Introduction of RAVONSICS project

ZENG Hai[1], YANG Ming[2], and YOSHIKAWA Hidekazu[3]

1. Engineering Center, State Nuclear Power Automation System Engineering Company, No. 7,Cangwu Road, Shanghai, 200233, China (zenghai@snpas.com.cn)
2. College of Nuclear Science and Technology, Harbin Engineering University, No. 145, Nantong Street, Nangang District, Harbin, 150001, China(yangming@hrbeu.edu.cn)
3. College of Nuclear Science and Technology, Harbin Engineering University, No. 145, Nantong Street, Nangang District, Harbin, 150001, China (yosikawa@kib.biglobe.ne.jp)

Abstract: This paper introduces the international cooperative research project called RAVONSICS (Reliability and Verification and Validation of Nuclear Safety I&C Software) which is being carried on by 7 Chinese partners including universities, research institutes, utilities, vendors, and safety regulatory body. The objective of RAVONSICS is to bring forwards the methodological development in China for the software reliability evaluation and the software verification technique. The paper gives brief summary of the background, research topics, and the present status of RAVONSICS project. RAVONSICS works cooperatively with its European sister project HARMONICS, where the both projects will share the common target to improve the software reliability evaluation and testing methodologies and techniques.
Keyword: software reliability; verification and validation; digital I&C; safety-critical system

1 Introduction

As the "central nerve system" of a very complex industrial process system such as nuclear power plant (NPP), the highly reliable Instrumentation & Control (I&C) system will provide correctly the right functions which are always desirable not only for the end users of NPPs but also for the suppliers of I&C systems. The digitalization of nuclear I&C system in recent years has brought a lot of new features for nuclear I&C system. On one side digital technology provides more functionalities, and it should be more reliable and robust. On the other side, digital technology brings new challenge for nuclear I&C system, especially on the reliability of its software running on the hardware component.

The software provides flexible functionalities for nuclear I&C system, but it also brings the difficulties to evaluate the reliability and safety of it because of the complexity of software. The reliability of software, which is indispensable part of I&C system, will have essential impact on the reliability of the whole system, and people definitely want to know what the reliability of this intangible part is. The methods used for the evaluation of reliability of hardware system hardly work for software, because the inherent difference of failure mechanism exists between software and hardware. Failure in software is systematically induced by design error, while failure in hardware is randomly induced by the material and during the production.

To continue the effort on this hot topic and to try to achieve consensus on the potential methodology for software reliability evaluation, a cooperative research project called RAVONSICS (Reliability and Verification and Validation of Nuclear Safety I&C Software) is being carried on by 7 Chinese partners which include university, research institute, utility, vendor, and safety regulatory body. The objective of RAVONSICS is to bring forwards the methodologies for the software reliability evaluation, and the software verification technique.

RAVONSICS works cooperatively with its European sister project HARMONICS, and the both projects will target the software reliability evaluation and testing methodologies and techniques.

This paper describes the research topics of RAVONSICS, and the cooperation among partners and the updated status of the project. RAVONSICS is one of the first China-EURATOM cooperative project, and the first cooperative project on assessment of software reliability in China. RAVONSICS, together

Received date: January 29, 2015
(Revised date: February 3, 2015)

with the sister project HARMONICS, will bring efforts from almost 12 partners together. The 12 partners take roles like university, research institute, utility, vendor, and nuclear regulatory body, and RAVONSICS will try to achieve consensus on the hot topics in this way.

2 Research topics

RAVONSICS is a nuclear energy research project funded by Chinese government. RAVONSICS aims at the hot topics of reliability assessment of software of Instrumentation and Control (I&C) System of Nuclear Power Plants (NPPs), and try to find out the applicable methodology of both quantitative and qualitative assessment of reliability of I&C system software. As a measure to provide the direct evidence of correctness of software, verification technology is also included in this project. The evidences on the reliability of nuclear I&C system software acquired by reliability assessment and verification are then provided to support the claims of safety justification of software.

