Proceedings of the Korean Nuclear Society Spring Meeting
Gyeongju,, Korea, 2004

A Study on the Development of Color Assignment Criteria for Defense-in-Depth Risk Evaluation

Huichang Yang, Sung Soo Choi

Atomic Creative Technology
1688-5 Shinil-dong, Daeduk-gu
Taejun, Korea 306-230

Hae Chul Oh, Mi Ro Seo, Myoung Ki Kim

Korea Electric Power Research Institute
Moonji-dong, Yusung-Gu
Taejun, Korea 305-380

Abstract

Defense-in-depth in nuclear safety can be defined as a hierarchical development of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers, in normal operation, anticipated operational occurrences and, for some barriers, in accidents at the plant. The blended approach in which both qualitative an quantitative risk evaluation were adopted became necessary to enforce the defense-in-depth in nuclear safety while enhancing the safety and minimizing the utility and regulatory burdens by focusing safety significant structures, systems, and components. In this study, SFATs for the Reactivity Control safety function were developed as an example case and SFAT based on the Technical Specifications requirements showed much conservative evaluation results than SFAT based on the functional criteria which were derived from the deterministic engineering judgment. The most important element in development of defense-in-depth evaluation trees such as SFATs, the consistent and inclusive understanding and interpretation about the defense-in-depth in nuclear safety.

1. Introduction

Defense-in-depth in nuclear safety can be defined as a hierarchical development of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive materials and workers, the public or the environment, in normal operation, anticipated operational occurrences and, for some barriers, in accidents at the plant in IAEA International Nuclear Safety Advisory Group report, INSAG-10[1]. Since the risk-informed regulations were adopted by USNRC, many researches and applications to enhance the plant safety by managing the plant risk were performed. The quantitative risk measures such as core damage frequencies and large early release frequencies were used in risk management for at power operation of nuclear power plants. The risk management using quantitative risk measures utilizing PSA insights were quiet effective and helpful to derive the vulnerabilities in nuclear safety. However, the quantitative risk measures using PSA cannot reveal all weakness of nuclear safety for all range of operations and all challenges such as shutdown/outage operation and various external events. The qualitative risk evaluation methods based on the deterministic judgment and decision tree logics were adopted to compensate the quantitative approached in risk management. These blended approaches are used for configuration risk management which utilized the virtues of both quantitative and qualitative risk evaluation methodologies.

In this qualitative risk evaluation, the determination of minimum criteria for the plant safety features to perform the safety function which is necessary to terminate or mitigate the accident progression is very important because all colors which represent the plant safety status should be determined based on those minimum requirements. The most general requirements for the safety features were those in Technical Specifications which are based on safety analysis in Final Safety Analysis Report and use the deterministic engineering judgment either. Since the risk-informed approaches came into the enhancement of nuclear safety, Technical Specifications were evaluated that those are based on the too much conservative evaluation for the capabilities to the challenges, therefore the enhancement of Technical Specifications using the risk insights from various risk analysis of both quantitative and qualitative approaches is necessary. The other minimum criteria for plant safety features are success criteria used in probabilistic safety assessment in which the different criteria to give credit to certain configurations or alignments were used and those criteria were different one from Technical Specifications for some safety features.

Several criteria for the minimum safety features were developed to reveal the difference and the importance of minimum requirements for configuration risk management to balance the risk and safety of nuclear power plants. Using Safety Function Assessment Trees(SFATs) in ORAM-Sentinel[2], the deterministic logics to evaluate the capability of reference systems to perform a specific safety function were developed and the color assignment criteria which mean the minimum requirement were developed based on the several different approaches. Finally the different paths to different end states in SFAT were compared to show the importance of the proper color assignment criteria for configuration risk management using blended approach.

