Developmental study of advanced human system interface design method for digital I&C+HMIT -a preliminary study for passive safety PWR AP1000

MA Zhanguo[1], YOSHIKAWA Hidekazu[1, 2], NAWAZ Amjad[1], and YANG Ming[1]

1. Foundational Science on Nuclear Safety and Simulation Laboratory, College of Nuclear Science and Technology, Harbin Engineering University、Harbin 150001, China, (E-mail address:mazhanguo2013@163.com)
2. Professor Emeritus Kyoto University, Kyoto, Japan

Abstract: A new methodology of designing and evaluation of digital HSI (human system interface) is proposed for the support of plant operators' supervisory control of fully automated large-scale complex NPPs (nuclear power plants). The proposed method utilizes the object-oriented software for plant DiD (defense-in depth) risk monitor with the combination of accident simulation by an advanced nuclear safety analysis code RELAP5/MOD4. The practical developments for the details of the proposed methodology are in progress by an example practice for the SBLOCA (small break loss of coolant accident) case of passive safety PWR (pressurized water reactor) AP1000.

Keyword: human system interfaces; supervisory control; plant DiD risk monitor; RELAP5/MOD4; AP1000

1 Introduction

There is a firm belief in nuclear safety regulation that human error is typical one of source of trouble and accident so that human element should be excluded out of the control loop of the automatic safety systems. Even though, in the plant, the engineered safety feature systems are designed to cope with the design basis accident (DBA) when the automated systems are working as designed and planed. At this situation the human are work as monitoring. However, even if complete automated system is realized, there will be a possibility of failure of automated system. So during the DBA in addition with the automated system failures, the human must take over the control of the plant to ensure the safety. Therefore under the circumstance human element cannot be excluded out of the safety control systems. But how to include "human element" in the safety control system is a traditional paradox in "supervisory control".

The authors of this paper would like to propose a new ideas for designing and evaluating advanced HSI (Human System Interface) of the I&C (Instrumentation and Control) + HMIT (Human Machine Interface Technology) for such advanced nuclear power reactor (NPP) based on inherent safety concept. A passive safety PWR (AP1000) [1] will be taken as the concrete target of this study because AP1000 adopts many automatic safety functions to exclude human intervention.

2 Framework of advanced HSI design method for digital I&C+HMIT

The current issue of the advanced HSI design is to answer what will be appropriate human role to maintain high safety level for any level of operation. The purpose of the presented authors' study is to answer by developing experimenting tools by the integrated use of two types of computer simulation, *i.e.*, plant simulation and knowledge based information processing. As shown in Fig.1, it is the framework to integrate the plant simulation and knowledge based information processing for the advanced HSI design. The plant simulation simulates all the aspects of plant such as the transient and the accident of the plant. The plant behavior is simulated under all the possible conditions and the plant sequences are acquired. Then the knowledge base of the simulated plant is built up and the plant configurations in the plant DiD risk monitor [2] software can be defined as the different actors that are defined to simulate the interaction behavior in the plant *e.g.*, PLANT actor which is defined to simulate the nuclear plant, the OPERATOR actor and SUPERVISOR actor which are defined to simulate the operators and supervisor respectively in the main

Received date: November 24, 2016
(Revised date: November 29, 2016)

control room. Last, the plant interactions between the actors are simulated to help the design of the HSI and design the human role in the plant from normal operating to coping with the accidents that may occur during the plant operation.

The proposed idea is a methodological framework for both design and evaluation of digital I&C + HMIT system by introducing the following three elements: (i) automatic diagnosis, (ii) automatic selection of operation procedure, and (iii) co-ordination of bi-directional communication between human (operators) and machine (automated system), with automatic processes of the above functional modules of (i) and (ii). The essence of designing and evaluating the HSI composed by those three elements can be schematically depicted as shown in Fig. 2.

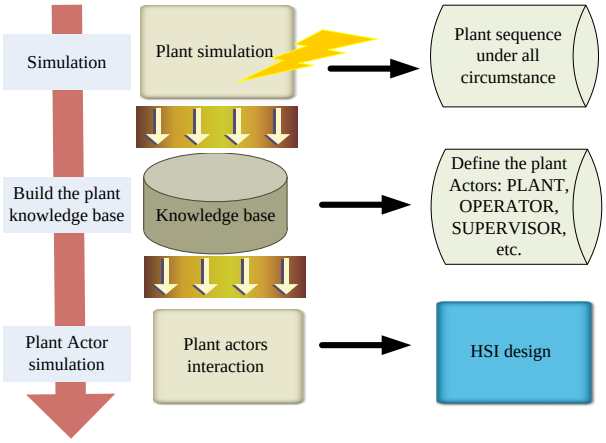

Fig. 1 Framework of integrating the simulation and knowledge based information processing.

