A Review on Developing Industrial Standards to Introduce Digital Computer Application for Nuclear I&C and HMIT in Japan

Hidekazu Yoshikawa

KOREAN NUCLEAR SOCIETY

http://dx.doi.org/10.5516/NET.04.2013.703

A REVIEW ON DEVELOPING INDUSTRIAL STANDARDS TO INTRODUCE DIGITAL COMPUTER APPLICATION FOR NUCLEAR I&C AND HMIT IN JAPAN

HIDEKAZU YOSHIKAWA
Professor Emeritus Kyoto University
Yoshida-Honmachi, Sakyo-ku, Kyoto-shi, 606-8501 Japan
E-mail : yosikawa@kib.biglobe.ne.jp

Received February 12, 2013

A comprehensive review on the technical standards about human factors (HF) design and software reliability maintenance for digital instrumentation and control (I&C) and human-machine interface technology (HMIT) in Japanese light water reactor nuclear power plants (NPPs) was given in this paper mainly by introducing the relevant activities at the Japan Electric Association to set up many industrial standards within the traditional framework of nuclear safety regulation in Japan.

In Japan, the Fukushima Daiichi accident that occurred on March 11, 2011 has great impact on nuclear regulation and nuclear industries where concerns by the general public about safety have heightened significantly. However for the part of HF design and software reliability maintenance of digital I&C and HMIT for NPP, the author believes that the past practice of Japanese activities with the related technical standards can be successfully inherited in the future, by reinforcing the technical preparedness for the prevention and mitigation against any types of severe accident occurrence.

KEYWORDS : Digital I&C; Human-machine Interface; Main Control Room, Human Factors; Software Reliability; Software V&V: Industrial Standard;

1. INTRODUCTION

Rapid progress of Information, Communication Technology (ICT) has been contributing to the technical improvement of design, operation and maintenance of nuclear power plants in general and especially in the advancement of instrumentation and control (I&C) systems and human-machine interface technologies (HMIT). But on the other hand of various merits of technical improvement by ICT, the complexities and multiple functionalities brought by the extensive computer application for the nuclear I&C and HMIT have made it more difficult than before in the safety evaluation to the introduced systems in the actual plants.

In Japan, where light water reactor technologies had been introduced from the US in late 1960s, the development of full digital I&C and HMIT systems had been initiated in the 80's-90's for both PWR and BWR plants by the collaboration of all nuclear power utilities and nuclear power plant vendors with the governmental support of Ministry of International Trade and Industries (MITI). The first introduction of full digitalized I&C and main control room (MCR) was for the first Advanced Boiling Water Reactor (ABWR) plant Kashiwazaki-Kariwa No. 6 unit of Tokyo Electric Power Company (TEPCO) which started commercial operation in 1996, while for PWR Tomari No.3 unit of Hokkaido Electric Power Company was the first fully digitalized I&C and MCR in commercial operation in 2009.

During the process of introducing full digital I&C and HMIT systems for both PWR and BWR plants constructed in Japan, the technical guidelines for full digital I&C and HMIT systems had been gradually set up by the Japan Electric Association (JEA) as the several domestic industrial standards in Japan, which are not only consistent with basic principles on nuclear safety in the world and the related international standards but also comply with national laws for nuclear, guidelines issued by Nuclear Safety Commission, ministerial orders by Nuclear and Industrial Safety Agency (NISA). Those industrial standards by the JEA had been utilized for the designing of the computerized MCRs for several newly constructed nuclear power plants and the replacement of old analog-type MCRs to digitalized MCRs in Japan.

It has been historically inevitable in Japan to have frequent large-scale earthquakes with sometimes accom-

panying high tides called tsunami. In July 2009, TEPCO's Kashiwazaki-Kariwa nuclear power station (seven units) where the both units 6 and 7 are full digital MCR ABWR plants, had been hit by Chu-etsu-oki earthquake (magnitude 6.8). In March 2011, TEPCO's Fukiushima Daiichi, and Fukushima nuclear power stations (ten units), Tohoku Electric Power Company's Onagawa and Higashi-Dori nuclear power stations (four units) and Japan Atomic Power Company's Tokai Daini nuclear power station (one unit) were all hit by Higashi-Nihon earthquake (magnitude 9) with the highest tsunamis afterwards bringing severe accidents at four units of the Fukushima Daiichi nuclear power station. There were no full digital MCR plants among fifteen units hit by the Higashi-Nihon earthquake in 2011.

The effect of the severe accident at Fukushima Daiichi nuclear power station was so enormous that the traditional framework of nuclear power regulation had to be totally altered in Japan. In September 2012, major governmental institutions of nuclear regulation, i.e., nuclear safety commission in Cabinet Office and NISA in MITI, were abolished to be integrated into a new institution called Nuclear Regulation Agency (NRA) with the nomination of six commissioners for the also newborn Nuclear Regulatory Committee which has power to decide on nuclear regulation independent from cabinet control. Recently, the NRA has been busy revising almost all legitimate institutions and guidelines related with national regulation on nuclear safety with a completion deadline of July 2013 by reflecting on all lessons learned from the Fukushima Daiichi accident, which includes several important issues on I&C and HMIT for nuclear power stations as well as for several facilities related with nuclear emergency response.

In this paper, the comprehensive review will be made on the industrial standards for HF design and software reliability maintenance of digital I&C and HMIT for NPP which was established by the JEA and has been widely used in Japan as the standard method for introducing digitalized MCRs in nuclear power plants. In which follows, basic principles of nuclear safety with specific issues for nuclear I&C and HMIT will be introduced in Chapter 2, a brief history of introducing digital I&C and HMIT in Japan in Chapter 3, technical standard setup activities at the Japan Electric Association in Chapter 4, summarized contents of JEA's standards for human factors design and software reliability of digital I&C and HMIT in Chapter 5, and the impact of the Fukushima Daiichi accident to nuclear I&C and HMIT in Japan in Chapter 6 before the concluding remarks of this paper.

2. BASIC PRINCIPLES OF NUCLEAR SAFETY ISSUES OF NUCLEAR I&C AND HMIT

According to G. Petrangelli in his book titled "Nuclear Safety" [1], he pointed out eight basic principles of nuclear safety as listed in Table 1.

