The Basic Idea of Quantitative Model of Reactor Protection System Considering Stochastic Process

Hitoshi Muta[a]
[a] Tokyo City University, Tokyo, Japan

Abstract: In nuclear power plants such as ABWR and the latest PWR, digital instrumentation and control system have been installed increasingly to reactor emergency shutdown system which is one of the important safety functions. However, it has been found that it is difficult to model the digital equipment reliability in probabilistic risk assessment (PRA). And some of issues such as taxonomies of failure modes have been studied in the international framework, OECD/NEA/WGRisk task group called DIGREL.
In this paper, the reactor trip actuation failure event logics and frequencies resulting from the multiple failures and the demand following the initiating event are analyzed qualitatively and quantitatively. This paper presents the example of the reliability analysis of the digital Reactor Protection System (RPS) considering stochastic process, the approach given by this paper will be applicable to establish the PRA model of digital RPS of the actual nuclear power plant.

Keywords: DI&C, RPS, Self-diagnostic Function; Stochastic Process; Markov Transition Model.

1. INTRODUCTION

Several PRA studies to model the digital safety system have been done so far. For example, in ABWR PRA conducted in Japan [1][2][3][4][5], conventional Fault Tree Analysis (FTA) technique was used in reliability analysis of the digital RPS. However, it has been found that it is difficult to model the digital equipment reliability in probabilistic risk assessment (PRA) using conventional FTA technique because FTA cannot simulate precisely state transition among various states and functions of digital equipment.
OECD/NEA CSNI WGRisk set up the task group DIGREL to develop the basis of reliability analysis method of the digital safety system and now discussing about several issues related to quantitative modeling including the taxonomies of digital system failure modes [6][7][8]. Although conventional FTA technique has been applied to reliability analysis of the digital RPS so far, introducing more dynamic approach is essential to properly assess the effects of repair or manual shutdown operation following detection of faults by self-diagnostic function. However, there is few PRA including dynamic reliability models of DI&C system currently, and dynamic approach is considered to be still in a trial stage.
In this paper, the reactor trip actuation failure event logics and frequencies resulting from the multiple failures and the demand following the initiating event are analyzed qualitatively and quantitatively. Then the comparison is made between the method obtained in this paper and FTA technique to clarify the difference.

[Notations and definitions]
P_i: probability of the state in i
λ_M [1/hr]: initiating event frequency (the probability of demand of the RPS per unit time at time t, given the RPS is not actuated at time t)
λ[1/hr]: constant hardware failure rate
λ_D [1/hr]: constant detected hardware failure rate
λ_U [1/hr]: constant undetected hardware failure rate
R [1/hr]: constant restart rate of the reactor (the probability of transfer per unit time at time t, given the system is in shutdown state at time t)

m [1/hr]: constant renewal rate of the reactor (the probability of renewal per unit time at time t, given the system is in ATWS at time t)
ω_C [1/hr]: ATWS frequency per unit calendar time in the steady state
ω_C^* [1/hr]: the part of ATWS frequency ω_C caused by the independent hardware failure and the demand
ω_C^{**} [1/hr]: the part of ATWS frequency ω_C caused by the common cause hardware failure and the demand
ω_R [1/hr]: ATWS frequency per unit reactor operational time in the steady state
ω_R^* [1/hr]: the part of ATWS frequency ω_R caused by the independent hardware failure and the demand
ω_R^{**} [1/hr]: the part of ATWS frequency ω_R caused by the common cause hardware failure and the demand

2. The Digital Reactor Protection System Description

The RPS is one of the most important functions to control reactivity, actuate reactor trip in an emergency situation and maintain the reactor in safe state. This accident sequences are defined as the anticipated transient without scrum (ATWS) event in PRA study and are very important to core damage risk [1]-[5]. Figure 1 is a simplified event tree that is focused on accident sequences of ATWS event. If neither does the RPS actuate nor do control rods insert successfully, ATWS event will occur. Generally, the RPS is typically consisted of multiple channels such as "1-out-of-2 twice" or "2-out-of-4" configuration, including several devices and complicated connections [9]. However, to make the discussion easier, the RPS is hypothetically assumed to be composed of two independent channels that are regarded as simple 1-out-of-2 configuration as shown in Figure 2. Here, reactor trip is actuated by two solenoid valves A & B opening in case that 1-out-of-2 channel of the RPS is activated with trip signal from a sensor.