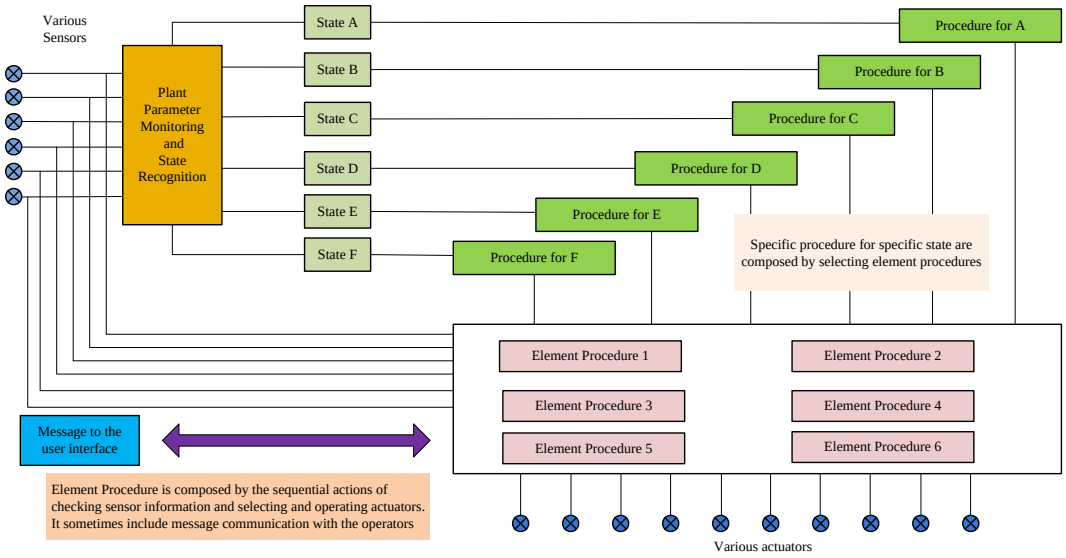

Fig. 2 Basic scheme of designing and evaluation of HSI for digital I&C + HMIT system.

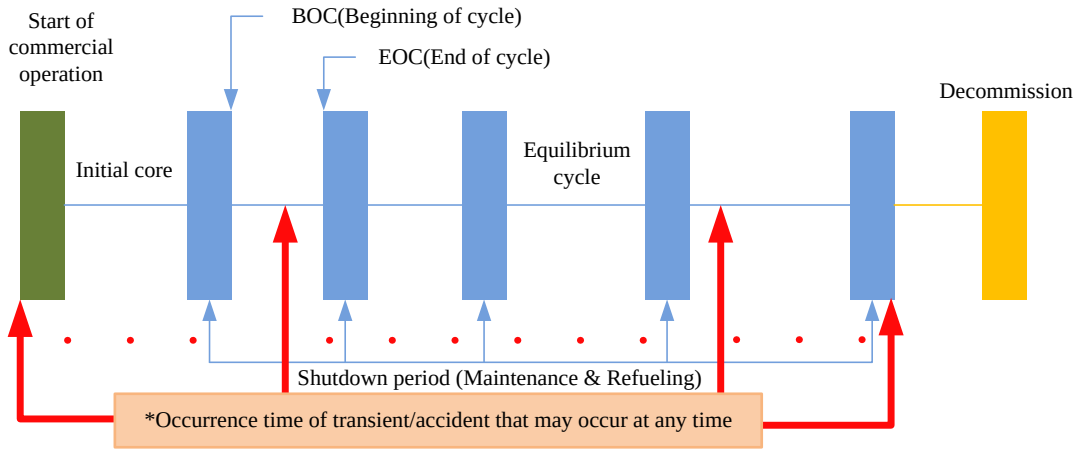

Fig.3 Different stages of plant operation in the whole life.

The automatic diagnosis element recognizes the plant states by monitoring the plant parameters. The procedures to cope with each corresponding plant states are automatically generated from the selection of the element procedures. Follow the procedures, the plant is operated by the various actuators and the message and parameters are displayed to the user interface.

For the practical design of HSI for real NPPs, the plant accident simulation should be performed by combination of high-level multi-physics reactor engineering computation such as steady state (SS) reactor core burnup calculation, SS thermal-hydraulic calculation in the reactor vessel including the reactor core and a proper plant accident simulator program for covering the whole plant life of the NPP. Wherein the essential points of the plant accident simulation can be summarized by the following arguments:

(i) All situations of plant conditions should be taken into account as depicted in Fig. 3. As shown in Fig.3, whole plant life has to be taken into account, *i.e.*, from the start of commercial operation until the decommissioning, and at any time in different cycles. And the occurrence time of transient/accident should be not only operation stage but also during shutdown.

(ii) Different types of physical phenomena will proceed not only during steady state operation but also in transient/accident situations. The analytical consistency of those different types of physical phenomena as is shown in Fig.4 has to be maintained for reactor core analysis such as to consider burnup effect of the whole reactor core and fuel pin irradiation effect, while reactor physics calculation and thermal-hydraulics calculation of the reactor core.