2. Blended Approach in Configuration Risk Management

Most nuclear power plants in US use the risk evaluation tools for configuration risk management such as ORAM-Sentinel, Safety Monitor, and EOOS. ORAM-Sentinel was originated from Outage Risk Management(ORAM) to manage risk during outage operations. There are so many different plant operating status during shutdown and outage operations that the quantitative risk assessment has the limit of uncertainties and because there is no clear definitions and requirements for such various plant operating status during outage, the qualitative approaches such as safety function assessment trees and plant transient assessment trees(PTATs) in ORAM were used to evaluate and manage the outage risk. The quantitative risk measures such as core damage frequencies and large early release frequencies were used as risk measures for at power or online operations generally. But the inherent limitation of quantitative risk evaluation methodology or PSA, the blended approach in which both qualitative an quantitative risk evaluation were adopted became necessary to enforce the defense-in-depth in nuclear safety while enhancing the safety and minimizing the utility and regulatory burdens by focusing safety significant structures, systems, and components. In ORAM-Sentinel, the risk and the level of defense-in-depth can be assessed by the deterministic trees and PSA module and the priorities of “Return-to-Service” and “Remain-in-Service” can be provided to the operators based on the maintenance schedules and the risk evaluation for the current configurations. During the process of assessing the configuration risk in terms of defense-in-depth by SFATs and PTATs, the predetermined criteria for the determination of plant status are used, and the plant status for given configuration is represented as a one color among four colors which are GREEN, YELLOW, ORANGE and RED.

The general definition of each status represented by color was presented in table 1. Each plant status was defined by the degree of risk increase, and RED color is assigned

Table 1. General Definitions of Overall Plant Safety Status

Color	Definition and Basis
Green	Defense-in-depth is well maintained, or maximum, for the safety function. Insignificant Risk Increase.
Yellow	Defense-in-depth is degraded, but is adequate for the safety function. Usually the plant is in a technical specification LCO. Significant Risk Increase.
Orange	Defense-in-depth is marginal for the safety function. This color usually indicates multiple LCOs are in effect. Very Significant Risk Increase
Red	Defense-in-depth is extremely challenged for restoration of the safety function under some or all accident events. This configuration should not be entered into voluntarily. Additionally, a Technical Specification Violation results in a RED result. Unacceptable Risk Increase

for the Technical Specification violation generally. In other words, ORANGE color is assigned to the status in which the current configuration meets the requirement specified in Technical Specifications. In other practice, the ORANGE color would be assigned to the status in which configuration meet the functional requirement to terminate or mitigate the accident sequences in terms of deterministic judgment. The latter case is more general in configuration risk management using blended approach.

3. Color Assignment Criteria for Deterministic Trees

The minimum requirements to perform safety function can be minimum number of specifics SSCs, trains, alignments or whole operational methods available, and this minimum can be defined as “N” in which N means number. If we have additional mean to the initiator, the number of methods available becomes “N+1” and this configuration can be defined as “YELLOW”, and “GREEN” with more mitigation methods. This approach is called as “Bottom-Up” because the first status to be defined is the bottom line or “ORANGE.” The other approach to assign colors is “Top-Down” approach in which the “GREEN” is defined as the status of “all available” which means all safety features needed to terminate and mitigate the accident sequence are available. If we loose one SSC or operational method, then the plant status becomes “YELLOW.” In top-down approach, there is a problem that there are so many yellow status that the “YELLOW” status becomes an additional requirements and the configuration which results “YELLOW” the operators or schedule planners hesitate to enter. This color assignment approach results too much restrict and conservative requirements utilities built by themselves. The bottom-up approach can provide an alternative approach to defined color criteria for the quantitative defense-in-depth evaluation and it becomes general approach for color assignment for risk monitors. The difference of color assignment by the each approach was illustrated in figure 1 simply.

In bottom-up approach, the most important element is to define the minimum requirements for safety functions. The Technical Specifications, PSA, and FSAR are referred to develop the color assignment criteria.

Since risk-informed regulations and operation technologies came into practice[3,4], many efforts were devoted to enhance the Technical Specifications for the purpose of improving plant safety and allowing flexibilities to utility, and reducing regulatory and utility burdens. For this case, the requirements from Technical Specifications and the deterministic functional requirement such as success criteria used in PSA show little differences. However, requirements specified in Technical Specifications to which risk insights were not applied has tendency to keep a lot of conservatism in it. For example, the success criteria in the state-of-the-art PSA for Korean nuclear power plants are less conservative compared with requirements in Technical Specification. Developing color assignment criteria based on such a restrict and conservative requirements, the plant status will be evaluated very conservative, as a result, the plant status would be “GREEN” or “RED,” and this situation was illustrated simply in figure 2.

