Available online at www.sciencedirect.com
ScienceDirect
Annals of Nuclear Energy 35 (2008) 353–362
annals of NUCLEAR ENERGY
www.elsevier.com/locate/anucene

System-level hazard analysis using the sequence-tree method

Hui-Wen Huang [a,b,*], Chunkuan Shih [a], Swu Yih [c], Ming-Huei Chen [b]

[a] Department of Engineering and System Science, National Tsing-Hua University, 101, Section 2 Kuang Fu Road, Hsinchu, Taiwan
[b] Institute of Nuclear Energy Research, No. 1000, Wenhua Road, Chiaan Village, Longtan Township, Taoyuan County 32546, Taiwan
[c] Department of Computer Science and Information Engineering, Ching Yun University, 229, Chien-Hsin Road, Jung-Li City, Taiwan

Received 20 February 2007; received in revised form 18 July 2007; accepted 22 July 2007
Available online 4 September 2007

Abstract

A system-level PHA using the sequence-tree method is presented to perform safety-related digital I&C system SSA. The conventional PHA involves brainstorming among experts on various portions of the system to identify hazards through discussions. However, since the conventional PHA is not a systematic technique, the analysis results depend strongly on the experts' subjective opinions. The quality of analysis cannot be appropriately controlled. Therefore, this study presents a system-level sequence tree based PHA, which can clarify the relationship among the major digital I&C systems. This sequence-tree-based technique has two major phases. The first phase adopts a table to analyze each event in SAR Chapter 15 for a specific safety-related I&C system, such as RPS. The second phase adopts a sequence tree to recognize the I&C systems involved in the event, the working of the safety-related systems and how the backup systems can be activated to mitigate the consequence if the primary safety systems fail. The defense-in-depth echelons, namely the Control echelon, Reactor trip echelon, ESFAS echelon and Monitoring and indicator echelon, are arranged to build the sequence-tree structure. All the related I&C systems, including the digital systems and the analog back-up systems, are allocated in their specific echelons. This system-centric sequence-tree analysis not only systematically identifies preliminary hazards, but also vulnerabilities in a nuclear power plant. Hence, an effective simplified D3 evaluation can also be conducted.

1. Introduction

Many recent NPP 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 control systems induce new failure modes that differ from those of analog control systems. Analog systems comprise logic circuits, each of which can obtain its own logical result independently. In contrast, a digital system is run on a computer. All the logic circuits are transferred to software, and all the logical computations should be performed by the CPU. Thus, all the software should be run by the CPU. The software should be allocated in memory, possibly producing problems of address conflict and memory overflow. The transfer digital data also raises issues of communication through the network. Redundant

Abbreviations: ABWR, advanced boiling water reactor; ADS, automatic depressurization system; ARI, alternate rod insertion; ATM, analog trip module; ATWS, anticipated transient without scram; BTP, branch technical position; CMF, common mode failure; CPU, central processing unit; D3, diversity and defense-in-depth; ECCS, emergency core cooling system; ESFAS, engineered safety features actuation system; FMCRD, fine motion control rod drive; FMEA, failure modes and effects analysis; FWP, feedwater pump; FTA, fault tree analysis; HPCF, high pressure core flooder; I&C, instrumentation and control; INER, Institute of Nuclear Energy Research; LOCA, loss of coolant accident; LPFL, low pressure core flooder; NPP, Nuclear Power Plant; NRC, Nuclear Regulatory Commission; NTHU, National Tsing Hua University; PCTran, personal computer transient analyzer; PHA, preliminary hazard analysis; RCIC, reactor core isolation cooling; RFC, recirculation flow control system; RHR, residual heat removal system; RIP, reactor internal pump; RPS, reactor protection system; Rx, reactor; SAR, safety analysis report; SBPC, steam bypass and pressure control system; SCM, software configuration management; SLCS, standby liquid control system; SSA, software safety analysis; SV&V, software verification and validation.

* Corresponding author. Address: Department of Engineering and System Science, National Tsing-Hua University, 101, Section 2 Kuang Fu Road, Hsinchu, Taiwan. Tel.: +886 (3) 4711400x6352; fax: +886 (3) 4711415.
E-mail address: hwhwang@iner.gov.tw (H.-W. Huang).

0306-4549/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.anucene.2007.07.010

system design can help resist against single failure. However, the redundant system typically implements the same software module as the original system. This indicates that software CMF can defeat the redundant system. Therefore, digital I&C systems must address issue of software failure. Branch Technical Position HICB-14 (BTP-14), "Guidance on Software Reviews for Digital Computer-Based I&C Systems (1997)", requests SV&V and SCM to reduce the number of software errors, and thus enhance software reliability. However, error-free software is impossible to achieve in a complicated digital system. In particular, some software faults are not detectable, because they take effect only in particular contexts. Therefore, SSA and D3 can improve the system safety wherever the software fault takes effect on the NPP. SSA identifies the system hazards introduced by software failure. D3 focuses on plant level defense against safety-related digital I&C system failure. Fault-tolerance techniques can successfully resolve software or hardware single failure. Lee et al. (2001) presented a best-estimate analysis methodology to perform defense-in-depth and diversity evaluation for the Korean Next Generation Reactor. Lee et al. (2006) also proposed an evaluation method of error detection coverage and fault tolerance to perform safety assessment of the digitalized system. Liu et al. (2007) employed state-based modeling to perform safety analysis of software product lines. However, software common mode failure can defeat the fault-tolerance architecture. D3 evaluation should be performed to cope with the software CMF issue. The US NRC states the requirement for D3 in Branch Technical Position HICB-19 (BTP-19), "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems (1997)" and SECY 93-087, "Defense against Common-Mode Failures in Digital Instrumentation and Control System, Staff Requirement Memorandum (1993)." Software CMF is the major concern. The diverse backup system is an acceptable consideration, and can be an automatic analog system with the same function or manual system-level actuation function. BTP-19 (1997) also endorsed NUREG/CR-6303, "Method for Performing Diversity and Defense-in-depth Analyses of Reactor Protection Systems (1994)" as an acceptable D3 analysis method. Although replacing the obsolete analog system is one of the objectives of I&C system digital upgrade, the digitalized NPP currently still need the analog system as a backup.