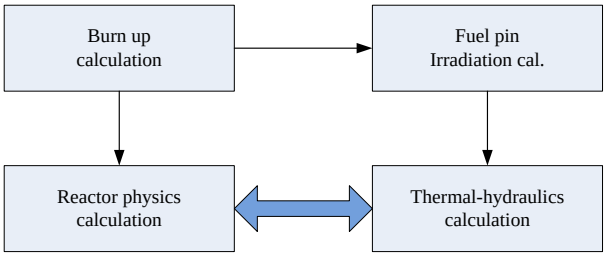

Fig.4 Different types of physical phenomena in the nuclear fuel and the reactor core.

(iii) Balancing the whole parts of the plant system should be considered on thermal-hydraulics aspect. That is, as shown in Fig.5, transient fuel pin behavior, reactor core characteristics, reactor vessel thermal-hydraulics, whole loop system, and whole plant system dynamics should maintain consistency between the different parts of thermal-hydraulic calculation.

(iv) Special consideration should be given not only on initial condition but also for disturbance condition to conduct on the respective simulation. Table 1 summarizes specific aspects for the consideration on both the initial condition and the setting of disturbances.

In order to improve both the efficiency and accuracy of nuclear safety analysis, the advanced simulation method has been long anticipated by utilizing AI (artificial intelligence). And in U.S.A., an emerging project called RAVEN (Reactor Analysis and Virtual control Environment) has been in progress at INL (Idaho National Laboratory) [3, 4].

Such a new trend of advanced computer simulation in nuclear safety analysis will be worthwhile to watch, but in this authors' work, the authors will utilize the conventional light water reactor safety analysis code RELAP5/MOD4[5] for performing various types of accident analysis for AP1000, because the major subject of this paper is related with the designing of advanced HSI.

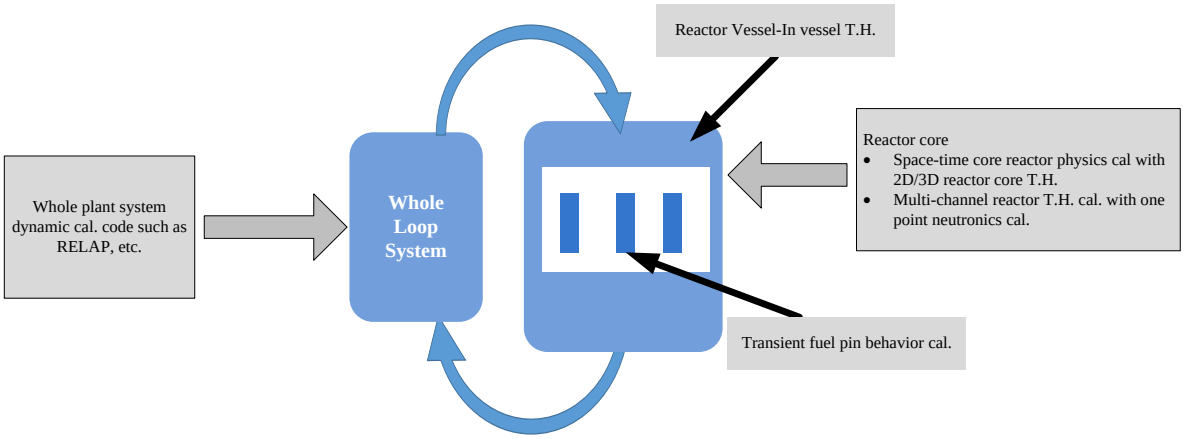

Fig.5 Different parts of thermal-hydraulic calculation in the whole plant system.

Table 1 Specific aspects of plant simulation for both of initial condition and disturbance consideration.

Assumed conditions	Selection of occurrence time for transient/accident	Remark
Initial condition	Initial Plant condition	Plant configuration based on state of plant
	Initial core condition such as fuel rod, reactor power shape, coolant condition, reactivity feedback condition, *etc.*	Result of SS irradiation calculation
Disturbance condition	Type of transient/accident scenario	LOF, TOP, LOCA, ATWS, *etc.*
	Influential factors to be assumed	External factors, human factors, common cause factors, *etc.*

3 Preliminary study for AP1000

3.1 Digitalized I&C+HMIT system of AP1000

The AP1000, the 3.5th generation PWR developed by Westinghouse, has the unique safety features of excluding human element in emergency operation by adopting inherent passive safety concept with the extensive use of automatic control. The plant construction of AP1000 has been progressing both in China and U.S.A.

Those AP1000 plants now under construction have been adopting the latest digital I&C+HMIT technologies, and this tendency is the same as those used in the latest plants of conventional PWRs. One example of the configuration of the digital I&C+HMIT system is shown in Fig. 6. The configuration example of various digitalized subsystems of the AP1000 is also indicated in Table 2. As you see from Table 2, different types of digital platforms including the CPU based digital systems (*e.g.* PMS, PLS and DDS) and FPGAs (Field programmable gate arrays) based digital system (*e.g.* DAS) have been employed for the diversity of the equipment to maintain the reliability requirement of the safety subsystems.

