DEVELOPMENTAL STUDY OF ADVANCED HIS DESIGN METHOD FOR DIGITAL I&C+HMIT OF PWR PLANT

Hidekazu Yoshikawa[*]
College of Nuclear Science & Technology, Harbin Engineering University
Harbin 150001, China
yosikawa@kib.biglobe.ne.jp

ABSTRACT

A new conceptual frame of how to design and validate a digital HIS (human interface system) on an innovative numerical simulation basis is proposed for the support of plant operators' supervisory control of various types of automated complex NPPs (nuclear power plants). The proposed conceptual framework utilizes the object-oriented software for plant DiD (defense-in depth) risk monitor with the combination of nuclear reactor accident simulation by an advanced nuclear safety analysis code RELAP5/MOD4. The conceptual frame proposed in this paper will be applied for an example practice for the SBLOCA (small break loss of coolant accident) case of passive safety PWR (pressurized water reactor) AP1000.

Key Words: human interface systems, supervisory control, plant DiD risk monitor, RELAP5/ MOD4, AP1000

1 INTRODUCTION

There has been a strong motivation in the automatic control engineering that human element is source of trouble and accident so that human should be excluded out of the control loop of the automatic systems. However, even if complete automated system is realized, there will be a possibility of failure of automated system. So in any 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 HIS (Human Interface System) 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 HIS DESIGN METHOD

The current issue of the advanced HIS 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.

2.1 How to Integrate Plant Simulation and Knowledge Based Information Processing

The basic idea of how to integrate the plant simulation and knowledge based information processing for the advanced HIS design is illustrated in **Fig.1**. Wherein, all aspects of plant behavior such as the

[*] Professor Emeritus Kyoto University, Japan

transient and the accident of the plant will be given by computer simulation. The plant behavior is simulated under all possible conditions, and the plant sequences can be acquired. Then the knowledge base for all conceivable transient/accident scenario of the simulated plant can be built up by the author's proposed the plant DiD risk monitor [2] with the associated AI knowledge based software system [3,4]. The plant DiD risk monitor software is based on object oriented processing for 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 control room. Lastly, various human machine interaction between machine and the various human actors are simulated to help for the designing of the HIS and the operating procedure from normal operating to coping with the accidents that may occur during the plant operation.

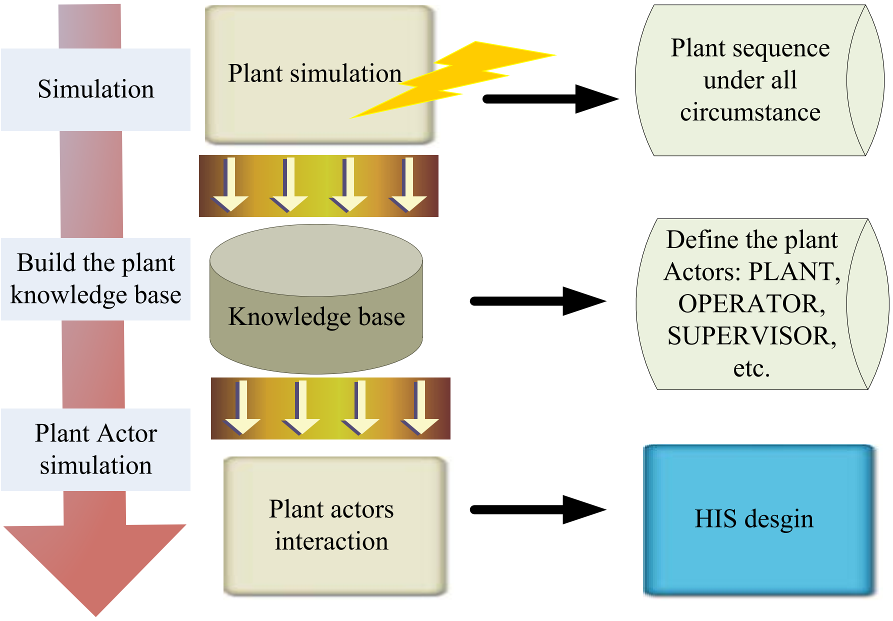

Simulation
Plant simulation
Plant sequence under all circumstance
Build the plant knowledge base
Knowledge base
Define the plant Actors: PLANT, OPERATOR, SUPERVISOR, etc.
Plant Actor simulation
Plant actors interaction
HIS desgin

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

The methodological framework for both design and evaluation of digital I&C + HMIT system is proposed 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 HIS composed by those three elements can be schematically depicted as shown in **Fig. 2**.

