Sensitivity Analysis of Digital I&C Modules in Protection and Safety Systems

Rahman Khalil Ur, M Zubair, G Heo
College of Engineering, Department of Nuclear Engineering: Kyung Hee University, Yongin Si, Gyeonggi Do, 446-701, Republic of Korea

E-mail: gheo@khu.ac.kr

Abstract. This research is performed to examine the sensitivity of digital Instrumentation and Control (I&C) components and modules used in regulating and protection systems architectures of nuclear industry. Fault Tree Analysis (FTA) was performed for four configurations of RPS channel architecture. The channel unavailability has been calculated by using AIMS-PSA, which comes out 4.517E-03, 2.551E-03, 2.246E-03 and 2.7613-04 for architecture configuration I, II, III and IV respectively. It is observed that unavailability decreases by 43.5 % & 50.4% by inserting partial redundancy whereas maximum reduction of 93.9 % in unavailability happens when double redundancy is inserted in architecture. Coincidence module output failure and bi-stable output failures are identified as sensitive failures by Risk Reduction Worth (RRW) and Fussell-Vesely (FV) importance. RRW highlights that risk from coincidence processor output failure can reduced by 48.83 folds and FV indicates that BP output is sensitive by 0.9796 (on a scale of 1).

1. Introduction
Nuclear Industry has lot of application in power generation, water desalination, thermal heat source, testing, well logging, food sterilization and preservation, material research and education. It is therefore essential that all these application must be applied safely and securely in order to keep public, environment and operating staff protected from harmful effects of radiation. Reliability and safety of components and systems used in this industry has become high level objective of prime importance. Commercial nuclear power plants and research reactors can be categorized broadly under the umbrella of nuclear industry. The further discussion in this article will be focused on research reactor.

The primary objectives of research reactors are education, research and analysis, so these are generally designed in the range of several kilo watts to few megawatts. According to IAEA TECDOC-1234, Research reactors with 0.250-2.0 MW power rating or $2.5 \times 10^{11}$ to $10 \times 10^{11}$ n/cm$^2$.s flux are termed low power reactor whereas research reactors ranging from 2- 10 MW power rating or $0.1 \times 10^{13}$ to $10 \times 10^{13}$ n/cm$^2$.s are considered as medium to high power research reactors [1]. Instrumentation & Control (I&C) systems used in early designs of research reactors were analogue whereas recently these are either designed using digital ones or being replaced with the digital I&C. The novel kind of issues has been observed with the use of digital I&C, which were not relevant in case of analogue. The salient issues are (1) weakness of digital systems for Common Cause Failure (CCF), (2) threat to cyber security and inter-channel communication, (3) need for highly integrated control room and (4) difficulty to assess the digital I&C reliability [2].
Research objective, in this article, is sensitivity analysis of I&C components and modules in Instrumentation and Control (I&C) architecture. In order to achieve this objective, the preventive maintenance optimization process has been developed to reduce unavailability and different architecture configurations were formulated and their fault trees were developed using AIMS PSA to estimate the unavailability. The failure combination or Minimal Cut Sets (MCS) related to Bi-stable Processor (BP) and Coincidence Processor (CP) are monitored and their risk importance measures are estimated in this study. The current article presents the analysis of four architectures.

2. Literature Review

Safety analysis of nuclear facilities specially research reactors and power plants can be divided into two categories viz. Deterministic Safety Analysis (DSA) and Probabilistic Safety Assessment (PSA). Regulatory bodies and operating organizations in nuclear operating nations have to perform both these analysis. IAEA is playing a key and leading role in these areas specially PSA. IAEA experts evaluated reliability data sources [3] analysed and compiled the component reliability data for PSA [4]. United State National Regulatory Commission (USNRC) performed a lot of study in the field of PSA. USNRC performed a reactor safety study jointly with education institutes in 1975 [5] and published a detail PSA procedure guide in 1983 [6]. USNRC consultants are working in the area of digital I&C systems [7] and industry averaged failure data analysis based on initiating events of PSA study [8].