Table 2 Example subsystems configuration of digital I&C+HMIT of AP1000 by Westinghouse

Abb.	Full name	Notes
PMS	Protection and Monitor System	Digital platform (ABB-AC160) Common Interface Module (CIM): use FPGA
DAS	Diverse Actuation System	Originally designed by FPGA. But by British Regulatory Review recommended WEC analogue 7340 series equipment
PLS	Plant control System	Digital platform (Ovation platform)
DDS	Data Display and Processing System	Digital platform (Ovation platform)
OCS	Operation and Control center system	
RMS	Radiation Monitoring System	
IIS	In-core Instrumentation System	
SMS	Special Monitoring System	
TOS	Turbine Operation System	

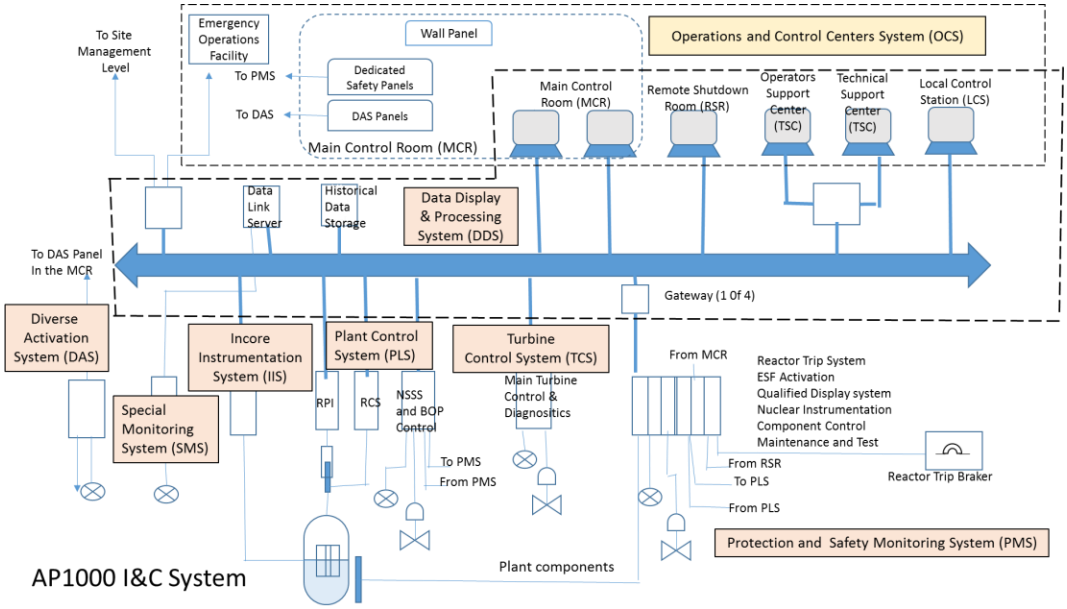

Fig.6 Configuration of digital I&C+HMIT of AP1000 by Westinghouse. [1]

