Transactions of the Korean Nuclear Society Autumn Meeting
PyeongChang, Korea, October 30-31, 2008

Understanding on the ISG about Digital I&C PRA

Y. M. KIM , C. H. Jeong and G. M. Oh
Korea Institute of Nuclear Safety
Ymkim@kins.re.kr

1. Introduction

There has been many efforts to execute the PRA for the software based digital I&C systems. The ISG (Interim Staff Guidance) is made for providing acceptable methods for evaluating digital I&C system risk assessments of new reactor by NRC [1]. The primary purpose of this paper is to understand the ISG and to discuss the main issue of it. The ISG is not intended to provide the information of digital I&C system risk assessments for risk-informed regulatory decision making. With considering the software, the modeling of digital I&C system is considered immature process. Till now, there is no consensus on the technology for reliability modeling of software-based digital system. The use of risk-informed decision making is beyond the scope of the ISG.

This paper is organized as follows. Section 2 describes the difficulties and limitations of the risk assessment of digital I&C system and section 3 shows the important issues of it. Section 4 shows the 12 review guidelines on how to review digital I&C system risk assessments. Section 5 concludes the paper.

2. Difficulties and Limitations

Software-based digital I&C systems has unique failure modes. There have been many researches for categorizing the failure modes of digital system especially for software because they occur in various ways depending on specific applications. For determining the failure modes of system, the level of detail needed in modeling the I&C system is also important factor [2, 3].

There are many difficulties and limitations for executing digital I&C PRA. Some of these are follows [1, 2]:

- It is very difficult to either accurately predict or verify failure rates.
- Extrapolation of statistical data of the same system used in a different operating environment or profile is not necessarily meaningful.
- Commonly used hardware redundancy techniques may not improve software reliability.

Due to data the lack of consensus in the technical community on appropriate modeling methodology, the assessment of digital I&C system risk for new plants has been limited to examining assumptions, performing sensitivity studies, and evaluating important measure values [2, 3].

3. Important Issues

The key of the digital I&C issue in PRA is modeling of software and assignment of failure probabilities. For constructing the regulatory guide, there are some important issues as follows [2, 3, 4, 5, 6]:

- Determine whether current state-of-the-art reliability modeling techniques for software are sufficient for regulatory applications
- The level of detail needed in reliability modeling of digital systems to support risk informing digital system reviews
- Getting failure data needed to support risk-informing digital system reviews
- Integration of DI&C PRA portion of the PRA into overall PRA reviews

4. Review guidelines

The reviewer should focus on mainly two factors that are the reliability of the digital I&C system and defense-in-depth and diversity of the mechanical and electrical systems into which the I&C is installed [2, 4]. The NRC has developed guidance on how to review digital I&C system risk assessments based on the lessens learned from previously accepted new reactor digital I&C system PRA review. ISG suggested following 12 guidelines for reviewers [1].

- DI&C PRA portion of the PRA as an integrated part of the overall PRA review
- Identification of failure mode of DI&C
- DI&C CCF events
- Uncertainties in DI&C modeling and data
- DI&C system equipment is capable of meeting its safety function
- Impact of external event
- Modeling the failure of control room indication
- Important scope, boundary condition, and modeling assumptions
- Acceptability of the recovery actions
- Method for quantifying software failures
- Monitoring systems
- Review resources allocation

ISG also suggested that above guidelines should be reflected adequately to guarantee the risk contributions of DI&C, including software, in the overall plant risk results.

4.1 DI&C PRA portion of the PRA as an integrated part of the overall PRA review

The level of review of the digital I&C portion should be proportional to the use of results and insights from the applicant's digital I&C risk assessment.

4.2 Identification of failure mode of digital I&C

As previously mentioned, it is very difficult to define failure modes of digital I&C systems. The reviewer should examine the most significant failure modes of the digital I&C risk assessment are documented and how the failure modes can fail the system.

4.3 DI&C CCF events

Review the identified CCF events and discuss how the applicant determined the probabilities associated with CCFs.

4.4 Uncertainties in DI&C modeling and data

Must perform a number of sensitivity studies that vary modeling assumptions, reliability data, and parameter values both at the component and system level.

4.5 DI&C system equipment is capable of meeting its safety function

The reviewer should confirm that digital I&C system equipment is capable of meeting its safety function under assumed environment.

4.6 Impact of external event

The impact of external events (i.e., seismic, fire, high winds, flood and others) has been addressed with regard to digital I&C.

4.7 Modeling the failure of control room indication

Evaluate the acceptability of how the failure of control room indication is modeled.

4.8 Important scope, boundary condition, and modeling assumptions

Evaluate the assumptions are realistic and the associated technologies which are documented and can be validated [6].

4.9 Acceptability of the recovery actions

Evaluate the acceptability of the recovery actions taken for loss of digital I&C functions.

4.10 Method for quantifying software failures

Quantifying methods for software failures should be verified. The methods should be sound and documented.

4.11 Monitoring program

The monitoring programs for ensuring that the digital I&C system remains highly reliable should be maintained soundly. The key assumptions for DI&C PRA should be under monitoring program.

4.12 Resources allocation for review

Resources allocation for review should be proportional to the use to be made of the PRA results. For limited use, limited review is appropriate.

5. Summary

In this paper, we describe and discuss the ISG (Interim Staff Guidance) of NRC. It is initial issue for use. It will be revised continuously through accepting industry comments and applying it to several real projects. Through the sensitivity analysis, ultimately we should evaluate whether the plant risk is sensitive to digital I&C reliability, especially software common cause failure. The results should be shown that the NPP risk importance of a digital I&C system not to be significant. Additionally, there are some elements that could be emphasized. First, good design and quality assurance processes should be first step of the digital I&C PRA processes. Second, hardware and software should be treated together as a system. Third, depth of the PRA modeling should be considered.

REFERENCES

[1] U.S. NRC, DI&C-ISG-03, "Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments," DI&C-ISG-03, Rev 0, August 11, 2008.
[2] U.S. NRC, Modeling of Digital I&C in Nuclear Power Plant Probabilistic Risk Assessments, Draft Industry Paper, 2007
[3] U.S. NRC, "Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessment," NUREG/CR-6901, Feb. 2006.
[4] U.S. NRC, "Standard Review Plan," "Guidance for the Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems,"
[5] U.S. NRC, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," RG 1.200, Rev. 1, Jan. 2007.
[6] U.S. NRC, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," RG 1.174, Rev 1, Nov. 2002.