4. SFAT Development for Reference Systems

Safety functions for Ulchin Nuclear Unit(UCN) 3 and 4 were defined in Functional Recovery Guidance(FRG), and the SFATs for the Reactivity Control safety function were developed as an example case.

In UCN FRG 3&4, there are three success paths for reactivity control and the first is control rod insertion, the second is boration with CVCS, and the third method is boration with SIS. The key SSCs for Reactivity Control safety function are RPS, DPS, charging pumps, high pressure safety injection pumps, refueling water storage tank, spent fuel pool and related injection paths. The requirements in Technical Specifications and success criteria used in PSA were represented in table 2.

In Technical Specifications, there is no requirement for Diverse Protection System(DPS) but DPS is in success criteria for reactivity control. As a boration makeup sources, Technical Specifications require RWST or SFP as an alternative source but SFP is not credited in PSA because the alignment for the flow path from SFP needs operator manual action.

Table 2. Requirements for Reactivity Control

	CR Insertion		Boration Sources and Path			Boration Pumps	
	RPS(CH)	DPS(CH)	RWST	SFP	Injection Path	Charging Pump	HPSI Pump
TS	3	X	1	1	1	1	1
PSA	2	2	1		1	1	1

Figure 1. Difference of color assignments by Bottom-Up and Top-Down Approaches

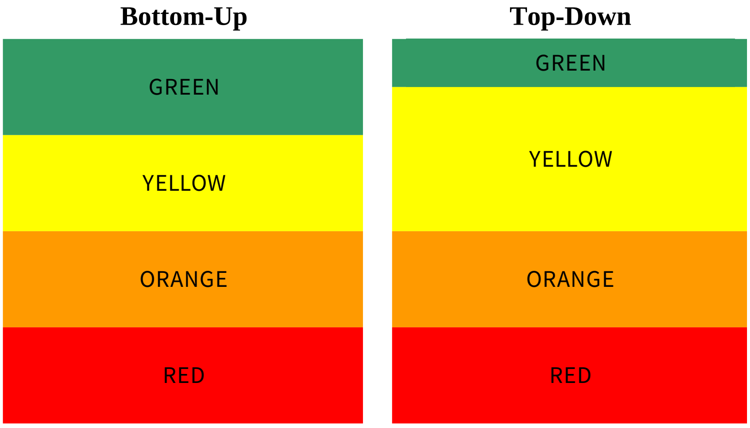
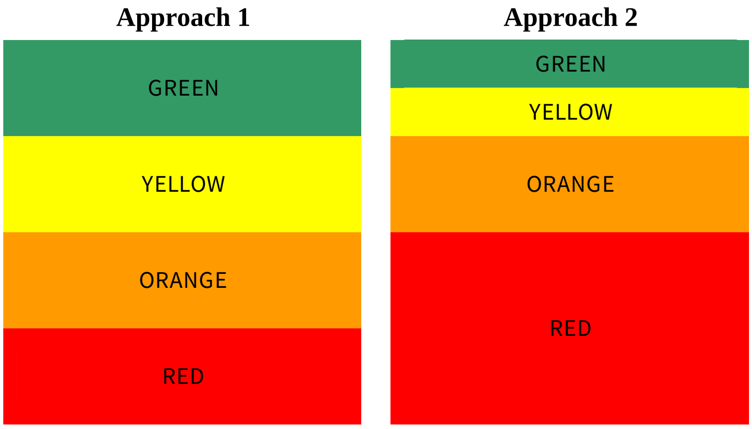


Figure 2. Comparison the color assignments by different approaches



For HPSI pumps, they are not requirement for boration but for emergency core cooling in TS. However, HPSI pumps are the one of main SSCs for boration in PSA. Considering the charging pumps are preferred mean to boration and have more redundancy than HPSI pumps, HPSI pumps might not be a minimum requirement for reactivity control safety functions but they can provide “+1” as an additional level of defense-in-depth in terms of diversity.