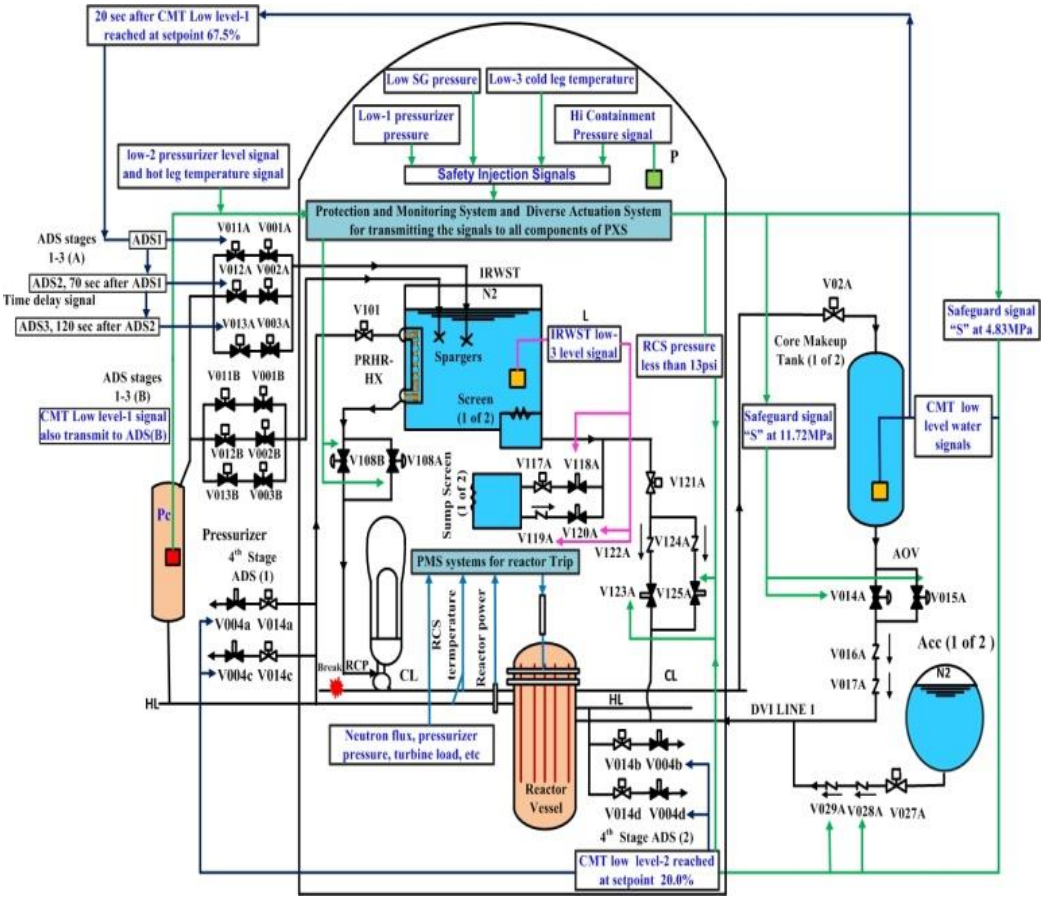

Fig.7 Configuration of passive safety system of AP1000 assumed in this study. [8]

3.2 Passive safety system of AP1000

3.2.1 Configuration of passive safety system

The configuration of passive safety system of AP1000 assumed in this study is illustrated in Fig.7, and the assumed subsystem configuration with the input-output signals and the activation conditions are shown in Table 3.

3.2.2 Working of passive safety system in SBLOCA

With the gradual decrease of reactor coolant pressure after the onset of SBLOCA in AP1000 plant,

individual subsystems will be activated and then turned off as the conditions given in Table 3. The temporal sequence of the activated subsystems is shown in Fig. 8.

3.2.3 Safety analysis of AP1000 by RELAP5/MOD4

The temporal sequence of individual subsystems as shown in Fig.8, is the "ideal situation" when every subsystem would work successfully as it planned in advance. That is, every sensor measures the right signal correctly, every alarm handling facility processes the logical judgment rightly to generate proper warning or trigger the right actuator correctly. However, if there is any failure in any step, then the behavior of the plant will become a different process than that given in Fig. 8.

There would be many possibilities of event progression or scenario if something would fails, and the probability of any branching of event progression may be estimated by utilizing the fault tree analysis/event tree analysis (FTA/ETA) conventionally used in probabilistic risk assessment (PRA)[6, 7].

Table 3 Assumed subsystem configuration with the input-output signals and the activation conditions [9, 10]

Activation systems	Phases of LOCA (injection and recirculation phases)		Detecting device	Actuation signals of RPS, PXS and PCCS	Time (sec) from LOCA	Components to be used for actuation in different phases
Reactor Protection system	Blow-down phase	Reactor scram (reactor trip)	Pressure sensors and temperature sensors	Hi-neutron flux, low coolant flow, over temperature. RCS 12.41Mpa,	5.2 sec	Reactor trip switchgear breakers.
		Safeguard signal "S"		RCS 11.72 MPa	6.4 sec	Safety actuation system
		Steam generator feedwater		After trip signals	8.4 sec	Feedwater control valve close
Passive Core cooling system		CMT injection system	RCS pressure sensor in pressurizer	Low-2 pressurizer pressure, safety injection signals, safeguard S signal at 11.72Mpa	9.4 to 85 sec	CMTs tanks, valves V014A to V017A
		PRHR system			9.4 to 3600 sec	PRHR-HX, V108A/B, V101
		Main steam isolation		After "S" signal	11.2sec	Isolation valves start to close
		RCP trip		After "S" signal	12.4sec	Pump trip
	Re-fill/ Reflood Phase	Accumulator start which stop CMT injection	RCS pressure sensor	S signal at 4.83Mpa RCS pressure	85 to 418 sec	ACC Tank, valves V027A to V029A
		CMT start again after Acc empty	Certain RCS pressure value	Accumulator empty signal	418 to 1800	CMTs tanks, V014A to V017A
	ADS blow-down Phase	ADS stage 1 (A/B)	CMT water level sensor	20sec after 67.5% liquid volume fraction in CMT	750 to 3600 sec	ADS 1, V001A/B, V011A/B
		ADS stage 2 (A/B)	Time delay timers	70sec after ADS-1 actuation	820 to 3600 sec	ADS2,V002A/B, V012A/B
		ADS stage 3 (A/B)	Time delay timers	120sec after ADS-2 actuation	940 to 3600 sec	ADS3,V003A/B, V013A/B
		ADS stage 4 (a/b/c/d)	Time delay timers	20.0% liquid volume fraction in CMT and 551sec after ADS3 actuate	1491 to 3600 sec	ADS 4, V004a/b/c/d, V014a/b/c/d
	IRWST injection phase	IRWST gravity injection lines flow	RCS pressure & CMT water level sensor	RCS pressure less than 89.6 KPa/13psi plus containment pressure	1800 to 3600 sec	IRWST tank, IRWST screen1, V121A to V125A
	Recirculation sump phase	Recirculation injection lines flow	IRWST low level water sensor	IRWST low-3 level signal	3600 to 6000sec	Sump, recirculation screen 1, V117A, to V120A
Passive containment cooling system	Containment cooling	Natural circulation of Air with water spray	Containment's temperature and Pressure sensors	Hi-2 containment pressure signal59psig, Hi containment temperature	30 sec to 72 hours after LOCA	PCCWST, V001A/B/C, V002A/B/C

