Comparative Assessment of Instrumentation and Control (I&C) System Architectures for Research Reactors

Rahman Khalil ur [a], Gyunyoung Heo [a*], Hanseong Son [b],
Youngki Kim [c], Jaekwan Park [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

Application of digital I&C has increased in nuclear industry since last two decades but lack of experience, innovative and naïve nature of technology and insufficient failure information raised questions on its use.

The issues has been highlighted due to the use of digital I&C which were not relevant to analog. These are the potential weakness of digital systems for Common Cause Failure, threat to system security and reliability due to inter-channel communication, need for highly integrated control room and difficulty to assess the digital I&C reliability [1, 2].

In the existing scenario, HANARO and JRTR have hybrid I&C systems (digital plus analog) whereas OPAL is fully digitalized. In order to authenticate the choice of fully digital I&C architecture for research reactor, it is required to perform assessment from risk point of view, cyber security as well other issues. The architecture assessment method and restrictions are discussed in the next part of article.

2. Architecture Assessment Approach

Assessment and optimization of I&C architecture for research reactor is one of the objective of this project, which is being targeted in this study. Optimized I&C architecture should have following features:

a. Independent and reliable to control and protect,
b. Least common cause failure (CCF) contribution,
c. Resistant to cyber-attack.

This article highlights two approaches qualitative and quantitative. Qualitative approach is used to evaluate independence and ability to cope the accidental scenarios whereas quantitative approach will focus on the CCF failure contributions and over all architecture failures.

2.1. Qualitative Assessment

Technical assessment focuses on requirements, design, source code, review to evaluate the independence of equipment in overall architecture. In this approach, hypothetical failures are postulated and equipment, system & I&C architecture are assessed against this failures to verify the Defense in Depth (DiD) design of I&C architecture. This method is based on Institute for Radiological Protection and Nuclear Safety (IRSN), which is defense in depth and diversity assessment [3]. This method assesses and verifies the design against the standard criteria and line of defense. The criteria of RG-1.75 & EEE Std. 384-1992 are:

- Independence of Class 1E Equipment and Circuits,
- Physical Independence of Electric Systems.

Overall I&C architecture of research reactor can be divided into three levels i.e. level 0, level 1 and level 2 for the independence evaluation to avoid common cause failures and other plausible failures. Level 0, level 1 and level 2 represent sensors & actuators, system modules and control room & console panels respectively. The basic information of I&C architecture to assess independence is safety classification, defense lines and equipment design. Level 0, 1 and 2 are defense lines which are defined in table 1. The division of I&C equipment, system and architecture are divided against these levels in figure 1.

Table 1: Definition of defense lines for assessment of architecture based on IAEA Standards [4]

Level 0	Maintaining the facility in the authorized domain (IAEA DiD Level 2 (INSAG10))	Sensors, Transmitters, Actuators, Actuation System
Level 1	Controlling accidents inside design hypotheses (IAEA DiD Level 3 (INSAG10))	Control, Protection and Processing Systems
Level 2	Preventing the degradation of accident conditions and limiting the effects of severe accidents (IAEA DiD Level 4 (INSAG10))	Monitoring, Control Room

2.1.1. Assessment Method

DiD assessment of I&C architecture can be used to evaluate two parameters; one is the independence of component and system in the overall architecture while the other is failure analysis of functions of equipment, system and architecture against the plausible events.

Dependence matrix between safety classes of architecture, equipment or system and function of corresponding device against defense lines (levels) can be prepared to verify the independence of each device and function in the overall architecture.

For failure analysis, a list of representative and probable events can be prepared and coupling of equipment, system and architecture with the event is prepared based on the function of defense line, as shown in figure 2. For instance, each system should be analyzed in detail against the single failure whereas overall architecture of all systems with interface should be considered in depth for power supply failure propagation.