In Fig.2, the functional module of plant parameter monitoring and state recognition will monitor various sensors and diagnose automatically to recognize the plant state. The output of this functional module of each time will be the estimated state X_i with its certainty value $C_{i.}$ When this certainty value X_i would exceed to a given threshold value, then the estimated state X_i will automatically trigger the corresponding procedure for $X_{i.}$ Procedure X_i will be generated beforehand by the combination of the elemental procedures. The generated procedures are basically composed by two elements: triggering and manipulating various actuators of plant equipment such as valves, dials, *etc.*, while the message generation and parameter displays to the human interface.

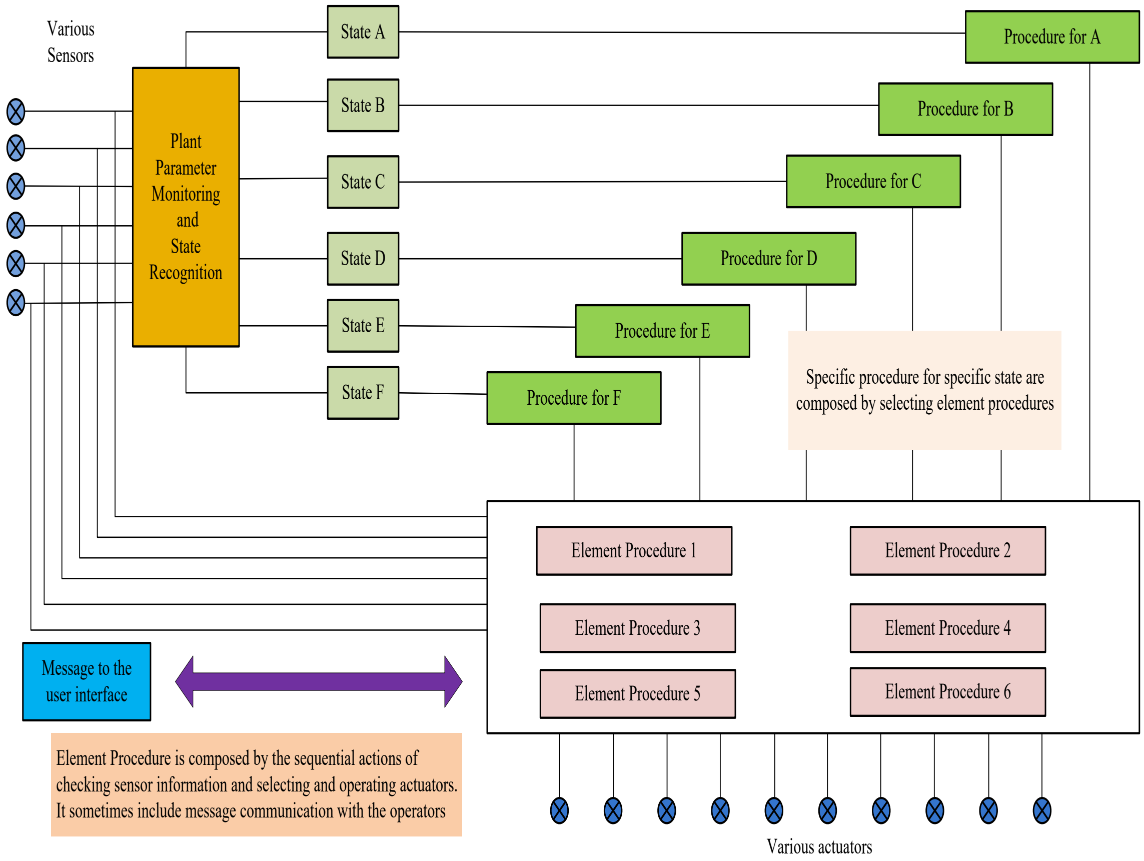


Fig. 2 Basic scheme of designing and evaluation of HIS for digital I&C + HMIT system

In Fig.2, elemental procedure is assumed to be composed by sequential actions of checking the sensor information and selecting and operating actuators. Those elemental procedure may be conducted by computer or by manual operation. Therefore, it is necessary for bi-directional transmission of the command between user interface and this block of storing elementary procedures, where not only various procedures of operating various actuators but also various message communication to the operator are included.