Several SSA techniques, including preliminary hazard analysis, failure modes and effects analysis, fault tree analysis, system modeling, software requirements hazard analysis, walkthroughs and simulator/plant model testing, are described in Annex D of IEEE 7.4.3.2-2003, "Identification and resolution of hazards (2003)". Markov chain modeling and dynamic flowgraph methodology can also be adopted in SSA. NUREG/CR-6430, "Software Safety Hazard Analysis (1995)" and IEEE Std. 1228-1994, "IEEE Standard for Software Safety Plans (1994)" described in detail the procedure for performing SSA. IEEE Std. 1044-1993, "IEEE Standard Classification for Software Anomalies (1993)" describes a uniform approach to classification of anomalies found in software and its documentation. Some SSA techniques adopt quantitative parameter, such as failure rate or transition probability, for PRA and risk-informed decision making. However, software faults are caused by design error. The mechanism of software failure is different from the aging process of hardware failure. It means the software failure rate is very hard to measure. Hence, qualitative techniques, such as PHA, FMEA, and FTA (without software failure rate), are the major SSAs adopted at INER, Taiwan (see Fig. 1). If the hazard cannot be successfully identified for some specific complex cases, simulator-based analysis will be used to analyze the dynamic relationships among I&C systems. If thermal hydraulic safety analysis is still required, then RETRAN (2007a, 2007b) or RELAP (2007) are applied to confirm the details (such as pressure boundary or fuel integrity) accurately. At INER, Swu et al. (2004) and Huang et al. (2005, 2006a,b, 2007a,b) have utilized the Simulator-based model technique by PCTran-ABWR (1981) for years. Micro-Simulation Technology (2007) produced PCTran-ABWR, a faster-than-real-time plant simulation computer code. This code was developed to evaluate the transients and accidents of ABWR. INER and NTHU (Taiwan) are involved in a long-term collaboration project to extend and improve this code. To clarify the properties of SSA techniques, Huang et al. (2006c,d) presented developed an evaluation method for software hazard identification techniques. The SSA team of INER adopted this evaluation method to obtain a strategy to adopt SSA techniques combination including PHA, FMEA, FTA (without failure rate), and a simulator-based model technique.

Conventional PHA adopts a critical function list and a checklist to guide and focus discussions. The role of the analyzed safety-related system, such as RPS or ECCS, in a postulated event or accident cannot be obviously clarified. Moreover, the relationship among the involved I&C systems still cannot be clearly described. Furthermore, since this conventional PHA is not a systematic technique, the analysis result depends strongly on the experts' subjective opinions. The analysis quality cannot be suitably managed. Therefore, this study presents a system-level sequence-tree-based PHA, which can systematically clarify the relationship among the major digital I&C systems.

The proposed sequence-tree-based technique has two major phases. The first phase applies a table to analyze each event in SAR Chapter 15, "Accident Analysis", for a specific system. The second phase adopts a sequence tree to identify the I&C systems that are involved in the event, how the safety-related systems work, and how the backup systems can be activated to mitigate the consequences of failure of the primary safety systems.

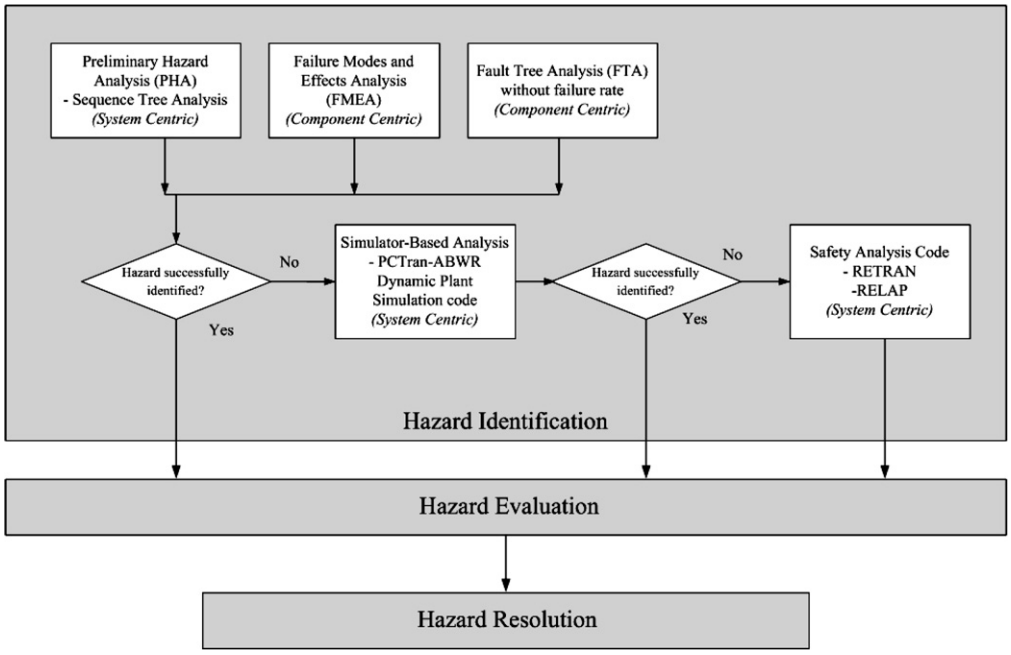

Fig. 1. Current hazard identification application status at INER.

