Management of Single Point Vulnerabilities based on Failure Analyses and a Mitigation Strategy

Eun-Chan Lee[1], Jang-Hwan Na

[1] *70, 1312-gil, Yuseong-daero, Yuseong-gu, 34101, eclee5639@khnp.co.kr*

Korea Hydro and Nuclear Power Co. (KHNP) experienced 51 plant trip events between February 2009 and January 2016; approximately 50% of these events resulted from failures of key components that were registered as single point vulnerabilities (SPVs). The management of SPVs is a key mission that drives the implementation of a systematic process to prevent loss of electricity production. However, because this process requires a large amount of resources, KHNP is focusing on establishing the technical foundation and a strategy to mitigate or remove the vulnerabilities stage-by-stage according to their priorities. First, the criteria for SPV screening are defined based on the failure mode and effect analyses (FMEA) of the plant systems. In this process, the importance related to the plant trip is defined as the trip criticality (TC) and it is assigned to the analyzed components. In addition, as a useful application of results from the failure analyses, KHNP is implementing a potential SPV (PSPV) evaluation that considers plant scrams and derates from multiple failures as well as plant trips due to the single failure of a component. This evaluation demonstrates the vulnerabilities at a plant level and integrates the supporting systems, which include the control systems, power blocks, lubricants, and cooling water, into the front line components such as pumps and valves. The evaluation results are reflected in the SPV Monitor, which is a tool that manages the potential SPVs, and it is used to conduct work management and to prepare to take mitigation actions during plant transients based on the trip risk profiles for preventive maintenance and corrective maintenance during plant operation. [1]

I. INTRODUCTION

Korea Hydro and Nuclear Power Co. (KHNP) operates 25 nuclear power plants in Korea, including an advanced design unit (APR1400). According to the operation history, 51 plant trip events occurred between February 2009 and January 2016; approximately 50% of these events resulted from failures of key components that were registered as single point vulnerabilities (SPVs). Currently, KHNP manages 15,129 SPVs through design changes and/or reliability improvements in order to eliminate or to mitigate their failure effects. SPVs are selected through failure analyses of the components in the plant trip-related systems. In this process, a new concept, which is the 'potential SPV', has been defined and began to be used in the preparation of mitigation strategies in which operators are ready to respond to emergent conditions or to take actions to prohibit authorization of work orders, including potential SPVs, through referring to the evaluation results of the plant trip model (SPV Monitor) during the establishment of the plant maintenance plan.

II. EVALUATIONS

The criteria for SPV screening are based on the failure mode and effect analyses (FMEA) of the plant systems. In this process, the importance related to the plant trip is defined as the trip criticality (TC) and it is assigned to the analyzed components. TC-1 components, which cause plant trips due to a single failure, are categorized as SPVs. In addition, TC-2 and TC-3 components are designated as potential SPVs because they cause plant trips from consecutive or multiple failures. Once components are selected as SPVs, a permanent solution is sought in order to install redundancies to mitigate their failure consequences, while preventive and/or predictive maintenance reinforcements are reviewed as short-term measures if alternatives to solve these design disadvantages are not available.

II.A. FAILURE MODE AND EFFECT ANALYSIS

The failure mode and effect analysis (FMEA) can be used as an analysis methodology to identify problems that lead to plant trips or accidents. This analysis method is a stage-by-stage process to locate potential failure elements that exist in the design, process, and plants. [2]

The components for FMEA are selected through reviewing the plant design documents, procedures, plant trip history, and functional importance determination (FID) information in the maintenance rules (MRs). After this scoping process, reliability block diagrams (RBDs) are prepared for analysis. Figure 1 is a RBD for FMEA of the rod control system with the Westinghouse design. When the preparation of RBDs is finished, the FMEA is started after the components inside the RBDs

are selected from the enterprise resource planning (ERP) database containing the plant equipment information. If there is no equipment information in the ERP database, analysts extract the components for the SPV analysis from the design documentation such as drawings, system descriptions, and vendor manuals. After the components for the SPV analyses are collected for all systems, the failure analyses to determine the SPVs are conducted through reviewing the relationships of the inputs and outputs of the modules inside the systems. The SPVs and potential SPVs are initially reviewed in this FMEA process.

The EPRI reference [2] recommends implementing both FMEA and fault tree analysis (FTA) in parallel in order to reduce the time and resources used. KHNP used this hybrid method to verify the FMEA results. That is, the FTA was used to prove and compensate the FMEA results with the system level failure effects because the FTA has an advantage of identifying the failure conditions and effects comprehensively at the plant level.