2.2 Practical Design Method of HIS for Real NPPs

For the practical design of HIS 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 in the following sub-sections.

2.2.1 Plant condition

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.

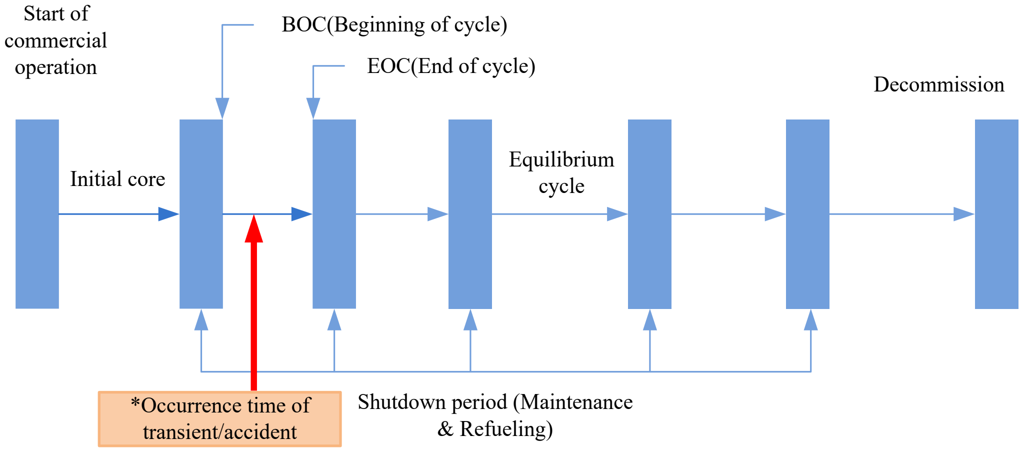

Start of commercial operation
BOC(Beginning of cycle)
EOC(End of cycle)
Decommission
Initial core
Equilibrium cycle
*Occurrence time of transient/accident
Shutdown period (Maintenance & Refueling)

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

2.2.2 Analytical consistency between different phenomena

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.

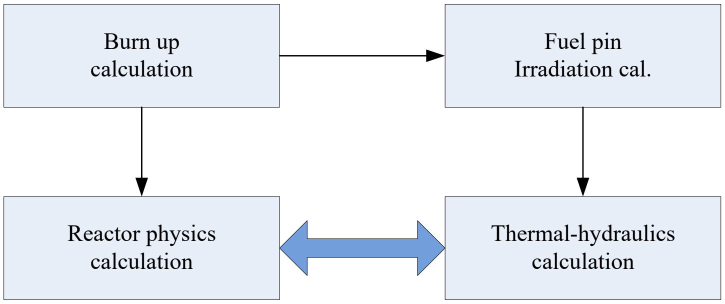

Burn up calculation
Fuel pin Irradiation cal.
Reactor physics calculation
Thermal-hydraulics calculation

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

2.2.3 Balancing the whole parts of plant system from thermal-hydraulics aspect.

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.

2.2.4 Considerations on both initial and disturbance conditions

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 disturbance conditions for transient/accident simulation by safety analysis code such as RELAP5/MOD4 [5] for the light water nuclear reactor nuclear power reactor systems such as PWR.