Table 1
Generic SAR event analysis table

Analyzed system	Section	Title	Event description	The role of analyzed safety-related I&C system	Mitigation means
The name of analyzed safety-related I&C system	SAR section number	SAR event title	The block describes the event sequence and the I&C system involved in the event	The block describes the role of analyzed safety-related I&C system in the event	How the diverse backup systems mitigate the consequence of event what if the analyzed safety-related I&C system fails to perform its designated function

2. SAR event analysis table

The SAR event analysis table can determine how a primary safety-related digital I&C system performs its function in an event, and how the mitigation method performs the backup function if the primary digital I&C fails. Table 1 presents a generic SAR event analysis table. The columns of an SAR event analysis table are "analyzed system", "section", "title", "event description", "the role of analyzed safety-related I&C system" and "mitigation method".

"Section" and "title" indicate the analyzed event, for example, "15.1.1 Loss of Feedwater Heating" or "15.2.1 Pressure Regulator Failure – closed". The "Event description" column describes the event sequence and I&C system involved in the event. "The role of analyzed safety-related I&C system" describes the role of the analyzed safety-related I&C system in the event. "Mitigation method" describes how the diverse backup systems mitigate the consequence of events if the analyzed safety-related digital I&C system fails to perform its designated function.

3. Sequence-tree method

NUREG/CR-6303 (1994) defines Echelons of defense as "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." For a nuclear power plant, "the echelons are the control system, the reactor trip or scram system, the Engineered Safety Features actuation system (ESFAS), and the monitoring and indicator system. The echelons may be considered to be concentrically arranged in that when the control system fails, the reactor trip system shuts down reactivity; when both the control system and the reactor trip system fail,[1] the ESFAS continues to support the physical barriers to radiological release by cooling the fuel, thus allowing time for other measures to be taken by reactor operators to reduce reactivity. All four echelons depend upon sensors to determine when to perform their functions, and a serious

[1] ESFAS is not for backing up the reactor trip system in case of failure. It is utilized to compensate for coolant loss exceeding the normal feed capacity. It is activated even if the reactor trip succeeds.

safety concern is to ensure that no more than one echelon is disabled by a common sensor failure or its direct consequences.''

The sequence-tree method can identify what I&C systems are involved in the event, how the safety-related systems work, and how the backup systems can be activated to mitigate the consequences of failure of the primary safety systems. The defense-in-depth echelons, namely the Control echelon, RPS echelon, ESFAS echelon, and Monitoring and indicator echelon, are arranged in the sequence tree to build the structure. All the related I&C systems, i.e. the digital systems and the analog back-up systems, are allocated in their specific echelons.

Fig. 2 illustrates a generic sequence tree. A sequence tree denotes a specific SAR event. Each SAR event is initiated by a transient initiation system. The transient initiation system can be a control system, an ESFAS system or a mechanical system. Abnormal behavior in a transient initiation system could induce a plant-level transient. For instance, in the ''Loss of Feedwater Heating'' event, closure of the steam extraction line to the heater can cause the loss of a feedwater heater. In ''Feedwater Controller Failure-Maximum Demand'' event, the root cause is postulated as a single failure of a control device. The former is a mechanical failure, while the latter is a control system failure. The transient initiation system can induce some plant parameter changes, such as a decrease in vessel water level or an increase in vessel pressure.

The control echelon contains non-safety equipment that routinely prevents reactor excursions toward unsafe operation regimes, and is adopted for normal operation of the reactor. A small transient can be eliminated by the control echelon and the reactor physical response itself. For instance, the feedwater control system can eliminate a small feedwater flow perturbation, so that the plant reaches the balanced state. However, if the transient is sufficiently violent, then the reactor might scram due to the low water level in the reactor vessel. The control echelon can also perform mitigation. For instance, runback or trip of reactor internal pumps by some pre-set condition can reduce the reactor core flow, and consequently reduce the reactor power.

The reactor trip echelon consists of safety equipment that is designed to reduce reactivity rapidly in response to an uncontrolled excursion. If the digital RPS does not perform the normal reactor scram, then the backup/alternative automatically initiates the reactor shutdown function to mitigate the consequences of this failure. For instance, ATM and FMCRD run-in are the backup/alternative reactor shutdown functions of RPS in ABWR. ATM, which receives hard-wired water level signal, can transmit a reactor trip signal to initiate FMCRD run-in at the setpoint below that of RPS. FMCRD run-in is a motor driven control rod insertion procedure, which is different from the hydraulic rod insertion mechanism of RPS. Manual scram by the operator through hard-wiring is the last defense line of the reactor trip echelon. However, the operator should rely on the monitoring and indication echelon to recognize the abnormal situation.

The ESFAS echelon consists of safety equipment that removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel and containment). The major system set of ESFAS for an ABWR is ECCS, which comprises digitized RCIC, HPCF and LPFL. Each of these systems can inject water by its specific low water level setpoint or high drywell pressure setpoint. Diverse means are designed behind the digital ESFAS systems to mitigate the software common mode failure of the digital system. The systems can be automatic analog systems or manual push-button systems.