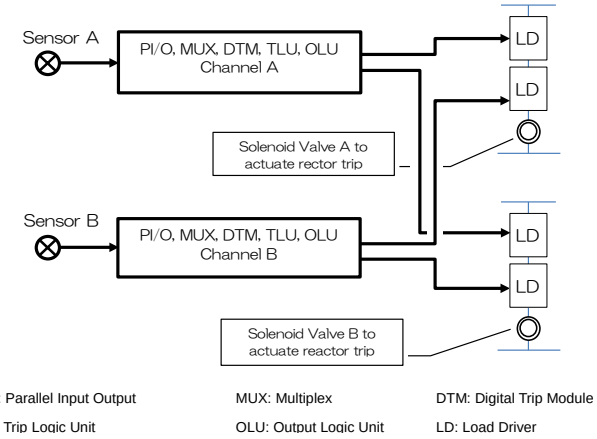


Figure 1. Outline of Simplified Digital Reactor Protection System (1-out-of-2 Configuration)

The following postulates are put on the RPS described above:

a) a hardware failure and a software failure are considered,
b) for the RPS hardware failure mode, the division level failure which is being discussed in DIGREL [6] is applied in this paper, so it is possible to be considered that hardware failure is defined as loss of function of a channel of the RPS including sensor, PI/O, MUX, DTM, TLU and OLU,
c) to avoid the reliability model too much complicated and to be focused on clarifying the validity of this approach, the failures of LDs, solenoid valves and control rod drive (CRD) system out of the logic circuits are assumed to be negligible,
d) the hardware failure mode in a channel of the RPS is classified into the common cause failure and the independent failure,
e) the common cause failure and the independent failure are respectively classified into the detected failure and the undetected failure,
f) the detected fault is detected instantly by a self-diagnostic function which runs continuously,
g) the undetected fault can be detected by a surveillance test which is executed at an interval of T,
h) to make discussion easier, the software fault is not considered in this paper,
i) a plant personnel starts to repair the failed channel of the RPS after detection of single hardware fault by self-diagnostic function or surveillance test,

j) a plant personnel makes the reactor shutdown immediately after a detection of hardware fault of both channels by self-diagnostic function or surveillance test,
k) a duration of shutdown operation is T_{SD},
l) the reactor returns to the initial state after the shutdown state and restarts, and
m) the reactor is renewed after the state of core damage following ATWS sequence.

The following statistical assumptions are made:
i) the initiating events and the failures of the RPS occur statistically-independently and randomly,
ii) the start of the initiating event can be modeled by the exponential distribution with the demand rate of λ_M,
iii) the reactor returns from shutdown state to the initial state by the constant transfer rate of R,
iv) the hardware fault in a channel of the RPS that is according to the postulate b), can be modeled by the exponential distribution with the total constant hardware failure rate of λ, which can be divided into a detected hardware fault and an undetected hardware fault.
v) a detected hardware fault can be modeled by the exponential distribution with the constant hardware failure rate of λ_D,
vi) an undetected hardware fault can be modeled by the exponential distribution with the constant hardware failure rate of λ_U,
vii) a repair of detected hardware fault can be modeled by the exponential distribution with the constant restoration rate of μ_R, which can be approximated as *(1/MTTR)*,
viii) a repair of undetected hardware fault can be modeled by the exponential distribution with the constant restoration rate of μ_R, which can be approximated as *(1/MTTR)*,
ix) a shutdown operation can be modeled by the exponential distribution with the constant transition rate of μ_{SD}, which can be approximated as $(1/T_{SD})$,
x) a mean failure-duration time of "single undetected hardware fault" can be approximated as *(T/2)*, a mean failure-duration time of either "independent double undetected hardware fault" or "superposition of independent undetected hardware fault and independent detected hardware fault" can be approximated as *(T/3)* and a mean failure-duration time of "common cause undetected hardware fault" can be approximated as *(T/2)*,
xi) the ratio of the common cause hardware failure to λ_D and λ_U is expressed as β,
xii) the reactor is renewed after core damage event following ATWS event by the constant renewal rate of m.