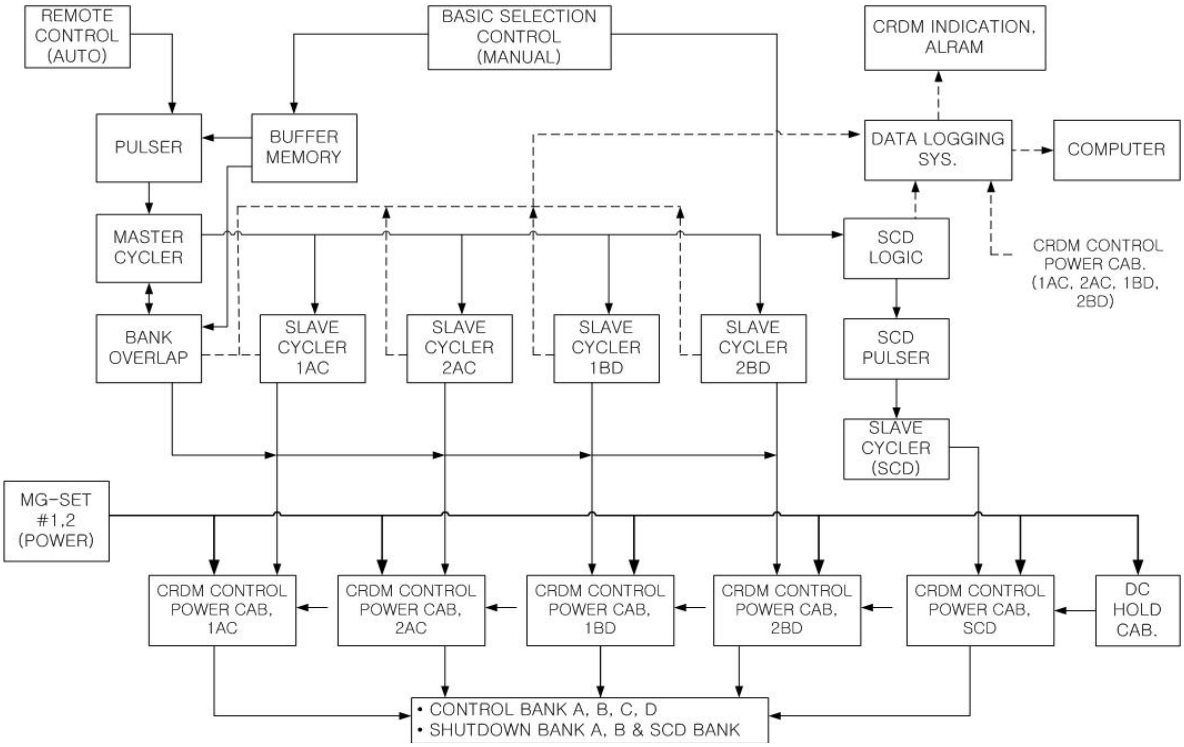

Figure 1. Reliability block diagram of the rod control system.

According to reference [2], FMEA can be used for activities to identify SPVs in the design stage because this method reviews a single failure mode, its failure mechanism, and its effects. In addition, it can meet the goal of satisfactorily understanding and analyzing a single failure and its cause systematically because FMEA is easy and simple compared with other methodologies. In contrast, it is difficult for FMEA to implement an evaluation that considers the effects of the potential common causes. In addition, FMEA cannot evaluate the operator action failures and system responses related to the interfaces with other systems. In particular, this method cannot manage abnormal conditions during operation with system design defects or misunderstanding of plant responses. Therefore, KHNP is reviewing and trialing other failure analysis methodologies and considering compensative or alternative analytic tools.

After the qualitative SPV analysis including FMEA was completed, the plant trip effects considering the support systems were evaluated using the integrated trip model reflecting the qualitative analysis results. Finally, the reliability data were assigned to the trip model in order to perform quantitative and logical SPV analyses. The tool used in this process is a fault tree. The results from the fault tree model were logically evaluated in order to screen the final critical components pertaining to plant trips at the plant level, including all supporting systems and interfaces.

