# Defense in depth concept for nuclear safety, functional modeling method and software reliability issues

YOSHIKAWA Hidekazu[1]

*1. College of Nuclear Science and Technology, Harbin Engineering University, 150001, Harbin, Heilongjiang, China (yosikawa@kib.biglobe.ne.jp)*

**Abstract:** An overview is made on the software reliability issue which comes from safety concern on computer application for instrumentation and control (I&C) and human-machine interface technology (HMIT) of safety-critical systems of nuclear power plant (NPP). The discussion starts from the deepening defense in depth (Did) concept with the historical repetition of severe accidents and the resultant strengthened regulatory requirements to the design and evaluation of the digital I&C and HMIT. A new functional modeling approach is proposed so that it can serve to analyze various aspects of software reliability issues for the NPP well balanced in safety, economy, and efficiency.

**Keyword:** software reliability; digital I&C and HMIT; defense in depth; functional modeling approach

## 1 Introduction

Light water reactor power plants utilize nuclear reactors instead of boilers used in conventional fossil power plants. In early days of 1960's when light water reactor power plants were first introduced, the plant instrumentation and control systems (I&C) of nuclear power plants (NPPs) had been composed by analog technology. However, digital computers had appeared in 1960's and in 70's the rapid technical progress of semi-conductor and LSI (large scale integrated circuit) prompted the microprocessor based computerization of process control in every industrial field.

Computer program is the source of realizing many valuable functions by computerization. However there had been strong objection in nuclear regulation to use computers for NPP by saying that computer is "unreliable and dangerous" because existence of hidden errors in the program may bring many possibility of troubles so that it is difficult to prove there are no errors in the program.

Although such conservative attitude of nuclear regulation against computer had been stronger than that of other industries, the computerization has become inevitable trend even in the nuclear industry since the earlier days of 80's. The historical development of the application of digital computer in nuclear power plants in Japan had started by the offline use of computer for recording the daily plant operation and automatic data log of plant system in the main control room. The online use of computer for process control had started for the peripheral process systems such as laundry and waste disposal processes, and then gradually expanded into major plant process control systems: First for non-safety class control systems such as plant power control system, and then for safety class control and safety systems such as reactor protection system and ECCS. The full digital I&C system with fully computerized main control board was first realized in 1996 at Kashiwazaki-Kariwa Unit 6 (ABWR) of Tokyo Electric Power Company.

In fact, the introduction of digital computer for nuclear industry was rather late compared with other industries such as for fossil plant and chemical plants. The safety concern on computer application for the nuclear I&C + HIMT (human machine interface technology) was so strong that the computer application for nuclear plant was slower than other process industries. But as a matter of fact, there has been no serious troubles in digital I&C + HMIT in both BWR and PWR in Japan since the first introduction of full digital I&C+HMIT in 1996.

These days, new digital devices and services of ICT (information and computer technology) appear year by year with new useful and convenient functions in

**Received date: February 1, 2015**
(Revised date: February 3, 2015)

the society. This is the bright side of computer, and this new trend is also affecting the nuclear I&C + HIMT. But there arise new issues such as internet security which will be the dark side of computer and ICT. Therefore, software reliability issue is still and will be also important issue in future.

In this paper, what is called defense in depth (Did) concept in nuclear safety will be first introduced in **2**, along with the historical experience of severe accidents in the past and its relation with digitalized I&C and HMIT technology. Then in **3**, the review will proceed to the introduction of functional model approach which has been developing as a viable modeling method for designing the digitalized I&C and HMIT systems to cope with various software reliability issues more widely and innovatively.

## 2 Defense in depth concept for nuclear safety

### 2.1 Design principles of NPP safety

According to a textbook on nuclear safety by G. Petrangeli [1], the essential point of design principles of NPP safety can be summarized as follows;

(a)Defense in depth: Multiple barriers against radiological releases to the environment,

(b)Four barriers: Nuclear fuel, Cladding, Pressure boundary of reactor coolant including reactor vessel and Containment,

(c)Barrier intactness is assured by three safety functions: STOP, COOL and CONTAIN, and

(d)Reliability of safety functions is enhanced by principles of diversity, redundancy and physical separation.