2.1 Software reliability assessment

The difference between the failure mechanism of hardware and software make it difficult to evaluate quantitatively the reliability of software. Unlike the random failure happens in hardware component which is caused by hardware degradation, the failure of software is systematic, closely related with the quality of software development, and there is no software degradation. There may be one way to evaluate the probability of software failure if we could quantitatively evaluate the quality of software development.

Another possible way to evaluate quantitatively the software reliability is to take the testing result of software into the consideration, with the assumption that the software reliability increases with the number of passed tests of software.

Different approaches of software reliability assessment will be researched and practiced, and the reliability model of software will be developed by using different approach.

2.2 Software verification

The verification of software is to provide evidence that the software perform the functions correctly per the requirements. Even though simulation test is a good way to test and verity the software, there is some drawback of simulation test, *e.g.*, it is very difficult or costly to claim 100% test coverage for the complex software. As a good complementary verification of software, formal verification provides another way to verify the software. Based on property assertion, formal verification is a systematic process of ensuring, through exhaustive algorithmic techniques, that a design implementation satisfies with the requirements of its specification. By using a formal verification tool, all possible executions of the design are mathematically analyzed without the need to develop simulation input stimulus or tests [1].

Statistical testing is another verification technology being studied in this project. As specified in "IEC 60880 Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions", Statistical approaches may be utilized to complement systematic approaches [2]. Presently statistical testing is not compulsory requirement in China, but is required in Europe for justifying software based systems when there is no access to the source code. In the UK, the regulator has encouraged that statistical testing should be performed and it has been employed to demonstrate reliability of safety-related programmable systems. In Finland, quantitative reliability assessment of I&C systems is mandatory in the highest safety category[11].

2.3Safety justification

Safety justification framework is a way to construct the software safety case to meet the safety assessment requirement of European nuclear safety regulatory body. Safety case is the document or documents produced by the licensee documentation to justify safety during the design, construction, manufacture, commissioning, operation and decommissioning phases of the installation [4]. Claim-Argument-Evidence (CAE) is the approach used in the safety justification process to develop safety case for safety related I&C system or software.

Safety case and CAE approach are UK practices to provide evidence by licensee for nuclear safety regulatory staff on the assessment of safety related I&C system or software. Although it is different from approach in China, these European practices are good methodology of reasoning and organizing all information of evidence on the safety of I&C system or software.

Figure 1 illustrates the relationship among the three topics of RAVONSICS, where reliability assessment and verification provide evidence for the safety justification, and the methodologies of the three research topics will be practiced in different cases.

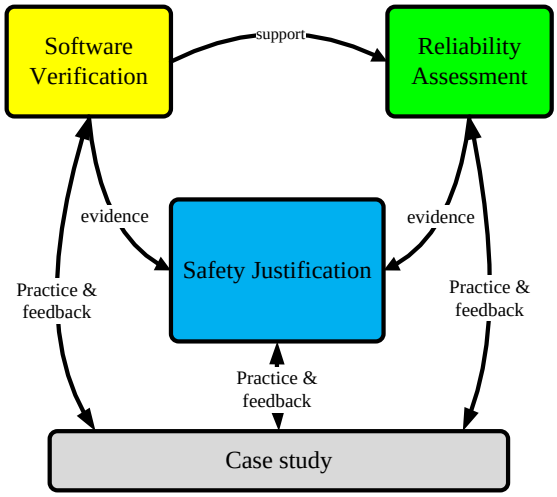

Fig.1 Topics relationship.

3 RAVONSICS methods

The research effort of RAVONSICS is mainly divided into three parts, quantitative software reliability assessment approaches, verification technologies including formal verification and statistical testing, and safety justification framework. As a starting point of research effort on hot topic of software reliability assessment in China, RAVONSICS paid more effort on some topics like reliability assessment and formal verification, but less effort statistical testing and safety justification framework, based on the nuclear regulatory requirement in China.