Among the eight principles in Table 1, the fifth principle of defense-in depth provision is considered as the specific characteristic of a nuclear safety system: There are four barriers of (i) fuel matrix, (ii)fuel cladding, (iii)reactor cooling circuit pressure boundary, and (iv)containment system in order to primarily prevent external release of radiological products which should be normally contained in the nuclear reactor and secondarily to mitigate the effect of radiological release in the event of nuclear accident. For this purpose, it is necessary to configure five levels of defense as illustrated in Table 2. And with regards to the digital I&C and HMIT as the subject of this paper, it should primarily concern with the levels 2 and 3 in Table 2.

There are two difficult issues for ensuring nuclear safety until the third level in Table 2.The first is the consideration of common cause failure [2] which should take into account not only internal causes by design, fabrication and maintenance of nuclear power plant but also external causes such as natural disasters, fires, airplane corrosion, etc, as described in Fig.1. You can see from Fig.1 that the

Table 1. Eight Technical Principles for Nuclear Safety

1	Adoption of proven engineering solution.
2	High quality of engineering applied to all aspects of the design, construction and operation.
3	Adequate quality assurance measures proportionate to the safety classification and qualification of structures, systems and components.
4	Safety analysis including its verification.
5	Defense-in depth provisions against common cause faults such as diversity, physical separation and barriers both for internal and external events.
6	Good practice of operation and maintenance including the provisions for the use of the lessons learned from past experience.
7	Safety culture and attention to human factors.
8	Provisions to ensure the documented adequacy of the operation organization and the independent role of he regulatory control bodies.

external causes will affect broader areas, systems and components than internal causes for the safety of nuclear power plants. The second one is what is called human factors or human error. Figure 2 shows the classification of human error mechanism which the author of this paper modified a bit from the original scheme by J. Reason [3] by classifying further whether or not the committed person has the intention to do so. Such human factors are also common cause factors as already appear in Fig.1, but from the point of designing I&C and HMIT the normal consideration will be given on human cognitive factors as highlighted in Fig.2.

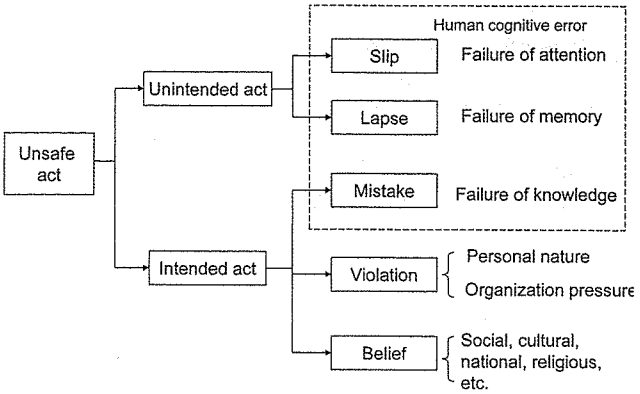

Fig. 2. Human Error to be Considered in Nuclear Safety

Table 2. Five Defense Levels of Nuclear Safety

Defense level	Objective	Essential means
Level 1	Prevention of abnormal operations and of malfunctions	Conservative design and high quality of construction and operation
Level 2	Control of abnormal operation and detection of malfunction	Control, limitation and protection systems and other surveillance characteristics
Level 3	Control of accidents included in the design basis	Engineered safety systems and accident procedures
Level 4	Control of the severe accident conditions of the plant, including the prevention of accident and mitigation of consequences	Additional measures and accident management
Level 5	Mitigation of the radiological consequences of significant releases of radioactive products	External site emergency plan

Clearness of fault cause	Influencing span of fault cause	Types of fault cause	Coupling mechanism	Analytical treatment
Clear	Whole plant	Earthquake	Spatial	Explicit
	Combined subsystem	Fire, flooding, tsunami, tornado	Spatial	Explicit
		Airplane collision Sabotage act	Spatial, human factors	
		Functional relation	Functional	
		Common share of support equipment	Functional	
		Change of physical environment by equipment failure	Spatial	
Randomly or steadily exist	Single subsystem	Physical environment (high temp., high pressure, etc.)	Spatial	Explicit
Unclear	Individual equipment	Human errors in design, fabrication, operation, and maintenance	Human factors	Parametric

Fig. 1. Consideration on Common Mode Failure

According to G. Petrangelli[1], he also pointed out three specific considerations for I& C and HMIT as listed in Table 3. In considering digital I&C and HMIT, more attention has been given to items 1 and 2 of Table 3 in the past: For item1 as the human factors consideration to prevent operator error in MCR, while for item 2 common cause countermeasures in the event of system down of computers for HMIT. However the item 3 of Table 3 pointed out the provisions against all loss of electric power to the MCR. In fact, the effect of tsunami attacking the whole plant after a large earthquake was an important factor in the Fukushima Daiichi accident.

3. BRIEF HISTORY OF INTRODUCING DIGITAL I&C AND HMIT IN JAPAN

Nuclear power development had been initiated in the latter half of the 1960s by introducing US light water reactor technologies (both PWR and BWR). Construction of nuclear power plants had been accelerated by experiencing oil shocks twice in the 70s, with expanding the domestication of nuclear power technologies until the 80s when traditional analog I&C and MCR from the US had been improved by more automation by digital technologies and the introduction of CRTs in the MCR which is called as hybrid MCR.

By reflecting the technical progress of computers in the 90s, automation and communication technologies had prevailed in many industries around the period. In Japan, a national project of developing new light water reactors, advanced PWR (APWR) and advanced BWR (ABWR), had been conducted by the cooperation of nuclear utilities and nuclear power vendors with governmental support through MITI, where the realization of full digital I&C and MCR was one of the big technical challenges at that time to improve various human factors problems of MCR as revealed in the TMI-2 accident in 1979 and Chernobyl accident in 1986. Concretely, the technical targets of improving human factors at MCR by full digital I&C and HMIT are shown in Table 4.

The appearance of full digital MCR of TEPCO's Kashiwazaki-Kariwa Unit 6 is shown in Fig. 3. This is the first ABWR which had started commercial operation in 1996.

There have been four ABWRs (Kashiwazaki-Kariha unit 6 and 7, Hamaoka Unit 5, and Shika Unit 2) already in operation and two units under construction (Shimane Unit 3 and Ohma plant) in Japan.