3. Analyses of ATWS event frequency

In this section, the process of ATWS event is analysed for the reactor equipped the RPS defined in the previous section.

3.1. *Core damage event logics and the fault tree*

In general, ATWS event could occur through one of the following sequential logics:
(A) an initiating event occurs in fault of both channels of the RPS, or
(B) both channels failure of the RPS occurs in a demand state after an initiating event.
It is obvious that those two logics are mutually exclusive. The two sequential logics for the core damage events are developed by the FTA technique with the priority AND-gate as shown in Figure 3 and Figure 4.
The top event, ATWS event (E-top), occurs when the logic of either "the demand and common cause hardware fault (E1)", "the demand and independent multiple hardware faults (E2)" or "the demand and the software fault (E3)" is true.
The first logic E1 becomes true when either Sequence #1-1 or Sequence #1-2 is true. Sequence #1-1: if a common cause hardware failure occurs in the demand state resulting from an initiating event, then ATWS event occurs. However, since the RPS is a stand-by system and initiating events must be prior to the actuation of the RPS, it is not necessary to consider this sequence. Sequence #1-2: if an

initiating event occurs in the common cause hardware fault resulting from a common cause hardware failure, then ATWS event occurs.
The second logic of E2 is classified into the sequences #2-1 through #2-6. Sequence #2-1: if the independent hardware failure of channel B occurs in the state resulting from a demand after an initiating event and an independent hardware fault of channel A, then ATWS event occurs. The other sequences can be expressed in the same manner such that #2-2 is "Demand>channel B failure>channel A failure", #2-3 is "channel A failure >Demand> channel B failure", #2-4 is channel B failure>Demand> channel A failure. However, these sequences are not needed being considered because of the reason same as excluding the sequence #1-1. Although one of the RPS channel is fault for the sequences #2-3 and #2-4, they can be treated same as #2-1 and #2-2 because one channel is enough to actuate the RPS.
The last logic is a software failure. Since this study doesn't focus precise method, a software failure is not considered furthermore. Although there is a probability that any combination of E1 and E2 occur simultaneously, it is considered that the probability is sufficiently small to be negligible based on the rare event approximation. This means that these three ATWS event logics E1 and E2 can be treated separately, and the ATWS frequency can be approximated by the summation of these ATWS event frequencies of these three logics in the following discussion. In the next section, ATWS event caused by independent hardware faults are analyzed as an example.

