Reliability analysis of digital I&C systems at KAERI

KIM Man Cheol

Integrated Safety Assessment Division, Korea Atomic Energy Research Institute, Daejeon, 305-353, Korea (charleskim@kaeri.re.kr)

Abstract: This paper provides an overview of the ongoing research activities on a reliability analysis of digital instrumentation and control (I&C) systems of nuclear power plants (NPPs) performed by the Korea Atomic Energy Research Institute (KAERI). The research activities include the development of a new safety-critical software reliability analysis method by integrating the advantages of existing software reliability analysis methods, a fault coverage estimation method based on fault injection experiments, and a new human reliability analysis method for computer-based main control rooms (MCRs) based on human performance data from the APR-1400 full-scope simulator. The research results are expected to be used to address various issues such as the licensing issues related to digital I&C probabilistic safety assessment (PSA) for advanced digital-based NPPs.

Keyword: probabilistic safety assessment; digital I&C; software reliability; fault coverage; human reliability analysis

1 Introduction

The global trend of nuclear I&C systems is the transition from conventional analog technology to advanced digital technology owing to the recent development of digital technology and the problem of the obsolescence of analog components. Therefore, verification of the safety of digital technology is a global issue, and the absence of established methods for a reliability analysis of digital I&C systems in NPPs is regarded as a bottleneck for a risk-informed technical framework. To address these issues, the development of basic technology for a reliability analysis of digital I&C systems in NPPs is currently ongoing at KAERI.

Even though various new safety issues are continuously arising as digital technology is introduced to NPPs, several issues specific to digital I&C systems are thought to be more important as related to the development of a reliability analysis of digital I&C systems in NPPs[1]: (1) software reliability, (2) fault coverage, and (3) human reliability in advanced digital-based MCRs.

Among the many modeling methods available, such as dynamic reliability analysis methods, which are considered to better reflect the characteristics of digital technology, research activities on the development of a reliability analysis of digital I&C systems in NPPs is mainly based on a fault tree analysis, as the modeling method has to be combinable with the conventional PSA modeling framework.

In this paper, the research activities at KAERI related to the reliability analysis of digital I&C systems in NPPs are introduced, with an emphasis on software reliability, fault coverage, and human reliability.

2 Software reliability

2.1 Introduction

One of the most critical factors in a digital I&C PSA is the reliability of the software used in the digital I&C systems. Software reliability is defined as the probability of failure-free software operation for a specified period of time in a specified environment. Software reliability is an important factor because software failures are, in general, considered one form of CCFs in digital I&C systems.

At KAERI, researches on four different approaches of software reliability estimation were performed, and an integrated model combining the four approaches was developed.

2.2 SRGM-based approach

It is generally known that software reliability growth models (SRGMs) cannot be applied to safety-critical software owing to a lack of software failure data. By applying the two most widely known SRGMs, Kim *et al*.[2] identified the possibilities and limitations of applying SRGMs to safety-critical software. Figure 1 shows the changes of the estimated total number of inherent software faults, which is a part of a software

Received date: December 2, 2012
(Revised date: January 4, 2013)

reliability result, calculated by the two software reliability growth models, as software failures are observed one by one. After 34th failure, the Jelinski-Moranda model estimated that the software failure probability is very small so that it can be used to perform safety-critical functions. However, it is also found that the expected total number of inherent software faults calculated by the software reliability growth models is highly sensitive to the time-to-failure data.

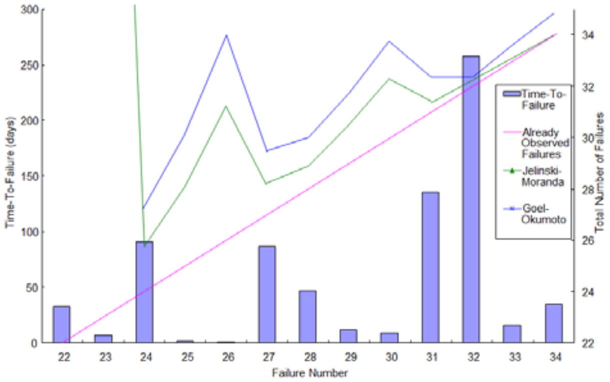


Fig. 1 Change of estimated total number of inherent software faults calculated by using two SRGMs.

In summary, it was found that SRGMs may be applied to demonstrate the high reliability of safety-critical software, but the high sensitivity of the software reliability to the software failure data and lack of sufficient failure data are identified as limitations that SRGMs should overcome before being applied to safety-critical software.

2.3 Metric-based approach

In a metric-based approach, it is basically assumed that measurable quantities exist in the software that can be related to the reliability of the software. One of the simplest examples is the number of lines in the software, because if the software is long, it is more probable to fail frequently.