The monitoring and indication echelon is a set of sensors and safety parameter displays. This echelon includes the primary digital monitoring and indication systems, and the diverse backup devices. The operator can identify the plant status while a transient is progressing from the status of this echelon. If RPS or ESFAS cannot perform their function properly, then the operator can take manual action with the monitoring and indication echelon to prevent further plant deterioration. Additionally, the analog monitoring and indication system is designed to back up the digital system in the event of software common mode failure.

The time-axis of the sequence-tree method can only roughly describe the sequence of activities in the event. The method cannot describe precisely the dynamic change of each parameter. A nuclear power plant simulation computer code should be adopted in this situation if further time-dependent details need to be recognized. Fig. 3 illustrates an example of trend plot analyzed using PCTran-ABWR. However, the trend plot cannot directly describe the relationships among the systems. Hence, a combination analysis is required to observe all the views of system interactions.

4. Case study

Two safety-related I&C system cases, each involving a specific SAR event, were analyzed. Conventional event analysis assumes that all the safety-related I&C system functioned properly. However, the case studies in this study assumed that one or more safety-related I&C systems failed. Moreover, the system-level interactions were analyzed, and the D3 means were also evaluated.

4.1. Reactor protection system

The RPS case study in this study analyzed the ''feedwater controller failure-maximum demand'' event by the ABWR SAR event analysis table and sequence-tree method. All the RPS-involved events in SAR should be selected and analyzed for a complete RPS analysis.

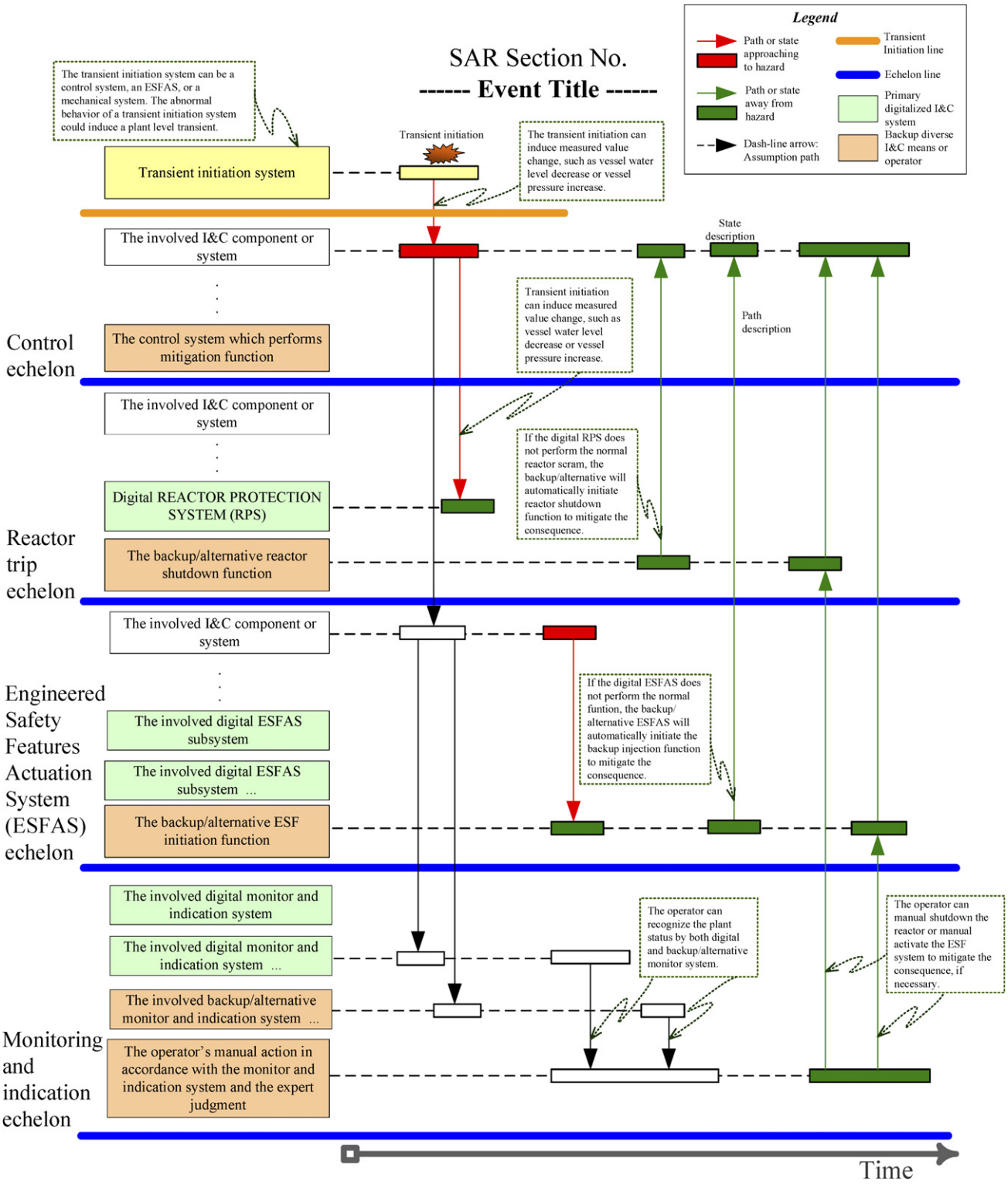

Fig. 2. Generic sequence tree.