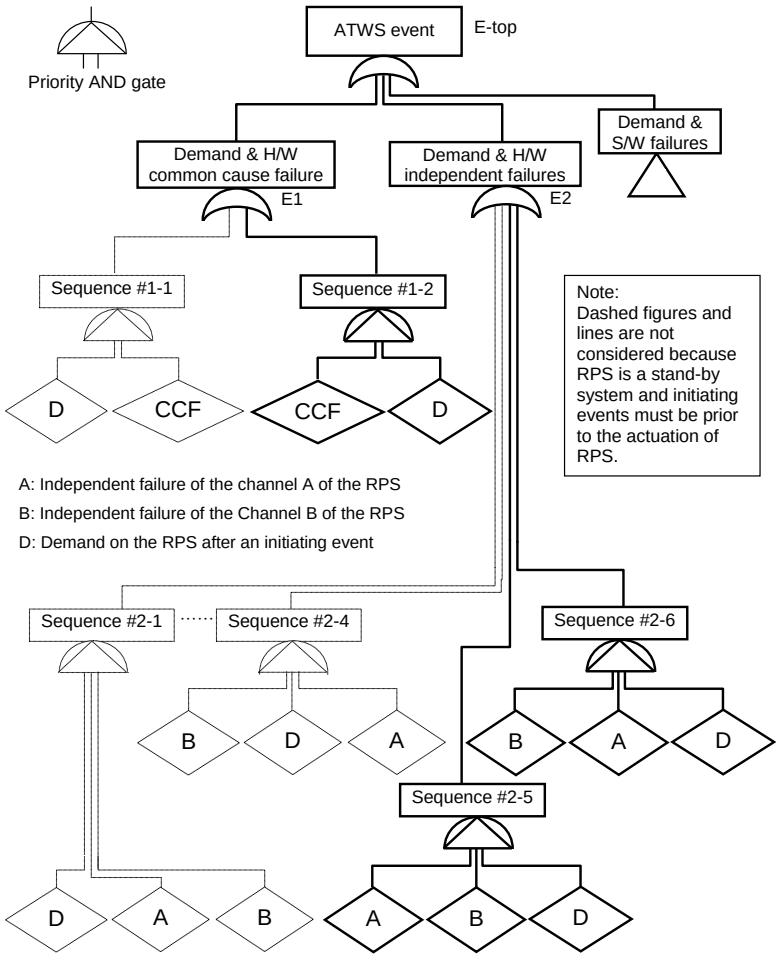


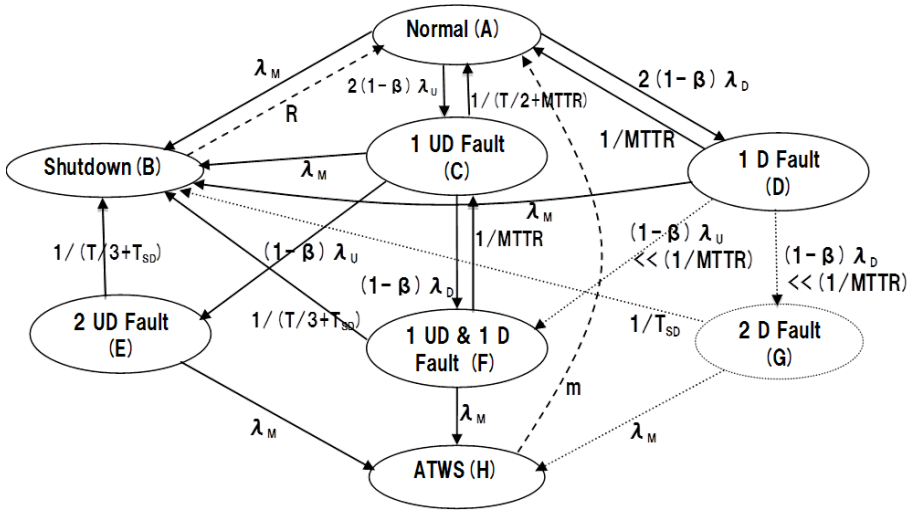
Figure 2 Outline of Simplified Digital Reactor Protection System (1-out-of-2 Configuration)

3.2. ATWS event caused by independent hardware faults

This can be modeled by a state-transition diagram as shown in Figure 5 based on the postulates a) through n), statistical assumptions i) through xiv) and sequential logics (A) and (B). Definitions of states are as follows:
State A: Normal state, there is no demand and faults,
State B: Shutdown state, a plant is not in an operation but in a safe state,
State C: One of the channels is in an undetected fault, but there is no demand,
State D: One of the channels is in a detected fault, but there is no demand,
State E: Both of the channels are in undetected faults, but there is no demand,
State F: One of the channels is in an undetected fault and the other is in a detected fault, but there is no demand,
State G: Both of the channels are in detected faults, but there is no demand, and
State H: Core damage state caused by ATWS.
The transitions and their transition rates are:

1) if a demand after an initiating event occurs in Normal State A, the reactor transfers from A to Shutdown State B, this occurs by the transition rate of λ_M; see statistical assumption ii),
2) if an undetected failure occurs in one of the channels in A, the reactor transfers from A to State C, this occurs by the transition rate of $2(1-\beta)\lambda_U$, in which the RPS is being repaired after a detection of undetected fault by surveillance test; see statistical assumption iv), vi) and xi),
3) if a detected failure occurs in one of the channels in A, the reactor transfers from A to State D, this occurs by the transition rate of $2(1-\beta)\lambda_D$, in which the RPS is being repaired after a detection of detected fault by self-diagnostic function; see statistical assumption iv), v) and xi),
4) the reactor returns from B to A, this occurs by the transition rate of R; see statistical assumption iii),
5) if the RPS is restored in C, the reactor transfers from C to A, this occurs by the transition rate of $\{1/(T/2+MTTR)\}$; see statistical assumption viii) and x),
6) if a demand after an initiating event occurs in C before restoration of undetected fault, the reactor transfers from C to B, in which one of the channels of the RPS is being actuated, this occurs by the transition rate of λ_M; see statistical assumption ii),
7) if another undetected failure occurs in C before restoration of undetected fault, the reactor transfers from C to State E, this occurs by the transition rate of $(1-\beta)\lambda_U$; see statistical assumption iv), vi) and xi),
8) if another detected failure occurs in C before restoration of undetected fault, the reactor transfers from C to State F, this occurs by the transition rate of $(1-\beta)\lambda_D$; see statistical assumption iv), v) and xi),
9) if the RPS is restored in D, the reactor transfers from D to A, this occurs by the transition rate of $(1/MTTR)$; see statistical assumption vii),
10) if a demand after an initiating event occurs in D before restoration of detected fault, the reactor transfers from D to B, in which one of the channels of the RPS is being actuated, this occurs by the transition rate of λ_M; see statistical assumption ii),
11) if another undetected failure occurs in D before restoration of detected fault, the reactor transfers from D to State F, this occurs by the transition rate of $(1-\beta)\lambda_U$; see statistical assumption iv) , vi) and xi), however, since this transition rate is generally much smaller than $(1/MTTR)$, so it is not necessary to consider this transition further,
12) if another detected failure occurs in D before restoration of detected fault, the reactor transfers from D to State G, this occurs by the transition rate of $(1-\beta)\lambda_D$; see statistical assumption iv), v) and xi), however, this transition rate is generally much smaller than $(1/MTTR)$, so it is not necessary to consider this transition further,
13) if a plant personnel makes the reactor shutdown successfully in E before a demand after a detection of simultaneous undetected fault of both channels by surveillance test, the reactor transfers from E to B, this occurs by the transition rate of $\{1/(T/3+MTTR)\}$; see statistical assumption ix) and x),
14) if a demand occurs in E before completion of shutdown operation, the reactor transfers from E to state H, this occurs by the transition rate of λ_M; see statistical assumption ii),
15) if a plant personnel makes the reactor shutdown successfully in F before a demand after a detection of simultaneous detected fault and undetected fault of each channel by self-diagnostic function and surveillance test, the reactor transfers from F to B, this occurs by the transition rate of $\{1/(T/3+MTTR)\}$; see statistical assumption ix) and x),
16) if one of the channels of the RPS is restored in F after a detection of detected fault by self-diagnostic function, the reactor transfers from F to C, this occurs by the transition rate of $(1/MTTR)$; see statistical assumption vii),
17) if a demand occurs in F before completion of shutdown operation, the reactor transfers from F to H, this occurs by the transition rate of λ_M; see statistical assumption ii),
18) if a plant personnel makes the reactor shutdown successfully in G before a demand after a detection of simultaneous detected fault of both channels by self-diagnostic function, the reactor transfers from G to B, this occurs by the transition rate of $(1/T_{SD})$; see statistical assumption ix). However, the probability in state G is quite small, because the transition rate from G to B is negligible as explained in 12), so it is not necessary to consider this transition,

19) if a demand occurs in G, the reactor transfers from G to H, this occurs by the transition rate of λ_M; see statistical assumption ii), however, the probability in state G is quite small as explained as 12) and 18), so it is not necessary to consider this transition, and,



UD Fault: Undetected Fault

D Fault: Detected Fault

Figure 3. A state-transition diagram of ATWS event for independent hardware failures

20) The reactor transfers from H to A by a renewal of the reactor, this occurs by the transition rate of *m*; see statistical assumption xii).

