Simulation, digital system validation and reliability

WONG Kin Wah

A-D Technology, Inc., 9F, 108-1, Minquan Rd., Sing-Tien Dist., New Taipei City, 23141, Taiwan, R.O.C. (kin.wong@adtech.com.tw)

Abstract: In the past nuclear power plant (NPP) instrumentation and control (I&C) systems are mostly based on analog technology. With the advancement of commercially available digital systems such as Programmable Logic Controllers (PLC) and Distributed Control Systems (DCS), digital technology has been widely used in new installations and in replacement of existing installations.

Validation and reliability assessment of digital systems in nuclear power plant applications are both important and challenging. The challenges are on how to perform dynamic, integrated and interactive testing of digital systems and how to quantify reliability assessment. In both areas an engineering simulator can play a role. In order to be able to play a role in validation testing and reliability assessment, the engineering simulator must satisfy the following criteria. The reactor core modeling should be based on advanced best estimate core modeling codes. The simulator should be a full scope simulator, *i.e.* it should include all the plant systems and the process and logic modeling should be the same as the actual plant. A V&V program should be implemented to assure that the implementation of the plant process and logic modeling are correct. In this paper a methodology on how to use simulation to perform validation and quantify assessment of digital systems are discussed and preliminary results for a specific application are also presented.

Keywords: full scope simulator; integrated and interactive simulation; validation and verification of digital systems; reliability evaluation

1 Introduction

Digital systems have been in application in many industries for many years, for example: Aerospace, Medical Devices, Defense Systems, Telecommunications, Transportation, Public Utilities, Process-oriented Industries, *i.e.* Chemical, Petro-Chemical, Electronics, Food, Textiles, etc. and Commercial Systems, *i.e.* Banking, Insurance, Stock Exchange, etc.

Digital systems for nuclear power plants (NPP) have technological characteristics very similar to those of digital system for other safety-critical applications in other industries, such as:

- Combination of hardware and software
- Input and output data handling
- Data processing
- Response time criteria
- Accuracy and correctness requirements

What distinguishes digital system applications in NPP from other digital system applications is the need to establish very high level of reliability and safety under a wide range of conditions and severe environment. Because of the potentially of far greater consequences of accidents in nuclear power plants, the digital systems must be relied upon to reduce the likelihood of even very low-probability events.

The major difference between analog and digital systems is that software is involved in digital systems instead of just hardware. Therefore, failure causes are complex due to combination of hardware and software failures and the fact that software is involved will result in additional complexity. It will be difficult to directly apply fault tree/event tree methodology to estimate failure probability similar to what have been done for equipment and hardware failures, reference [1]. Additionally cyber security will be an issue.

Some experts believe that software systems are not completely testable or observable. There is general believe that high-quality design processes will minimize the introduction of mistakes into the system design. High-quality design processes minimize the introduction of mistakes into the system design. However, the complexity of digital systems is such that, regardless of the rigor of traditional quality assurance processes used during the development life cycle, faults can remain undetected in a system. Major concerns of application of digital systems in

Received date: January 23, 2015
(Revised date: March 12, 2015)

nuclear power plants include: the large size and complexity of full-scope, plant-wide digital technology application; the appearance of new failure mode as compared to analog system; how to quantify software reliability and availability; the possibility of software common cause failures; data communication reliability and vulnerabilities and cyber security considerations.

The use of software in digital systems is a principal difference between digital and analog I&C systems. How to assure quality and reliability of software in digital systems is a different but important topic. There are no generally accepted evaluations criteria for safety-related software; rather, application of standards and guidelines, for example references [2], [3] and [4], are used to repeat best practices.

2 Software quality and reliability

It has been observed such as in reference [1] that most software qualities related to system safety, such as maintainability, correctness, accuracy, reliability, security, etc., are difficult to measure directly. It has also been observed that the good operating experience with particular software for a system in the past does not necessary ensure reliability of safety properties in a new application. Thorough reviews, analysis and testing by the stakeholder together with third party experts may help to reach an adequate level of assurance.

Common techniques used to assure software quality and reliability include performing:

- systematic inspections of software,
- planned testing with representative inputs from different parts of the systems domain,
- functional tests chosen to expose errors in normal and boundary cases,
- testing based on large numbers of inputs randomly selected from operational profiles,
- requirement and design review and inspections by experienced experts who did not participate in their construction, and
- Failure Mode and Hazard Analysis to identify states that, combined with environmental conditions, can lead to software failures.

