The Development of Defense-in-Depth for Nuclear Power Plant Digital I&C Systems

Yu-Jen Pan[1], Rung-Shiang Cheng[*2], Hui-Wen Huang[#3], Mao-Sheng Tseng[#4], Tsung-Chieh Cheng[#5]

Department of Computer and Communication Engineering, Ta Hwa Institute of Technology
No.1, Dahua Rd., Cyonglin Township, Hsinchu County 307, Taiwan (R.O.C.)
[1]yjpan@thit.edu.tw

[*]*Department of Computer and Communication, Kun Shan University*
No.949, Dawan Rd., Yongkang City, Tainan County 710, Taiwan (R.O.C.)
[2]rscheng@mail.kus.edu.tw

[#]*Nuclear Instrumentation Division, Institute of Nuclear Energy Research*
No. 1000,Wenhua Road, Chiaan Village, Longtan Township, Taoyuan County, 32546, Taiwan (R.O.C.)
[3]hwhwang@iner.gov.tw
[4]amtseng@iner.gov.tw
[5]tccheng@iner.gov.tw

***Abstract*—Modern Instrumentation and Control (I&C) Systems of Nuclear Power Plant (NPP) are moving into complete digitalization. However, digitalization for I&C could induce new failure modes, and impact the redundancy and defense-in-depth design characteristic which nuclear power plants rely on. The redundancy characteristic can be defeated by software common mode failure. The complexity of software could possess some paths which can interrupt or bypass defense-in-depth design. Therefore, the regulation requests that the new digitalized I&C NPP designs shall be performed defense-in-depth analysis to understand whether the defense-in-depth design is capable to resist the software design defects. In various defense-in-depth analysis methods, computer simulation for digital I&C systems of NPP is a crucial item. By simulating various case studies for defense-in-depth failure, the research people can understand and realize the event sequence, and can also derive various possible events to search the residual design vulnerability. This study attempts to development an optimum simulation control process for defense-in-depth of the digitalized I&C NPP and enhancement the performance efficiency of analysis software.**

***Keywords*—Safety-critical systems, Transient Without Scram, Back-up, PCTran**

1. INTRODUCTION

Many recent Plant designs utilize digital control systems. Digital control systems have the following advantages: 1) no setpoint drifting; 2) automatic calibration; 3) various improvement capabilities, such as fault tolerance, self-testing, signal validation and process system diagnostics, and 4) much detailed information helping operators to discover the plant status. However, digital I&C systems induce new failure modes that differ from those of analog control systems.

In digital instrumentation and control (I&C) systems, the negative effects are caused by software error. Due to the application of computerized I&C systems, the software error resulted new failure mode in systems. The potential for Common Cause Failure (CCF) and un-detectable software faults have become important issue as the software content of protection systems has increased. Software Safety Analysis (SSA) and Diversity and Defense-in-Depth (D3) analysis can enhance the system safety [1], [2].

This work developed an Anticipated Transient Without Scram (ATWS) analysis process which was incorporated with stand-alone ABWR (Advanced Boiled Water Reactor) analysis software for digital I&C NPP system. The purpose of this work is to improve and advance the existing model in PCTran-ABWR [3] and optimum the NPP simulation software. INER has been using this computer code as an NPP simulation model for Software Safety Analysis (SSA) and software Fault Injection (FI) of digital I&C research for years [4], [5].

2. THEOREM AND DESIGN

In Defense-in-Depth analysis, utilizing computer simulation is crucial item. We firstly explain the conception of Defense-in-Depth, and then presentations the procedure of Defense-in-Depth design for the digitalized I&C NPP.

2.1. Defense-in-Depth

Defense-in-depth is a principle of long standing for the design, construction and operation of nuclear reactors, and may be thought of as requiring a concentric arrangement of protective barriers or means, all of which must be breached before a hazardous material or dangerous energy can adversely affect human beings or the environment. "Echelons of defense" are specific applications of the principle of defense-in-depth to the arrangement of instrumentation and control systems attached to a nuclear reactor for the purpose of operating the reactor or shutting it down and cooling it. Specifically, the echelons are the *Control System*, the *Reactor Protection System* (RPS), and the *Engineered Safety Features actuation system* (ESFAS). Fig. 1 shows the correlation of three echelons.