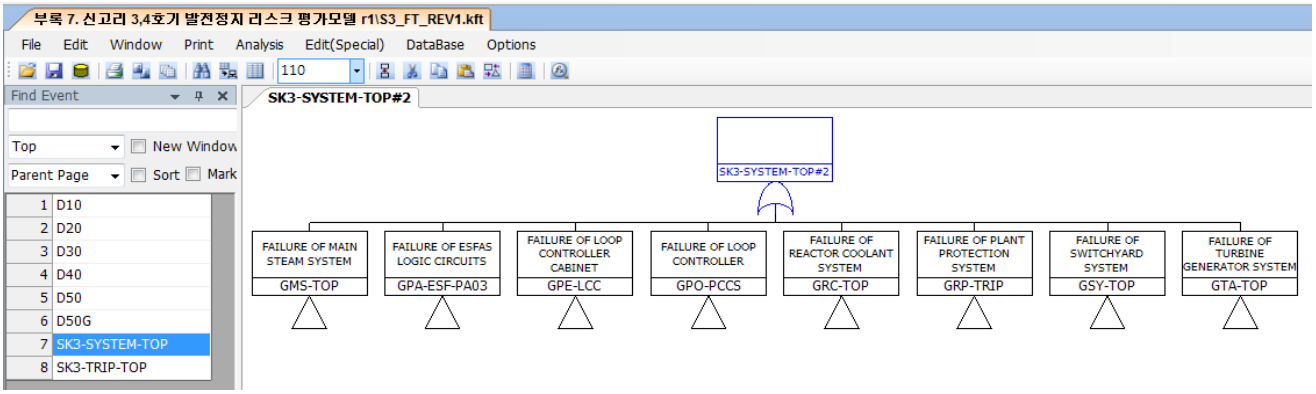

Figure 2. Plant trip-related systems for the fault tree analyses.

Figure 2 presents part of the fault trees of the trip-related systems in the APR1400 plant. Figure 2 includes the systems that cause a plant trip when their components fail or are spuriously actuated. However, each system in Figure 2 does not have all of their supporting systems, such as electrical systems, cooling systems, lubrication oil systems, and other interfaces for the trip-related components. However, the left side of Figure 2 implies that users can evaluate the trip model (SK3-TRIP-TOP) and derate models with all main/support systems integrated into the quantification software. The derate models include 10% derate to 50% derate (D10, D20, D30, D40, and D50) from the transients during the component failures because derates exceeding 50% power are regarded as plant trips in screening SPVs according to KHNP's SPV management guidelines.