The concept of defense in depth, which concerns the protection of the both public and workers, is the fundamental norm for the safety of nuclear installation, as was stated in Basic Safety Principles for Nuclear Power Plants (INSAG-12) [2] by IAEA in relation to the safety of nuclear power plant, "*All safety activities, whether organizational, behavioral or equipment related, are subject to layers of overlapping provisions, so that if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public at large. This idea of multiple levels of protection is the central feature of defense in depth*."

The objectives of defense in depth are as follows:

(a) Compensate for potential human and component failures,

(b) Maintain the effectiveness of the barriers by averting damage to the plant and the barriers themselves, and

(c) Protect the public and the environment from harm in the event that these barriers are not fully effective.

### 2.2 Defense in depth (Did) concept for nuclear safety

The Defense in depth (Did) concept defined by IAEA's INSAG-10 [3] is generally constituted by five layers. The object of each layer and the means to attain the objective is described as shown in Table 1.

**Table 1 Level of defense in depth**

| Level | Objective | Essential means |
|---|---|---|
| Level 1 | Prevention of subnormal operation and failures | Conservative design and high quality in construction and operation |
| Level 2 | Control of abnormal operation and detection of failures | Control, limiting and protection systems and other surveillance features |
| Level 3 | Control of accident within the design basis | Engineered safety features and accident procedures |
| Level 4 | Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents | Complementary measures and accident management |
| Level 5 | Mitigation of radiological consequences of significant releases of radioactive materials | Off-site emergency response |

According to INSAG-10 by IAEA, it is necessary to take into account of the following items to configure Did concept;

(a) For the effective implementation of defense in depth, some basic prerequisites apply to all measures at Levels 1 to 5. These prerequisites, which are interrelated and are fulfilled as part of policy for safe design and operation, are (i) appropriate conservatism, (ii) quality assurance and (iii) safety culture.

(b) The general objective of defense in depth is to ensure that a single failure, whether equipment failure or human failure, at one level of defense, and even combinations of failures at more than one level of defense, would not propagate to jeopardize defense in depth at subsequent levels. The independence of different levels of defense is a key element in meeting this objective.

(c) The existence of several elements of defense in depth does not justify continued operation in the absence of one element. Thus all the elements of defense in depth are normally available when a plant is at power and an appropriate number of available elements is required at other times.

### 2.3 Defense in depth (Did) concept- its reality and NPIC&HMIT

The defense in depth concept by IAEA seems to reflect on the historical evolution of nuclear safety regulation. That is, (i)the major concern of nuclear safety had been basically the provision until level 3 before TMI-2 accident (1979), while (ii) provision of levels 4 and 5 were strongly recommended by IAEA after the disaster of Chernobyl accident in 1986. Many supplementary recommendations by IAEA such as (a), (b), and (c) mentioned in 2.2 are considered to reflect on the warning of organizational accident by James Reason by his famous “Swiss Cheese model” as is shown in Fig. 1 which shows the analogy of organizational accident as the multiple failure of defense in depth layers by a certain trigger event. [4]

Generally speaking, there are two important factors to consider as such trigger events for all levels of Did. They are common cause factors and human factors that may negate the provision of Did to give rise big accidents such as TMI-2 accident and Chernobyl accident. However, as a matter of fact in Japan, the implementation of the levels 4 and 5 had not been so seriously considered by both nuclear regulation and NPP operators even though they knew the consequence of severe accident from Chernobyl accident. This was why Fukushima Daiichi accident had happened in 2011. This Japanese case is also a bad example of “Swiss Cheese model”, where the assault of extraordinary big earthquake and tsunami to nuclear power plants had caused all loss of electrical power and heat sink.

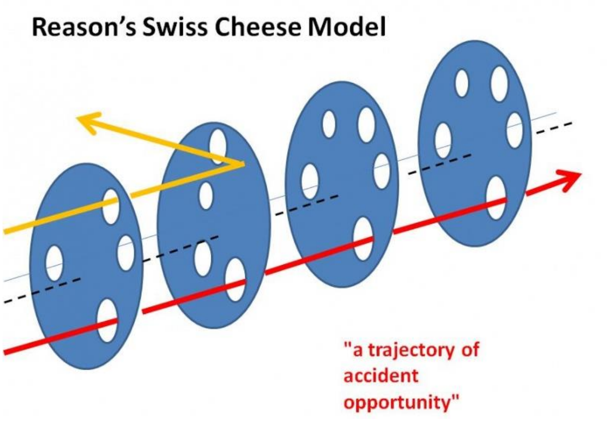
Reason’s Swiss Cheese Model
"a trajectory of accident opportunity"

Fig. 1 Swiss cheese model.