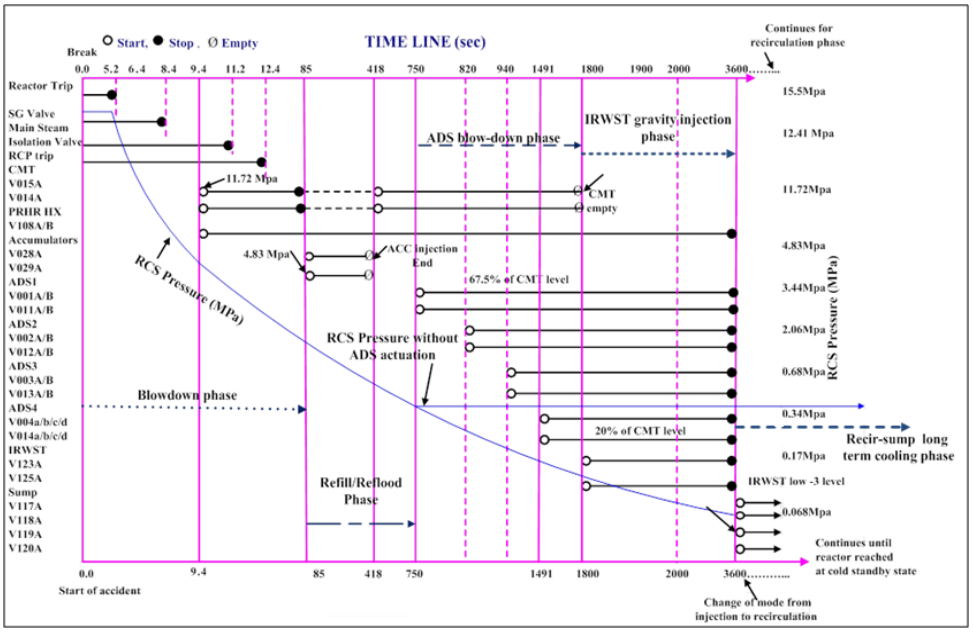

Fig. 8 Activation sequence of safety system in case of SBLOCA.[8]

When the possibility of unanticipated event progression would be very high by conducting FTA/ETA, what would happen in the plant system in such case could be investigated by computer simulation by using advanced safety analysis code such as RELAP5/MOD4. And moreover, there would be more advanced method such as RAVEN for more efficient and reliable conduction of PRA by the combination of FTA/ETA and RELAP5/MOD4.

3.2.4 Automatic monitoring of passive safety system by plant DiD risk monitor

It is said that AP1000 does not need any human intervention by the adoption of inherent passive safety with many automatic functions, which means that there are no need of operators in the main control room nor need of operators work. On the contrary, the operators of AP1000 have to confirm whether those safety functions of AP1000 work as they are planned. And if something would fail they have to resolve the problem just in time so that the plant may not develop into dangerous state. This is the same manner as that requested in conventional NPPs, and this is the essential feature of supervisory control of automated systems.

At this point, the authors of this paper would like to go back to the proposed scheme as introduced in Fig. 2, in order to set to work on developing effective HSI to support the supervisory operator of AP1000 by the combination of RELAP5/MOD4 accident simulation as mentioned in 3.2.3. In the authors' preliminary study towards this goal, the following issues should be studied in advance:

(1) Scenario classification of accident progression on the accident simulation cases conducted by RELAP5/MOD4.
In this paper, the following two cases were calculated by RELAP5/MOD4 by assuming that the both are high possibility of occurrence: (i) SBLOCA with successful reactor shutdown, and (ii) SBLOCA and failure of reactor shutdown. The case (ii) is the situation what is called as ATWS (anticipated transient without scram). In this case, it will be difficult to recover the plant state by the safety subsystems given in Table3. In fact, if the case (ii) happens in AP1000, the other safety subsystem called DAS (diverse activation system) should work to prevent from developing to an unfavorable reactor condition. Even in case (i), if any of the subsequent subsystems of PXS (Passive core cooling system) would fail to work, there would be the possibility of developing into various worried situations which might lead to a reactor core melt accident.

(2) Reduction of space-time co-relationship between plant I&C signals and the computed output of accident analysis by RELAP5/MOD4.

The measured signals by the plant I&C are calculated from the simulated variable signals by the first order input and output model. And the errors are estimated as the random errors that follow the Gaussian distribution.

