Example Plant Model for an International Benchmark Study on DI&C PSA

Sung Min Shin[a*], Hyun Gook Kang[b], Jinkyun Park[a], Wondea Jung[a]
[a] *Integrated Safety Assessment Division, KAERI, Daedeok-daero 989-111, Yuseong, Daejeon, 305-353, Republic of Korea*
[b] *Department of Mechanical, Aerospace and Nuclear Engineering, RPI, 110 Eighth Street, Troy, NY 12180, USA*
[*] *Corresponding author: smshin@kaeri.re.kr*

1. Introduction

Internationally most of instrumentation and control (I&C) functions in nuclear power plants (NPPS) are being digitalized due to obsolescence of safety-grade analog components. Thanks to the extended features of digital systems, they are expected to contribute to the enhancement of both economy and safety. In this context the risk quantification due to these digitalized safety systems became more important. Although there are many challenges to address about this issue, many countries agreed with the necessity of research on reliability quantification of DI&C system. Based on the agreement of several countries, one of internal research association is planning a benchmark study on this issue by sharing an example digitalized plant model and let each participating member develop its own probabilistic safety assessment (PSA) model of digital I&C systems.

2. Outline of the benchmark study

2.1 Objective and scope of benchmark study

The objective of this study is to provide a benchmark comparison among the developed digital I&C risk models by participating member countries and to promote the development of well-agreed method of digital I&C PSA.

The scope of the study is to develop practical models based on the provided system description. The modelling technique used in the model development does not have to be limited to conventional techniques such as fault trees (FT) or event trees (ET) but it is recommended to use them for efficient comparison. Models must be able to accommodate the characteristics of digital systems such as fault tolerant feature, software, and network communication. This study focuses on one example accident case: Loss of main feedwater (LMFW) for the convenience of comparison.

2.2 Systems in example plant model

2.1.1 Front-line safety systems

The example plant model represents a fictive Boiling Water Reactor (BWR), which equips with 4-redundant trains for each safety system except Filtered Containment Venting system (FCV). Safety systems in this model are arranged in Table. 1 and Fig. 1, and Fig. 2 shows the electric system in the example plant, respectively.

Table 1. Safety systems in example plant model [1]

ACP	AC power system
CCW	Component cooling water system
EFW	Emergency feedwater system
MFW	Main feedwater system
RSS	Reactor scram system
ADS	Automatic depressurisation system
ECC	Emergency core cooling system
FCV	Filtered containment venting system
RHR	Residual heat removal system
SWS	Service water system.
HVA	Heating, venting and air conditioning system

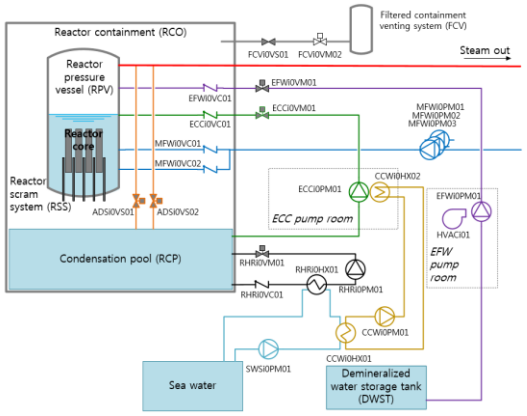


Figure 1. One train of front-line safety systems [1]

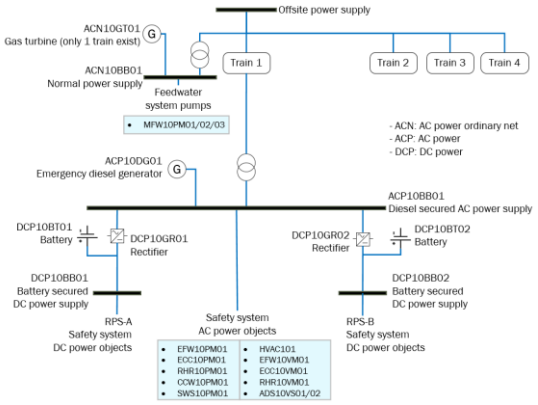


Figure 2. Electric systems in the example plant model [1]

2.2.2 Digitalized I&C systems

The hierarchy of a safety I&C system is illustrated in Fig. 3 which is referred to failure modes taxonomy developed by NEA/CSNI [2].

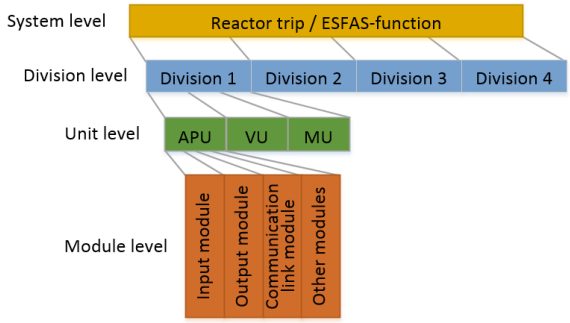


Figure 3. Hierarchy of safety I&C system

The architecture of the safety I&C system is presented in Fig. 4. The RPS has 4 physically separated but functionally identical divisions and each division is subdivided into two, called RPS-A and RPS-B. The two subsystems are responsible for different I&C functions in order to have diversity in safety functions and each subsystem consists of two units:

· Acquisition and Processing Unit (APU): This unit acquires process-related information from sensors, and perform calculations to determine the division output.

· Voting Unit (VU): This unit receives the results determined by the APUs in RPS-A (or RPB-B) of all divisions and performs 2 out of 4 voting in normal condition where all four divisions are available.