Research institutes and design companies are also focusing on PSA, as it can be used in risk based designing and operation. PSA has ability to identify the importance of I&C systems in nuclear facilities based on risks. Risk significance deriving sensitivity analysis of reactor trip system due to software induced common cause failure was performed by Shahabeddin et al [9]. M. Zubair et al performed quantitative and qualitative analyses of safety parameters by using an online risk monitor system (ORMS), which can check the availability of I&C systems and monitor it during severe accident [10]. Human reliability analysis is an important constituent of PSA and human error probabilities are highly contributing failures during operation and maintenance activities. Poong et al attempted to introduce advanced Man Machine Interface System (MMIS) which will be reduce human error probability [11]. In this article, I&C component based sensitivity analysis was performed first time and it is a novel concept to identify the risk significant components instead of system and addressing them in designing I&C architecture, which will be leading towards risk based designing approach.

3. Analysis technique

Probabilistic Safety Assessment (PSA) is a systematic approach which is used in nuclear, chemical and aviation industry to analyze the system failure in terms of system unavailability and to predict the failure scenarios. In PSA it is also important to identify primary function of each component. In nuclear industry, PSA is used to validate the design of nuclear power plant against set of Postulated Initiating Events (PIEs) [12]. PSA analysis frame work consists of Initiating Event Analysis, Accident Sequence Analysis, and System Analysis etc. Since this article is focused on sensitivity analysis of a system, so Fault Tree Analysis (FTA) technique was opted for system analysis. Fault tree is a good technique for the analysis of complex system, as it yields cut sets showing the failure of components in combinations.

The tool, used to perform Fault Tree Analysis, is AIMS-PSA package. This tool is developed by Korean Atomic Energy Research Institute (KAERI). AIMS software performs the analysis of risk models that are composed of event tree and fault tree. It is used in risk evaluations of nuclear plant’s PSAs or risk assessment of chemical plants.

4. System Configuration

Instrumentation and Control (I&C) systems are designed to control, protect and monitor the safe operation of commercial power plants and research reactors in order to maintain safety functions:

   a) Controlling the reactivity in the core,
   b) Cooling the core to avoid Departure from Nucleate Boiling Ratio (DNBR) violation,
c) Confining the radioactivity
Reactor Control System is responsible for regulating the reactor power level using Control Rods (CRs) within set margin of operation during normal operation. It can perform the reactor control function including reactor start up, changing power levels, and maintaining the power at required level. Reactor Protection System (RPS) is a scram system that initiates the reactor trip to protect the core by inserting shutdown control rods, when operating parameters exceeds the set point or external hazard happens. Monitoring system is responsible to monitor the reactor parameters after and before the design basis accident. The system of interest in this research is reactor protection system and from now on architecture description will be related to RPS.

Architecture of RPS consists of field sensors, Bi-stable Processors (BP), coincidence logic, and circuit breakers to release control rods. Reactor protection system has inter-channel redundancy as well as intra-channel redundancy and this redundancy varies from plant to plant based on design features. Usually RPS consists of four channels in high power reactors with trip logic of 2/4 whereas three redundant and physically separated channels may work 2/3 trip logic for small or low power reactors. Instead of overall reactor protection system, only architecture of a single channel is articulated with four different configurations to see sensitivity effect.

4.1. Architecture Configuration-I
RPS single channel architecture configuration-I is shown in Figure. 1. Configuration-I consists of a single bi-stable processor BP_A and single coincidence processor CP_A and circuit breakers to trip with 2/3 logic. This configuration is very basic for a channel and has no inter-channel redundancy. Inter-channel redundancy means redundant modules within a channel whereas intra-channel redundancy is based on number of channels.

![Figure. 1. RPS single Channel architecture configuration-I](image)

4.2. Architecture Configuration-II
In architecture configuration-II, redundancy is added in bi-stable processors to evaluate the impact on single channel. Configuration-II is depicted in Figure. 2. RPS channel configuration –II consists of a bi-stable processor BP_A1 & BP_A2, a CP processor CP_A and circuit breakers to trip with 2/3 logic.
4.3. Architecture Configuration-III

In order to observe the sensitivity of CP module on single channel failure, coincidence processors is added in the channel, the configuration-III is given in the Figure. 3. RPS channel configuration –II consists of a bi-stable processor BP_A, redundant pair of CP processors CP_A1 & CP-A2 and circuit breakers to trip with 2/3 logic.
4.4. Architecture Configuration-IV

Architecture with inter-channel redundancy of BP & CP modules is shown in Figure 4. In this configuration, channel architecture consists of redundant bi-stable processors BP_A1 & BP_A2, redundant pair of CP processors CP_A1 & CP_A2 and circuit breakers to trip with 2/3 logic.