3.1 Reliability assessment approaches

Three approaches, which are Multilevel Flow Models (MFM), Bayesian Belief Network (BBN), and Net Flow Model, are researched and practiced in RAVONSICS. MFM is a good way to analyze the relation between the function and structure of the system to be evaluated, and BBN and Flow Net Model are two ways to evaluate the software reliability.

3.1.1Multilevel Flow Models (MFM)

Multilevel Flow Modeling (MFM) is a methodology for modeling of industrial processes on several interconnected levels of means-ends and part-whole abstractions. The basic idea of MFM is to represent an industrial plant as a system which provides the means required to serve purposes in its environment. MFM has a primary focus on representation of plant goals and functions and provide a methodological way of using those concepts to represent complex industrial plant. Figure 2 shows the basic common elements and symbols used in MFM. [5]

A digital feed-water control system (DFWCS) of a simplified pressurized water reactor was selected as the case to practice MFM methodology in RAVONSICS. Figure 3 shows the simplified schematic of DFWCS. As shown in Fig. 3, the feed-water system is consisted of pump, tank, valve, piping and controller. It is supposed that the valve is in OPEN state and keeps the aperture constantly. The controller keeps the water level stable by monitoring the tank level to control the pump speed[6].

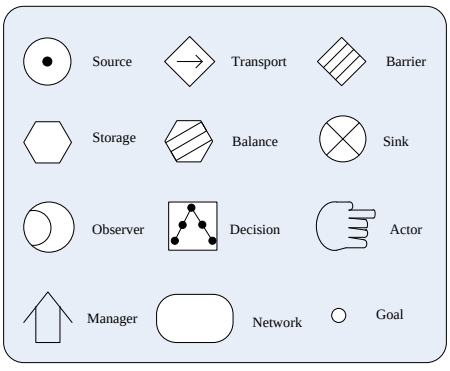

Fig.2 Basic common elements and symbols of MFM.

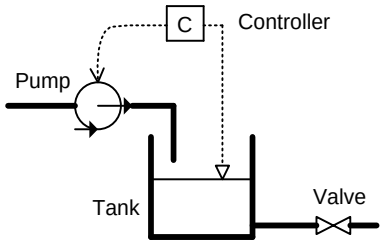

Fig.3 Simplified schematics of DFWCS.

Figure 4 shows the model based on MFM approach. As shown in Fig. 4, G1 stands for system goal, which means maintain the tank level and realized by function sto1. Mfs1 is the system mass flow which describes the water flow process; efs1 is the energy flow which describes the pump power supply; cfs1 is the control flow, and obj1 is pump speed control objective, con1 is control method, related information is labeled upon the relations; ifs is information flow which describes the control process [6].

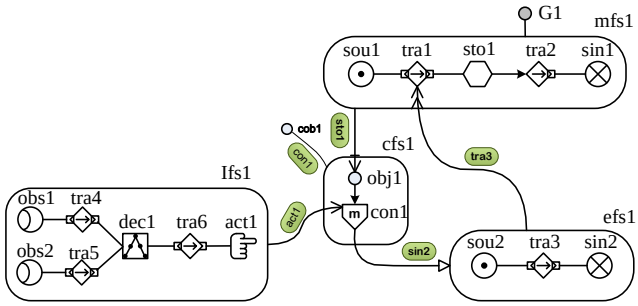

Fig.4 MFM model of DFWCS.

3.1.2 Bayesian Belief Network (BBN)

BBN is a probabilistic graphical model depicting a set of random variables and their conditional independencies via a directed acyclic graph. Here, "acyclic" means the graph does not form a feedback loop[7].The idea of using BBN to software reliability assessment is to evaluate software reliability by evaluating the activities in the software development life cycle which shall meet with the requirements set by the relevant national and international standards.