(3) Hierarchical representation of the configuration of AP1000 plant as seen from safety systems.
The hierarchical representation is modeled in the plant DiD risk monitor software. The top level is the actor level and the following level is the main function or sub systems in corresponding actor. Then the last level is the detailed devices for each system. There are different hierarchical models for different configurations of the plant.

(4) Anomaly detection from the input-output signals of I&C system with the logical judgment for the part of the automated systems.
The calculated measured signals are connected with the plant DiD risk monitor and the setpoints and logics are modeled in the plant DiD risk monitor software. The measured signals are inputted to the plant DiD risk monitor during the simulation to detect the anomaly and calculate the logic.

(5) Estimation of risk as the possibility of reactor core melts accident, and the generation of proper instruction to avoid risk in accordance with the risk level.
The risk monitor calculates the risk and generates the message and instructions for the operators using all the inputs from the simulation and the plant knowledge base.

The design steps are illustrated in Fig. 9. Normally the FTA/ETA is firstly conducted for the plant systems and the scenarios are selected based on the analysis result. Then RELAP5/MOD4 simulation (item 1) is carried out to build the knowledge base (item 3) using the plant simulation results. The measured signals (item 2) are calculated from the simulated variable signals using the first order model with random errors. Then the calculated measured signals are connected with the automation systems (item 4) to simulate the interactions between the actors in the plant DiD risk monitor system. Lastly the core melt risk is estimated and the instructions and messages are generated to help the operators. Currently, the authors have been engaged in the works on how to design and implement into the risk monitor system so as to realize online real time processing. Wherein, the connection with the results of RELAP5/MOD4 simulations will be utilized for the cases of the accident cases of SBLOCA with scram, failed scram and delayed scram.

Then by utilizing those information (1) to (5), the authors' developed software system of plant DiD risk monitor[2] will be applied to realize as an integrated HSI for AP1000 operators to help them to monitor the behaviors of safety subsystem and inform them by proper message in case of risky state. The image of the display by this support system will be as shown in Fig. 10.

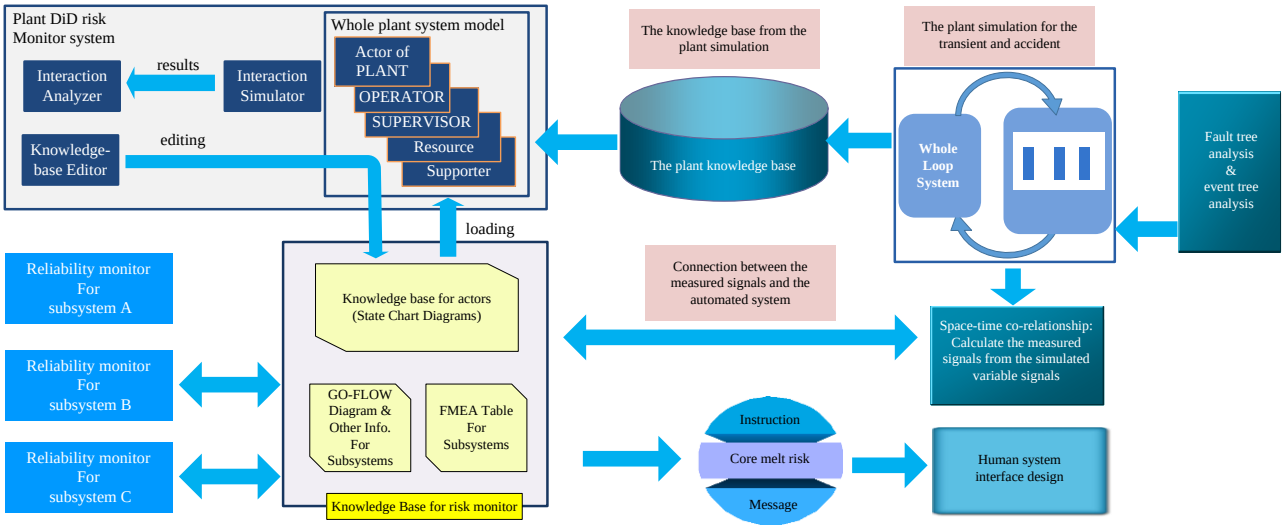

Fig. 9 The HSI design work steps.