To develop a limiting logic path in SFAT using such various requirements, the principle of determining the level of defense-in-depth is necessary. There might be a question that the level of defense-in-depth could increase by additional available SSC, trains, or operational methods. To compare the difference of minimum requirement for limiting logic path determination from various principles, several matrices were developed and the requirements for limiting logic paths were represented in those matrices as table 3 and 4. To consider the High Risk Evolutions(HRE), the minimum requirements for ORANGE status were enforced to the “N+1” requirement.

In table 3, the requirements specified in Technical Specifications, rule 1, were applied strictly. In table 4, the minimum requirements based on the deterministic judgment for the reactivity control safety function considering performance criteria from Technical Specifications, PSA, and other technical documents, rule 2, were represented.

Figure 3 and 4 show the SFATs for reactivity control safety function based on the color assignment rules represented in table 3 and 4 respectively. In figure 3, reactivity control SFAT based on rule 1 was illustrated and SFAT based on the rule 2 was illustrated in figure 4 respectively.

5. Conclusion and Remarks

In table 5, the numbers of end states were compared along with the colors. The limiting logic paths in SFATs are paths to the ORANGE, and RED status in case of bottom-up approach. The SFAT based on the Technical Specifications requirements showed much conservative evaluation results than SFAT based on the functional criteria which were derived from the deterministic engineering judgment.

For example, in rule 2, HPSI pumps are not the minimum requirement as long as at least 2 channels of RPS or DPS are available with 1 charging pump and boration source are available. For HPSI pumps, in the other SFATs such as Core Cooling, they are the critical SSCs and they must be the minimum requirement. The case of HPSI pumps is illustrated in figure 5.

Table 3. Minimum requirements for reactivity control safety function based on TS (Rule 1)

HRE	REACTOR TRIP METHODS		BORATION SRC INCLUDING PATH			BORATION METHODS		DID LEVEL*	STATUS	REMARK
	RPS	DPS	RWST	SFP	PATH	CHG P/P	HPSI P/P			
NO	1		1		1	1	1	5	ORANGE	ORANGE=N
NO	1			1	1	1	1	5	ORANGE	N=5
YES	1		1		1	2	1	6	ORAMGE	ORANGE=N+1, WHEN HRE
YES	1		1		1	1	2	6	ORAMGE	N=6
YES	1			1	1	2	1	6	ORAMGE	
YES	1			1	1	1	2	6	ORAMGE	

* DID level is the number of SSCs needed for the safety function

Table 4. Minimum requirements for reactivity control safety function (Rule 2)