Here the author of this paper would like to discuss on the area of I&C and HMIT, where the provision of Did for Levels 2, 3 and 4 is important. The control system and safety-critical system will be improved for the reliability and safety of the machine systems, and both the operator support system and the operation procedure will be improved by the introduction of computerized automation. There have been many design concepts by the introduction of computer: First to maintain and enhance system safety such as fail-safe, fault tolerant, robust, and resilience. Second to prevent human error in human computer interaction by applying the knowledge on human cognitive, situation awareness, human-machine cognizant system, *etc.*

There are many reasons why software reliability has become a hot issue by the introduction of computerized automation. It is very important to see and understand the whole human-machine system from functional modeling aspect to cope with the software reliability issues to maintain safety of the target system.

## 3 Functional modeling method and its relevance to software reliability

### 3.1 Functional modeling method

What is functional modeling? A functional model in systems engineering and software engineering is a structured representation of the functions (activities, actions, processes, operations) within the modeled system or subject area. A function model is a graphical representation of a system’s function within a defined scope. The purposes of the function model are to describe the functions and processes, assist with discovery of information needs, help identify opportunities, and establish a basis for determining product (design) and service costs (operation and maintenance).

Multilevel Flow Model (MFM) is an example of such functional modeling method to describe function, structure, and process of various industrial systems.[5] MFM can describe such functional relationships by noticing the flows of mass, energy and information in various processes dealt in chemical industries and energy industries, use specific graphical representation to reduce various support tools for process operators to navigate operation procedure, diagnose the causes of troubles, *etc.* But MFM is not the monopoly of functional model. For the analysis and evaluation of software reliability, there have been a lot of methods and software tools in the fields of system science, software engineering, knowledge information processing, human factors engineering, *etc.*, developed to meet with the specificities of the various problems. Those are also the intellectual resources for the functional modeling approaches for software reliability issues.

**3.2 Software reliability issues in NPP**

The software reliability issues will be broadly discussed in relation with safety aspect in the area of I&C and HMIT, by stressing the importance of severe accident prevention for sustainable development of nuclear power in the world. The subjects in the subsequent sub sections will start with the lessons from the experience of big severe accident, TMI-2 accident, Chernobyl accident and Fukushima Daiichi accident.

3.2.1 Lessens from TMI-2 accident

The beginning of TMI-2 accident was the failure of a feed water pump which had been automatically detected and then switched to the auxiliary pump. This was as supposed to act normally, but the false display of plant equipment status on the control board had induced the operator’s misunderstanding of the plant status. This led to the consecutive mal-operation of the plant status towards more dangerous stage of severe accident (nuclear fuels in the reactor core began to melt partially), and as the result, the citizen around the plant had to evacuate.

After the TMI-2 accident, safety researches of nuclear reactor had been strengthened on the thermal-hydraulic behavior of reactor core in accident as well as human factors issues at human -machine interface.

Many lessons were pointed out for human factors issues from the TMI-2 accident as listed below, and they are related with the reinforcement of the levels 2, 3 and 4 of Did concept.

(i)Improvement of emergency operation procedure, education and training of operators,
(ii)Need of operator support tool both in the MCR and outside of MCR such as SPDS,
(iii)Habitability of MCR in severe accident situation,
(iv)Reliable sensors even in severe accident condition ( esp. water level sensor),
(v)Addition of safety engineer in MCR, and
(vi)30 minutes rule.

3.2.2 Lessons from Fukushima Daiichi accident

Before Fukushima Daiichi accident in 2011 in Japan, the nuclear society all over the world had experienced the largest nuclear accident in the world history. That was the Chernobyl accident occurred in former Soviet Union in 1986. The largest lesson from this accident was the importance of safety culture in the whole society to deal with nuclear power.