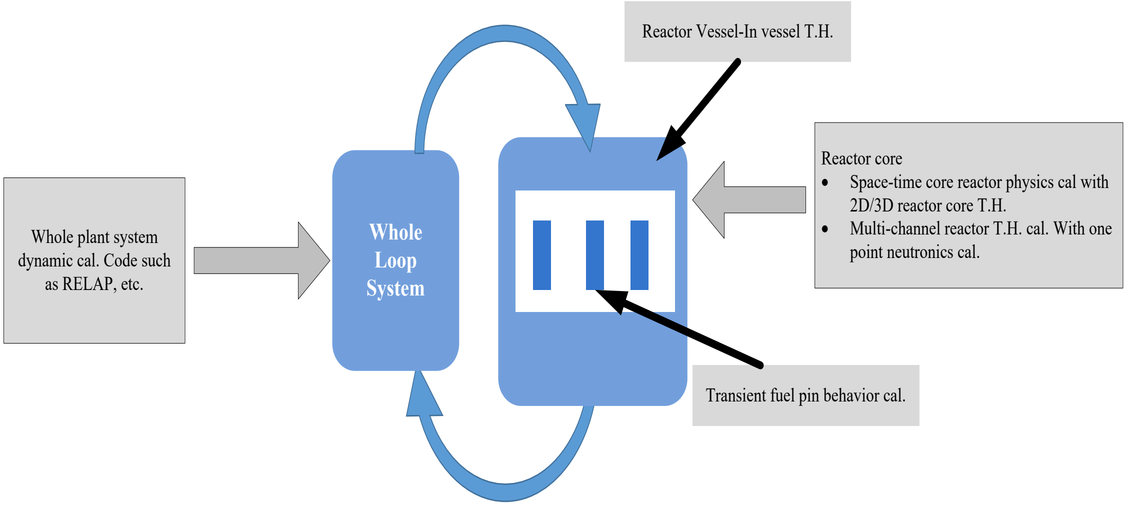
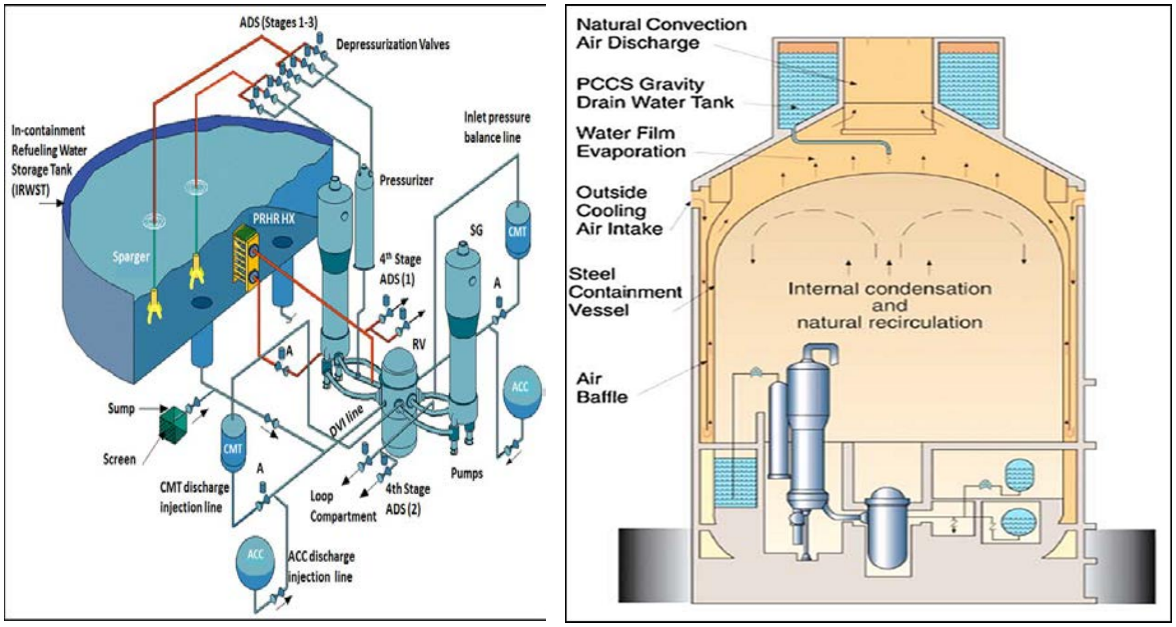

Reactor Vessel-In vessel T.H.
Reactor core
• Space-time core reactor physics cal with 2D/3D reactor core T.H.
• Multi-channel reactor T.H. cal. With one point neutronics cal.
Whole plant system dynamic cal. Code such as RELAP, etc.
Whole Loop System
Transient fuel pin behavior cal.