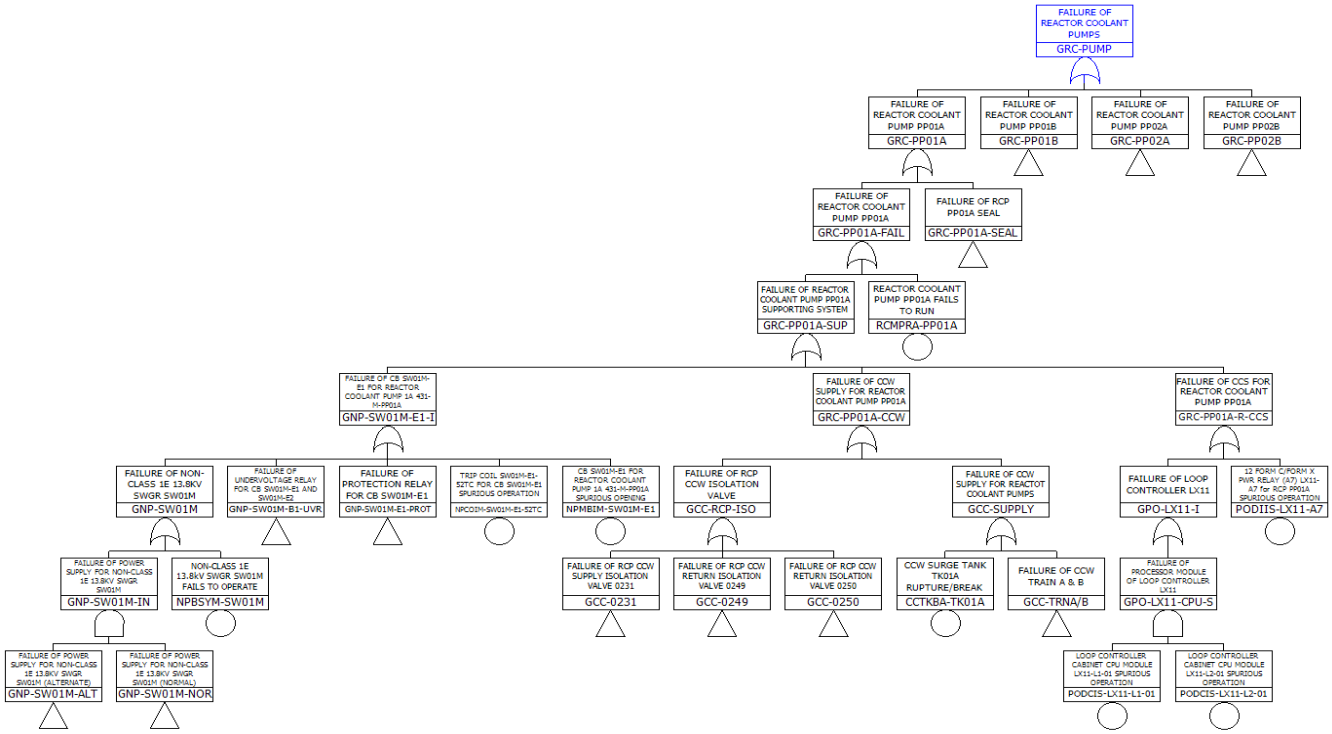

Figure 3. Fault trees of the reactor coolant pumps with support systems.

Figure 3 presents a fault tree that causes the failure (trip) of the reactor coolant pumps (RCPs). This figure covers most plant trip cases due to the RCP failure from electrical failures, mechanical failures, and spurious control signals, as well as failure of the RCP itself. Therefore, although the component for the analysis is only one RCP, there are several systems that need to be reviewed in order to identify the possible plant trip combinations.

II.B. SYSTEM IMPROVEMENT

KHNP is implementing the design changes for the SPVs that were identified through the system failure mode and effect analysis. Most design changes focus on the improvement to obtain redundancy in order to prevent a plant trip due to a single failure. Table 1 includes the design changes in the trip-related systems of three plants from 2013 to 2015. The primary aim of the changes is to install redundancies for the SPVs, such as protection relays for the electrical power systems, I/O modules for the main feedwater turbine control system, and controllers in the control rod system. In addition, some plants are implementing a functional change, e.g. modification of the protection circuits for large power transformers, after confirming other types of functions for the original protection. The plant engineering team has established a plan for these design changes when the SPV list is prepared or revised, and they track whether the design changes are completed according to the planned schedule. They also seek alternative performance monitoring technologies that are available if significant resources cannot be invested into the design changes.

Table 1. System improvements for SPVs.

Department	System	Component Name	Type	Improvement		
				Design Change	PM	Completion
Electrical	Main Power	M-TR, UAT WINDING TEMP HI HI	Switch	E-DC-01	-	March 2014
Electrical	Aux Power	RCP Digital Prot. Relay	Protective Relay	E-DC-02	-	February 2013
I&C	Main Feedwater	Automatic Closure Logic Circuits of MFCV	Printed Circuit Board	C-DC-01	-	October 2014
I&C	Stator Cooling	Temp Controller for Stator Cooling	Controller	C-DC-02	-	February 2013
Electrical	Main Power	GEN. DIFF. RELAY	Protective Relay	E-DC-03	-	April 2014
Electrical	Main Power	M-TR DIFF. RELAY	Protective Relay	E-DC-04	-	April 2014
Electrical	Main Power	IPB GND FAULT RY	Protective Relay	E-DC-05	-	April 2014
Electrical	Main Power	UNIT OVERALL DIFF. RELAY	Protective Relay	E-DC-06	-	April 2014
Electrical	Main Power	350/351A Over Current Relay	Protective Relay	E-DC-07	-	April 2014
Electrical	Main Power	EXCITATION TR PROTECTION RELAY	Protective Relay	E-DC-08	-	April 2014
Electrical	Main Power	M-TR, UAT Sudden Pressure Relay	Protective Relay	E-DC-09	-	November 2014
I&C	Main Feedwater	FWPT 01 SERVO VALVE Controller	Controller	C-DC-03	-	April 2014
I&C	Main Feedwater	FWPT 01 SPEED CONTROLLER	Controller	C-DC-04	-	April 2014
I&C	Main Feedwater	TA01 AXIAL POSIT PRB & INDICAT	Controller Panel	C-DC-05	-	April 2014
I&C	Main Feedwater	TA01 TBN END AXIS INDICAT	Controller Panel	C-DC-06	-	April 2014
I&C	Main Feedwater	RELAY MOD FWPP TA01 BRG VIB	I/O Module	C-DC-07	-	April 2014
I&C	Rod Control	Coil Drive actuation logic	Printed Circuit Board	C-DC-08	-	November 2014
I&C	Rod Control	Phase sync pulse & CEA select logic	Printed Circuit Board	C-DC-09	-	November 2014
I&C	Rod Control	ZCD Card for Subgroup #1	Printed Circuit Board	C-DC-10	-	November 2014
I&C	Main Steam	MSIV Solenoids	Solenoid Valve	C-DC-11	-	November 2014
Mechanical	Condensate	Condenser Expansion Joint	Expansion Joint	-	Revise PM DB	June 2015