Based on requirements of Branch Technical Position 7-14 Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Systems and the relevant international standards on software of I&C systems of NPPs, a BBN model of software reliability evaluation is constructed, as illustrated in Fig. 5 as High level BBN model. Sub-models are constructed for each part of BBN model shown in Fig. 5.For example, Project Management Plans evaluation sub-model is constructed for "Organization" part in Fig 5. Totally 13 Sub-models are constructed for all the six parts shown in Fig. 5.Various questions of different category are developed for each sub-model, and questionnaires are designed to obtain *a priori* probability, and then the conditional probability of each sub-model can be calculated by predictive inference approach of BBN, and the software reliability as shown in Fig. 5 will be obtained after we have the conditional probability of each part in Fig. 5[7].

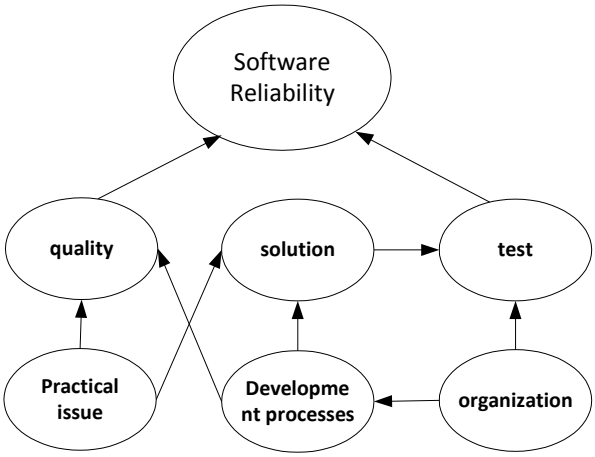

Fig.5 High level BBN model.

3.1.3 Flow Network Model (FNM)

FNM is being researched in RAVONSICS to evaluate the software reliability based on the testing results of software and the software architecture. The FNM is illustrated in Fig. 5, in which a software is modeled by node and edge. Node represents the starting point, stopping point, and branching point of software, and edge represent the software code between 2 nodes.

The idea of FNM is that the failure probability of each edge will decrease with the number of passed test. If *a priori* failure probability of one edge is $q_i = 10^{-m_i}$, and m_i is the failure metrics of which is a positive real number and can be estimated according to the past performance and complexity of the code, or developer experience, then the failure probability of the edge will be $q_i = 10^{-h_i m_i}$ after it has been tested for h_i times and passed the

h_i times of tests. If the h_i test fail, the *priori* failure probability is reset to another estimated value.

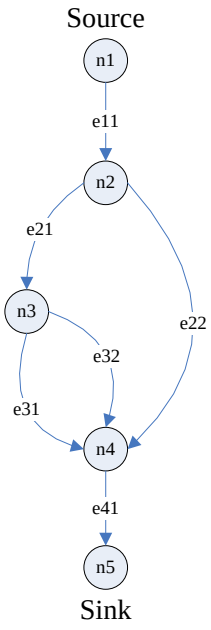

Fig.6 FNM model.

3.2Verification technology

The verification technology which RAVONSICS focused on will not cover the complete verification activities specified in IEEE 1012[12]. Two specific verification technologies for additional confidence building instead of excellence of production [3] are researched in RAVONSICS. The one is formal verification for Programmable Logic (PL) of Field Programmable Gate Array (FPGA), while the other is the statistical testing method.

3.2.1 Formal verification

Formal verification is a systematic process of ensuring, through exhaustive algorithmic techniques, that a design implementation satisfies the requirements of its specification. By using a formal verification tool, all possible executions of the design are mathematically analyzed without the need to develop simulation input stimulus or tests. Formal verification is specifically to prove functional correctness of a Register Transfer Level (RTL) model of FPGA[1].

Property Specification Language (PSL) is used to specify the property of RTL code of one FPGA PL, where the used PSL is specified in IEEE 1085 Property Specification Language (PSL) [8]. After the property specification is defined for the RTL code, then the property specification is input into Questa®Formal which is the formal verification software tool developed by Mentor Graphics Corporation. Together with RTL code of FPGA PL, the result of formal verification will show whether or not the property meet with the requirement of property specification.