In addition to the APUs and VUs, the RPS includes another I&C unit for operator actions, abbreviated by MU (Manual control Unit). This unit is for the manual actuation of the primary circuit depressurization.

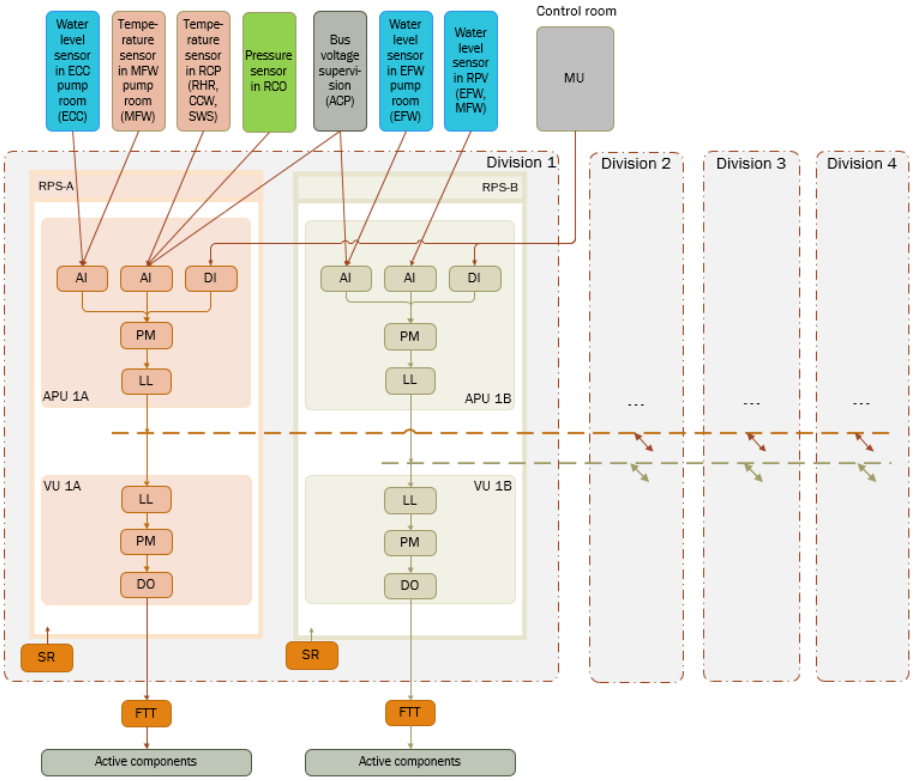
The I&C units are composed with several I&C modules, and each division has their own sensors which are identical according to types but physically separated between divisions. Each subsystem is powered by individual sub-rack (indicated as SR in the figure) which includes power supply from DC electricity buses (whose failures are DCPi0BB01/02) and has the fault tolerant technique (indicated as FTT) module which will be explained in chapter 4. For simplification, modules in MU and FTT are not considered, and all the connections except those between LLs are hard-wired ones of which failure probability are ignored.

2.2.3 Other information

Failure information and activation signals for components in each system are provided in separate document referring to relevant materials [3].

The example digital I&C protection system is designed with fault tolerant features, which provides means to detect failures and marks faulty signals. In this study, although certain type and mechanism are not specified, it is assumed that some portion of failures in I&C modules in APU and VU can be detected by the FTT in real time through inspection of output after VU. The reliability of FTT module on failure detection is assumed to be 99%.

Generally dedicated software will be implemented to each level of component. If identical software is installed to multiple redundant processors, it will cause the failures of multiple components together. That is, it is possible to represent those failures by a basic event based on the effect of software failure to a certain level of I&C component (system/division/I&C unit/I&C



module). The failure effects of software are arranged as in Table 2. It is assumed that a CCF exists between the failures of application software if identical software is used in RPS-A and RPS-B.

Table 2. Assumed CCF failure data for software modules [4]

Effect	Definition effect	Prob.
1AF[1]-APUs	Loss of one function of all APUs in one subsystem of all divisions	3E-5
1AF[1]-VUs	Loss of one function of all VUs in one subsystem of all divisions	2E-5
APUs-1SS[2]	Loss of one group of redundant APUs in one subsystem of all divisions	1E-5
VUs-1SS[2]	Loss of one group of redundant VUs in one subsystem of all divisions	1E-5
1SSs	Loss of one subsystem of all divisions	1E-6
SYS	Loss of complete system (all subsystems of all divisions)	1E-7

[1] Application function
[2] Subsystem

3. Conclusions

Although the DI&C systems are being applied to NPPs, of which modeling method to quantify its reliability still ambiguous. Therefore, an internal research association is planning a benchmark study to address this issue by sharing an example digitalized plant model and let each member develop their own PSA model for DI&C systems. This study is expected to provide a chance to compare strength and limitation of different approaches, further valuable insights for future model development.

REFERENCES

[1] Authén, S., Holmberg, J.-E., Tyrväinen, T., Zamani, L. Guidelines for reliability analysis of digital systems in PSA context — Final Report, NKS-330, Nordic nuclear safety research (NKS), Roskilde, 2015.
[2] Failure modes taxonomy for reliability assessment of digital I&C systems for PRA, report prepared by a task group of OECD/NEA Working Group RISK, NEA/CSNI/R(2014)16, Paris, 2015.
[3] Reliability Data of Components in Nordic Nuclear Power Plants, 7th edition, The TUD Office, Vattenfall Power Consultant, 2010.
[4] Bäckström, O., Holmberg, J.-E., Jockenhövel-Barttfeld, M., Porthin, M. & Taurines, A. Software reliability analysis for PSA: failure mode and data analysis, NKS-341, 2015.