Table 2 presents an analysis of the RPS case study event. The "feedwater controller failure-maximum demand" event is presented in SAR Section 15.1.2. This event assumes feedwater controller failure at maximum demand. In this case, the feedwater flow rises due to the abnormally high speed of two turbine-driven feedwater pumps. The water level rises to the high-level set point (Level 8), inducing main turbine trip and feedwater pump trip. Consequently, the water level falls to the low-level set point (Level 3), which induces reactor scram. The analyzed safety-related I&C system, namely digitalized RPS, triggers a scram signal due to a low reactor-vessel water level (Level

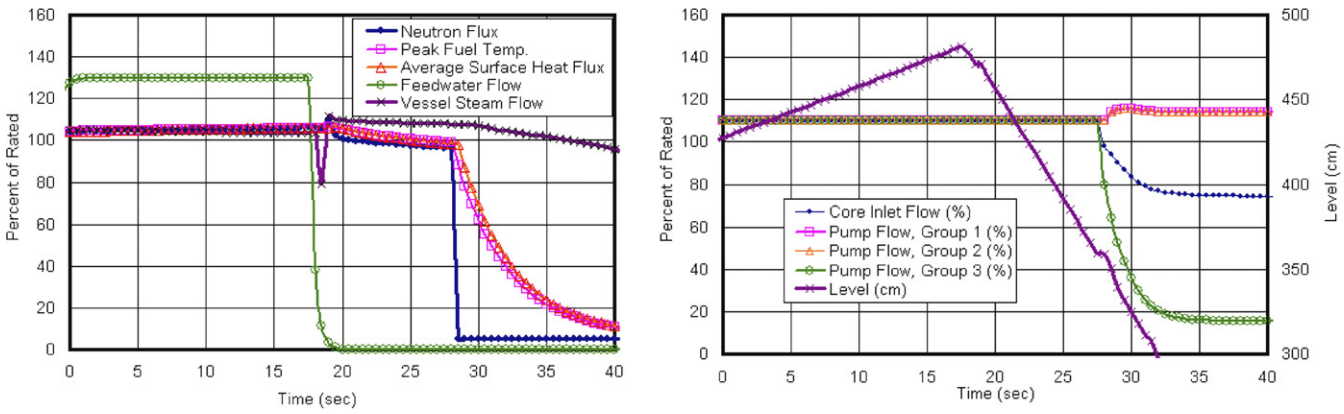

Fig. 3. Example of trend plot analyzed by PCTran-ABWR.

Table 2
Analysis table case study on RPS failure event

Section	Title	Event description	The role of analyzed safety-related I&C system	Mitigation means
SAR Section 15.1.2	Feedwater controller failure – maximum demand	• Feedwater controller failure leading to maximum demand • Feedwater flow rises • Water level rises to high level induces turbine trip and feedwater pump trip • Water level falls to low level induces reactor scram	RPS triggers scram signal due to low reactor vessel water level (Level 3)	If RPS fails to scram when the level falls to Level 3, then the following diversified mitigation means are initiated (1) When water level is below Level 2, the analog trip module (ATM) will initiate alternate rod insertion (ARI), fine motion control rod drive (FMCRD) run-in to shut down the reactor. Boron Injection is initiated at 3 min after water level reaches Level 2 (2) The hard-wired level indication and low-level alarm notify the operator to manually scram the reactor

3). If the digitalized RPS fails to scram when the level falls to Level 3, then the following diverse mitigation means are initiated. (1) The analog trip module (ATM) initiates the alternate rod insertion (ARI) and fine motion control rod drive (FMCRD) run-in to shutdown the reactor when the water level falls below Level 2. (2) Boron Injection is initiated at 3 min after the water level reaches Level 2. (3) The hard-wired level indication and low-level alarm notifies the operator to scram the reactor manually.

Fig. 4 displays the RPS sequence-tree case study. In the "feedwater controller failure-maximum demand" event, the feedwater control system is the transient initiator, causing the water level to rise to Level 8. In the control echelon, the high reactor water level signal triggers the feedwater pump trip and the main turbine trip to prevent water from flowing into the main steam lines. The 10 turbine bypass valves rapidly open to release the steam to avoid high reactor pressure. Since the reactor power is still at a high level, and no feedwater enters the reactor vessel, the water level falls to low (Level 3). Four RIPs are tripped due to the low water level.

In the reactor trip echelon, Level 3 is the reactor scram setpoint. If the reactor is normally scrammed, then the water level change rate falls significantly. This case study assumed that the digitalized RPS fails to trip the reactor (i.e. ATWS) due to software CMF. The hazards of RPS failure can be identified as (1) the water level continuously falls rapidly, and (2) the core uncovery potential rises simultaneously. Some diverse backup means were designed to mitigate the hazard. ARI and FMCRD run-in are initiated if the water level subsequently drops to Level 2. To avoid using the common signal type software CMF, the analog water level instrument is diverse from the primary digital water level signal. The ATM transmits the reactor shutdown signals ARI, FMCRD run-in and SLCS when the water level is below Level 2. The ARI can open the alternate valves to release a hydraulic driving force, so that control rods can be inserted. This alternate driving force is