When a design change cannot be implemented according to the short term plan, KHNP headquarters establishes a long term plan for the major system improvements while the plants prepare the reinforced preventive maintenance or predictive maintenance for critical equipment that is difficult to provide redundancy. Recent operating experiences [3] have demonstrated that some plant trips result from failures in the mechanical components, which are difficult to have redundancy. One example is leakage of the rubber packing for the expansion joints of the condensers. This leakage caused the condenser vacuum degradation, which led to a turbine generator trip. The maintenance teams revised the ERP database to include the detailed preventive maintenance and performance monitoring tasks for the critical components in order to identify the degradation or damage due to aging or stress during outage maintenance or online inspection. In addition, the replacement frequency and inspection cycle were shortened to one refueling cycle from the long-term period.

II.C. DATA ANALYSIS

For the quantitative SPV evaluation, several reliability data sources were reviewed in the development of the reliability database for the components in the trip model. The failure mode and failure rate per component type in the data sources were confirmed in order to apply the reliability data to the fault trees of the 14 trip-related systems. The representative reliability database among these data sources is the ERPI utility requirement document [4]. However, other data sources must be reviewed because the systems, components, and failure modes for this quantitative SPV analysis include data that are not

addressed in the current probabilistic safety assessment (PSA) reliability database. Generic reliability database sources were reviewed considering practices in order to select the database priority used in the quantitative trip model in the reference plant, the available information regarding the components and their failure modes, the data results from recent operating experiences, and the details of the data analyses. Finally, the component reliability database for the quantitative SPV model (integrated trip model) was established through combining these data sources.

Table 2. Reliability data for the trip model.

No.	Dept.	Type	Description	Failure Mode	Failure Rate	Unit	Reference
1	I&C	AI	I/O Card, Analog	Fail to Operate	1.31E-06	/Demand	PCS (Vendor) DB
2	I&C	AI	I/O Card, Analog	Spurious Actuation	2.62E-08	/Hour	PCS (Vendor) DB
3	I&C	AR	Analyzer	Spurious Actuation	5.0E-06	/Hour	Savannah River GDB
4	I&C	BR	Bistable Relay	Fail to Operate	1.00E-05	/Demand	Savannah River GDB
5	I&C	BR	Bistable Relay	Spurious Actuation	3.00E-07	/Hour	Savannah River GDB
6	I&C	CM	Communication Module	Fail to Operate	6.00E-08	/Hour	Savannah River GDB
7	I&C	DI	I/O Card, Digital	Fail to Operate	8.20E-07	/Demand	PCS (Vendor) DB
8	I&C	DI	I/O Card, Digital	Spurious Actuation	1.64E-08	/Hour	PCS (Vendor) DB
9	I&C	FT	Transmitter, Flow	Fail High/Low	4.52E-06	/Hour	PSA DB
10	Electrical	GF	Ground Fault Detector	Spurious Actuation	1.62E-06	/Hour	IEEE-500 DB
11	Electrical	GF	Ground Fault Detector	Fail to Operate	2.97E-06	/Hour	IEEE-500 DB
12	I&C	HF	Transmitter, Electrical	Fail High	4.40E-08	/Hour	IEEE-500 DB
13	I&C	HF	Transmitter, Electrical	Spurious Actuation	3.00E-06	/Hour	Savannah River GDB
14	I&C	IN	Indicator	Spurious Actuation	1.0E-05	/Hour	Savannah River GDB
15	I&C	IN	Indicator	Fail to Operate	1.0E-05	/Hour	Savannah River GDB
16	I&C	IU	Computational Module	Fail to Operate	1.40E-06	/Hour	NUREG/CR-4639
17	I&C	IV	Instrument Power Supply (loop)	Fail to Operate	6.00E-05	/Demand	NUREG/CR-5500 Vol.2 PP.18

The SPV database including the failure modes and failure rates of the components in the systems was applied to the fault tree in order to calculate the annual plant trip frequency. For example, the annual trip frequency of a plant with a Westinghouse design is calculated in Table 3 based on the Fussell-Vesely (FV) importance after quantification of the integrated trip model.