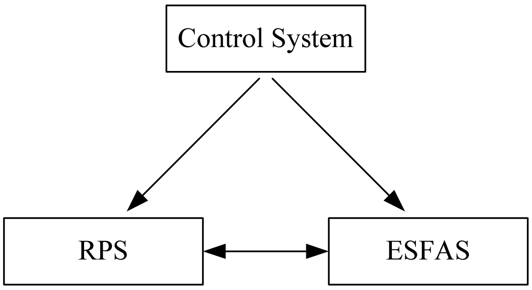

Fig. 1 Echelon diagram showing interactions

When the *Control System* fails, the system will transfer the single of demand to RPS or ESFAS, and then performance the procedure of protection system. However, CCF and un-detectable software faults may affect digital I&C systems operation, thus development a back-up system is extremely needed.

2.2. Back-up of Control System

The *Control System* of digital I&C NPP plays key role that the system can control total NPP safety by delivery digital signals in different echelon. When system can not normally operate, the condition of ATWS will lend to serious nuclear energy safety events. ATWS is one of the "worst case" accidents, the accident could happen if the system that provides a highly reliable means of shutting down the reactor (scram system) fails to work during a reactor event (anticipated transient). As Fig. 2 shows, the *Control System* can not perform normal operation, due to CCF affect digital I&C system.

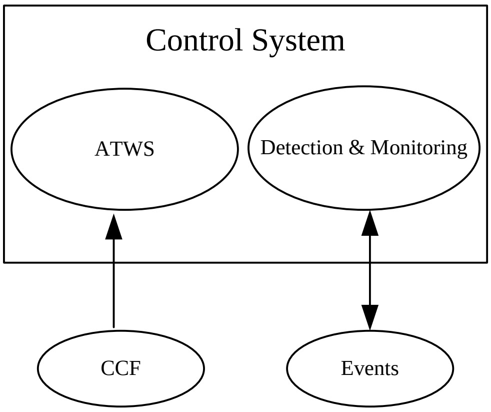

Fig. 2 The diagram of control system operation procedure

We design a back-up process to Control System in order to avoid ATWS accident, this back-up is arranged in *Safety System Logic and Control* (SSLC) system. Fig. 3 shows the SSLC system to back-up of *Control System*. In normal condition, the *Control System* can operate in regular state by connection of detection / monitoring and events. However, when CCF and un-detectable software faults affect the system, the SSLC provide the emergent back-up system to deal the ATWS accident.

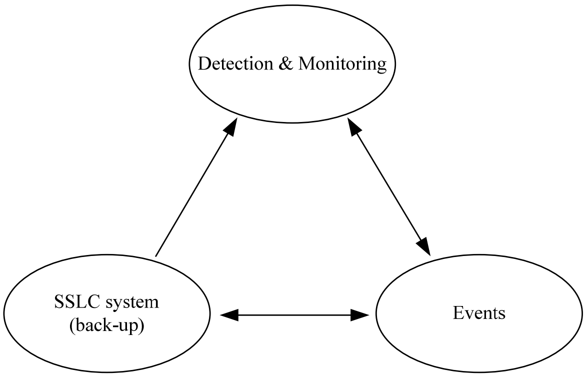

Fig. 3 SSLC diagram showing interactions

3. PCTRAN

PCTRAN is a reactor transient and accident simulation software program that operates on a personal computer (Fig. 4(a)). Since its first release in 1985, Micro-Simulation Technology has been constantly upgrading its performance and expanding its capabilities. Numerous versions and plant models have been installed in countries around the world.