The lessons of this Chernobyl accident have been reflected on the levels 4 and 5 of the defense in depth safety concept by IAEA. But both the nuclear regulation and nuclear industries in Japan had not paid much attention and effort to the prevention and mitigation of severe accident by false complacency that the Japanese nuclear technology is so superior that there are no possibilities of severe accident in Japan.

There has been strong criticism in Japan that Fukushima Daiichi accident was caused by the deterioration of safety culture among nuclear societies, but the direct cause of the Fukushima Daiichi accident was extraordinary plant situation of all loss of electric power and loss of heat sink, which were initiated by the superposition of extraordinary big earthquake caused by seabed plate boundary movement with the ensuing assault of biggest tsunami in Japanese historical record.

Thereby, the lessons from Fukushima Daiichi accident are preparedness against very rare events in addition to the deterioration of safety culture in nuclear organization. The origins of very rare events to be considered are not only various possibility of natural disaster but also of human origin such as terrorist attack, airplane collision, virus invasion to the network, *etc*. The following countermeasures have been introduced or under consideration in Japan:

(1) Strengthening logistic preparedness of electric power, heat sink, water resource, human resource, education and training for prevention and mitigation of the consequence of severe accident which would be caused by enormous natural hazards such as earthquake, tsunami, *etc*.

(2) Further strengthening of fire protection measures such as (i)Replacement to non-flammable cables, and (ii)Distance keeping of safety-important buildings from forest,

(3) 9.11 countermeasures : Introduction of various countermeasures against terrorist attack including airplane collision, and

(4) Security measures against virus invasion into the computer network and digital control systems.

### 3.3 Various approaches on NPP software safety

Various approaches related with the improvement of software reliability in the areas of I&C + HMIT are briefly summarized in this section.

#### 3.3.1 Design evaluation methods of software reliability and the supporting tools

Regarding the computer application for safety-critical systems, there are two cases of software reliability, (a)reliability of single software implemented in the computer, and (b)reliability of the whole system of hardware and software comprised by computer itself, IO, register, memory, and communication channels.

There are two issues in case (a), that is, (a-1) how to produce high reliability programs (reliable programing method such as structured programing, program diagnosis tool, automatic program generation, *etc*.), (a-2) Method of analyzing and evaluating the reliability of the developed software (software V and V).

In case (a-2), there are two kinds of software V and V. One is that the software V and V is either objective evaluation by which software reliability is evaluated by formal method or theorem proof like judging true or false of theme, or rather objectively such as stochastic test by data analysis. The other type of software V and V is subjective method such as expert judgment, questionnaire, Hierarchical Analytic Procedure, and Bayesian Belief Network, *etc*.

In case (b),the size of the target and the scope of evaluation become so large that the whole system will be decomposed into several elementary modules of software elements, and then will apply appropriate methods of case (a) to conduct V and V for individual modules. Another issue in case (b) is by what way the whole system can be validated in a real working condition of the whole system. Since the I&C and HMIT systems normally work by human machine interaction mode, it will be necessary to take into account and special attention to human factors for the V and V of the whole system.

#### 3.3.2 Setup activity of industrial standards

As was already mentioned in the introduction 1, the full digital I&C system with fully computerized main control board was first realized in 1996 for Japanese ABWR. However, there had been no appropriate standards in the world at that time for both the designing and evaluation of this new full digital I&C and HMIT. Therefore, those V and V methodologies for digital I&C+HMIT for safety-critical system of the ABWR plant had been exploited by the corporation of nuclear utilities, vendors and university researchers. The research and development experience on designing, producing and conducting the V and V for the nuclear digital I&C and HMIT system had been reflected on making the related industrial standards. Those industrial standards of full digital I& C + HMIT were published by the Japan Electric Association (JEA), endorsed by Ministry of Economy, Trade and Industry (METI) of Japan, and widely used in nuclear industry in Japan.

As for the industrial standards set up by the JEA for the software reliability installed in the digital I&C +HMIT [6], the codes on software for safety-critical systems generally specify the execution procedures of the development and V and V process in accordance with the international standard on quality assurance together with the recommendation of utilizing graphical tool of automatic program generation with avoiding the use of complex branching of program flow. Concerning both the development and production for the computerized main control board, the related guide recommends the positive usage of various methods and knowledge in the field of human factors engineering and cognitive psychology for realizing better harmony between human and machine.