5. Modelling and failure data

The function of each channel of RPS is to initiate a signal if the input from digital input coming from the core protection calculator (CPC) and analogue sensor input from plant field exceeds the set point parameters. The signal coming from CPC or sensor is compared with set point value in bi-stable processor of each channel and trip signal and/or engineered safety initiation signals are generated. This function failure is modelled as a top gate failure in the fault tree. The interfaces of single channel are with (1) other channels, (2) engineered safety feature actuation system (ESFAS), (3) testing module (TM), (4) control cabinets through network buses and (5) field sensors and digital inputs. The modelling of TM module and ESFAS module is ignored in this analysis.

Success Criteria: The channel is said to be successful, if it generates 3/4 digital output signals from CP. The time window used for quantification of running failures is 372 hours. It is based on the surveillance and testing period, which is assumed to be one month and its half (T/2), is taken as time window.

CCF Modelling: Beta factor failure model is for circuit breakers common cause failure and output signal failure from coincidence processor modules. It inserts some conservativeness in the result, which may be changed to MGL or other model in future.

Failure Data: Generic and online available databases are used for this analysis, as shown in Table I. The salient reference databases are NUREG/CR-5500 [13], IAEA TECDOC 0930 [14], NUREG/CR-4550 [15], IAEA TECDOC 504 [3] and failure data reports [16].

6. Risk Importance Measures

Risk importance analysis is a sensitivity study which is performed to find the impact of a single failure or combination of failures of basic events on the overall failure of system. Using importance measures,
risk significant basic events can be identified. The sensitivity study differentiates basic events, components into high risk significant and low risk significant components and helps the utilities to focus on their surveillance & maintenance cost management [9].

Common importance measures are of many kinds like Birnbaum sensitivity measure, Improvement Potential, Risk Achievement Worth (RAW), Risk Reduction Worth (RRW), Criticality Importance and Fussell-Vesely (FV) measures. Few of them are discussed in the current article. The risk significance sensitivity criteria are defined in table II by American Society of Mechanical Engineers (ASME).

### Table 1. Reference failure data used in FTA

| Component          | Failure Mode                        | Failure Probability | Source                     |
|--------------------|-------------------------------------|---------------------|---------------------------|
| Bi-Stable          | Fails to Provide Output             | 7.10E-06            | IAEA TECDOC-930           |
|                    | Module output failure               | 2.20E-03            | NUREG/CR-6579             |
|                    | Bi-stable hardware failure         | 3.89E-07            | Generic Database          |
| Coincidence Logic Module | Fails to Provide Output             | 7.10E-06            | IAEA TECDOC-930           |
|                    | Module out failure                 | 2.20E-03            | NUREG/CR-6579             |
| Circuit Breaker    | Relay fail to open                  | 1.00E-04            | NUREG/CR-4639             |
| Network Bus        | No update from bus                 | 6.00E-05            | EUT Report 93-E-276 [8]   |
| I&C Transmitters   | Output Fails during Operation      | 4.06E-5/h           | IAEA TECDOC-930           |

6.1. Fussell-vesely (FV) Importance

FV importance is a relative measure of failure contribution of a basic event to overall system failure. In simple calculations, it is percentage failure contribution from a basic event. In terms of minimal cut sets, FV is the ratio of unavailability $F_i(x)$ of $i$th cut set to total unavailability of system, as defined in equation (1).

$$FV_i = \frac{\text{Failure of cutset with $i$th basic event}}{\text{Total system failure/unavailability}}$$

$$FV_i = \frac{F_i(x)}{\sum_{i=1}^{n} F_i(x)}$$ (1)

FV is direct indication of the unavailability of the component in the system analysis. Larger the FV importance, the higher component would be sensitive to risk.

### Table 2. ASME Sensitivity Criteria for Risk Significance

| Sensitivity Parameters | Risk Significance |
|------------------------|-------------------|
| FV > 0.005             | > 2.0             |
| < 0.005                | < 2.0             |
6.2. Risk Achievement Worth (RAW)
Risk Achievement Worth is defined as factor by which the unavailability will increase, if the failure of component or basic event is certain. RAW helps to identify the most crucial and critical components or failure modes, which are significant with respect to risk.

\[
RAW_i = \frac{F(1)}{\sum_{j=1}^{n} F_j(x)}
\]  

(2)

Where
\[
\sum_{i=1}^{n} F_i(x) = \text{total unavailability of system that is summation of unavailability of all cut sets.}
\]
\[
F(1) = \text{total unavailability with basic event probability or cut set unavailability set equal to 1.0.}
\]