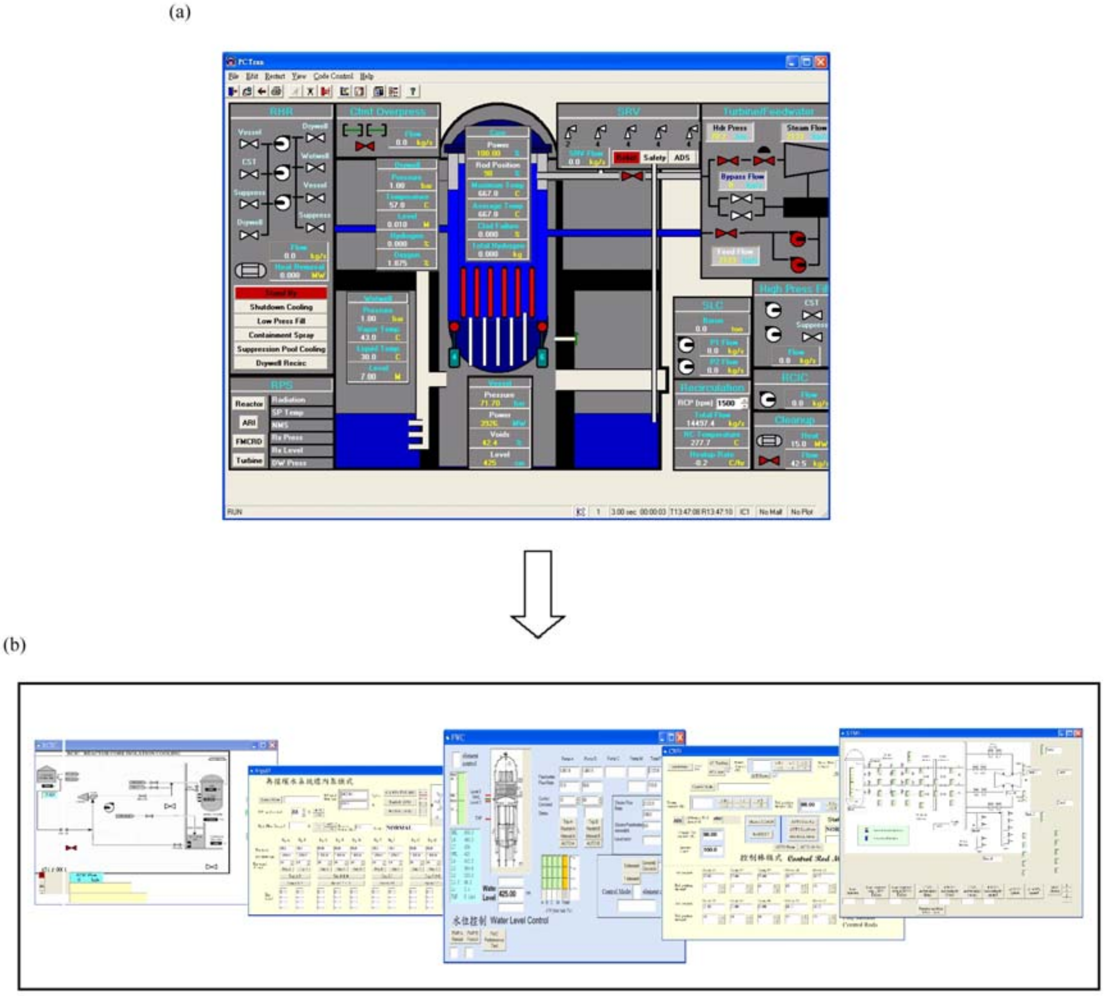

Fig. 4 Reactor transient simulation program (a) the windows-based graphic user interface (GUI) (b) the augmentation modules of software program

Advancement in modern 32-bit microprocessors and the windows-based graphic user interface (GUI) has completely revolutionized the simulation technology. It is now possible to automate the preparation work and actual exercise on a desktop computer. Since 1998, the source code of PCTran has been converted into Microsoft Visual Basic 6.0. Operation of the GUI adheres strictly to the specifications of the Microsoft Windows environment. Data input/output are in MS Office's Access database format. Reports and data can be transferred conveniently through all Windows-based software products over the entire exercise network. In recent years, our research group have developed several modules in PCTran (Fig. 4(b)). These modules not only advance simulated efficiency, but also enhance analysis ability.

4. Results

In this section, we present three system states. Firstly, the system is normal condition, and then we invent a dead event to *Control System* and observation the result of back-up system operation. Lastly, the system is set another annulment condition for proof accuracy of back-up system. Table 1 lists operating conditions of three states. In all test conditions, the system power is set as critical norm.