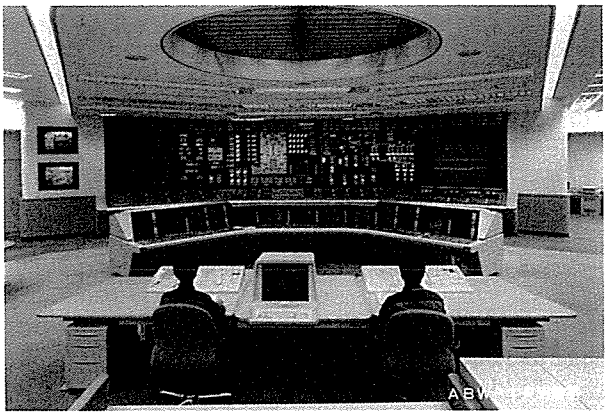

Fig. 3. Full Digitalized Main Control Room for Japanese ABWR

Table 3. Three Specific Considerations for NPIC + HMIT

1	Design provisions intended to give operators enough time to respond to event and to ensure adequate man-machine interface including operator-support means intended to facilitate their task.
2	Where a microprocessor-based reactor protection system is used, the presence of a backup system of traditional type or other means to ensure protection against malfunctions, included those involving the software is assured.
3	Presence of emergency electric power supply sources including portable ones, but different from the traditional emergency sources, either by type of machine and by type of fuel.

Table 4. Technical Targets of Full Digital I&C + HMIT in Japanese PWR and BWR

Objectives by human factors aspect	Technical means
Information sharing (improvement of communication ability)	Large display panel
Reduction of workload	Compact operation console Touch operation by flat displays
Reduction of human errors	Expansion of automation range
Amenity	Windows, illumination and living rooms for the comfort of operators

Conversely, the construction of the first APWR plant in Tsuruga in Japan has been delayed by various political reasons. Therefore the full digital I&C and HMIT for conventional PWR was realized at Tomari Unit 3 of the Hokkaido Electric Power Company. The Tomari Unit 3 started its commercial operation in 2009. The apperance of full digital MCR of Tomari Unit 3 is shown in Fig.4.

The replacement of old analog I&C and HMIT of conventional PWR plants by full digital I&C and HMIT had been also conducted by Ikata Unit 1 and 2 of the Shikoku Electric Power Company in 2009.

The history of introducing full digital I&C and HMIT in Japan is summarized in Table 5, where also shown is the statistics of the number of unplanned shutdowns by failure of a full digital system. There were 19 unplanned shutdowns for seven nuclear power plants which employ full digital I&C and HMIT system, but there were no failure of full digital system. At present all seven nuclear power plants in Table 5 were forced into a shutdown state due to safety concerns in the aftermath of the Fukushima Daiichi incident in March 2011

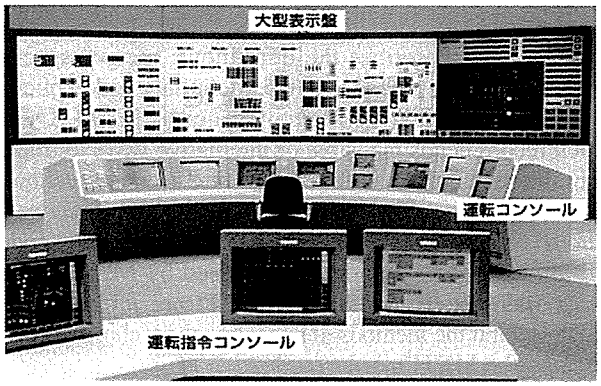

Fig. 4. Full Digitalized Main Control Room for Japanese PWR

4. TRADITIONAL TECHNICAL STANDARD SETUP ACTIVITIES IN JAPAN

In this chapter, the relationship between nuclear regulation and industrial standards in Japan will be first explained before detailing the current efforts of the Japan Electric Association to set up industrial standards for Japanese nuclear industries.

4.1 Hierarchy of Nuclear Standards in Japan

Nuclear power facilities are not only electric facilities but are also responsible for protecting employees and the

Table 5. History of Introducing Full Digital I&C+HMIT in Japan

Year	No of full digital systems	Note	Unplanned shutdown	Reactor scram	ECCS start
1996	1	Kashiwazaki-Kariha-6	0	0	0
1997	2	Kashiwazaki-Kariha-7	0	0	0
1998	2		2	1	0
1999	2		2	1	0
2000	2		1	0	0
2001	2		1	0	0
2002	2		1	0	0
2003	2		0	0	0
2004	3	Hamaoka-5	1	1	0
2005	4	Shika-2	0	0	0
2006	4		2	1	0
2007	4		2	1	0
2008	4		2	0	0
2009	7	Tomari-3 Ikata-1,2 (replace)	4	1	0
2010	7		1	0	0
2011 - 2012	7	All plant shutdown after Fukushima Daiichi accident	0	0	0
Total	7		19	6	0

general public from radioactive exposure. Therefore, the safety of nuclear facilities was regulated in Japan by several laws and orders by different ministerial organizations: electric business act by Ministry of Economy, Trading and Industry (METI), various laws and orders by Nuclear Safety Commission and Ministry of Education, Science and Technology (MEXT), etc, depending upon the specific issues and facilities involved. In addition, it has been normally submitted from the governmental divisions to the disposal of individual industries to decide the technical details to meet the objectives set by laws and ministerial orders. This is the reason why there exist so many technical standards which are set up by various academic societies and industrial associations not only domestically but also internationally. Figure 5 shows the relationship between nuclear regulation by national laws and industrial standards set up by public institutions in Japan by classifying four levels of hierarchy in nuclear regulation, that is, objective, functional requirement, performance requirement and permissible execution method.

In Fig. 5, the correspondence is indicated between the technical criteria (which is described in the Ministerial order No.62 issued by METI based on Electric Business Act) and the industrial standard set by the Japan Electric Association (JEA). The JEA considers the safety measures of nuclear power plants as one of the electric facilities which are regulated by Electric Business Act in the following ways: (i)Conformity to technical standards given in Electricity Business Act is the minimum requirement on performance for construction, maintenance and operation, (ii)Independent safety measures should be taken by the facility operators, and (iii)Industrial standards to describe the technical details on materials, design, fabrication, testing, quality assurance, etc., should be set by industrial societies and associations, through a socially open, fair and justified process.

There are many academic societies and technical associations which are contributing to setting up various industrial standards in response to the operators of various electric facilities, and for the nuclear power generating facilities. Among them, Atomic Energy Society of Japan, Japan Mechanical Society and Japan Electric Association are major institutions to set up various industrial standards based on their respective expertise.