Generally speaking, the authorized industrial standards in Japan have the four layers structure as shown in Table 2. The first layer is to specify goals for a certain industrial product and it is enacted by the national law. The second and third layers specify requirements of functions and performance, respectively, and they are issued as ministerial ordinance from the responsible ministerial offices. The fourth layer describes the acceptable implementation methods which are established as codes and guides by academic institutions and associations which are organized by academia, engineers and technicians of specific area. Those codes and guides are industrial standards and they are endorsed by the ministerial offices that it fits to those requirements given in the second and third layers. However, not all of the industrial standards are endorsed by ministerial offices.

**Table 2 Hierarchy of authorized industrial norm in Japan**

| Level | Subject specified | Issuing body |
|---|---|---|
| Level 1 | Goal | National law |
| Level 2 | Functional requirement | Ministerial ordinance |
| Level 3 | Performance requirement | Ministerial ordinance |
| Level 4 | Acceptable implementation method | Industrial standards endorsed by ministry |

### 3.3.3 PRA method for digital safety-critical systems

Digital I&C + HMIT systems have been expanding in many nuclear developing countries either by adopting them in new nuclear power plants or by modernization of the old plants, wherein the old concerns for computer application in nuclear power plants have been reviving from nuclear regulatory bodies worldwide. To cope with this situation, there have been compromising approach seen in many digitalized main control rooms with parallel implementation of backup control panel of analog control board by saying the countermeasure against common cause failures. Another requirement from the nuclear regulators who advocate the extensive use of probabilistic risk assessment (PRA) for the nuclear industry also ask to review the safety of digital I&C + HMIT systems by using PRA.

The difficulty of conducting PRA for digital I&C and HMIT systems lies in that by using the probabilistic method by ET/FTA it is impossible to deal with infinite possibilities of state changes by computer. There is similar limitation to deal with human-machine interaction by the intrinsic human nature of variability and diversity.

Many researches have been underway of developing PRA methods for digital I&C + HMIT systems in order to overcome this intrinsic difficulty of combinatory explosion. Although it may be premature understanding for those researches, the author of this paper assumes that they would resolve the issue so that the span of the evaluation range be restricted for meaningful risk evaluation by (i) noticing the correspondence between goal, objective and function with the structure of the system, and by (ii)focusing on important and plausible scenarios for the consequence of the fault.

### 3.3.4 Appearance of new digital devices

Since the appearance of microprocessor, there have been many various digital I&Cs have been implemented in nuclear power plants. With the rapid progress of LSI technology, multi-purpose microprocessors starting from 8-bit CPU have been developing to 16-bit, 32-bit, and 32-bit CPU on one hand, while digital processors for specific purpose have been appearing. These days, usage of PLC and

FPGA have been in progress for nuclear I&C systems together with the exploitation of evaluation method of software reliability for those new digital I&C systems.

### 3.3.5 International harmonization of nuclear regulation

The safety concern for the introduction of digital I&C + HMIT in nuclear power plant has been provoking attention of nuclear regulators internationally, and these days the international activities have been expanding from the information exchange to harmonizing the regulation internationally about the issue by utilizing the international organization such as IAEA and OECD/NEA.

The MDEP（Multinational Design Evaluation Program) [7] was established in 2006 as a multinational initiative to develop innovative approaches to leverage the resources and knowledge of the national regulatory authorities who are currently or will be tasked with the review of new reactor power plant designs. MDEP comprises 14 countries' nuclear regulatory authorities and is structured under 5 design-specific working groups and 3 issue-specific working groups which meet several times a year. The OECD/NEA facilitates MDEP's activities by acting as technical secretariat for the program. The MDEP Digital Instrumentation and Controls Working Group (DICWG) were approved by MDEP's Policy Group in March 2008 and meets approximately 3 times a year. All MDEP members and the IAEA are invited to participate in this working group's activities.