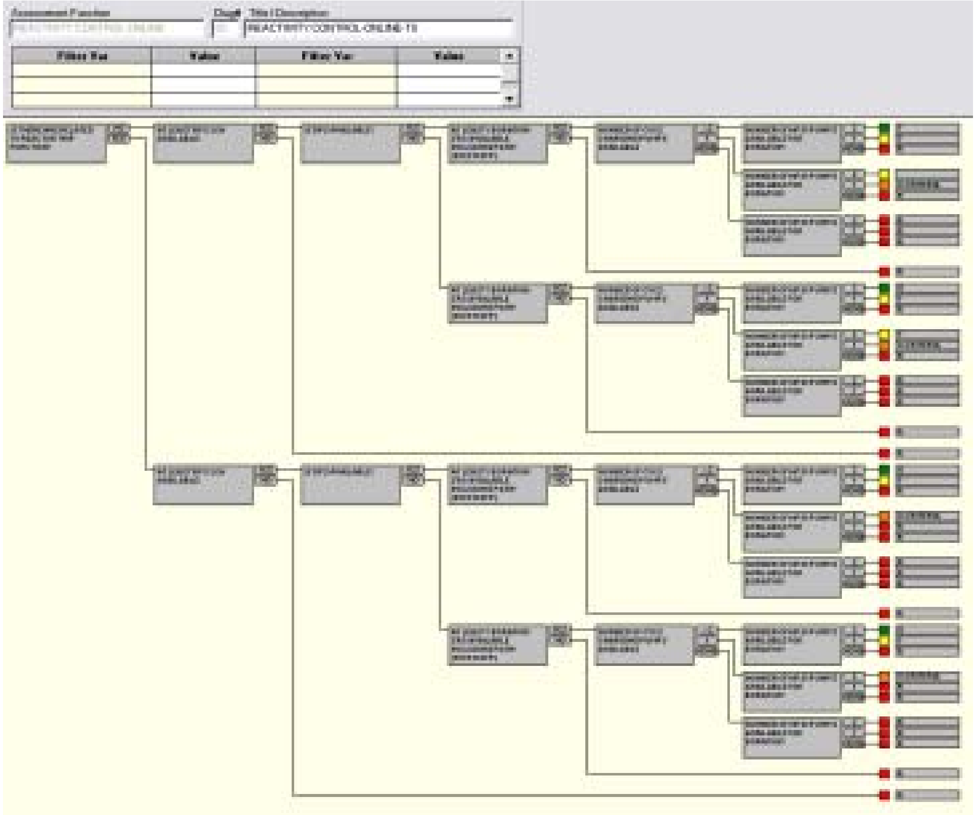
HRE	REACTOR TRIP METHODS		BORATION SRC INCLUDING PATH			BORATION METHODS		DID LEVEL*	STATUS	REMARK
	RPS	DPS	RWST	SFP	PATH	CHG P/P	HPSI P/P			
NO	1		1		1	1		4	ORANGE	ORANGE=N
NO	1			1	1	1		4	ORANGE	N=4
NO	1		1		1		1	4	ORANGE	
NO	1			1	1		1	4	ORANGE	
YES	1	1	1		1	1		5	ORAMGE	ORANGE=N+1, WHEN HRE
YES	1	1	1		1		1	5	ORAMGE	N=5
YES	1	1		1	1	1		5	ORAMGE	
YES	1	1		1	1		1	5	ORAMGE	
YES	1		1		1	1	1	5	ORAMGE	
YES				1	1	1	1	5	ORAMGE	
YES				1	1	1	1	5	ORAMGE	

* DID level is the number of SSCs needed for the safety function

Table 5. Comparison of end states by color assignment principles

Status	Rule 1	Rule 2
GREEN	4	13
YELLOW	6	10
ORANGE	4	7
RED	28	12
Total Number of End states	42	42

Figure 3. Reactivity control SFAT based on rule 1



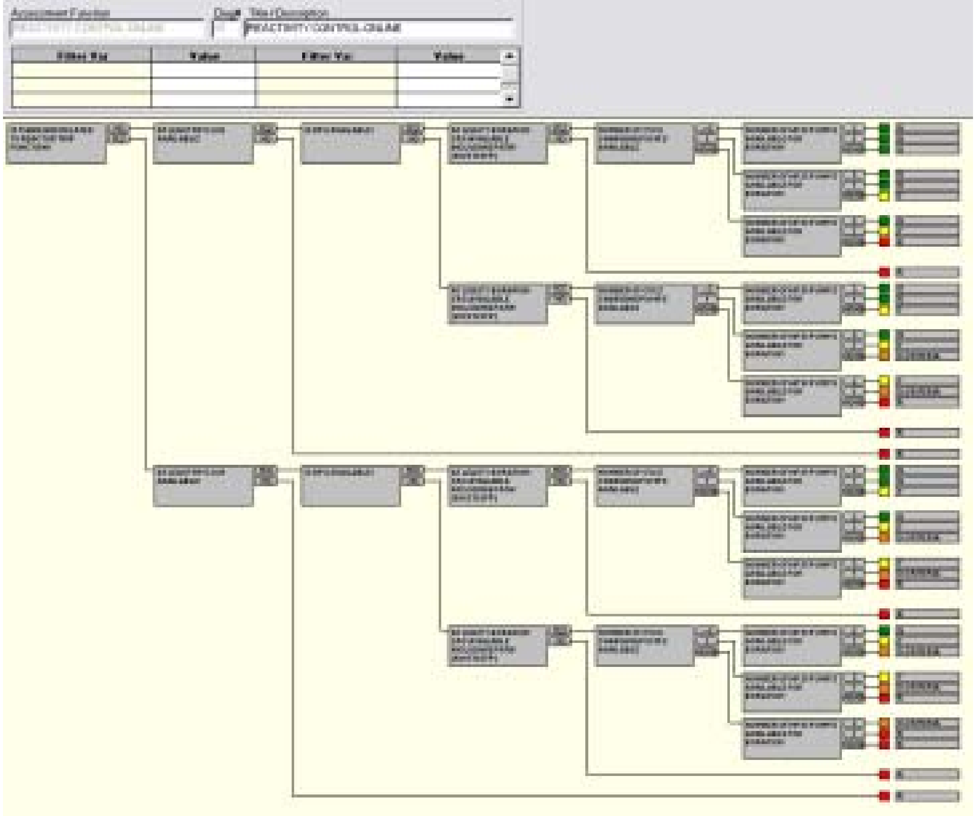
Assessment Function: REACTIVITY CONTROL ONLINE