4.2 Industrial Standards Setup Activity at the Japan Electric Association

There are two kinds of industrial standards by the Japan Electric Association: (i) Code indicated as JEAC-XXXX which describes the definitions, means, specifications, methods, procedures, etc., definitely and explicitly as requirement, and (ii) Guide indicated as JEAG-XXXX which recommends plausible or alternative ways to implement the requirement within the present stage of technical knowledge. As to the relationship with the hierarchy of national regulation as shown in Fig.5, there are many codes and guides by JEA which are endorsed by METI. Those codes and guides endorsed by METI are interpreted to clearly exhibit the methods of executing the technical criteria given by the METI's order.

At JEA, the Japan Electrotechnical Standards and Codes Committee has been generally in charge of setting up various industrial standards for various electric facilities, while the Nuclear Standards Committee of JEA has been responsible for those of nuclear power facilities from the special aspect of nuclear power facilities. As seen from Fig. 6 of the configuration of Nuclear Standards Committee of JEA, there are seven subcommittees to set up industrial standards for safety design, structure, nuclear fuels, quality assurance, anti-seismic design, radiation management, and operation and maintenance for nuclear power facilities.

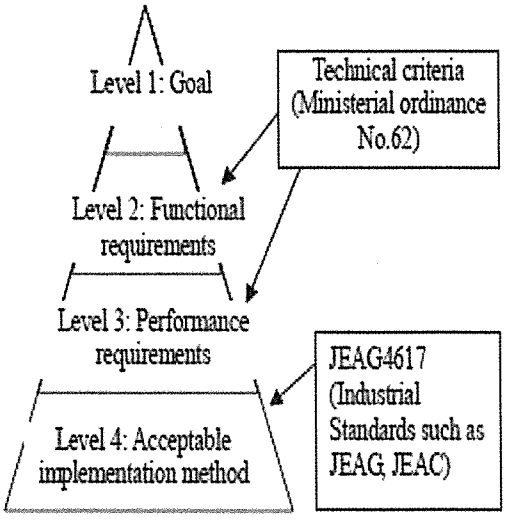

Fig. 5. Technical Criteria and Industrial Standards in the Hierarchy of Nuclear Safety Regulation in Japan

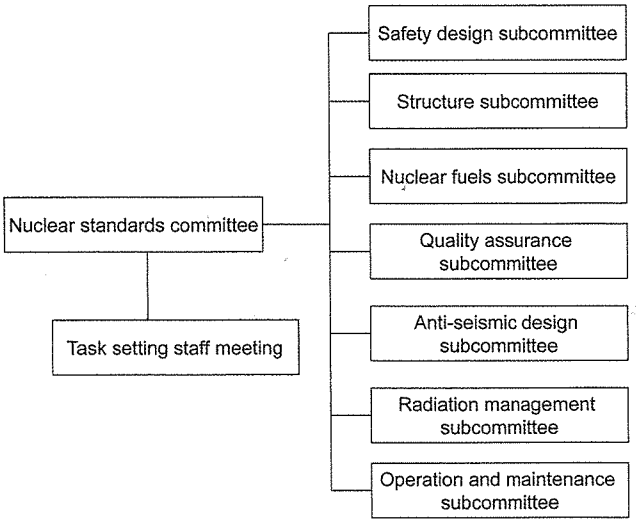

Fig. 6. Composition of Nuclear Standards Committee of the Japan Electric Association

The author of this paper has previously contributed as the chair of Safety design subcommittee for ten years between 2002 and 2011, and all the codes and guides of JEA which the author of this paper committed to set up and update during the period are listed in Table 6.

All the codes and guides in Table 6 are classified into four categories of (i) Definition of classification and designing safety grade electrical and mechanical equipments, (ii) General safety provision of plant facilities, (iii) Safety protection system, and (iv) Main control room, with the ID number and the full names of individual standards. The contents of all standards are described by Japanese. Individual standards can be available from JEA upon request.

The essential points of two standards, JEAG 4621-2007 (Guide on evaluating instrument drift of safety protection system) and JEAG 4617-2005 (Guide on development and design of computerized human interface of main control room), are published in English as the journal papers[4,5].

5. HUMAN FACTORS DESIGN AND SOFTWARE RELIABILITY OF DIGITAL I&C AND HMIT IN JAPAN

Adoption of full digital I&C and HMIT for nuclear power plants has nowadays become a common trend

Table 6. Codes and Guidelines for Safety Design of Nuclear Power Plants Established by the Japan Electric Association

Class	ID No.	Names of codes and standards
Definition of classification and designing safety grade electrical and mechanical equipments	JEAC 4602-2004	Code on defining the range of reactor coolant pressure boundary and reactor containment
	JEAC 4605-2004	Code on defining the range of engineered safety facilities of nuclear power plant and the related facilities
	JEAG 4612-2010	Guide on classifying the importance of electrical and mechanical equipments of safety functions
	JEAC 4603-2010	Code on designing electric power supplies important for safety
	JEAG 4611-2009	Guide on designing instrumentation and control systems of safety functions
	JEAG 4623-2008	Guide on verifying anti-environmental performance of instrumentation and control systems of safety functions
General safety provision of plant facilities	JEAG 4608-2007	Guide on anti-thunder designing of nuclear power plants
	JEAC 4626-2010	Code on fire protection design of nuclear power plants
	JEAG 4607-2010	Guide on fire protection design of nuclear power plants
	JEAG 4627-2010	Guide on designing emergency response facility of nuclear power plants
Safety protection system	JEAC 4604-2009	Code on designing safety protection system
	JEAC 4620-2008	Code on applying digital computer for safety protection system
	JEAG 4609-2008	Guide on verification and validation of digital safety protection system
	JEAG 4621-2007	Guide on evaluating instrument drift of safety protection system
Main control room	JEAC 4624-2009	Code on designing to prevent operation error in main control room
	JEAG 4617-2005	Guide on development and design of computerized human interface of main control room
	JEAC 4622-2009	Code on operators' radiation protection in accident condition of main control room

around the nuclear developing countries, where it seems to become a hot topic of discussion around many countries as to the methodological developments to introduce full digital I&C and HMIT. They are (i)software reliability evaluation of computerized reactor protection system, and (ii) evaluation of the adaptability of full digital MCR to the operators.

The solutions to the above questions had been implemented in Japan during the development and implementing process of full digital I&C and HMIT for both PWR and BWR, by introducing the corresponding industrial standards for the both of them, as the combinations of code and guide established by the Japan Electric Association as listed in Table 7 for (a)Software V&V for Digital Safety System and (b) Human Factors Design of Main Control Room, which are consistent with the hierarchy of national nuclear regulation as already shown in Fig. 5. Concerning the configuration of full computerized MCR, it is assumed to equip with such human interface facilities by such arrangement in a typical control room as is shown in Fig. 7.