6.3. Risk Reduction Worth (RRW)
RRW measures the amount by which total risk or unavailability will decrease, if the failure of a basic event or minimal Cut Set (MCS) is zero. RRW also helps to identify the critical components or failure modes; if these are successful system reliability would increase. The mathematical form of RRW is given by equation (3).

\[
RRW_i = \frac{\sum_{j=1}^{n} F_j(x)}{F(0)}
\]  

(3)

Where
\[
\sum_{i=1}^{n} F_i(x) = \text{total unavailability of system that is summation of unavailability of all cut sets.}
\]
\[
F(1) = \text{total unavailability with basic event probability or cut set unavailability set equal to 0 (granted success).}
\]

7. Results and Discussion
Fault Tree Analysis was performed for four configurations of RPS channel architecture, given in Fig. 1-4. The channel unavailability for each architecture calculated using AIMS-PSA package are elaborated in table III, these are 4.517E-03, 2.551E-03, 2.246E-03 and 2.7613-04 respectively. It can be observed that unavailability decreases by 43.5 % & 50.4% by inserting partial redundancy whereas maximum reduction of 93.9 % happens when double redundancy is added in architecture configuration IV.

| Table 3. Unavailability Results of Architecture configurations |
|--------------------------------------------------------------|
| case | Channel Unavailability | % Decrease in Unavailability | Configuration |
|------|------------------------|------------------------------|---------------|
| I    | 4.52E-03               | Reference                    | 1 BP +1 CP    |
| II   | 2.55E-03               | -43.5                        | 2 BP +1 CP    |
| III  | 2.24E-03               | -50.4                        | 1 BP +2 CP    |
| IV   | 2.76E-04               | -93.9                        | 2 BP +2 CP    |

The top Cut Sets (CS) of each configuration are considered for risk importance analysis. Risk importance analysis in terms of FV, RAW and RRW is calculated in table IV. The salient features of importance analysis are as follow:

a) Importance Analysis of top cut sets of architecture configuration –I shows that both BP and CP module are of equal importance and their output failures are more sensitive to risk. It can be observed from the results depicted in first two rows of table IV.
b) Top minimal cut set from each architecture configuration II & III highlights the output failure from CP and BP module respectively. Sensitivity parameters depict that both failure modes are significant. Failure of CP output is more sensitive. 

c) In double redundant architecture, common cause failure of bi-stable processor modules is dominant failure mode and sensitive to risk.

Table 4. Sensitivity Analysis of top cut sets

| case | Cut Sets                                      | P(cut set) | FV     | RAW  | RRW |
|------|-----------------------------------------------|------------|--------|------|-----|
| I    | RPS-CHA-CFG0-BP-DO-F                         | 2.20E-03   | 0.4871 | 221.90 | 1.95 |
|      | RPS-CHA-CP-CFG0-DO-F                         | 2.20E-03   | 0.4871 | 221.90 | 1.95 |
|      | RPS-CHA-CP-CFG0-HD-F                         | 8.52E-05   | 0.0188 | 222.37 | 1.02 |
|      | RPS-CHA-CPA-DO-F                             | 2.20E-03   | 0.8627 | 445.26 | 48.83 |
| II   | RPS-CHA-BPA12-DO-CCF                         | 2.20E-04   | 0.0862 | 446.14 | 1.11 |
|      | RPS-CHA-BP-DO-F                              | 2.20E-03   | 0.9796 | 392.29 | 7.29 |
|      | RPS-CHA-CPA1-AB1AB2-CCF                      | 2.79E-05   | 0.01242| 393.15 | 1.01 |
|      | RPS-CHA-CPA2-CN12-CCF                        | 6.00E-06   | 0.0026 | 3622.08 | 4.92 |
|      | RPS-CHA-BPA12-DO-CCF                         | 2.20E-04   | 0.7968 | 3622.78 | 1.11 |
| III  | RPS-CHA-CPA1-AB1AB2-CCF                      | 2.79E-05   | 0.1010 | 3622.85 | 1.02 |
|      | RPS-CHA-CPA2-CN12-CCF                        | 6.00E-06   | 0.0217 | 3622.85 | 1.02 |

RRW and FV importance of cut-sets of all architecture configurations is plotted against the cut set numbers, as shown in the Figure 5. The cut sets corresponding to cut set numbers are given in table V. It can be observed that highest RRW is from cut set # 5 which is of the order of 50, indicating that the risk will reduce by factor of fifty if CP output is reliable. On contrary to RRW, FV importance highlights cut set # 4 (CS-4) as sensitive failure, which related to output failure of BP. Moreover FV indicates that CS-2 to CS-4 has high importance. CS-2, CS-3 & CS-4 are related to BP failure modes while CS-5 and CS-6 are CP failure modes.