Table 3. Annual trip frequency of the trip-related systems.

Systems	System Designator	Annual Trip Freq.	Portion
RPS/ESFAS	SB, SE	0.27132	61.15%
Main Turbine	AC, CB, CC, CD, CE, CH, CP, CV	0.04492	10.12%
Main Power	MA, MB, MC, MD	0.03944	8.89%
Auxiliary Power	NA, NB, NG, NH, NK, PB, PG, PK, PQ	0.02595	5.85%
Secondary Component Cooling	EB	0.02257	5.09%
Reactor Coolant	BB, BG	0.01994	4.49%
Rod Control	SF	0.00622	1.40%
Main Feedwater	AE, AF, FC	0.00485	1.09%
Condensate	AD, CG	0.00418	0.94%
Main Steam	AB, CT	0.00222	0.50%
Instrument Air	KA	0.00160	0.36%
Interposing Logic	RL	0.00036	0.08%
Primary Component Cooling	EG	0.00012	0.03%
Circulating Water	DA	0.00000	0.00%
Total	-	**0.44368**	**100.00%**

II.D. APPLICATION TO MITIGATION STRATEGY

As a useful application of the results from the failure analyses, KHNP initiated the potential SPV (PSPV) management to implement a risk mitigation strategy for plant trip prevention. This strategy evaluates the trip risk from multiple failures as well as plant trips due to the single failure of a component. For this, the evaluation logics for the PSPV are created using the integrated fault trees that include the frontline components and their support systems. This evaluation logic, which is described in equation (1) and equation (2) below, is included in the software that is designated as SPV Monitor, which is a tool that manages potential SPVs. SPV Monitor is used to manage work based on the trip risk profiles for preventive maintenance and corrective maintenance during plant operation.

In equation (1), A_i is a primary component for normal plant operation, and B_i is a backup component of a major component. JA_i is a component that provides a primary component with a control function; EA_i is a component that supplies the driving power for a primary component; MA_i is a component that injects cooling water and lube oil into a primary component. JB_i is a component that provides a backup component with a control function; EB_i is a component that supplies driving power to a backup component; MB_i is a component that injects cooling water and lube oil into a backup component.

Equation (1) consists of the combination logics that cause the plant trips when there are no failure inputs to the SPV Monitor. When a component fails, the failure probability of the component is converted from its specific failure probability value to 1. This changed probability of 1 is applied in equation (1).

$$Trip = \sum_{i=1}^{n} [A_i \times B_i + A_i \times (JB_i + EB_i + MB_i) + B_i \times (JA_i + EA_i + MA_i) + (JA_i + EA_i + MA_i) \times (JB_i + EB_i + MB_i)] \quad (1)$$

For example, when component A_1 becomes unavailable in the plant trip combination of the system with single major components and single supporting components in two trains, this failure combination is changed to equation (2) because the changed value of A_1, i.e. 1, is input to the combination logic. Therefore, the B train components, which are expressed as a single cutset in the cutsets containing terms with the two components multiplied, are changed to the SPV components. This change to SPV from PSPV also results from the failure of the supporting system components in the same train.

$$Trip = B_1 + JB_1 + EB_1 + MB_1 + B_1 \times (JA_1 + EA_1 + MA_1) + (JA_1 + EA_1 + MA_1) \times (JB_1 + EB_1 + MB_1) \quad (2)$$

An analyst using SPV Monitor must recognize that a plant transient could be prevented by recovery actions of operators during the failure of components. In addition, the analyst should understand what failure sequence leads to a plant trip when operator actions fail during a plant transient.