Concerning (a)Software V&V for Digital Safety System, functional requirements for digitalized reactor protection system are summarily listed up in Code on applying digital computer for safety protection system (JEAC4620-2008).

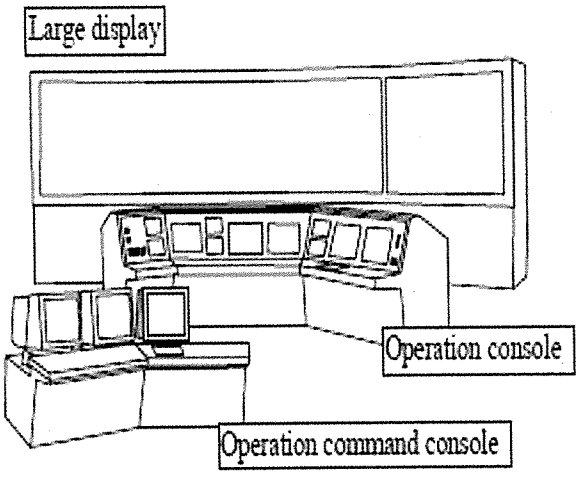

Fig. 7. An Example Configuration of Computerized Human-machine Interface for Monitoring and Operation

This corresponds to the requirement for the reliability of reactor safety protection system in the guideline of safety design of light water reactors given by the nuclear safety commission. The detailed methodologies to realize the designing of the target safety protection system and the procedures to prove the designed system are formulated as Guide on verification and validation of digital safety protection system (JEAG4609-2008).

Concerning (b) Human Factors Design of Main Control Room, the guideline of safety design of light water reactors given by the nuclear safety commission requires that the designing of MCRs should prevent the operators' error be the MCRs analog or digital. This general requirement statement is described in details as Code on equipment designing to prevent operation error in the main control room (JEAC 4624-2009). The detailed methods of developing the standard design of digital MCR, validating the standard MCR design, and applying the standard design for introducing into real plant to meet its real objective and restriction are described in Guide on development and design of computerized human interface of the main control room (JEAG4617-2005).

In order for the operators to operate the plant rightly without error, it is necessary that the operators should master a certain level of relevant knowledge and skills for nuclear power plant operation with a certain amount of job experience. Although it is outside of this paper, there is the relevant standards to specifying the method of operators' education and training established by the Operation and maintenance Subcommittee of Nuclear Standards Committee of the Japan Electric Association.

The more detailed contents of the Codes and Guides for both (a) and (b), are described in 5.1 and 5.2, respectively. It will then be briefly explained in 5.3 how the digital computer application for I&C and HMIT for nuclear power plants has been made in Japan.

5.1 Software V&V for Digital Safety System

5.1.1Code on Applying Digital Computer for Safety Protection System (JEAC4620-2008)

The code JEAC4620-2008 describes the functional requirements for the digitalized safety protection system

Table 7. Logical Order of Industrial Standard for HF Design and Software V&V of Digital I&C+HMIT

Software V&V for Digital Safety System	
Code	Code on applying digital computer for safety protection system
Guide	Guide on verification and validation of digital safety protection system
Human Factors Design of Main Control Room	
Code	Code on equipment designing to prevent operation error in main control room
Guide	Guide on development and design of computerized human interface of main control room

as listed in Table 8. It requires that the system should be equipped with the protective functions both against malfunction in the event of troubles and false activation during normal operation with high reliability. It also describes eighteen items of functional requirements.

Among those eighteen items not only it includes redundancy, independency, physical separation from normal I&C system, etc., which are common to a conventional analog-type safety protection system, but also it requires several features specific to digital system such as self-

Table 8. Code on Applying Digital Computer for Safety Protection System

ID	Subject	Content
1.	Requirement	Attain high reliability by considering both unavailability and malfunction rate. The following requirement items must be satisfied.
1.1	Functions in the event of transients, accidents and earthquakes	Both reactor shutdown system and engineered safety system should initiate automatically in the event of those situations.
1.2	Accuracy and response time	Digital safety protection system should satisfy both conditions of accuracy and response time as a whole system composed by computer and the related hardware.
1.3	Redundancy	Redundant configuration should be taken so that it does not lose intended functions against single fault or single takeoff or bypass.
1.4	Independency	Independency of each channel is taken by electrical and physical separation between channels so that it does not lose its function by a single channel failure.
1.5	Separation from instrument and control system	Even in case of partial sharing between the both, electrical separation should be considered. Also functional separation is taken when communication is shared.
1.6	Function in case of failure	Fail safe state should be attained in case of unfavorable situation such as loss of driving power, etc.
1.7	Testability	Maintenance of soundness and redundancy should be confirmed by testing even during power operation.
1.8	Environmental condition	Anti-seismic, anti-surge and the other anti-hazardous characteristics are considered.
1.9	Use of emergency power source	Electric power source of digital safety protection system should be supplied by emergency in-station power system so that electric power can be supplied even in case of loss of external power or loss of all AC power.
1.10	Parameter value change	Parameter values of the digital protection system can be manually changed.
1.11	Selection of input variables	As many as practically available, input variables of the digital protection system should be the corresponding directly measurable signals.
1.12	Completeness of protect action	Once started, the protect action of the protection system should be continued until its completion.
1.13	Manual operation	If necessary, reactor shutdown system or engineered safety system can be operated manually.
1.14	Display of activation and bypass	When the protection system is activated, the cause should be displayed on the main control board. Also the state of bypass or out of inline of the system equipment or channel should be continuously displayed on the board.
1.15	Self diagnosis function	Self diagnosis can be made independently for each channel by appropriate period of time, with the result being announced to the operator when anomalies are detected,
1.16	Cutoff of external network	External effect should be prevented by cutting off external network.
1.17	Protection measure against unplanned software alteration	Appropriate protective measures are taken against unplanned software alteration to the software system installed on the digital protection system.
1.18	Quality management	The quality of digital computers and the software system should be assured by the three QM activities: (i) Software life cycle management (ii) Software configuration management (iii) Software verification and validation activity
2.	Common cause fault measure	Hardware equipment should be prepared within rational range, in order to ensure further reliability from the aspect of defense-in depth safety.

diagnostic function, countermeasures against unplanned change of software, etc. It also requires the alternative means as the countermeasure against all loss of functions of digital system by common cause failures. This code had been endorsed by NISA that it satisfies the technical criteria requested by MITI's ministerial order.