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.*


ADS (Stages 1-3)
Depressurization Valves
Inlet pressure balance line
In-containment Refueling Water Storage Tank (IRWST)
Pressurizer
PRHR HX
Sparger
SG
CMT
4th Stage ADS (1)
A
RV
ACC
Sump
Screen
DVI line
CMT
A
CMT discharge injection line
Loop Compartment
4th Stage ADS (2)
Pumps
ACC
ACC discharge injection line
Natural Convection Air Discharge
PCCS Gravity Drain Water Tank
Water Film Evaporation
Outside Cooling Air Intake
Steel Containment Vessel
Internal condensation and natural recirculation
Air Baffle

(a)Passive core cooling system (PXS) (b)Passive containment cooling system (PCCS)

Fig.6 Configuration of passive safety system of AP1000 assumed in this study [6,7]

3. PELIMINARY STUDY FOR AP1000

3.1 **Passive Safety System of AP1000**

AP1000 is a generation 3.5 PWR plant which was developed by Westinghouse to enforce safety function of conventional PWR plant by adopting passive safety concept with the increase of automatic function [6,7]. The configuration of passive safety system of AP1000 is illustrated in **Fig.6**. It is basically composed by two passive safety systems: (a) Passive core cooling system (PXS), and (b) Passive containment cooling system (PCCS). The plant response with time at Small break loss of coolant accident (SBLOCA) of AP1000 is assumed to be activation of reactor protection system, PXS, and PCCS, Phases of LOCA (injection and recirculation phases), Detecting device, Actuation signals of RPS, PXS and PCCS, *etc*. After the onset of SBLOCA in AP1000 plant, reactor coolant pressure will decrease gradually in time as shown in Fig.7, where the activation and turn off conditions of individual subsystems are also indicated.

3.2 Safety Analysis of AP1000 by RELAP5/MOD4

The temporal decrease of reactor coolant pressure as shown in **Fig.7** with the associated on-off sequence of individual safety subsystems is the “ideal situation” when every subsystem works successfully as it planned; every sensor measures the right signal correctly, every alarm handling facility processes the logical judgment rightly, and generate proper warning messages or trigger the right actuators correctly. However, if there happens any failure in any step, then the plant behavior will be different from Fig.7.

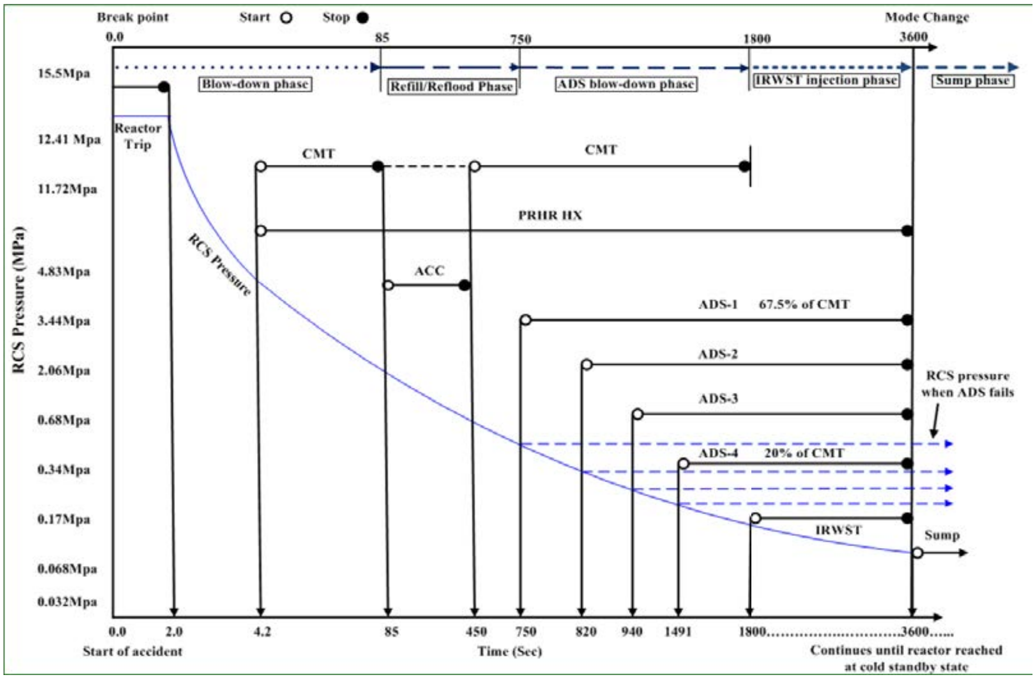


Fig.7 Activation sequence of safety system in case of SBLOCA[6,7]

In fact, there would be many possibilities of event progression if something would fails. The probability of any branching of event progression may be estimated by fault tree analysis/event tree analysis (FTA/ETA) conventionally used in probabilistic risk assessment (PRA)[8].