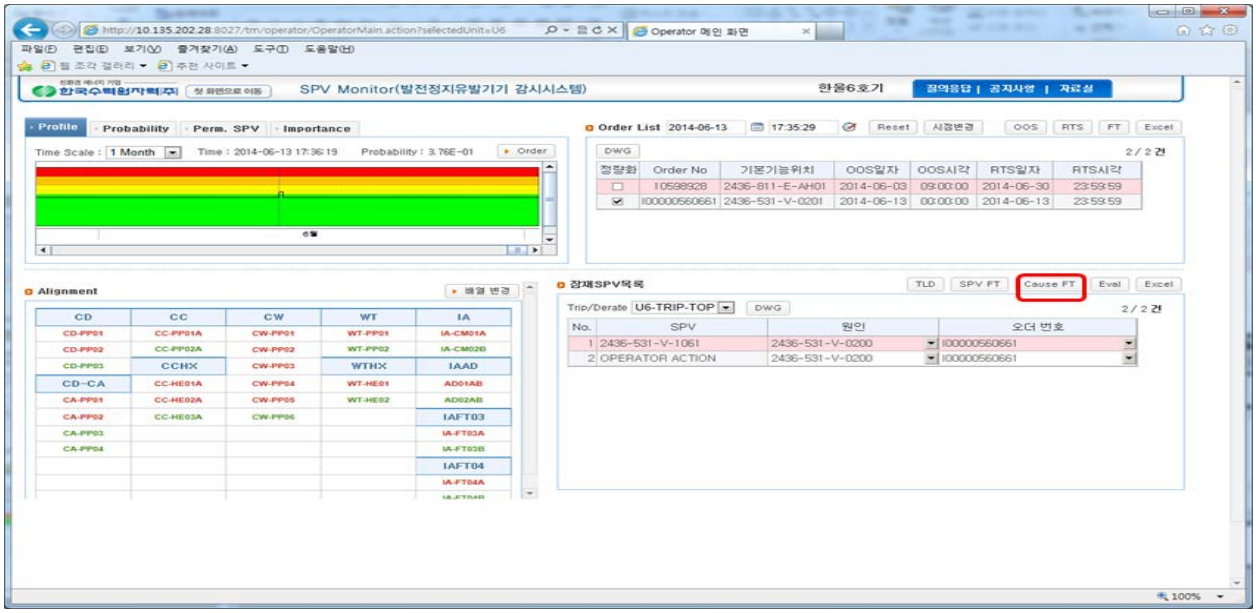

Figure 4. Screenshot of the main window in SPV Monitor.

Operators attempt to recover the system anomaly during the plant transient from the abnormal condition of the system. SPV Monitor can evaluate the process that operators use to recover plant turbulences to the normal state using the abnormal operation procedures during the plant transient.

The work order in Figure 4 evaluates the specific failure event of the control of the condensate polishing bypass valve (531-V-0200) malfunctioned after the condensate polishing inlet valve (531-V-0201) failed. The result explained that the V1061 and operator recovery failure were created as potential SPVs and the plant trip risk increased from the Green level to the Yellow level. Operators can be alert on standby and open V1061 to prevent the plant trip from the loss of condensate to the feedwater pump suction according to the abnormal operation procedure, if the bypass valve (V0200) is spuriously closed during inspection of the malfunction of the V0200 control circuits.

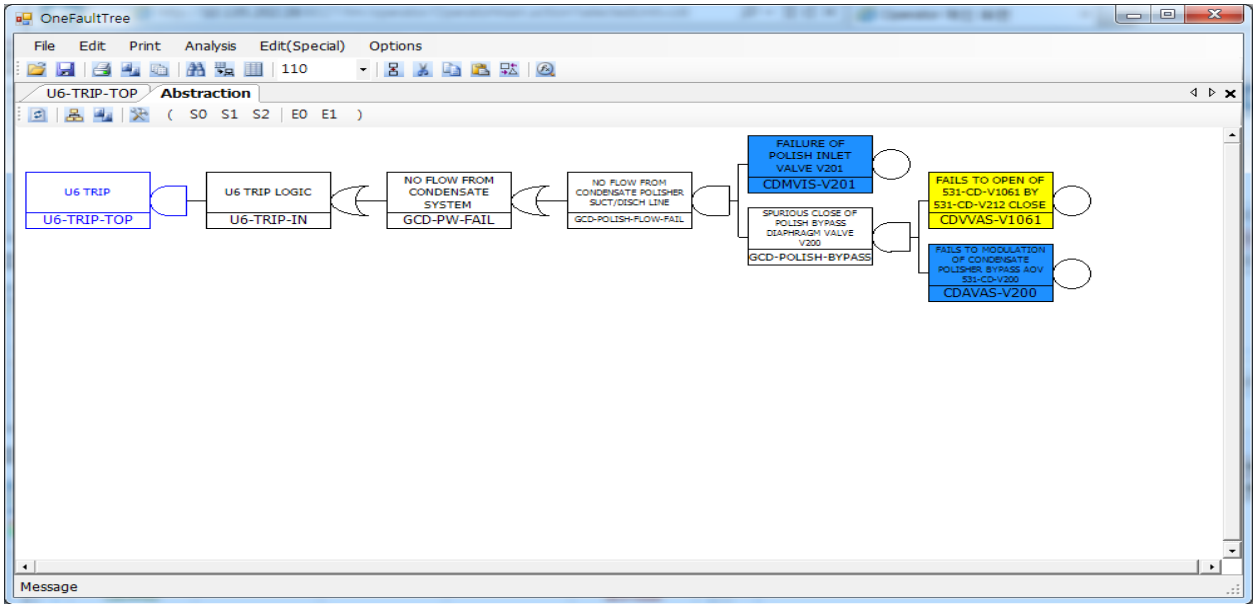

Figure 5. Trip logic diagram from the condensate polishing system failure.