5.1.2 Guide on Verification and Validation of Digital Safety Protection System (JEAG4609-2008)

This guide JEAG4609-2008 describes guidance information on the verification and validation to the software implemented into the digital safety protection system such as objective, execution methods (execution procedure, members of execution, document management and software tools for V&V), software reutilization and software configuration management.

Design and fabrication process and the V and V activity of digital safety protection system are separately made by different teams independently. As shown in Fig.8 for the whole, it begins with the verification 1 to verify the design specification of the digital safety protection system and the fundamental plan of V and V activity. According to thus verified hardware-software design requirement specification, both the designing and fabrication of hardware and software are separately conducted, and finally both hardware and software are integrated. The sequential activities of verification 2, 3 and 3 are made during the individual processes

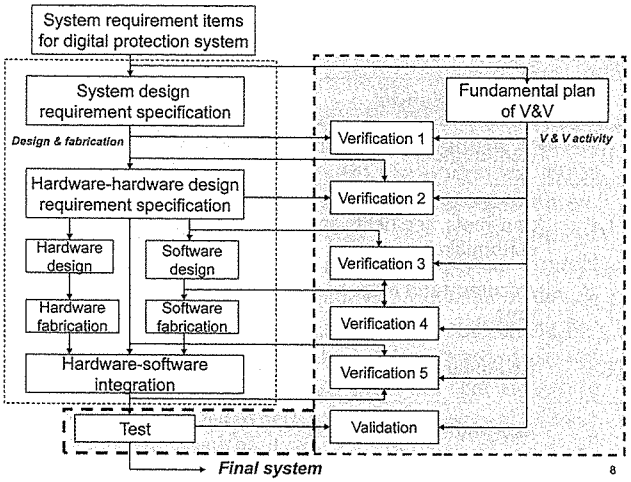

Fig. 8. Verification and Validation of Digital Safety Protection System

Table 9. Guide on Verification and Validation of Digital Safety Protection System

Software verification & validation		
1.	Objective of verification & validation (V&V)	
	1.1	V & V activity is to assure that the system requirements for digital safety protection system are rightly realized in the processes of design, fabrication, test and alteration.
	1.2	The verification activity is made to check the consistency between upstream specification and downstream one in design and fabrication processes by the following aspects. (a) System requirement items for digital protection system are rightly reflected in hardware-hardware design requirement specification. (b) Software is designed and fabricated based on the hardware-hardware design requirement specification. (c) Software is designed so that it is able to conduct on V&V.
	1.3	Validation activity is made in test process to confirm that the total system after the software is integrated into hardware realizes rightly the system requirements for digital safety protection system.
2.	Execution of V&V	
	2.1	Execution procedure and content of V&V (See Fig.8)
	2.2	V&V team (Members should be different between those involved in design and fabrication and those involved in V&V.)
	2.3	Documentation control (Both for design and fabrication and for V&V activities)
	2.4	Software tool management (When software tools are used for either (i)software design, generation and testing or (ii) software for V&V purposes, those software tools under quality management should be employed.
3.	V&V for software re-utilization The range and justification of re-utilization should be clarified for each task of software design and generation.	
Software configuration management		
1.	Configuration management based on documentation for the alteration of both design requirement specification and software, especially with the reason, place and the influenced ranges. If necessary, V&V should be made on the altered part.	
2.	The software identical to the one implemented in the protection system should be separately preserved.	

of design and fabrication of the hardware and software in accordance with the hardware-software design specification, and then verification 5 is conducted at the integration stage of hardware and software. Finally the V and V is completed by conducting validation test.

The international IEEE Standard 1012-1998 [6] and IEEE Standard 7-4.3.2-2003 [7] were utilized in setting up this domestic guide JEAG4609-2008.

5.2 Human Factors Design of Main Control Room

5.2.1 Code on Equipment Design to Prevent Operation Error in Main Control Room (JEAC 4624-2009)

This code JEAC 4624-2009 summarizes the functional requirements on designing the main control room applicable for the different types of control room (analog, hybrid and full digital). As listed in Table 10, it depends on a variety of factors such as (i)environmental conditions and arrangement of equipments in the area of the main control room where operators monitor and operate the plant, (ii)task allocation between human and machine, task division between different operation members, and the way of information share, (iii)panel layout in the main control board, display, alarm and operation support system, and control input equipments, and (iv)the ways of developing, fabricating and updating.

This code has been endorsed by NISA that it satisfies with the technical criteria requested by METI's ministerial order to prevent MCR operators from committing operation error.

5.2.2 Guide on Development and Design of Computerized Human Interface of Main Control Room (JEAG4617-2005)

This guide JEAG4617-2005 gives the guidance to realize the requirements given in the code JEAC 4624-2009 concretely as the human interface of computerized MCR. As shown in Table 11, the contents of this code are (i)functional requirements, (ii)design requirements, (iii)development process and fabrication design process, and (iv) V&V process.

Both the development of the standard MCR design and the fabrication design process of the MCR of the individual plant are illustrated in Fig. 9. The left-hand side flow in Fig. 9 is when a digitalized MCR as shown in Fig.7 will be developed as the standard design. It starts from the functional requirement process to reduce functional requirement specification on the basis of both the development objective and functional requirement, proceed to standard design process to be made on the basis of not only the development objective and functional requirement but also design requirement, conduct on V&V process and finally reduce the resultant standard design specification. On the other hand of standard MCR design, the right-hand flow in Fig. 9 corresponds to the fabrication design of individual MCR in an actual plant. In this case, the original standard design specification will not be directly applied but modify it in accordance with the actual plant condition and design requirement. The modified specification will be then checked through the V and V process to reduce the fabrication design specification to be referenced for real fabrication of the MCR.

Both international standards of IEC 60964 [8] and NUREG-0700 rev.2 [9] were utilized in setting up this domestic guide JEAG4617-2005.

5.3 Actual Introduction of Digital I&C and HMIT System in Japanese Nuclear Power Plants

The nuclear utilities and vendors view the relation between the codes and guides by the Japan Electric Association as described in both 5. 1 and 5.2 by the following way. The codes give more clear information on the functional requirements than by the regulatory requirements for designing the facilities, systems, components and equipments. The guides recommend useful information on usable models, methods, procedures, etc, for designing and fabricating the facilities, systems, components and equipments in accordance with the specifications given by codes.