Diag#:

Title/Description: REACTIVITY CONTROL-ONLINE-15

Filter Var	Value	Filter Var	Value

Figure 4. Reactivity control SFAT based on rule 2



Assessment Function: REACTIVITY CONTROL ONLINE

Diag#:

Title/Description: REACTIVITY CONTROL-ONLINE

Filter Var	Value	Filter Var	Value

In other words, the flexible interpretation of Technical Specifications is necessary to evaluate the status of each safety function independently, and to make defense-in-depth decision trees more useful in real applications at plants as a tool for compensation of Technical Specifications as long as consistency for determination of limiting logic paths in deterministic decision trees, and as long as there are contingency plans for ORANGE and RED status in consistent basis.

As we can see from table 5, the most important element in development of defense-in-depth evaluation trees such as SFATs, the consistent and inclusive understanding and interpretation about the defense-in-depth in nuclear safety.

References

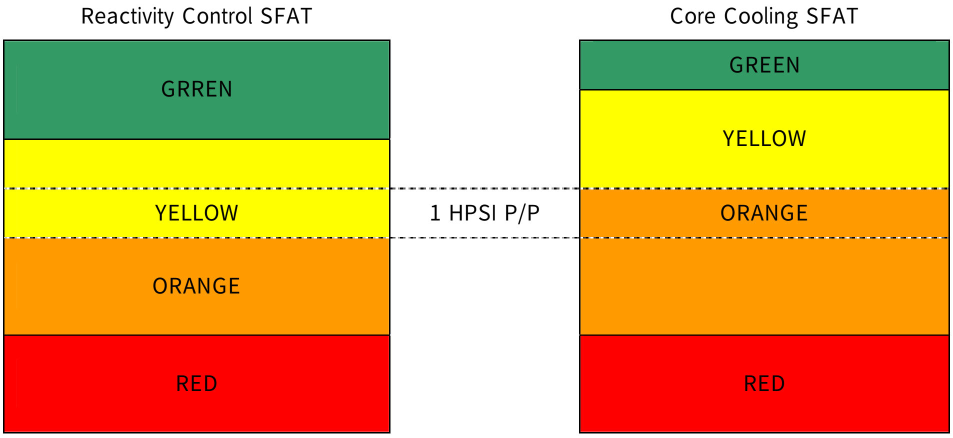
[1] IAEA, “Defense in Depth in Nuclear Safety,” INSAG-10, 1996

[2] EPRI, "ORAM-Sentinel Development and ORAM Integration at Catawba and McGuire," EPRI TR-106802, 1998

[3] U.S. NRC, "Final Policy Statement on the Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities," SECY-95-126, 1995

[4] U.S. NRC, “An Approach for Plant Specific, Risk-Informed Decisionmaking: Technical Specifications,” Regulatory Guide 1.177, 1998

Figure 5. Example of HPSI pumps in different SFATs


Reactivity Control SFAT
Core Cooling SFAT
GRREN
GREEN
YELLOW
YELLOW
1 HPSI P/P
ORANGE
ORANGE
RED
RED