring and control performance also has been improved by adopting the digital technology. Likely to the trend, the digitalization has been a key issue in I&C design of research reactor and digital systems have been chosen for reactor protection, control and monitoring except few analog systems for diverse mean or cost problem.

2.2 Issues on Research Reactor I&C and MMIS

Most of I&C and MMIS architecture of research reactors are expected to those of commercial NPPs due to their nature characterized by nuclear chain reaction. However, unlike the commercial NPPs, research reactors cannot operate continuously due to frequent trips and test and/or maintenance of I&C [1]. There are distinguished features in operating engineered safety features. Physical and functional I&C architecture of existing research reactors is analogous which will be digitalized to make it more safe, autonomous and continuously operable. I&C and MMIS could be devised for research reactors similar in functionality and safety and different in architecture of commercial NPP.

2.2.1 Concept of Graded Approaches

Graded approach for safety systems and regulatory requirements of research reactor is the process, based on IAEA recommendation, in which control measures and conditions should stringently be applied keeping eye on likelihood and possible consequences of loss of these control and condition along with the risk associated [2]. Here graded approach is that the stringent regulatory requirements will be applied to the NPP systems to sort out systems important to safety and security for research reactor with the intention to make them digital and integrated in MMIS. This is the objective of this project.

2.2.2 *Cyber Security*

The cyber risk of I&C systems is generally analyzed based on the occurrence possibility and the degree of affection of the threats according to the identified vulnerabilities [3, 4]. The countermeasures against the cyber risk are prepared according to the analysis results [5]. The loss of secrecy, perfection and availability are the parameters which affect the degree of affection of the threats. The occurrence possibility of the threats can be obtained qualitatively or quantitatively based on cost effectiveness and objective, such as quantitative may be

preferred in the case when numerical data of cyber threats is required.

The cyber security issues of research reactors can be addressed differently from those of commercial plants, as research reactors have short periods of operation and various operation modes relatively compared to commercial nuclear power reactors. This means that the operator interventions in research reactors are more frequent than those in commercial reactors and occurrence possibility of cyber threats will be more probable. Therefore, it is necessary to consider the degree the human operator intervention in research reactor operation, which can be directly related to degree of responsibility of control system during the reactor operation. Hence the level of control, which in turn is degree of responsibility of control system, should be considered to analyze the occurrence possibility of cyber threats and prepare the countermeasure against the cyber threats. Through this research, a level of control based analysis method for the estimation of occurrence possibility of cyber threats and a cyber risk analysis method for research reactors will be established. The cyber risk analysis method may provide technical bases with the countermeasures against the threats for research reactors, which is also the aim of this research.

2.2.3 Software V&V

Unlike the cyber security, software verification and validation issues of research reactors should not be addressed differently from those of commercial plants [3, 4]. At the very least, when the software safety grade is determined to consider the depth of verification and validation, it may be necessary to take a different approach. Research reactors have short periods of operation and various operation modes relatively compared to commercial NPP. This means that the operator interventions in research reactors are more frequent than those in commercial reactors. Considering that software takes a major role of the reactor operation, we can know that the affection to the reactor safety depends on software use frequency. Therefore, the criticality of software of research reactors is higher than that of commercial reactors.

Based on this, this research suggest that the level of software control, which is defined as to what degree is software responsible for the reactor protection and control, should be considered to evaluate the software safety grade for research reactors and determine the depths of verification and validation according to the grade. Through this research, a level of software control based evaluation method for the software safety grad and a verification and validation depth decision method for research reactors will be established.

2.2.4 Human factor engineering

Regulatory guides [6, 7] for NPPs require many considerations on Human Factor Engineering (HFE) because operators should take many types of equipment in large scale control room carefully. In case of research reactors, functions or tasks allocated to operators may be fewer than those of NPPs. Also, the possibility of recognition error, which is the most important factor of human error, may be low because information required for operators for control research reactor is comparatively not well developed and formulated like commercial power plant. There is no disagreement that appropriate analysis and assessment as graded approaches need to be applied to research reactor. Therefore, it is important to find proper approaches, and provide justification of exemption for each HFE elements in research reactor.

3. Discussions and Further Study

In this study, a solid long term vision regarding research reactor I&C and MMIS, consistent with the project objectives, is defined which will support reliable, safe and viable operation of research reactors. The application of graded approach and development of digital I&C for research reactor on the same lines of commercial power plant is also salient aspect of this research.

The cyber risk analysis method will be established to estimate occurrence possibility and ultimately cyber risk of research reactor. It is intended that an evaluation method for the software safety and verification and validation depth decision method for research reactors will be established. Human factor analysis should be performed for research reactors and suitable approach will be devised.

ACKNOWLEDGEMENT

This work was supported by Advanced Research Center for Nuclear Excellence (ARCNEX) program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology. (Grant Number: 2011-0031773)

REFERENCES

[1] International Atomic Energy Agency, The Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors, Draft safety Guide, DS351 Draft 7, March 15, 2011.
[2] International Atomic Energy Agency, Terminology used in Nuclear Safety and Radiation Protection, International Atomic Energy Agency, Vienna, 2007.
[3] Regulatory Guide 1.152 Rev 2, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants
[4] IEEE Standard 7-4.3.2-2003, Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, 2003.
[5] NIST SP800-82, "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security", September 2006.
[6] U.S NRC, Human Factors Engineering Program Review Model, NUREG-0711 Rev 2,
[7] U.S NRC, Human-System Interface Design Review Guidelines, NUREG-0700 Rev 2.