Shi *et al.*[3] summarized the lessons learned from the application of test coverage (a metric) to a software application program for the purpose of a reliability analysis. Even though the test coverage was considered to be promising for software reliability estimation compared to other software engineering measures, the major obstacle was found to be the identification of the model parameters. A direct adoption of the parameters for a specific software application provided in the literature to other software applications was found to be inappropriate because such parameters were found to be application-specific, as shown in Fig. 2 where it can be seen that the relation between the branch coverage and the defect coverage is different depending on the software programs (DS2, DS3, and DS4).

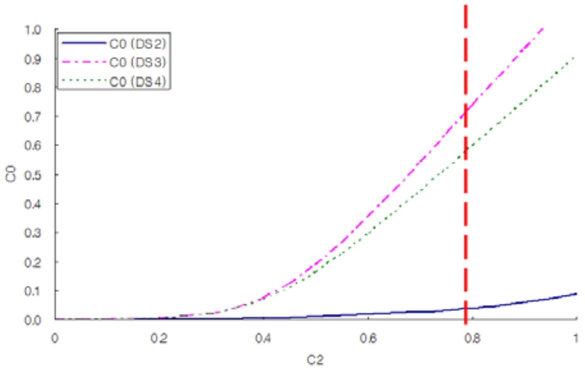


Fig. 2 Relation between the branch coverage (C2) and defect coverage (C0).

2.4 BBN-based approach

With the recognition of lack of software failure data during software development, a Bayesian belief network (BBN)-based approach started to receive a lot of attention as a framework for combining not only software failure data or software testing data but also various other information such as expert judgments, the quality of the software development process, and so on. Eom *et al.*[4] summarized the development of a BBN model for an estimation of the number of remaining faults in safety-critical software, which is one of the key parameters for a reliability analysis of the software, after the software development life cycle is completed. Considering that the safety-critical software developed for use in NPPs is subject to strict software verification and validation (V&V) activities, the BBN model by Eom *et al.*[4] tried to reflect the information obtained from software V&V activities and a regulatory review process, which are thought to have a strong relation with the reliability of the software, and with the reliability analysis of safety-critical software.

2.5 Test-based approach

One of the most straightforward ways in estimating the reliability of a software program is to perform software testing with a large number of test cases. However, the major difficulty was found that a large amount of software testing is required to demonstrate whether a software program has more than enough reliability than required. For example, it was found that almost 100,000 software tests without failure should be performed to demonstrate that the probability of a software failure on demand is less than 0.0001 with the confidence level of 99.99%.

In an effort to reduce the amount of necessary software testing, Kang *et al*.[5] developed an input-profile-based software failure probability quantification method, with consideration of two important characteristics of software testing. The first is that the input profile should properly reflect the fact that the input parameters are physical values, and the second is that software testing with the same input value does not need to be repeated because the response of the software is deterministic for each specific input to the software. With only 27 inputs, it could be demonstrated that the software failure probability is zero for the reactor trip function of a reactor protection system (RPS).

2.6 Integrated approach

After extensive review of the advantages and disadvantages of different software reliability analysis methods, a new software reliability analysis method was developed by integrating the advantages of different software reliability analysis methods, such as the BBN-based method, SRGM-based method, and the test-based software reliability assessment method, with a consideration of the software development process.

The basic idea behind the new software reliability analysis method is that different software reliability analysis methods require different kinds of data, and therefore the availability of various kinds of data makes it possible to apply more than two different software reliability analysis methods. When the software V&V documents exist, the BBN-based approach can be applied to produce the total number of faults in the software.

When the debugging history of the software exists, SRGMs are applied to estimate the unavailability of the software. At this point, if the total number of faults is estimated by using the BBN-based approach, it is used in estimating the unavailability of the software instead of estimating it again with the SRGMs. If there exists the result of software tests, it can be used to update the estimated unavailability of the software estimated by the BBN-based approach and the SGRMs. In this way, various data related to not only the software itself but also the development process of the software are also integrated into the integrated approach for a better estimation of the software reliability. How to integrate different kinds of results from different software reliability analysis methods is a challenge that needs to be addressed.[6]

3 Fault coverage

3.1 Introduction

Fault coverage is defined as the probability that a system properly processes an occurring fault in the system. Fault coverage is important because it is a measure used to estimate the effectiveness of self-diagnosis features of digital I&C systems, which prevents the failures of digital I&C systems from various component failures, including CCFs. Because theoretical approaches for an estimation of the fault coverage of a digital I&C system have many limitations, an approach based on fault injection experiments is considered as the most promising ways of estimating the fault coverage.