Table 10. Code on Equipment Designing to Prevent Operation Error in Main Control Room

No.	Target	Content
1	Monitoring and operation area, main control room	Comfortable environmental condition (temperature, illumination, noise)
2		Layout and work space to prevent undue workload to the operators (task allocation between man and machine, between operators, information share, etc.)
3	Main control board	Panel layout
4		Display system, alarm system, operator support system
5		Control functions (easy operation to prevent human error, interlocks) , visualize state of automatic operation
6		Application of verification and validation process for the development, implementation and replacement

Table 11. Guide on Development and Design of Computerized Human Interface of Main Control Room

Subject	Contents	
1.Functional requirements	1.1 Ensuring monitor and operation functions for every plant state	
	1.2 Selection of necessary equipments of monitor and operation functions to ensure safety functions	
	1.3 Ensuring time allowance of operators' operation action	
	1.4 Reliability maintenance of information integration function by computer	
	1.5 Notify loss of its function	
2.Design requirements	2.1 Information system (appropriate monitoring and operation system, information navigation)	
	2.2 Information presentation (layout, shape, integration, fit to operators' habit, readability and visibility, presentation format, hardware display)	
	2.3 Controllers and actuators (consistent layout, shape, grouping, selection and operation method fit to operators' habit, touch operation, basically no GO output by a single operation, etc.)	
	2.4 Alarm system (alarm reduction, display of first hit alarm, alarm hierarchy by importance, operators' reset function, etc.)	
	2.5 Large display (Visibility by all operators, automatic display change, control by operator, etc.)	
	2.6 Operation support system (Presentation of necessary support information and its explanation, etc.)	
	2.7 Work space (ergonomics design of layout, shape, illumination, etc.)	
	2.8 Selection of auxiliary equipments in the main control room	
3.Development process and fabrication design process	See Figure 9	
4.Verification and validation process	4.1 Formation of evaluation team (operator, human interface designer, ergonomist)	
	4. Procedure and contents of verification & validation	4.2.1 Reduction of evaluation items
		4.2.2 Setting evaluation criteria
		4.2.3 Evaluation method (Desk-top evaluation by check list, Mock up, Dynamic evaluation, Simulator experiment)
		4.2.4 Selection of events to be evaluated
		4.2.5 Feedback to the design specification and re-evaluation
		4.2.6 Documentation

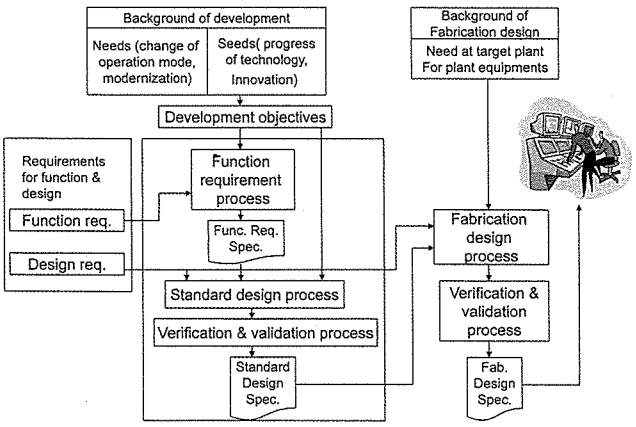

Fig. 9. Development Process and Fabrication Design Process of Computerized Human-machine Interface

At this point, the author of this article would like to summarize by what way the real introduction of digital computers for the I&C and HMIT systems had been conducted in the nuclear power plants in Japan from the limited experience of the late 80s and early 90s.

5.3.1 Introduction of Digital Computers for Nuclear I&C and HMIT by Kansai Electric Power Company

The Kansai Electric Power Company (KEPCO) is the monopoly company of electric power supply in the Kansai area of Japan. The KEPCO had been the leader company of PWR introductions in Japan since the first commercial operation of Mihama No.1 unit in November 1970. KEPCO

has now eleven PWR units in three nuclear power stations all located in the Wakasa Bay area.

The application of digital computers in PWR plants at KEPCO had been directed into three areas: (i)expansion of plant automation, (ii)modernization of main control room (MCR), and (iii)extended capability of data logging, transmission and communication for plant management. The author's report [10] summarizes the first two issues of (i) and (ii) at the time of 1994.

According to Ref.[10] the expansion of plant automation in PWRs by digital computers had started to replace the analog control systems with digital computers from peripheral independent processes such as waste management system to digitalization of various plant control systems by using micro processors. Introduction of micro processor based digital control systems for most of non-safety class systems had been successfully realized in KEPCO's Ohi No. 3 Unit in 1991 and No.4 Unit in 1993.

The application of micro-processors for safety-class components (reactor protection systems and engineered safety facilities) together with the full digital MCRs had been extensively conducted for both APWR and ABWR by the cooperation of all nuclear utility companies and nuclear power plant vendors in Japan in the early 1990s. From the preceding development stages of non safety class micro processor based control system until the time of safety class digital safety systems, the V and V technologies for software reliability of micro processor based digital control system in nuclear power plants had been established in nuclear vendors by utilizing POL (problem oriented language) with constant time step control by avoidance of complicated multiple steps or nesting in programming. The software tools by graphical interface for easy programming and error checking had been also developed based on POL. The development processes of full digital safety systems and full digitalized MCRs are the same basis technologies being established during the realization of full digitalized I&C and HMIT for both ABWR and PWR in Japan, and the experience and knowledge obtained through the developments had been said to be documented as the relevant industrial codes and guides by the JEA.

5.3.2 Proving Test of the Reliability of Nuclear I&C

The test of proving the reliability of nuclear I&C systems for both BWR and PWR in Japan was conducted between 1984 and 1989 by Nuclear Power Engineering Test Center under the sponsorship of MITI [11]. The targets equipments had been (i) preamplifiers and motor modules of SRM and IRM of reactor neutron instrumentation, (ii) pressurizer heater terminal, (iii)high range area monitor, (iii) instrumentation rack, and (iv)software logic controller. The conducted proving test was composed by two kinds of test: (i) performance degradation by the continuation of long time normal power operation (thermal aging, radiation aging, vibrating aging and mechanical aging), and (ii) performance endurance test under accident conditions of temperature, steam, radiation and chemical spray. The test results of this proving test were reflected to the establishment of an industrial guide by the JEA in Table 6: Guide on verifying anti-environmental performance of Instrumentation and control systems of safety functions(JEAG 4623-2008). Since this proving test had been made under LOCA condition, it cannot be said that the reactor instrumentation may endure the severe accident condition as was occurred at the Fukushima Daiichi accident.