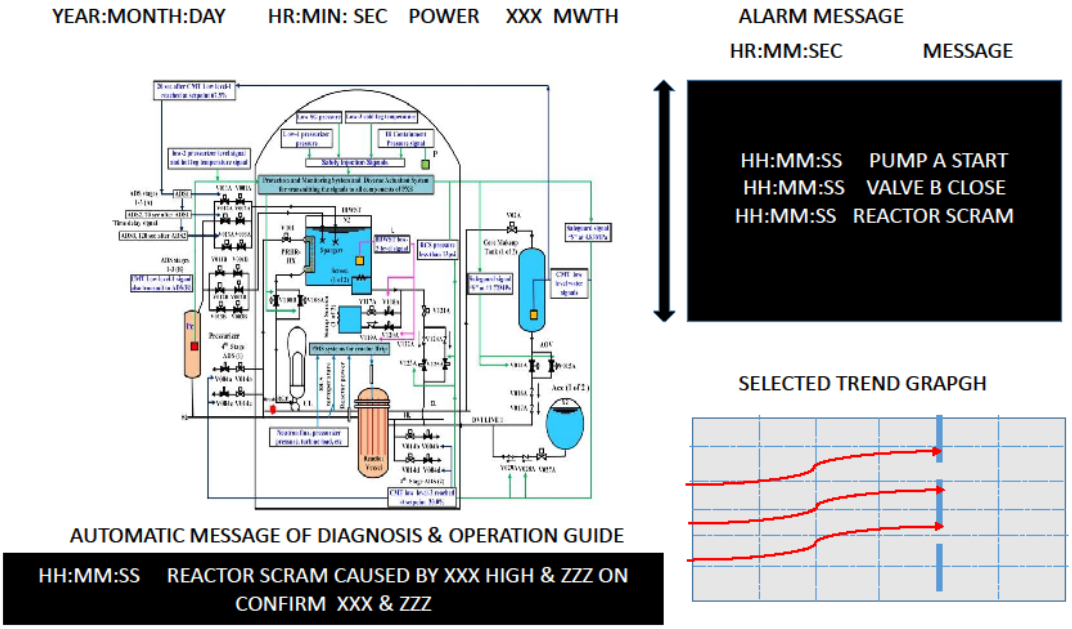

Fig.10 Display image of the proposed HSI for a AP1000 example systems.

4 Conclusions

In order to strengthen nuclear power plant safety, many person who believe human is the source of failure have been claiming to employ more features of inherent passive safety and use of full automatic control, in order to exclude human elements from the safety control system. However, it always remains the paradox of supervisory control that human has to cope with difficult situation when fully automated system fails to work.

In this study, a new methodology of designing and evaluation of digital HSI was proposed for the support of plant operators' supervisory control of fully automated large-scale complex NPPs. The proposed method will utilize the object-oriented software for plant DiD risk monitor with the combination of accident simulation by an advanced nuclear safety analysis code RELAP5/MOD4. The practical development for the details of the proposed methodology is in progress by an example practice for the SBLOCA case of passive safety PWR AP1000.

Nomenclature

AI	Artificial intelligence
ATWS	Anticipated Transient without Scram
DAS	Diverse Actuation System
DiD	Defense in Depth
FPGA	Field Programmable Gate Array
FTA/ETA	Fault Tree Analysis/ Event Tree Analysis
HSI	Human System Interface
HMIT	Human Machine Interface Technology
I&C	Instrumentation and Control
INL	Idaho National Laboratory
NPP	Nuclear Power Plant
PXS	Passive Core cooling system
PCCS	Passive containment cooling system
PRA	Probabilistic Risk Assessment
PWR	Pressurized Water Reactor
RAVEN	Reactor Analysis and Virtual control Environment
SBLOCA	Small Break Loss of Coolant Accident
SS	Steady State

References

[1] WESTINGHOUSE: "AP1000 European Design Control Document", rev 1. Westinghouse Electric Company (2011).

[2] MA, Z., and YANG, M.: Knowledge-based software design for Defense-in-Depth risk monitor system with the preliminary study for AP1000 application, Nuclear Safety and Simulation, Vol. 7, Number 1, July 2016, 74-87.

[3] ALFONSI, A., RABBIT, C., MANDELLI, D., COGLIANTI, J.J., and KINOSHITA, R.A.: RAVEN as a tool for dynamic probabilistic risk assessment: software overview, International Conference on Mathematics and Computational Methods Applied to Nuclear Science & Engineering (M&C 2013), Sun

Valley, Idaho, U.S.A., May 5-9, 2013, American Nuclear Society, La Grange Parl, IL. 2013.

[4] MANDELLI, D., ALFONSI, A., SMITH, C., and RABIT, C.: Generation and use of reduced order models for safety applications using RAVEN, Transactions of the American Nuclear Society, Vol.113, Washington, D.C., November 8-12, 2015.

[5] FLETCHER, C.D., and SCHULTZ, R. R.: RELAP5/MOD4 Code Manual Volume V: User's Guidelines, NUREG/CR-5535, INEL-95/0174, June 1995.

[6] U.S. NRC: Probabilistic Risk Assessment (PRA),

[7] http://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html (As of July 31, 2016)

[8] HASHIM, M., YOSHIKAWA, H., and YANG, M: Addressing the fundamental issues in reliability evaluation of passive safety of AP1000 for a comparison with active safety of PWR, Nuclear Safety and Simulation, Vol. 4, Number 2, June 2013, 147-159.

[9] Westinghouse Electric Company, AP1000 design control document. Accident analysis. Westinghouse Electric Company; 2009.

[10] YANG, J., WANG, W., QIU, S., TIAN, W., SU, G., and WU, Y: Simulation and analysis on 10-in. cold leg small break LOCA for AP1000, Annals of Nuclear Energy, 2012, 81-89.