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 accompanying 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.