TABLE 1
OPERATING CONDITIONS

State	Arrangement		
	Monitoring	ATWS	SSLC
1	110 (%)	off	off
2	110 (%)	on	on, in 120 (%)
3	110 (%)	on	on, in 135 (%)

4.1. Numerical Data

State 1: In normal state, the pressure is set 110 (%). When system encounters accidental event, the pressure of system will increase until reaching the critical value (110). Simultaneously, the system will trip and keep steady state. Fig. 5 shows the system can be controlled in safe situation by protection procedure of self-system. In Fig. 5(b), the pressure starts to increase slowly in 10 sec, and then a more sharp variation takes place in 26 sec. The system occurs trip about 27 sec (power = 108.6%), therefore the system power has rapid decreasing in approximate time (see Fig. 5(a)).

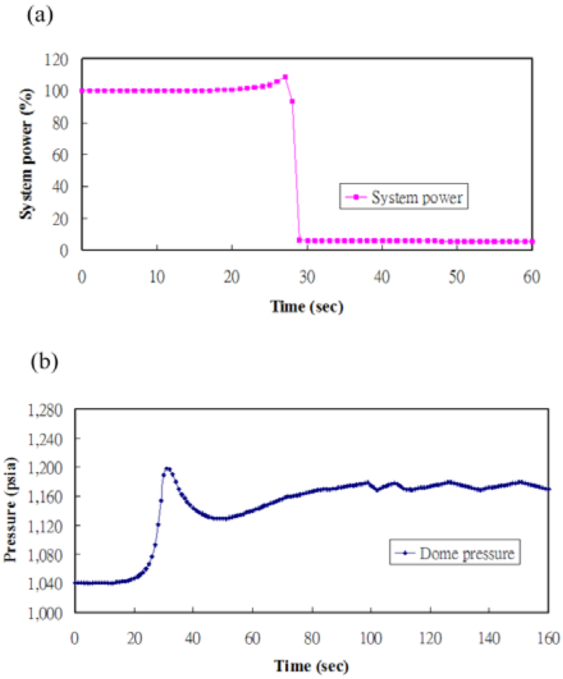

Fig. 5 Variation of system in state 1 (a) power, (b) pressure

State 2: The system is assumed the CCF to affect the system normal function. Therefore, we set a critical value (system power = 120 %) to SSLC for monitoring system safety and observation whether the back-up of SSLC has automatic operating ability to protect the system safety. In Fig. 6(a), the system power has slowly increasing in 10 sec, and then the system power exceeds critical value in 28 sec (110.9%). However, protection procedure of self-system does not turn on to maintain the stable of system state. The system power increases ceaselessly to 123.2 % (29 sec), the back-up of SSLC automatically starts to perform the protection system safety procedure. Therefore, the system has trip and keep stable state. We can obtain resemble trend in Fig. 6(b). The pressure starts to increase slowly in 10 sec and has rapid decreasing in approximate time.

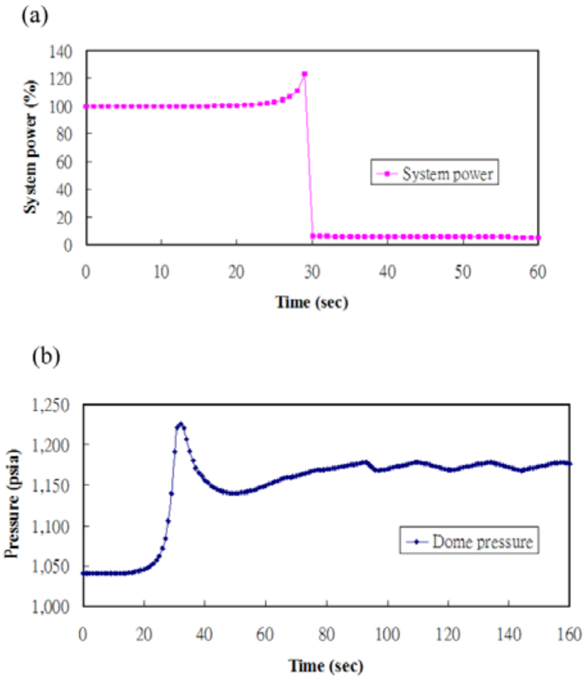

Fig. 6 Variation of system in state 2 (a) power, (b) pressure

State 3: In this testing process, the starting value of back-up is set in 135%. We obtain alike result with state 2. The system power exceeds critical value in 28 sec (110.9%) and then adds to 123.3% (29 sec), but the system does not start the back-up procedure. The system power exceeding the limit of SSLC is occurrences in 30 sec (149.7%) and back-up of SSLC start to defense ATWS accident. The total variation of system state is shows in Fig. 7.