When the possibility of unanticipated event progression would be 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. In this respect, the authors conducted on parametric simulations of SBLOCA accident in AP1000 by using RELAP5/MOD4, where the following two cases were calculated by assuming that the both are high possibility of occurrence [9]:

(1) SBLOCA with successful reactor shutdown, and
(2) SBLOCA and failure of reactor shutdown.

The case (2) is what is called ATWS (anticipated transient without scram). In this case, it will be difficult to recover the plant state by the safety subsystems which are assumed in Fig.7.In fact, if the case (2) 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 (1), 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.

3.3 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. This means that there is no need of operators in the main control room nor need of operators work. But this argument of no need of operator intervention is unrealistic, if you know the reality of plant operation, because when SBLOCA happens, the operators of AP1000 have to confirm whether those safety functions of AP1000 work as they are planned. And moreover, if something wrong happens to fail in a certain subsystem would not work as planned, the operators in the control room 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 author 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 HIS system to support the supervisory role of operators of AP1000. In the authors' preliminary study towards this goal, the following issues should be studied in advance:

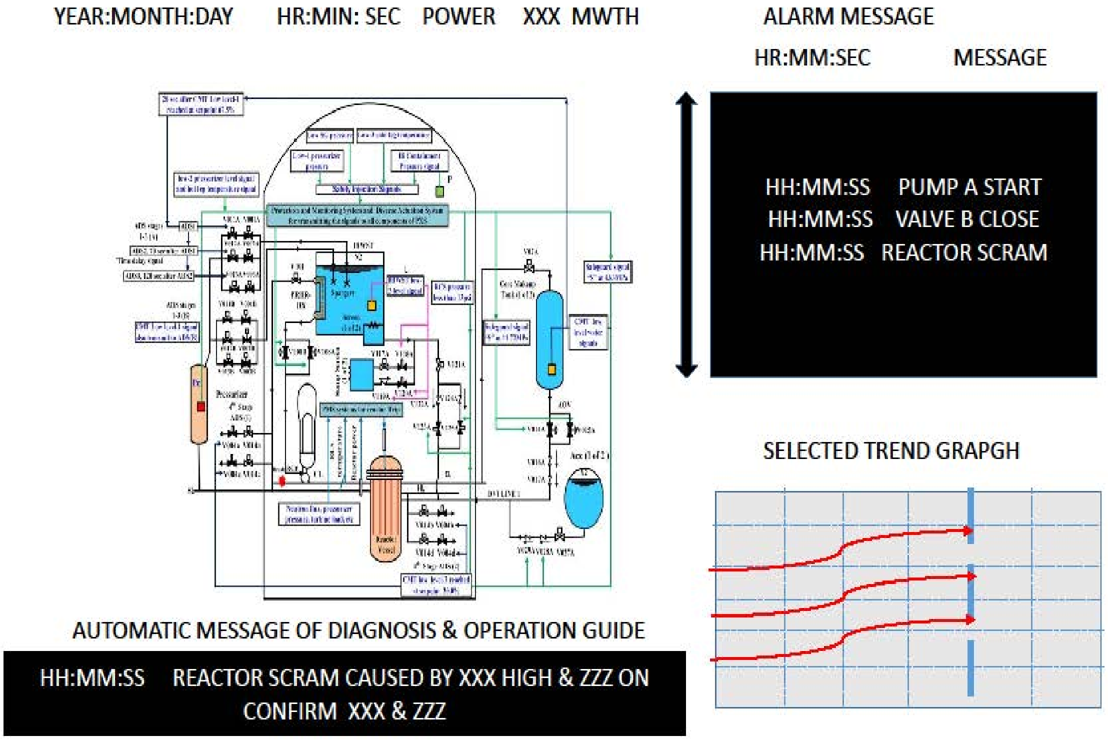
(1) Scenario classification of accident progression on the accident simulation cases conducted by RELAP5/MOD4,
(2) Reduction of space-time co-relationship between plant I&C signals and the computed output of accident analysis by RELAP5/MOD4,
(3) Hierarchical representation of the configuration of AP1000 plant as seen from safety systems,
(4) Generation of simulated plant sensor signals by using RELAP5/MOD 4 computed result of plant parameters (assumed transfer function of instrumentation system and superimposition of measurement noise and sensor drift for calibration, etc., are considered),
(5) Comparison with the simulated plant sensor signal with threshold values of various warning and scram values to simulate the generating warning and alarming message and generation of automated safety function,
(6) Implementation of anomaly detection, state classification and appropriate procedure selection from the input-output signals of I&C system with the logical judgment for the part of the automated systems, and
(7) Estimation of risk as the possibility of reactor core melt accident, and the generation of proper instruction to avoid risk in accordance with the risk level.