However, the major difficulty associated with the fault injection experiments is that a huge number of experiments are necessary to obtain a meaningful estimate on the fault coverage of a digital I&C system.

3.2 Fault injection experiments

In fault injection experiments, a fault is intentionally inserted into a digital I&C system, and whether the inserted fault is properly is observed. After repeating such experiments, the ratio of the number of properly processed faults over the total number of inserted faults is calculated to obtain an estimate of the fault coverage of a digital I&C system.

The development of a fault coverage assessment methodology for fault tolerant features such as mutual monitoring and self-diagnosis was performed.[7] For this purpose, a method based on fault injection experiments was developed. After comparing the advantages and weaknesses of various fault injection experiment methods, software implemented fault injection experiments with run-time fault injection were selected as a method for estimating the fault coverage of digital I&C systems. Fault injection experiments were performed on a real digital safety system as shown in Fig. 3, and fault coverage is estimated based on the experimental results.[8]

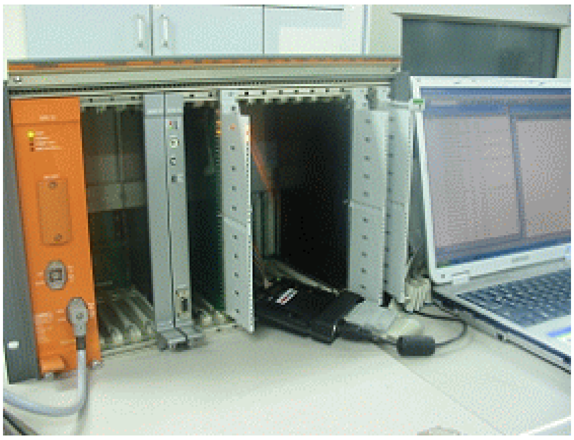


Fig. 3 Fault injection experiments with a digital I&C system.

During the fault injection experiments, it was found that fault coverage is dependent on various factors including the target digital system. It means that each system has its own fault detection coverage, and therefore the generalized value of the fault detection coverage is not feasible.

It was also found that a significant amount of inserted faults did not have any effect on the operation of the digital I&C system. In other words, the “no effect” faults were more important than expected. The implication of this finding on the safety of the digital I&C systems in NPPs needs to be further investigated. This fault coverage estimation method based on fault injection experiments is also considered as a practical method for verifying the safety of safety-related digital equipment and systems.

4 Human reliability

4.1 Introduction

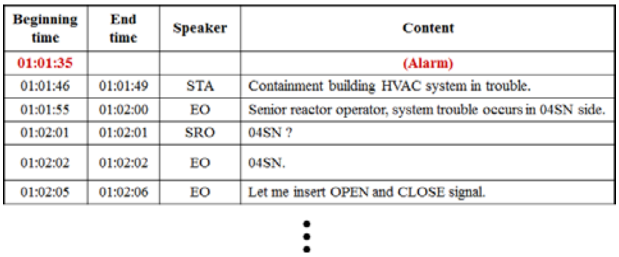
Because of the different operational environment in digital-based MCRs compared to conventional analog-based MCRs, a human reliability analysis method for computer-based MCRs needs to be developed. After consulting human reliability experts, a human reliability analysis method for digital-based MCRs was developed.[9]

4.2 Human error in digital system maintenance

Khalaquzzaman *et al.*[10] developed a model for estimating the reactor spurious shutdown frequency of a digital-based reactor protection system caused by the unavailability due to random failures and maintenance human errors. The model was also used for the optimization of the periodic testing frequency of the digital-based reactor protection system with the consideration of risk-cost and public risk perception.

4.3 Data collection in APR-1400 simulator

One of the best ways to develop a new human reliability analysis method for digital-based MCRs is to collect operator performance data in full-scope simulators. KAERI staffs have accumulated experience in collecting and analyzing operator performance data in full-scope simulators, and based on this experience various research results have been produced such as the development of a standard communication protocol for NPP MCR operators.[11] Operator performance data in an APR-1400 full-scope simulator were collected, and various analyses such as a protocol analysis and timeline analysis are currently ongoing, as shown in Fig. 4.



Beginning time	End time	Speaker	Content
01:01:35			(Alarm)
01:01:46	01:01:49	STA	Containment building HVAC system in trouble.
01:01:55	01:02:00	EO	Senior reactor operator, system trouble occurs in 04SN side.
01:02:01	01:02:01	SRO	04SN ?
01:02:02	01:02:02	EO	04SN.
01:02:05	01:02:06	EO	Let me insert OPEN and CLOSE signal.

⋮

Fig. 4 Communication log for a protocol analysis.