Table 5. Sensitivity Analysis of top cut sets

| Cut set # | RRW | FV     | Cut set                              | Remarks                        |
|-----------|-----|--------|--------------------------------------|--------------------------------|
| CS-1      | 1.11| 0.0862 | RPS-CHA-BPA12-DO-CCF                 |                                |
| CS-2      | 1.95| 0.4871 | RPS-CHA-CFG0-BP-DO-F                 | RPS-CHA-CFG0-BP-DO-F           |
| CS-3      | 4.92| 0.7968 | RPS-CHA-BPA12-DO-CCF                 | RPS-CHA-BPA12-DO-CCF           |
| CS-4      | 7.29| 0.9796 | RPS-CHA-BP-DO-F                      | RPS-CHA-BP-DO-F                |
| CS-5      | 48.83| 0.8627| RPS-CHA-CPA-DO-F                     | RPS-CHA-CPA-DO-F               |
| CS-6      | 1.95| 0.4871 | RPS-CHA-CPA-AB1AB2-CCF               | RPS-CHA-CPA-AB1AB2-CCF         |
| CS-7      | 1.11| 0.1010 | RPS-CHA-CPA2-CN12-CCF                | RPS-CHA-CPA2-CN12-CCF          |
| CS-8      | 1.02| 0.0188 | RPS-CHA-CPA-AB1AB2-CCF               | RPS-CHA-CPA-AB1AB2-CCF         |
| CS-9      | 1.02| 0.0217 | RPS-CHA-CPA2-CN12-CCF                | RPS-CHA-CPA2-CN12-CCF          |
8. Conclusion
The study has been conducted to analyze risk importance of BP and CP modules and failure modes related to them. It is found that output failure from BP and CP modules is highly significant to risk. RRW highlights that risk from coincidence processor output failure can reduced by 48.83 folds and FV indicates that BP output is sensitive by 0.9796 (on a scale of 1).

In order to cope with this situation, if the redundancy is added to these components, direct failures reduce but common cause failure mode becomes prominent mode of failure, as highlighted by CS-1, CS-3, CS-7 and CS-9 of table V. The study will be continued to analyze unavailability in future, but two additional factor cost and safety category of components would be added to find an optimized architecture for research reactors and remedies to these sensitive failures would be found out.

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

References
[1] International Atomic Energy Agency (IAEA) 2001 IAEA TECDOC-1234 Vienna
[2] Rahman KU, Heo G, Son H, Kim Y, Park J 2012 Transactions of the Korean Nuclear Society 979-80 Korea
[3] International Atomic Energy Agency (IAEA) 1988 IAEA TECDOC-504, Vienna
[4] International Atomic Energy Agency (IAEA) 1988 IAEA TECDOC-478, Vienna
[5] U.S National Regulatory Commission 1983 NUREG/CR-2300 Washington
[6] U.S National Regulatory Commission 1975 WASH-1400, Virginia
[7] U.S National Regulatory Commission 1998 NUREG/CR-6579, Washington
[8] U.S National Regulatory Commission 2007 NUREG/CR-6928, Washington
[9] Kamyab S, Reza M, Nematollahi, Shafiee G 2013 Annals of Nuclear Energy 57 294-303
[10] Zubair M, Ahmed R, Heo G 2013 International Journal of Energy Research ER .3080
[11] POONG HYUN SEONG et al, 2013 Nuclear Engineering and Technology, VOL.45 NO.2, NET.04.2013.700
[12] International Atomic Energy Agency (IAEA) 2010 Specific Safety Guide SSG-3, Vienna
[13] U.S National regulatory Commission 1998 Reliability Study NUREG/CR-5500, Washington
[14] International Atomic Energy Agency (IAEA) 1997 IAEA TECDOC-0930 Vienna
[15] U.S National regulatory Commission 1990 NUREG/CR-4550 Washington
[16] Bollen MHJ 1993 Literature Search for Reliability Data of Components in Electric Distribution Networks, EUT Report 93-E-276 (ISSN 0167-9708), Eindhoven University of Technology, Netherlands