An application specific FPGA PL for OPDT (Overpower △T)protection function is practiced as a study case by using formal verification. The functional property and timing property are verified by using formal verification [9].

3.2.2 Statistical testing

The use of software statistical testing provides the potential to demonstrate the estimated system reliability, but the most important practical limitation is the very high number of tests necessary to demonstrate that a system is highly reliable. It can require prohibitively long execution times if all the tests are to be performed on the final system [3].

The preliminary study on statistical testing is included in RAVONSICS to find out what is the statistical testing and how to do it. No real statistical testing will be carried out in RAVONSICS because there is no compulsory requirement from Chinese Nuclear Regulatory Body presently and because of the unavailability of full scope simulator.

3.3 Safety justification framework

With cooperation with HARMONICS, which is the sister project of RAVONSICS funded by European Commission, Claim-Argument-Evidence (CAE) approach for safety justification is introduced and included in RAVONSICS. Claims are assertions put forward for general acceptance. They are typically statements about a property of the system or some subsystem. Claims that are asserted as true without justification become assumptions and claims supporting an argument are called sub-claims. Evidence is used as the basis of the justification of the claim. Sources of evidence may include the design, the development process, prior

field experience, testing, source code analysis or formal analysis. Arguments link the evidence to the claim. They are the "statements indicating the general ways of arguing being applied in a particular case and implicitly relied on and whose trustworthiness is well established", together with the validation for the scientific and engineering laws used[10].

Unlike HARMONICS, RAVONSICS focuses only on the preliminary follow up study on safety justification framework which integrates rule-based, goal-based and risk-informed approaches. The objective of the follow up study is to find good way to organize all the information required to assess the safety of software. The safety review of safety critical software in China will follow the requirement of China nuclear regulations [13].

4 International cooperation

RAVONSICS is one of the first China-EURATOM cooperation projects based on "Agreement between EURATOM and China for R&D Cooperation in the Peaceful Use of Nuclear Energy" which was signed in April 24, 2008, and the related national cooperation in China is also included in RAVONSICS. There are totally 12 partners from RAVONSICS and HARMONICS who are working together to achieve the consensus on the methodology of assessment of software reliability for I&C system of NPPs. All partners are shown in Table 1.

Table 1Cooperation Partiers

Project	Organization	Country
RAVONSICS	State Nuclear Power Automation System Engineering Company	China
	Harbin Engineering University	China
	Institute for Standardization of Nuclear Industry	China
	Jiangsu Nuclear Power Company	China
	Nuclear Radiation Safety Center	China
	China Techenergy Company	China
	Shanghai Automation Instrumentation Company	China
HARMONICS	VTT	Finland
	Électricité de France (EDF)	France
	Institute for Safety Technology (ISTEC)	Germany
	Adelard LLP/CSR (ADEL)	UK
	Swedish Radiation Safety Authority (SSM)	Sweden

To start the cooperation among Chinese partners, a Consortium Agreement (CA) was signed by all Chinese partners, and Consortium Committee was established by members from each partner. Yearly consortium committee meeting was held to have discussion and communication among partners, and make agreement if needed. Accession document for new partners shall be agreed by consortium committee and approved by chair of consortium committee.

After Consortium Agreement (CA) was signed, Coordination Agreement between RAVONSICS and HARMONICS was discussed, agreed and signed by all Chinese partners and European partners. Yearly coordination committee meeting was held to have discussion and communication among partners, and make agreement if needed.

Besides all the consortium committee meetings and coordination committee meetings, various technical workshops were held to have technical discussion on all the hot topics of both projects. Figure 7 is the photo taken at the kick-off meeting of both project on March, 2011 in Shanghai, and Fig. 8 is the photo taken at the technical workshop on November, 2014 in Shanghai.