Because of the above descriptions 11), 12), 18) and 19), it is not necessary to consider state G and transitions from D to F, from D to G, from G to B and from G to H. The state-transition diagram presents the following simultaneous equations in a steady state:

$$P_A + P_B + P_C + P_D + P_E + P_F + P_H = 1, \quad (1)$$

$$\{\lambda_M + 2(1-\beta)\lambda_U + 2(1-\beta)\lambda_D\} \cdot P_A = R \cdot P_B + \frac{1}{\frac{T}{2} + MTTR} \cdot P_C + \frac{1}{MTTR} \cdot P_D + m \cdot P_H, \quad (2)$$

$$R \cdot P_B = \frac{1}{\frac{T}{3} + T_{SD}} \cdot P_E + \frac{1}{\frac{T}{3} + T_{SD}} \cdot P_F + \lambda_M \cdot P_D + \lambda_M \cdot P_C + \lambda_M \cdot P_A, \quad (3)$$

$$\{\frac{1}{\frac{T}{2} + MTTR} + \lambda_M + (1-\beta)\lambda_U + (1-\beta)\lambda_D\} \cdot P_C = 2(1-\beta)\lambda_U \cdot P_A + \frac{1}{MTTR} \cdot P_F, \quad (4)$$

$$(\lambda_M + \frac{1}{MTTR}) \cdot P_D = 2(1-\beta)\lambda_D \cdot P_A, \quad (5)$$

$$(\lambda_M + \frac{1}{\frac{T}{3} + T_{SD}}) \cdot P_E = (1-\beta)\lambda_U \cdot P_C, \quad (6)$$

$$(\frac{1}{\frac{T}{3} + T_{SD}} + \frac{1}{MTTR} + \lambda_M) \cdot P_F = (1-\beta)\lambda_D \cdot P_C \quad (7)$$

and

$$m \cdot P_H = \lambda_M \cdot (P_E + P_F). \quad (8)$$

Based on Figure 5 and the definition, the ATWS frequency caused by the independent hardware fault and the demand per unit calendar time in the steady state, ω_C is given as

$$\varpi_C^* = \lambda_M \cdot P_E + \lambda_M \cdot P_F (= m \cdot P_H). \quad (9)$$

From equations (1) through (9), ω_C^* becomes

$$\varpi_C^* = \frac{(\lambda_M \cdot X_1 + \lambda_M \cdot X_2)}{1 + X_1 + X_2 + X_3 + X_4 + \frac{1}{R} \cdot \left(1 + \lambda_M (X_3 + X_4) + \frac{X_1 + X_2}{\frac{T}{3} + T_{SD}} \right) + \frac{\lambda_M}{m} \cdot (X_1 + X_2)} . \quad (10)$$

Here,

$$X_1 = \frac{(1-\beta) \cdot \lambda_U}{\lambda_M + \frac{1}{\frac{T}{2} + MTTR}},$$

$$X_2 = \frac{(1-\beta) \cdot \lambda_D}{\lambda_M + \frac{1}{MTTR} + \frac{1}{\frac{T}{3} + T_{SD}}},$$

$$X_3 = \frac{\frac{1}{\frac{T}{2} + MTTR} + \lambda_M + (1-\beta)(\lambda_D + \lambda_U) - \frac{1}{MTTR} \cdot X_2}{2(1-\beta) \cdot \lambda_U}$$

and

$$X_4 = \frac{2(1-\beta) \cdot \lambda_U \cdot X_3}{\lambda_M + \frac{1}{MTTR}} .$$

Since ω_R^* which is defined as the ATWS frequency caused by the independent hardware fault and the demand per unit reactor operational time in the steady state, can be obtained by normalized by operational time, ω_R^* is given as

$$\varpi_R^* = \frac{\varpi_C^*}{1 - P_B - P_H} . \quad (11)$$

Moreover, equation (11) can be rewritten as

$$\varpi_R^* = \frac{\lambda_M \cdot (X_1 + X_2)}{1 + X_1 + X_2 + X_3 + X_4} . \quad (12)$$

It is easily found that equation (12) does not include the parameter of R and m. This means that ω_R^* is not affected by the value of R and m (>0). Namely, because P_B and P_H become null when $R \rightarrow \infty$ and $m \rightarrow \infty$ (see equation (10)), equation (12) is equal to equation (10) in which $R \rightarrow \infty$ and $m \rightarrow \infty$. In addition, the reciprocal of ω_R^* is equal to the meantime from the state A to H, because the ATWS frequency of the reactor is equal to the reciprocal of mean time from the initial state to ATWS in the steady state.