Then by utilizing those information (1) to (7), the authors' developed software system of plant DiD risk monitor will be applied to realize as an integrated HIS for AP1000 operators to help them monitor the behaviors of safety subsystem, inform them by proper message in case of risky state. The image of the display by this support system is as shown in **Fig. 8**, where all the necessary information of plant system and I&C including PXS and PCCS and their current operation condition are displayed together with alarm message, automatic operation guidance and time trend of selected plant parameters to be monitored for specific situation.

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, an effective offline 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.

4. CONCLUDING REMARKS

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 HIS was proposed for the support of plant operators' supervisory control of fully automated large-scale complex NPPs. The primitive idea towards this direction was presented in this paper.



HH:MM:SS PUMP A START
HH:MM:SS VALVE B CLOSE
HH:MM:SS REACTOR SCRAM

HH:MM:SS REACTOR SCRAM CAUSED BY XXX HIGH & ZZZ ON
CONFIRM XXX & ZZZ

Fig.8 Display image of HIS of AP1000 by plant DiD risk monitor

The essence of the proposed method can be stated as the following ways: (i) plant DiD risk monitor developed as an object-oriented AI tool by UML (Unified Modeling Language) will describe the dynamic state transition model of the whole interactions of both human and machine elements, (ii) behaviors of various components, systems and the whole plant are simulated by various computer codes to the respective situations of defense in depth: level 1 (normal operation), level 2 (anticipated transient), level 3 (design basis accident), level 4 (severe accident) and level 5 (radioactive release from the plant to the environment), and (iii) appropriate human interface design of the NPP operators' supervisory control and management can be conducted by the combination of the plant DiD risk monitor (i) and the simulator programs (ii) either by offline and online. Therefore, the proposed idea can be applied for the support of plant operators' supervisory control of various types of automated complex NPPs (nuclear power plants) ranging from conventional type LWRs, passive safety type LWRs and to innovative reactors such as molten salt reactors.

A preliminary development for the details of the proposed methodology has been in progress [10] by an example practice for the SBLOCA case of passive safety PWR AP1000 by plant Did risk monitor software by using calculated result of RELAP5 MOD4.

5. NOMENCLATURE

ATWS	Anticipated Transient without Scram
DAS	Diverse Actuation System
DiD	Defense in Depth
FTA/ETA	Fault Tree Analysis/ Event Tree Analysis
HIS	Human Interface System
HMIT	Human Machine Interface Technology
PXS	Passive Core cooling system
PCCS	Passive containment cooling system
SBLOCA	Small Break Loss of Coolant Accident
UML	Unified Modeling Language

6. References

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

[2] YOSHIKAWA,H. Designing of comprehensive risk analysis system for multiple layers of defense-in depth concept, Nuclear Safety and Simulation, Vol. 6, Number 2, June 2015, 116-125.

[3] YOSHIKAWA, K., NAKAGAWA, T. Development of plant DiD risk monitor system for NPPs by utilizing UML modeling technology, USB Proc. IFAC HMS 2016 in Kyoto, August 30-September 2, 2016, Kyoto, Japan.

[4] YOSHIKAWA, H., NAKAGAWA, T., Yang, M., XIA, H. A study of developing a plant Did risk monitor for resilient severe accident management, USB Proc. PSAM13, October 2 – 7, 2016,

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

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

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

[8] U.S. NRC: Probabilistic Risk Assessment (PRA), http://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html (As of July 31, 2016).

[9] NAWAZ, A., YOSHIKAWA, H., YANG, M., HUSSAIN, A. Comparative analysis of AP1000 reactor during SBLOCA with and without reactor SCRAM using RELAP5 MOD4, ISSNP2016-047, CD Proc. ISSNP2016, September 26-28, 2016, Chengdu, China.

[10] MA, Z., 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.