3 Safety and reliability assessment methods

Appropriate methods for assessing safety and reliability are the key to establishing the acceptance of Digital systems in NPPs. Methods must be available to support:

- Estimates of reliability
- Assessments of safety margins
- Comparisons of performance with regulatory criteria such as quantitative safety goals
- Overall assessments of safety

There are in general two types of methods that can be used for safety and reliability assessment. They are deterministic techniques and probabilistic techniques. A combination of the two methods is generally used in safety and reliability assessment.

Design basis accident analysis belongs to the deterministic type. It is a deterministic assessment of the response of the plant to a prescribed set of accident scenarios. An agreed-upon set of transient events are imposed on analytical simulations of the plant. Then assuming defined failures, the plant systems must show to be effective in keeping the plant within a set of defined acceptance criteria.

Probabilistic Risk Assessment (PRA) or Probabilistic Safety Assessment (PSA) techniques are used to assess the relative probability and effects of contributing events on system-level safety or reliability. These analyses are typically performed using fault tree/event tree analysis.

There is controversy within the software engineering community as to whether an accurate failure probability can be assessed for software or even whether software fails randomly. A good software quality assurance methodology is a prerequisite to providing a basis for the generation of bounded estimates for software failure probability. Bounded estimates for software failure probabilities can be obtained by processes that include valid random testing and expert judgment. Uncertainty and sensitivity analysis can help to estimate and quantify the impact of parameter uncertainties to the system. A good Engineering Simulator (ES) will be able to help to gain understanding, increase confidence and

reduce uncertainty in Digital System quantitative assessment.

4 Application of engineering simulator in digital system validation testing

An ideal test environment for digital I&C validation will be to connect the digital I&C system(s) to be tested to a nuclear power reactor and operate the nuclear power reactor in different scenarios to generate numerous different sets of test signals to test the digital I&C system(s). However, this will not happen. In the past, techniques that were used to generate test signals for validation testing include using test fixtures and test tools to generate limited amount of test signal and using simple simulators to generate limited and approximate test signals. However, this kind of test environment will not be sufficient to perform validation testing for large complex digital systems implemented in a nuclear power plant. In reference [5], a personal computer based automatic test tool for validation testing of digital safety systems in ABWR nuclear power plants in Japan was presented. In this paper a personal computer based Engineering Simulator (ES) that was used for validation testing of digital systems in a nuclear power plant in Taiwan will be described. In order to be used for digital system validation, the ES must be able to perform dynamic, integrated, interactive and close-loop testing.

Dynamic testing means performing testing of the dynamic response of the digital systems under different operational scenarios (normal, abnormal, transient and accident) of the nuclear power plant. Integrated testing means performing testing of the digital systems as an integral part of the total plant rather than as isolated individual systems. Interactive testing means performing testing of the digital systems including human system interactions. Close-loop testing means that there will be feedback from the plant to the system to be tested.

The following criteria are suggested for an ES to be used as a digital system validation test platform:

- The core modeling should be based on advanced best estimate core modeling codes.
- The process and logic modeling should be complete and the same as the actual plant.
- A rigorous V&V process should be implemented to assure that the implementation of the plant process and logic modeling is complete and correct.
- Tools and processes should be in place to facilitate performance of testing and present and record test results.

In this paper we call an engineering simulator that satisfies the above criteria a Full Scope Engineering Simulator (FSES). In the next section an example in using a FSES to perform digital system validation is described.

5 An example of FSES based digital system validation

The Lungmen Nuclear Power Station (LMNPS in Taiwan, consists of two Advanced Boiling Water Reactor (ABWR) units. The digital I&C system that is implemented in the Lungmen Project is called Distributed Control and Information System (DCIS). Figure 1 shows an overview of the Lungmen NPS DCIS system. The Lungmen DCIS consists of a non-safety part and a safety part. The non-safety part of the DCIS mainly consists of Invensys IA equipment, GEIS triple modular redundant (TMR) equipment, MHI and Hitachi equipment. GEIS triple modular equipment includes the Feedwater Control System (FCS), the Recirculation Flow Control System (RFCS), the Steam Bypass and Pressure Control System (SBPC), and the Automatic Power Regulator (APR). MHI equipment includes the Turbine Control System (TCS). Hitachi equipment includes the Rod Control and Information System (RCIS) and Radwaste Control System. Invensys IA equipment includes the rest of the non-safety systems. All the non-safety systems are connected together through an Invensys high performance mesh network system. Non-Invensys systems connect to the Invensys network system via Invensys gateways. Safety part of the DCIS mainly consists of GE NUMAC equipment and DRS equipment. The GE NUMAC equipment includes the Safety System Logic and Control/Reactor Trip and Isolations Functions (SSLC/RTIF) and the Neutron Monitoring System (NMS). The DRS equipment includes the

Safety System Logic and Control/Engineered Safety Features (SSLC/ESF). The safety systems connect to the Invensys network system via GE Multi-Vendor Devices (MVDs).