5 Conclusions

This paper provides an overview of the research activities on the reliability analysis of digital I&C systems at KAERI. The research activities include the development of a new safety-critical software reliability analysis method by integrating the advantages of existing software reliability analysis methods, a fault coverage estimation method based on fault injection experiments, and a new human reliability analysis method for computer-based MCRs based on human performance data from an APR-1400 simulator.

The research results are expected to be used for various future applications such as (1) supporting industries in conducting digital I&C PSAs, (2) supporting licensing issues related to a digital I&C PSA, (3) design feedback of digital I&C for future NPPs, and (4) support of other industries where the safety verification of digital technology is required.

Nomenclature

ATWS	anticipated transient without scram
BBN	Bayesian belief network
CCF	common cause failure
ESF	engineered safety features
I&C	instrumentation and control
KAERI	Korea Atomic Energy Research Institute
MCR	main control rooms
NPP	nuclear power plant
PSA	probabilistic safety assessment
RPS	reactor protection system
SRGM	software reliability growth model
V&V	verification and validation

Acknowledgement

This work was partly supported by Nuclear Research & Development Program of the National Research Foundation of Korea (NRF) grant funded by the Korean government (MEST) (grant code: 2012-011506).

References

[1] KANG, H.G., KIM, M.C., LEE, S.J., LEE, H.J., EOM, H.S., CHOI, J.G., and JANG, S.C.: AN OVERVIEW OF RISK QUANTIFICATION ISSUES FOR DIGITALIZED NUCLEAR POWER PLANTS USING A STATIC FAULT TREE. NUCL ENG TECHNOL, 2009, 41:849-858.

[2] KIM M.C., JANG, S.C., and HA, J.: POSSIBILITIES AND LIMITATIONS OF APPLYING SOFTWARE RELIABILITY GROWTH MODELS TO SAFETY CRITICAL SOFTWARE. NUCL ENG TECHNOL, 2007, 39:145-148.

[3] SHI, Y., KIM, M.C., and SMIDTS, C.: Lessons learnt from the application of the test coverage RePS. In: Proceedings of Sixth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC&HMIT 2009), Knoxville, Tennessee, USA, 2009.

[4] EOM, H.S., PARK, G.Y., JANG, S.C., SON, H.S., and KANG, H.G.: V&V BASED REMAINING FAULT ESTIMATION METHOD FOR SAFETY-CRITICAL SOFTWARE OF A NUCLEAR POWER PLANT. ANN NUCL ENERGY, 2013, 51:38-49.

[5] KANG, H.G., LIM, H.G., LEE, H.J., KIM, M.C., and JANG, S.C.: INPUT-PROFILE-BASED SOFTWARE FAILURE PROBABILITY QUANTIFICATION FOR SAFETY SIGNAL GENERATION SYSTEMS. RELIAB ENG SYST SAFE, 2009:1542-1546.

[6] KIM, M.C., and JANG, S.C.: Several high level issues in reliability assessment of safety-critical software in nuclear power plants. In: Proceedings of ICI (ISOFIC + CSEPC + ISSNP) 2011, Daejeon, Korea, 2011.

[7] KIM, M.C.: Two insights and their implications in fault detection coverage of digital I&C systems. In: Proceedings Of Seventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2010), Las Vegas, Nevada, USA, 2010.

[8] CHOI, J.G., LEE, S.J., HUR, S., LEE, Y.J., and JANG, S.C.: Fault Detection Coverage Quantification of Automatic Test Functions of Digital I&C System in NPPs. In: Proceedings of ICI (ISOFIC + CSEPC + ISSNP) 2011, 2011.

[9] LEE, S.J., KIM, J., and JANG, S.C.: HUMAN ERROR MODE IDENTIFICATION FOR NPP MAIN CONTROL ROOMS OPERATIONS USING SOFT CONTROLS. J NUCL SCI TECHNOL, 2011, 48:902-910.

[10] KHALAQUZZAMAN, M., KANG, H.G., KIM, M.C., and SEONG, P.H.: A MODEL FOR ESTIMATION OF REACTOR SPURIOUS SHUTDOWN RATE CONSIDERING MAINTENANCE HUMAN ERRORS IN REACTOR PROTECTION SYSTEM OF NUCLEAR POWER PLANTS. NUCL ENG DES, 2010, 240: 2963-2971.

[11] KIM, M.C., PARK, J., JUNG, W., KIM, H., and KIM, Y.: DEVELOPMENT OF A STANDARD COMMUNICATION PROTOCOL FOR AN EMERGENCY SITUATION MANAGEMENT IN NUCLEAR POWER PLANTS, ANN NUCL ENERGY, 2010, 37:888-893.