SPV Monitor provides a risk evaluation process for the work scheduling department and methods for operators to be able to mitigate the analyzed risk. This mitigation strategy that manages plant transients is expected to have positive effects on plant trip prevention when several work orders are in progress for authorization, i.e. when the maintenance or tests for electrical components, mechanical components, and instrumentation components are planned to occur simultaneously, which potentially leads to a condition where the redundancy of the trip-related systems might be lost due to their combined out-of-service state. It is not easy to identify the combined maintenance or tests affecting the trip risk within a short time because operators or analysts must refer to several drawings and procedures one-by-one in order to recognize the trip risk, while SPV Monitor evaluates this trip risk instinctively using its trip logics.

Figure 5 presents a trip logic diagram (TLD) that explains why the risk increase is indicated in the SPV Monitor main display in Figure 4. In addition, Figure 5 depicts a plant trip sequence in which V1061 becomes a potential SPV as a result of the maintenance of V0200 and V0201. The condensate system has one bypass valve (V0200) whose modulation is automatically controlled according to the differential pressure between the inlet and the outlet of the condenser polishing plant (CPP). There is another manual bypass valve (V1061) that operators manipulate to supply condensate water to the feedwater suction during the failure of the bypass control valve (V0200). Therefore, V1061 changes to an SPV from a PSPV when both V0200 and V0201 are closed.

III. CONCLUSIONS

The management of single point vulnerabilities (SPVs) is a key mission that is driving the implementation of a systematic process to prevent loss of electricity production. However, because this process requires a large amount of resources, KHNP is focusing on establishing a technical foundation and a strategy to mitigate or remove the vulnerabilities stage-by-stage according to their priorities.

For the SPV management, SPVs were initially selected through analyzing how the failed components affect the systems and what consequences occur during plant operation according to their importance (trip criticality, TC). In addition, the final SPVs were determined through fault tree analyses considering the effects of the supporting systems and interfaces. This hybrid analysis separated the critical components that caused plant trips or derates due to multiple failures as well as a single failure. In this process, the potential SPVs (PSPVs) were defined as components whose consecutive failures result in plant trips or power derates. SPV Monitor, which was developed to manage these potential SPVs, evaluates the plant trip risk of work orders and the resultant potential SPVs during normal plant operation. Therefore, work schedulers or operators focus their attention on the analyzed potential SPVs before authorizing work.

The analysis of potential SPVs using SPV Monitor provides an opportunity for operators to mitigate emergent conditions based on the analyzed insights regarding the operator actions for the affected components during a plant transient. In addition, SPV Monitor notifies the operators of the trip risk due to the overlap of several work orders in order to prevent plant trips resulting from inadequate work management or human error. Although SPV management originated from the operating experiences, skills, and knowledge of plant employees, it has been developed to be an advanced process in which the utility determines SPVs based on the FMEA results, oversight reliability improvements, and work management for the SPVs using the risk monitor interfaced with the ERP database.

Currently, some plant engineers, maintenance staff, and operators may not have accumulated sufficient experience and knowledge because the age of employees working in nuclear power plants is becoming lower. Therefore, the plants should be operated under process-based maintenance management equipped with standardized and easily accessible supporting systems, as well as training for job qualification. This advanced and optimized SPV management tool, which consists of failure analysis, selection of SPVs considering their importance, management of potential SPVs, work scheduling based on trip risk analysis, and establishment of a transient mitigation strategy, is expected to contribute to safe operation of nuclear power plants in the long term.

REFERENCES

1. KHNP, "*Development of SPV Monitoring System for Shin-Kori unit 1,2,3,4 and Shin-Wolsong unit 1,2*", 2015
2. EPRI, "*Hazard Analysis Methods for Digital Instrumentation and Control Systems"*, pp 4-1 to 5-53, Palo Alto, 2014
3. Operation Performance Information System (OPIS), "*Accident and Failure Information"*, KINS (2015)
4. EPRI, *"Advanced Light Water Reactor Requirement Document,"* EPRI-NP-6780-L, Rev.7, December, 1995