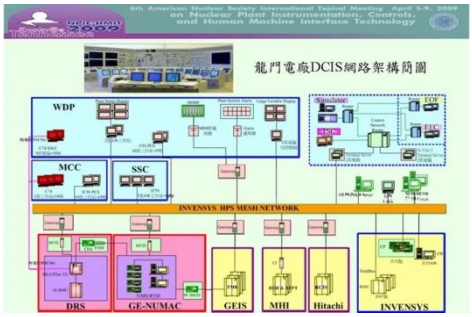

Fig.1 Lungmen NPS DCIS overview (reference [6]).

The Lungmen FSES was constructed based on the Lungmen Full Scope Simulator (FSS). It was built in full compliance with U.S. regulatory requirements and industry standards. Software V&V was performed throughout the software life cycle of the implementation in accordance with applicable industry standard (reference [7]), including:

- Requirement Phase
- Design Phase
- Implementation Phase
- Test Phase

The Lungmen FSES is implemented in a PC based Windows environment using WSC's 3KeyMaster platform, reference [8]. The core modeling is based on a best estimate transient analysis computer code, TRACS/NEMO. The complete modeling of FSES, including core modeling and logic and process modeling of 105 plant systems, is hosted in one PC.

The core modeling code TRACS/NEMO is a combination of 2 computer codes: TRACS and NEMO. TRACS [9] belongs to the family of TRAC computer codes that are called best estimate thermal-hydraulic codes. These codes were developed with the objective of calculating as realistic and accurate as possible, of the evolutions of key parameters involved in operating and transients in nuclear power plants.

The logic and process modeling of the 105 plant systems were developed based on the same logic and process design of the real plant. Translation software was developed to translate the human system interface displays and functions so that the FSES displays and user functions are exactly the same as the real plant.

Figure 2 shows the configuration of FSES based digital system validation test platform that was used to perform validation of the Lungmen DCIS.

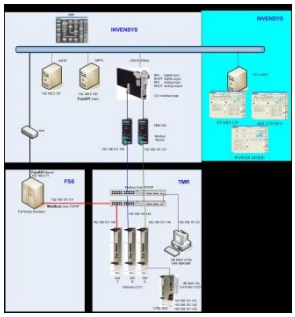

Fig.2 Configuration of FSES based digital system validation test platform.

The FSES is connected to Invensys IA equipment via an Invensys network system and is connected to GEIS TMR equipment via a MODBUS over TCPIP datalink. The Invensys IA equipment and GEIS TMR equipment that were validated by this platform were the same as those used in the real plant. The FSES was used to generate full range of I/O inputs under different plant operational scenarios to test the Invensys and GEIS equipment. Figure 3 and Figure 4 show a physical view of the actual equipment that was used in the validation testing. Figure 3 shows the actual Invensys equipment and Figure 4 shows the actual GEIS TMR equipment.

Fig.3 Physical view of FSES based digital system validation test platform – 1.

Fig.4 Physical view of FSES based digital system validation test platform – 2.

A full range of dynamic test inputs were generated by this test platform to perform validation tests including the following:

- Visual Display Unit (VDU) Display Validation
- Alarm Validation
- I/O Validation
- Logic Validation

Test coverage included validation of all active component status/data and all control component functions, validation of all alarms, validation of all analog and digital I/O signals and validation of all the logics.

Additional advantages of the FSES platform are:

- Software tools can be developed in the Full Scope ES to generate many sets of random input signals to facilitate collection of good statistically data for reliability evaluation.
- The data collected will be applicable to the specific digital system that is under testing and will be for the specific NNP that will be installing this digital system as compared to generic data that may not be applicable.
- The testing scenarios and test data can be recorded and are repeatable for future reference.