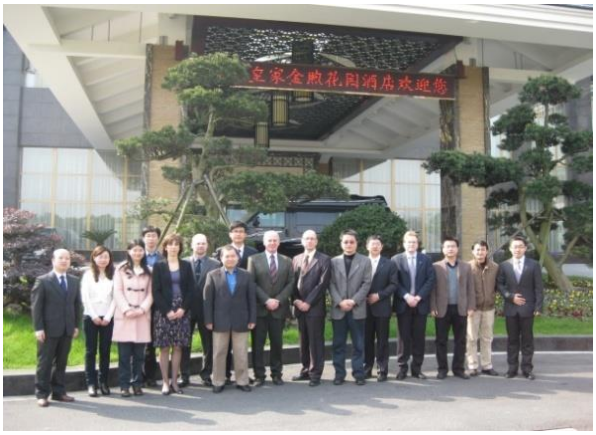

Fig. 7 Kick-off meeting.

Fig.8 Technical workshop of RAVONSICS.

RAVONSICS is a good start for the broad and solid international cooperation, as well as a good start for solid cooperation among Chinese partners. Technical discussion and communication break the barrier among organizations, and help to reach consensus on the methodology. Even though we have open access to each partner of RAVONSICS for all the deliverables of RAVONSICS, Intellectual Property is carefully managed by Consortium Agreement and Coordination Agreement.

5 Conclusion

RAVONSICS focuses on the hot topics of assessment of reliability of software of I&C system of NPPs. European practices of justifying safety of software is introduced by RAVONSICS, and various technologies of reliability assessment and verification are researched and studied in RAVONSICS. With the effort paid by RAVONSICS partners, we have made a good step forward toward more reliable software of I&C system of NPPs in China. RAVONSICS is also a good start of deep and broad international and national cooperation in China, and its experience makes it a good reference of more research cooperation which will happen in the future.

References

[1] PERRY Douglas L., and FOOSTER Harry : Formal Verification for Digital Circuit Design, The McGraw-Hill Companies, Inc., 2005.

[2] IEC 60880 Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions, 2006

[3] HOLMBERG Jan-Erik, GUERRA Sofia, THUY Nguyen, JOSEF Märt, and BO Liwång : HARMONICS — EU FP7 Project on the Reliability Assessment of Modern Nuclear I&C Software, NPIC&HMIT 2012, San Diego, CA, July 22-26, 2012

[4] Safety Assessment Principles for Nuclear Facilities, Office for Nuclear Regulation, 2006

[5] LIND Morten : An introduction to multilevel flow modeling, Nuclear Safety and Simulation, Vol. 2, Number 1, March 2011

[6] ZHANG Chao, and ZENG Hai: Study on MFM Method for Digital I&C System Reliability Modelingand Analysis, the 9thInternational Topical Meeting onNuclear Plant Instrumentation, Control, andHuman Machine Interface Technologies, February 22-26, 2015, The Westin Charlotte, Charlotte, NC, USA.

[7] LIU Ying : Research on the Nuclear Safety-Level D-I&C Software Reliability Method Based on the BBN, Dissertation for the Master Degree, Harbin Engineering University, March, 2014.

[8] IEEE 1850/IEC IEC 62531Property Specification Language (PSL), 2012, Institute of Electrical and Electronics Engineers, Inc

[9] YU Wenzhuo : Formal verification on the FPGA of instrument and control systems in nuclear power plants, Thesis Submitted toTsinghua Universityin partial fulfillment of the requirementfor the degree ofMaster of ScienceinNuclear Science and Technology, May,2014.

[10] BISHOP Peter, BLOOMFIELD Robin, and GUERRA Sofia : Safety Justification Frameworks : Integrating Rule-based, Goal-basedand Risk-informed Approaches, NPIC&HMIT 2012, San Diego, CA, July 22-26, 2012

[11] Finnish regulatory guide YVL E-7, Electrical and I&C Equipment of a Nuclear Facility

[12] IEEE 1012 IEEE Standard for Software Verification and Validation, 2004, Institute of Electrical and Electronics Engineers, Inc

[13] HAF 102 Safety Requirements of Nuclear Power Plant-Design, 2004, China Nuclear Safety Authority