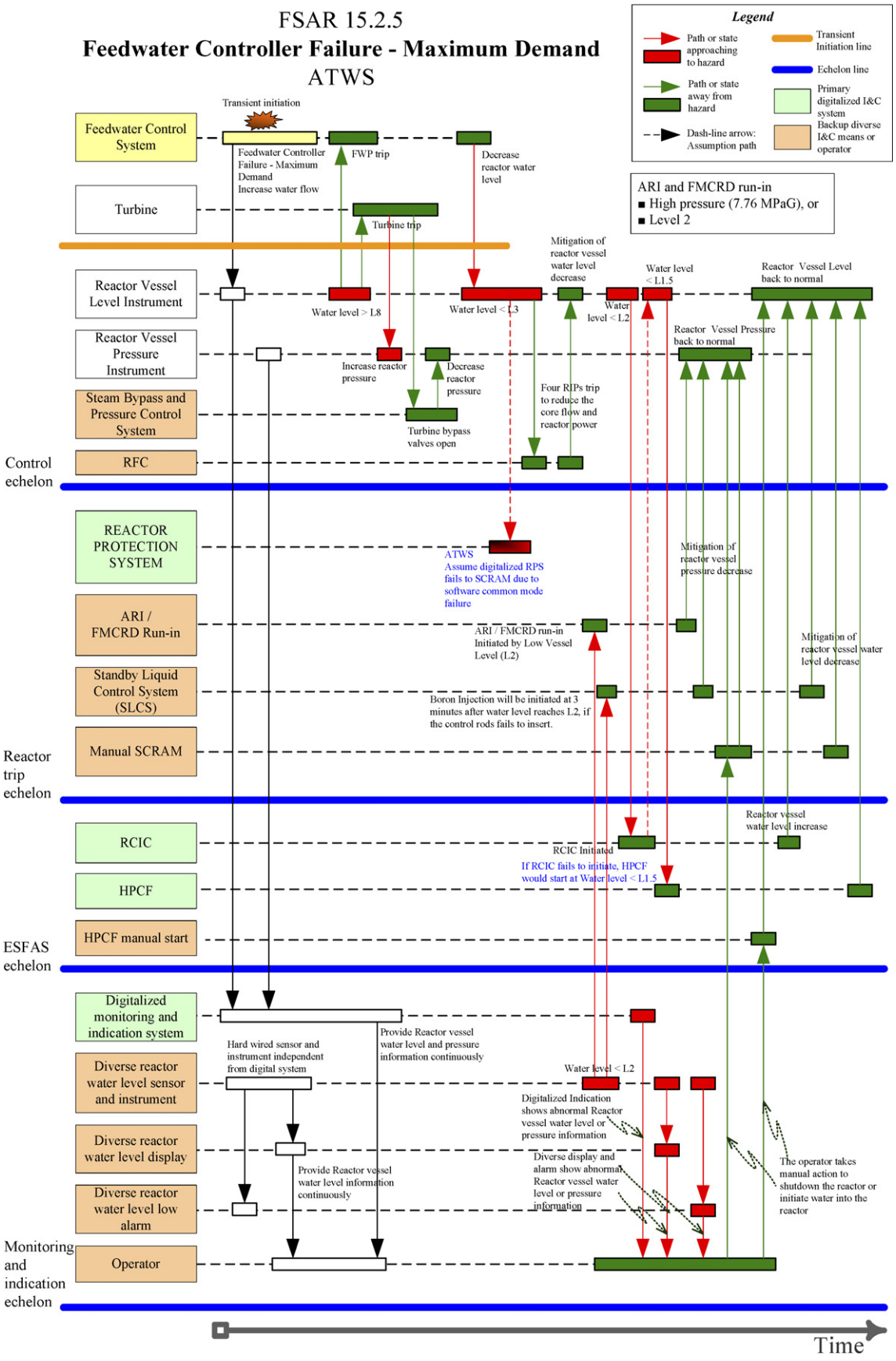

Fig. 4. RPS sequence tree case study.

not as strong as that of the primary reactor scram. The FMCRD run-in adopts a motor to insert the control rods, and takes even longer to perform reactor shutdown. The SLCS injects boron to the reactor 3 min after the water level reaches Level 2 if the control rod still fails to insert. Hard-wired manual scram is the last defense line of reactor shutdown performed by the operator.

In the ESFAS echelon, RCIC is initiated if the water level reaches Level 2. If the reactor is successfully scrammed, then RCIC begins to inject water into the reactor vessel to avoid core uncovery. However, the high reactor power consumes water quite rapidly in the ATWS case. Consequently, the water level might reach Level 1.5 and initiate HPCF. Manual HPCF hard-wired initiation is an alternate means to ensure that the reactor core can be covered under water.

In the monitoring and indication echelon, the digitalized monitoring and indication system continuously provides information about the water level and pressure of the reactor vessel. Additionally, the diverse reactor water level sensor and instrument, the diverse reactor water level display and the diverse reactor water level low alarm can provide alternate information to help the operator determine whether to take manual action to shut the reactor down or inject water into the reactor. This analysis result of the case study reveals that the diverse mitigation means design is sufficient to protect the fuel and the NPP in the "feedwater controller failure-maximum demand" event.

4.2. Emergency core cooling system

The ECCS case study analyzed the "LOCA-HPCF line break" event in the ABWR SAR event analysis table and sequence-tree method. ECCS is designed to mitigate the consequence of LOCA. All the ECCS-involved events in SAR should be selected and analyzed for a complete ECCS analysis. A significant improvement in ABWR is the redesign of the recirculation pumps with an outer loop recirculation line to reactor internal pumps. Hence, the major LOCA considerations are the main steam line break, the feedwater line break and the HPCF line break, which are much less severe than the recirculation line break.

Table 3 shows the event analysis of the ECCS case study. The "LOCA-HPCF line break" event is described in SAR Section 6.3. The event initiator is the HPCF line break. The water level starts to fall due to LOCA. The reactor scrams when the water level falls to Level 3. RCIC is initiated when the water level falls to Level 2. This event assumes one HPCF line break, meaning that another HPCF cannot start due to diesel generator failure. No HPCF water is injected when the water level falls below Level 1.5. MSIV closes when the water level falls to Level 1.5. Finally, ADS is opened, and RHR/LPFL starts to inject water to the reactor vessel, when the water level reduces to Level 1. Table 3 also describes the roles of RCIC, ADS and RHR/LPFL. The table also lists the mitigation procedures for handling the software common failure. If ADS fails to open or LPFL fails to be initiated due to software common mode failure, then the operator can recognize the water level decreasing to Level 1 by digital or diverse water level indication, and manually open ADS or start RHR/LPFL by hard-wiring.