6 Discussion of digital system reliability assessment

Currently there is no consensus in the methodology of quantifying software reliability. FSES will be able to play a role in the development of such a methodology. Reference [10] identifies some common limitations in Quantitative Software Reliability Models (QSRMs) for digital protection systems of NPPs. Table 1 provides a listing of the common limitations of QSRMs and how FSES can be used to address these limitations.

Table 1 Common limitations of QSRMs

	Common Limitations of QSRMs	FSES Advantages
Test profile vs operational profile	It is commonly known that test profiles may not realistically represent operational profiles	FSES test data will include all modes of operations; normal, transient, accident
Context specificity	Software failures are sensitive to the context (environment) in which the software is operating	Software failures in different operation modes in FSES environment are the closest to the actual environment
Demonstration of high reliability	It is expected that a digital reactor protection system (RPS) should have at least the reliability of the analog RPS it replaces (i.e., a failure probability on demand on the order of 10-5). Statistically it would require undertaking hundreds of thousands of tests without failure to demonstrate this kind of reliability	It will be easier to undertake hundreds of thousands of tests in FSES environment compared with other methods
Failure-mode-specific modeling	Depending on the level of detail of system modeling, quantification of the failure probabilities for lower level failure modes might be needed	FSES method does not require quantification of failure probabilities for lower level failure modes
Common Cause Failure (CCF) of	If the redundant channels of a safety-related system, that is, an	CCF can be modeled and tested easily in FSES method

two diverse digital system	RPS or ESFAS, run identical software, they would all fail given a software failure that leads to loss of channel function

7 Concluding remarks

A real time full scope engineering simulator that is built in accordance with applicable regulatory and industry standards and based on advanced best estimate reactor neutronics and thermal-hydraulics codes will be a powerful tool in digital system validation testing and reliability quantification. Such a FSES will provide the environment that will allow dynamic, integrated, interactive and close loop validation testing to be performed effectively and efficiently.

There is still no consensus in the methodology of quantifying software reliability because several factors contribute to the quantifying software reliability as shown in Fig. 5. A FSES can be used to collect statistical data in quantifying software reliability from those different aspects of software quality, software complexity, software testing and further user experience. Therefore, FSES can play an important role in this very important area.

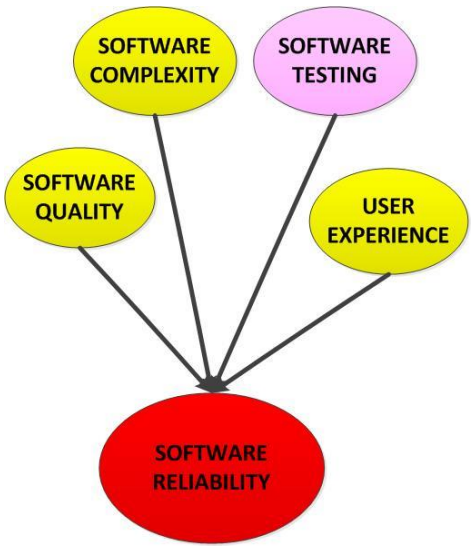

Fig.5 Factors contributing to software reliability.

References

[1] U.S. National Research Council, "Digital Instrumentation and Control Systems in Nuclear Power Plants, Safety and Reliability Issues, Final Report", 1997.

[2] U.S. Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants".

[3] IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations".

[4] IEEE Std 7-4.3.2, "Standard Criteria for Digital Computers in Safety Systems for Nuclear Power Generating Stations".

[5] FUKUMOTO Akira, HAYASHI Toshifumi, NISHIKAWA Hiroshi, SAKAMOTO Hiroshi, TOMIZAWA Teruaki, and YOMOMURA Tadayuki: "A verification and validation method and its application to digital safety systems in ABWR nuclear power plants", Nuclear Engineering and Design 183 (1998) 117-132.

[6] CHEN C. C., *et al.*: "Engineering V&V for DCIS Lungmen Nuclear Power Plant", NPIC&HMIT 2009, Knoxville, Tennessee, April 5-9, 2009.

[7] IEEE Std 1012, "IEEE Standard for Software Verification and Validation".

[8] "3KEYMASTER Graphical Engineering Station User Guide", Western Services Corporation.

[9] ANDERSEN J. G. M., and SHUAG J. C., "TRACS – BEST ESTIMATES SIMULATION IN REAL TIME", General Electric Nuclear Energy.

[10] NUREG/CR-7044, "Development of Quantitative Software Reliability Models (QSRMs) for Digital Protection Systems of Nuclear Power Plants", July 2011.