5.3.3 Comparison of APWR's I&C Design with EPRI URD

In Ref [10], it is interesting that the inter-comparison was made between the design conditions of Japanese APWR and those of EPRI's URD for advanced light water reactors [12]. Among many compared items, the following items are interesting ones: (i)the MTBF (mean time between failure) of total system was five years by EPRI URD, while that was 100 years by Japanese APWR design, (ii) MTBF of key system parts was 14 days by EPRI URD while that by Japanese APWR, 1 months, (iii) MTTR (mean time to repair) by EPRI URD was 4 hours average with 8 hours maximum, while the target of MTTR was 30 minutes by Japanese APWR design, while (iv) there is a great discrepancy on severe accident preparedness between EPRI URD and Japanese APWR design. That is to say, Japanese APWR design aims at higher reliability for normal operation and maintenance, whereas it lacks on the provision for nuclear severe accident. Concretely speaking, there is no correspondence between EPRI URD and Japanese APWR design as to the provision of Technical Support Center (TSC) and Emergency Operating Facility. It is also notable that in Ref.[10] it pointed out the need of introducing various I&C system for Japanese APWR with respect to severe accident management.

6. IMPACT OF FUKUSHIMA DAIICHI ACCIDENT TO NUCLEAR I&C AND HMIT DESIGNING

Now it is a common understanding in Japan as the main reason why four units of TEPCO's Fukushima Daiichi nuclear power station failed after the largest earthquake followed by highest Tsunami in Japanese historical record. Before Fukushima Daiichi accident, severe accident provision in nuclear power station had been left to utility's voluntary activity reviewed by national regulatory body in Japan (both Nuclear Safety Commission (NSC) and Nuclear and Industrial Safety Agency (NISA). TEPCO could not prevent the core melt and hydrogen explosions in four units one by one after the Tsunami hit the mainland. After the Fukushima Daiichi accident, TEPCO almost became bankrupt for various reasons related to the Fukushima Daiichi accident, and both NSC and NISA were

dissolved to form newly Nuclear Regulation Authority (NRA) under the Ministry of Environment. Now the NRA has been busy with reforming all laws and orders concerned with nuclear regulation in Japan, where the legislature reformation of severe accident prevention and counter-measures are central issues to be revised until July 2013 [13], in order to cope with the restart application by the electric power companies of all shutdown nuclear power plants in Japan after the Fukushima Daiichi accident.

This redirection of nuclear safety regulation also requested that the I&C and HMIT designing should cope with the level 4 in Table 2 of five defense levels of nuclear safety from the former levels 2 and 3. Since the direct cause of Fukushima Daiichi accident was largely the earthquake and the ensuing tsunami, it was already pointed out the necessities to take into account of the following enforcement into the present nuclear I&C system: (i) Addition of I&Cs to endure severe accident- Pressure, water level, temperature sensors to endure severe accident condition, and addition of filtered vent with enforced communication channels, and (ii) Backup electric power preparation for maintaining air condition, illumination, and radiation filter in MCR.

7. CONCLUDING REMARKS

A comprehensive review on the technical standards on human factors (HF) design and software reliability maintenance for digital instrumentation and control (I&C) system with human-machine interface technology (HMIT) in Japanese light water reactor nuclear power plants (NPPs) was given in this paper mainly by introducing the relevant activities at the Japan Electric Association to set up many industrial standards within the traditional framework of nuclear safety regulation in Japan.

In Japan, the Fukushima Daiichi accident occurring on March 11, 2011 had a great impact on nuclear regulation and nuclear industries where concerns by the general public about safety have heightened significantly. However for the part of HF design and software reliability maintenance of digital I&C and HMIT for NPP, the author believes that the past practice of Japanese activities with the related technical standards can be successfully inherited in the future, by reinforcing the technical preparedness for the prevention and mitigation against any types of severe accident occurrence.

ACKNOWLEDGEMENTS

The author of this paper would like to express his appreciation to Mr. Yoshiaki Tamura of the Japan Electric Association, for his kind help to the author's introducing the activities of the Japan Electric Association.

REFERENCES

[1] G. Petrangeli, *Nuclear Safety*, 1st ed., Chapter 9 Defence-in-depth, Elsevier Butterworth-Heinemann, Oxford (2006).
[2] A.Mosleh, "Procedure for Treating Common Cause Failure in Safety and Reliability Studies"; In : Appendix A. A Data Classification System, EPRI NP-5613, pp.A.1~A.15 (1988).
[3] J. Reason, *Human Error*, Cambridge University Press, Cambridge (1990).
[4] T. Mishima, H. Nishi, Y. Tamura and Y. Nakagawa, "Development and Design Guideline for Computerized Human-Machine Interface in the Main Control Rooms of Nuclear Power Plant", *International Journal of Nuclear Safety and Simulation*, vol.1-2, pp.166-169 (2010).
[5] T. Tanaka, I.Ueyama, Y.Tamura and K.Nakagawa, "Standardization on Evaluating Instrumentation Drift of Safety Protection Systems as an Industrial Guideline in Japan", *International Journal of Nuclear Safety and Simulation*, Vol.2-1, pp.77-82 (2011).
[6] Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Verification and Validation", IEEE Standard 1012-1998 (1998).
[7] Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations", IEEE Standard 7-4.3.2-2003 (2003).
[8] International Electrotechnical Commission, "Design for Control Rooms of Nuclear Power Plants", IEC 60964(1989).
[9] U.S. Nuclear Regulatory Commission, "Human-System Interface Design Review Guidelines", NUREG-0700 rev.2 (2002).
[10] H.Yoshikawa, T.Magari, Y. Yamamoto, "A Review on Progress of Man-Machine Interface System Design for Japanese PWRs", Technical Reports of the Institute of Atomic Energy Kyoto University, Report No.214 (1994).
[11] A. Sekiguchi, H. Yoshikawa, K. Takumi, K. Shibata, "Proving Test on the Reliability of Electrical Equipment and Instrumentation for Nuclear Power Station", *Proc. Int. ENS/ANS Conf. on Thermal Reactor Safety (NUCSAFE 88)*, Vol.4, pp.1386-1395, Avinion, France, Oct.2-7, 1988.
[12] Electric Power Research Institute,"Advanced Light Water Reactor Utility Requirement Document, Volume II, ALWR Evolutionary Plant, Chapter 10. Man-Machine Interface Systems", (1992).
[13] Homepage of Nuclear Regulation Authority, Japan. See URL(http://www.nsr.go.jp/english/)