Fig. 5 presents the case study of the ECCS sequence tree. In the "LOCA-HPCF line break" event, the HPCF line break is the event initiator, which results in an abrupt fall in the water level. Two HPCF divisions are designed in ABWR. This event assumes that following one HPCF line break, another HPCF cannot start owing to diesel generator failure. Hence, no HPCF loops can inject water into the reactor vessel. No control system in the control echelon is involved in the event. The reactor vessel level instruments play an essential role in initiating the ESFAS echelon systems. The level instrument only measures the water level, and transmits it in analog signals. The digital I&C systems in the reactor trip echelon and the ESFAS echelon convert these analog signals into digital signals.

Table 3
Analysis table case study on HPCF failure event

Section	Title	Event description	The role of analyzed safety-related I&C system	Mitigation means
SAR Section 6.3	LOCA-HPCF line break	• Assume HPCF line break • Rx scram due to water level falling to Level 3 • RCIC initiated due to water level falling to Level 2 • HPCF line is broken, therefore no HPCF injection, when water level falls to Level 1.5 • MSIV closed due to water level falling to Level 1.5 • ADS opened and LPFL initiated due to water level falling to Level 1	• RCIC initiated due to water level falling to Level 2 • ADS opened and RHR/LPFL initiated due to water level falling to Level 1	If ADS fails to be opened or LPFL fails to be initiated due to software common mode failure, then (1) No diverse means in the main control room can perform ADS open or LPFL (2) The operator can recognize the water level falling to Level 1, and notifies the maintenance personnel to open ADS or initiate RHR/LPFL

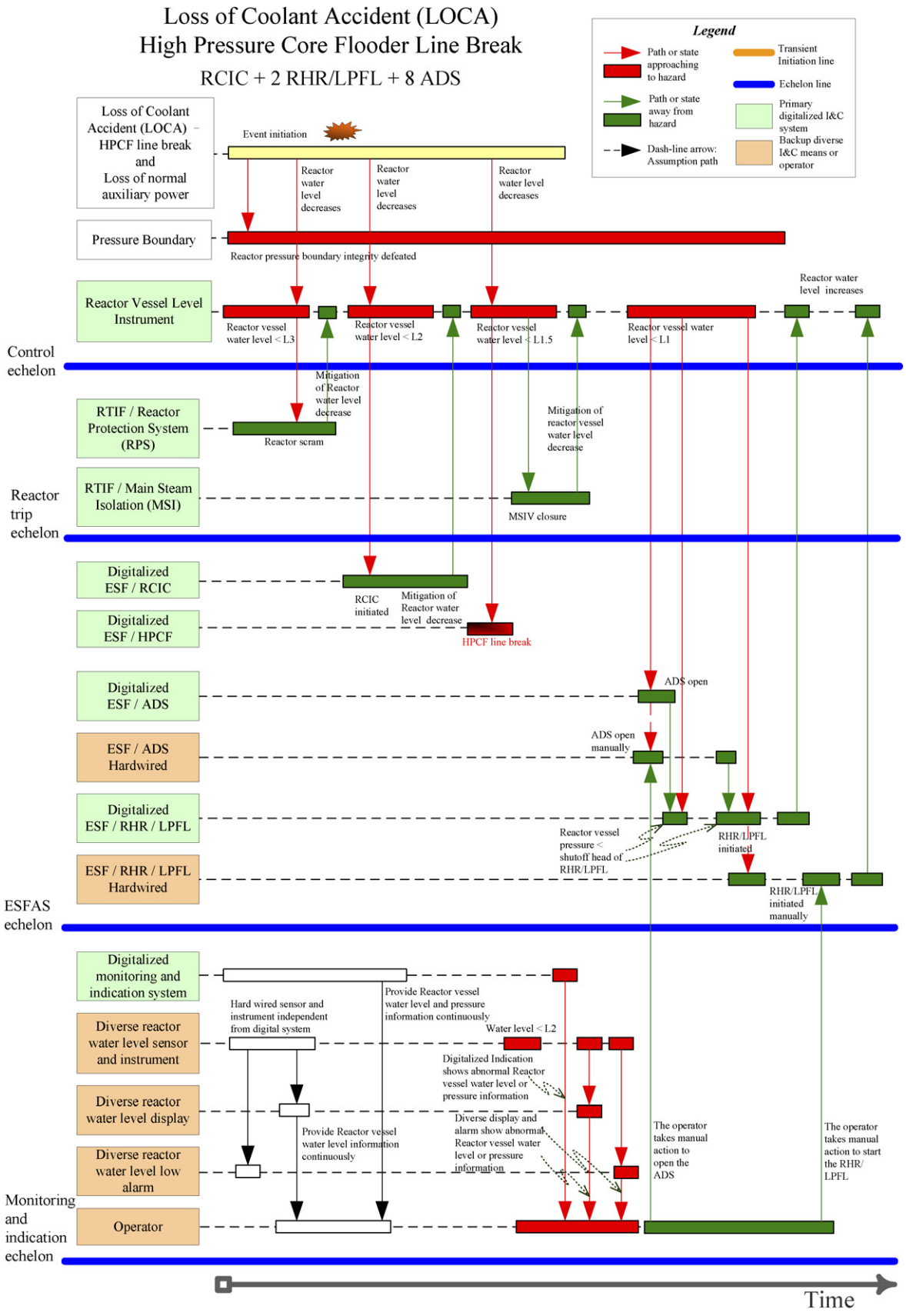

Fig. 5. ECCS sequence tree case study.