The DICWG's main objectives to harmonize and converge national codes, standards and regulatory requirements and practices in this area while recognizing the sovereign rights and responsibilities of national regulators in carrying out their safety reviews of new reactor designs. The DICWG interacts regularly with IEC (International Electro-technical Commission) and IEEE (Institute of Electric and Electronics Engineers)

### 3.3.6 Defense in depth safety concept and software reliability

The nuclear society around the world has expanded the nuclear power utilization for those fifty years notwithstanding three experiences of severe accidents (TMI-2 accident in 1979, Chernobyl accident in 1986, and Fukushima Daiichi accident in 2011). The defense in depth concept for nuclear safety has been expanded and accordingly the number of safety requirements for nuclear power plants has been growing each time the nuclear society overcome the severe accident. On the other hand, the nuclear industries have been challenging for new reactors with reinforced safety against severe accident.

For these 20 years, new light water reactor plants such as ABWR, AP1000, EPR, APR1400, *etc*., have been appearing in the world. Among them, both AP1000 and EPR are new type light water reactors (Build-in type) to enhance safety measures against severe accident by employing automatic passive safety functions, core melt cooling and retention measures, *etc*. On the other hand, Japanese nuclear utilities who experienced Fukushima Daiichi accident are going to restart their conventional light water reactor plants by giving them patchwork reinforcement to endure severe accident. This is another type of safety measure called Add-on type.

Many nuclear developing countries around the world have been discussing on the safety goal of nuclear power plant with conducting on international comparison of regulatory requirement against severe accident prevention by organizing the international forum in IAEA and OECD/NEA. However it will be difficult to say that Built-in type is superior to Add-on type for severe accident prevention and mitigation, and it would be also difficult to say that there is no difference between the both type if the reactor satisfies with the safety goal or regulatory requirements against severe accident.

At this point, the author of this paper would like to address another safety issue in severe accident by raising a question *“Will it improve the operational efficiency and operational skills of operators of the real nuclear plant by such way of regulation?”* In order to improve the nuclear power technology which will be well balanced in safety, economy, and efficiency, it is expected to create a new methodology that can serve to analyze various aspects of software reliability issues by innovating functional modeling approach as introduced at the beginning of this section 3. Although not dealt in this paper, a developmental study of comprehensive risk analysis system by functional modeling approach [8] by the author of this paper is motivated towards this direction.

## 4 Conclusions

Application of digital computer to nuclear power plant has been a traditional safety concern by nuclear regulation. These days, along with the expansion of digital I&C and HMIT for safety-critical system, this traditional concern has been reviving by the name of software reliability, and it has been recognized over the world as the important issue on nuclear regulation.

On the other hand of software reliability, defense in depth concept of nuclear safety has been more and more reinforced with the historical repetition of severe accidents worldwide. As the result, the regulatory requirement to the safety of nuclear power plant has been increased and intensified year by year.
In this paper, the author gave a broad overview on the software reliability issue from the relationship between the defense in depth safety concept and digital I&C and HMIT in order to give the readers insights on the technical direction and the issues at hand.

In the future, it is expected to create a new methodology that can serve to analyze various aspects of software reliability issues by innovating functional modeling approach, and then utilize it actively to improve the nuclear power technology which will be well balanced in safety, economy, and efficiency.

## References

[1]PETRANGELI, G.: Nuclear Safety, Oxford, Elsevier, Chapter 9 Defence in depth, 2006, 89-91.

[2]IAEA: INSAG-12 Basic safety principles for nuclear power plants 75-INSAG-3 Rev.1, Vienna, 1999.

[3]IAEA: INSAG-10 Defence in depth in nuclear safety, Vienna, 1996.

[4]REASON, J.: Managing the risks of organizing accidents, Ashgate Publishing Limited, 1997.

[5]LIND, M. , and ZHANG, X.: Applying functional modeling for accident management of nuclear power plant, Nuclear Safety and Simulation, 2014, 5(3):186-196.

[6]YOSHIKAWA, H.: A review on developing industrial standards to introduce digital computer application for nuclear I&C and HMIT in Japan, Nuclear Engineering and Technology, 2013, 45(.2), 165-178.

[7]OECD/NEA: Multinational Design Evaluation Program (MDEP),
http://www.oecd-nea.org/mdep/ (As of February 1st, 2015)

[8]YOSHIKAWA, H., YANG, M., and ZHANG, Z. : Integrated functional modeling method for NPP plant Did risk monitor and its application for conventional PWR, Nuclear Safety and Simulation, 2014, 5(3):205-212.