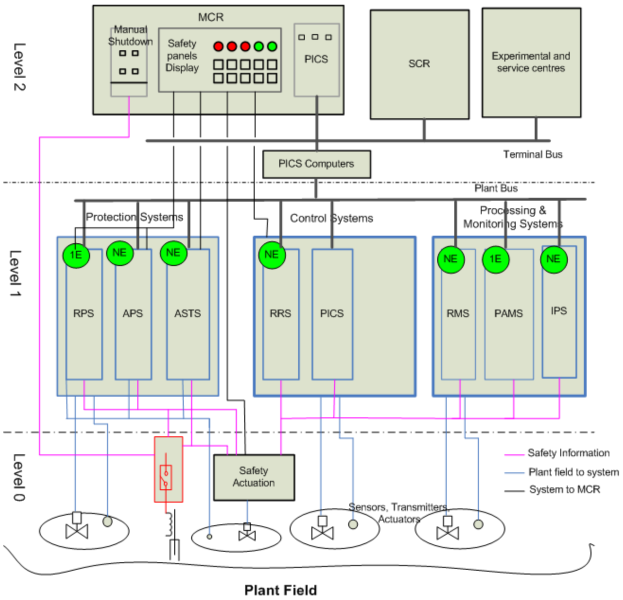
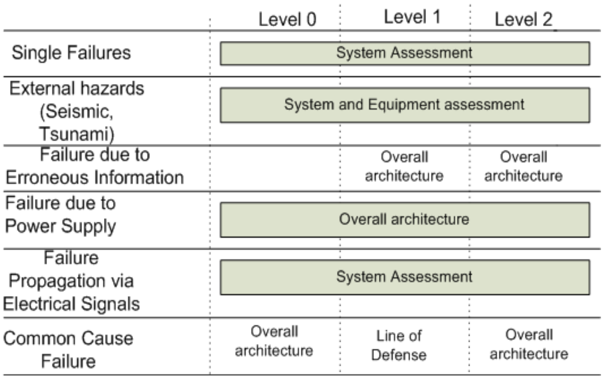


Figure 1: Division of I&C Architecture in levels for assessment[†]



	Level 0	Level 1	Level 2
Single Failures	System Assessment		
External hazards (Seismic, Tsunami)	System and Equipment assessment		
Failure due to Erroneous Information		Overall architecture	Overall architecture
Failure due to Power Supply	Overall architecture		
Failure Propagation via Electrical Signals	System Assessment		
Common Cause Failure	Overall architecture	Line of Defense	Overall architecture

Figure 2: Assessment of devices for the plausible events

2.2. Quantitative Assessment

As it is supposed that use of digital I&Cs will introduce prominent CCF failures. In order to verify this thought, architecture should be assessed quantitatively and then it can be decided about the fate of part of architecture or 1E equipment which is contributing more. Similarly the optimization of I&C architectures, which is one of the objective of this study, can be achieved through the quantitative assessment. The different combination of I&C such as fully digital, hybrid and fully analog can be analyzed using the PSA model (risk quantification) and then finalize the least risk contributing as optimum. But there are few limitations, which are described below.

3. Assessment Restrictions

Review of generation III nuclear power plants (EPR) revealed that application of digital I&C in nuclear industry, in general, generates new issues which may lead to naïve safety threats. Moreover, the assessment of these safety hazards is more difficult; and may cause higher uncertainties in risk assessment [5]. The highlighted restrictions are as follow:

i. Failure mode taxonomy of digital I&C component is not in well-developed form. Rather no standard failure modes have been developed due to lack of experience.
ii. Lack of failure data of digital I&C is another issue.
iii. Existing PSA model does not give detail modeling of digital I&C systems.

4. Results and Discussions

In this study, methods for the assessment of architecture in terms of independence between safety classes & defense lines for each equipment and system and risk (CDF) are explained. Qualitative approach was applied to assess independence and the each equipment & architecture against each defense level is analyzed to perform function against the plausible failures based on this approach. Quantitative technique is based on PSA, which quantifies the risk in form of CDF and contribution of I&C failures. These two methods will jointly be used to optimize I&C architecture with high reliability and least CCF failure.

ACKNOWLEDGEMENT

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

REFERENCES

[1] US National regulatory Commission, The United States of America Fifth National Report for the Convention on Nuclear Safety, NUREG-1650 Rev.3, pp.23, September 2010.

[2] John Bickel, Digital is safe enough, Nuclear Engineering International, magazine November 2009, pp. 20-23, and 2009.

[3] Jean Gassino, Pascal Régnier, Assessment of the overall Instrumentation & Control architecture of the EPR FA3 project, Institut de Radioprotection et de Sûreté Nucléaire, DSR/SAMS, France.

[4] International Atomic Energy Agency, Defense in Depth in Nuclear Safety, INSAG-10, Vienna, 1996.

[5] Dr. C. Hirsch, Dr. H. Hirsch, Assessment of I&C Problems of the EPR, Study commissioned by Greenpeace Nordic, Neustadt Germany, 2010.

[†] NE - Non-nuclear safety grade,