In the reactor trip echelon, the reactor is scrammed when the water level reduces to Level 3. The MSIV is closed when the water level reduces to Level 1.5. Since this case study concentrates on ECCS, it does not address software common mode failure in the reactor trip echelon. If the RPS and ESFAS adopt the same operating system, then failure in the software common mode might defeat both echelons simultaneously.

In the ESFAS echelon, RCIC is initiated if the water level reaches Level 2. ADS is opened, and RHR/LPFL is initiated to inject water to the reactor vessel when the water level drops to Level 1. If software common mode failure defeats the digital ADS or RHR/LPFL I&C system, then the operator should manually initiate the system by hard-wiring.

In the monitoring and indication echelon, the digitalized monitoring and indication system continuously provides reactor vessel water level and pressure information. Additionally, the diverse reactor water level sensor and instrument, the diverse reactor water level display and the diverse reactor water level low alarm can provide alternative information to notify the operator to initiate the ADS or RHR/LPFL system by manual hard-wiring.

If automatic analog backup ADS and RHR/LPFL I&C systems are adopted, then the operator's work load and responsibility can be shared when a software common mode related event happens.

5. Conclusion

This study has successfully developed a system-level sequence-tree-based PHA that can clarify the relationships among the major digital I&C systems. This system-centric technique cannot only identify preliminary hazards, but also vulnerabilities in a nuclear power plant. Hence, inadequacies in the analog back-up systems or hard-wired manual initiation design can be improved, i.e., an effective simplified diversity and defense-in-depth evaluation can also be performed. Two case studies are demonstrated in this paper, namely an RPS related case and an ECCS related case to prove the feasibility of this method.

Manual action is the last line of defense in the all echelons in the NPP. If the D3 design includes sufficient automatic analog backups, then the operator's working load and responsibility can be properly shared when a software common mode related event occurs. Additionally, the US NRC established the position on D3 for the advanced reactors in the document BTP-19, noting that, "The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions." This means that the utilities can adopt industrial grade analog I&C systems as the backups of digital system without being suffered by the safety grade regulatory process.

Acknowledgement

The authors thank Dr. Jong-Rong Wang, Li-Hsin Wang, Yuan-Chang Yu, Ben-Ching Liao of INER and Wei-Yi Yang, Wan-Tsz Tu, Hung-Chih Hung, Shu-Chuan Chen of NTHU for their technical assistance.

References

Branch Technical Position HICB-14, 1997. Guide on Software Review for Digital Computer-Based Instrumentation and Control System, USNRC, Washington, DC, USA.

Branch Technical Position HICB-19, 1997. Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems, USNRC, Washington, DC, USA.

Huang, H. et al., 2005. Development and Application of a Simulation Framework for Investigating Human Computer Interaction Process, 19th Sino-Japanese Seminar on Nuclear Safety, Taipei, Taiwan.

Huang, H. et al., 2006a. Digital I&C Failure Events Derivation and Analysis for ABWR, Dependability of Computer Systems 2006 (DepCoS '06), Szklarska Poręba, Poland.

Huang, H. et al., 2006b. Digital Instrumentation and Control Failure Events Derivation and Analysis by Frame-Based Technique, ICONE14, Miami, Florida, USA.

Huang, H. et al., 2006c. Development of Evaluation Method for Software Safety Analysis Techniques, 15PBNC, Sydney, 15–20 October 2006.

Huang, H. et al., 2006d. Development of Evaluation Method for Software Hazard Identification Techniques, 5th NPIC & HMIT, Albuquerque, NM, USA.

Huang, H. et al., 2007a. Model extension and improvement for simulator-based software safety analysis. Nuclear Engineering and Design 237, 955–971.

Huang, H. et al., 2007b. Software failure events derivation and analysis by frame-based technique. Annals of Nuclear Energy 34, 307–318.

IEEE Std. 1044-1993, IEEE Standard Classification for Software Anomalies.

IEEE Std. 1228-1994. IEEE Standard for Software Safety Plans.

IEEE Std. 7-4.3.2-2003, IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations.

Lee, J. et al., 2001. 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 207, 95–104.

Lee, J. et al., 2006. Evaluation of error detection coverage and fault-tolerance of digital plant protection system in nuclear power plants. Annals of Nuclear Energy 33 (6), 544–554.

Liu, J. et al., 2007. Safety analysis of software product lines using state-based modeling. Journal of Systems Software. doi:10.1016/j.jss.2007.01.04.

Micro-Simulation Technology, 2007. <http://www.microsimtech.com/>.

NUREG/CR-6303, 1994. Method for Performing Diversity and Defense-in-depth Analyses of Reactor Protection Systems.

NUREG/CR-6430, 1995. Software Safety Hazard Analysis.

Po, L.C., 1981. A faster than real-time computer code for loss of coolant and feedwater transient prediction. ANS Transactions 39, 1056–1057.

RELAP5-3D Home Page, 2007. <http://www.inl.gov/relap5/>.

RETRAN-02, 2007a. <http://www.csai.com/retran/R02index.html>.

RETRAN-3D, 2007b. <http://www.csai.com/retran/R3Dindex.html>.

SECY 93-087, 1993. Defense against Common-Mode Failures in Digital Instrumentation and Control System, Staff Requirement Memorandum.

Swu, Y. et al., 2004. Development and Application of Risk Analysis Techniques for Digital I&C Systems, Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies NPIC & HMIT 2000, Columbus, OH, USA.