3.3. *ATWS event frequency*

For ATWS event caused by common cause hardware faults can be analyzed in the same manner described in the section 3.2. Therefore, ATWS event frequency per unit calendar time is

$$\omega_C = \omega_C^* + \omega_C^{**}, \quad (13)$$

and, ATWS event frequency per unit reactor operational time is

$$\omega_R = \omega_R^* + \omega_R^{**}. \quad (14)$$

4. CONCLUSION

Digital devices have been realizing advanced functions such as complicated control or self-diagnostic. On the other hand, the method based on conventional FTA technique has become difficult to analyse the effects of recovery or shutdown operation following detection of faults by the diagnostic function appropriately.

This paper shows that, taking account of the relationship among the RPS failures, demand after the initiating event, detection of RPS fault by self-diagnostic or surveillance tests, repair of the RPS components and plant shutdown operation by the plant operators as a stochastic process, the ATWS event can be modelled by the event logic fault tree and state-transition diagrams assuming the hypothetical 1-out-of 2 digital RPS. Then, the ATWS event frequency is formulated base on the state-transition diagrams. Because introducing more dynamic approach is essential to properly assess the effects of repair or manual shutdown operation following detection of faults by self-diagnostic function specific to the digital safety system as shown in this paper.
Thus the approach given by this paper will be applicable to establish the PRA model of the digital RPS of the actual nuclear power plant. For simplicity, this paper assumes simplified 1-out-of-2 configuration RPS. However, the approach given by this paper will be applicable to the analysis of actual RPS equipped 1-out-of-2 twice or 2-out-of-4 configuration.

References

[1] Nuclear Power Engineering Corporation (NUPEC). [The Report of Establishment of Level 1 PSA Method of ABWR Plant at Power Operation (1998)]. Japan: Nuclear Power Engineering Corporation; 1999. INS/M98-26. [Japanese]

[2] Nuclear Power Engineering Corporation (NUPEC). [The Report of Establishment of Level 1 PSA Method of ABWR Plant at Power Operation (1999)], Japan: Nuclear Power Engineering Corporation; 2000, INS/M99-29. [Japanese]

[3] Nuclear Power Engineering Corporation (NUPEC). [The Report of Establishment of Level 1 PSA Method for Internal Events at Power Operation = Reliability Analysis of Digital Reactor Protection System = (2002)]. Japan: Nuclear Power Engineering Corporation; 2003, INS/M02-29. [Japanese]

[4] Japan Nuclear Energy Safety Organization (JNES). [The Report of Establishment of Level 1 PSA Method for Internal Events at Power Operation = Improvement of Reliability Analysis of Digital Reactor Protection System (PWR) =]. Japan: Japan Nuclear Energy Safety Organization; 2007, JNES/SAE07-029. [Japanese]

[5] Japan Nuclear Energy Safety Organization (JNES). [The Report of Establishment of Level 1 PSA Method for PWR Plants at Power Operation = 3-Loop PWR Plant with/without Accident Management Countermeasures=]. Japan: Japan Nuclear Energy Safety Organization; 2009, JNES/SAE08-013. [Japanese].

[6] Stefan Authen, Jan-Erik Holmberg. Reliability Analysis of Digital Systems in a Probabilistic Risk Analysis for Nuclear Power Plants. NUCLEAR ENGINEERING AND TECHNOLOGY. 2012 June; VOL.44 NO.5.

[7] Ewgenij Piljugin, Stefan Authén, Jan-Erik Holmberg. Proposal for the Taxonomy of Failure Modes of Digital System Hardware for PSA. Paper presented at: 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference; 2012 June; Helsinki, Finland.

[8] Tsong-Lun Chu, Meng Yue, Wietske Postma. A Summary of Taxonomies of Digital System Failure Modes Provided by the DigRel Task Group. Paper presented at: 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference; 2012 June; Helsinki, Finland.

[9] Japan Nuclear Energy Safety Organization (JNES). [The Report of Improvement of Reliability Model of Digital Reactor Protection System]. Japan: Japan Nuclear Energy Safety Organization; 2010, JNES/SAE10-013. [Japanese]

[10] T Shimodaira, Y Sato and K Suyama. [Estimation of hazardous event rate for repairable 1-out-of-2 safety-related systems based on state transition models]. Trans of the institute of Electronics, Information and Communication Engineers. 2005 August; Vol.J88-A. No.8: P.962-973. [Japanese]