4.2. Data Analysis

In this study, the data is recorded in per second. Table 2 lists the occasion of SSLC switch on. In state 2, the power of system is 110.94 % in 28 sec. However, the protection procedure of self-system does not start to mitigate the NPP system. Due to the setting point of back-up system is 120 %, therefore SSLC start on in net time (power = 123.21 %) and then the power of system decreases to 6.19 % in 30 sec. For testing stabilization of back-up, the setting point of back-up system is altered to 130 % in state 3. Therefore, the power of system does not mitigate in 29 sec (power = 123.21 %). The back-up system starts on in 30 sec and mitigates the NPP system in 31 sec.

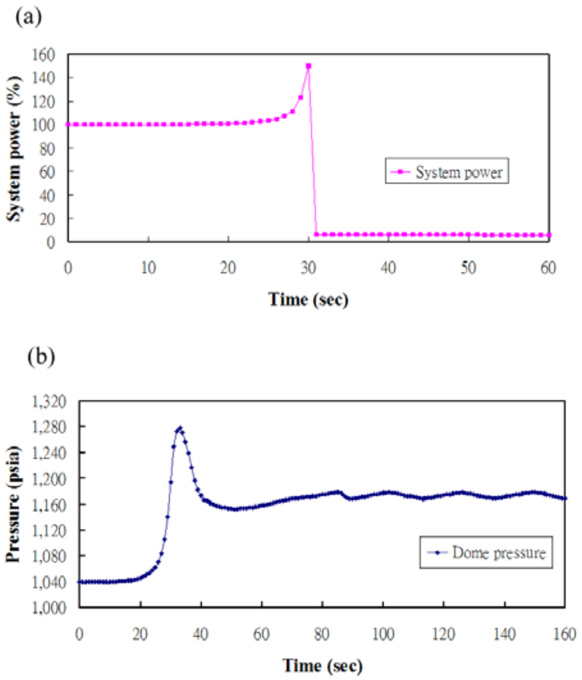

Fig. 7 Variation of system in state 3 (a) power, (b) pressure

TABLE 2
PROCEDURE OF SYSTEM SHIFTING

Power / Time / State	Time of SSLC Turn on		
	t – 1 (sec)	t (sec)	t + 1 (sec)
2	28 110.94%	29 123.21%	30 6.19%
3	29 123.21%	30 149.77%	31 6.15%

5. CONCLUSIONS

This study has proposed a back-up system based on reactor transient analysis program. The real performance results show that this back-up system (SSLC) able to protect the system. Beside, we test this back-up system by alteration time of back-up start on. The result shows this system can be perform effectively.

ACKNOWLEDGMENT

The authors gratefully acknowledge the financial support provide to this study by the Institute of Nuclear Energy research.

REFERENCES

[1] C. S. Lee, E. P. Chan, C. J. Choi, and J. T. Seo, “Defense-in-depth and diversity evaluation to cope with design bases events concurrent with common mode failure in digital plant protection system for KNGR,” *Nuclear Engineering and Design*, vol. 207, pp. 95-104, 2001.

[2] J. Liu, J. Dehilinger, and R. Lutz, “Safety analysis of software product lines using state-based modeling,” *Journal of Systems Software*, vol. 80, pp. 1879-1892, 2007.

[3] (2007) Micro-Simulation Technology. [Online]. Available: http://www.microsimtech.com/

[4] H.-W. Huang, M.-H. Chen, C. Shih, S. Yih, C.-T. Kuo, L.-H. Wang, Y.-C. Yu, and C.-W. Chen, “Development of Evaluation Method for Software Hazard Identification Techniques,” 5th NPIC&HMIT, Albuquerque, NM, USA, Nov. 2006.

[5] H.-W. Huang, C. Shih, S. Yih, M.-H. Chen, J.-M Lin, “Model Extension and Improvement for Simulator-based Software Safety Analysis,” *Nuclear Engineering and Design*, vol.237, pp. 955-971, 2007.