Proceedings of the Korean Nuclear Society Autumn Meeting
Yongpyong, Korea, 2003

ATWS Probability Quantification Considering the Effect of Digital Equipment

Hyun Gook Kang, Seung-Cheol Jang, Jaejoo Ha

Korea Atomic Energy Research Institute, P.O Box 105, Yuseong, Daejeon, 305-600
hgkang@kaeri.re.kr

Abstract

The risk concentration due to the multi-tasking feature would increase the importance of digital equipment in nuclear power plants' safety functions. This paper quantitatively presents the probability of anticipated transients without scram (ATWS) based on the fault tree analysis of Korea standard nuclear power plant (KSNPP) which includes the analysis on digital equipment in digital plant protection system (DPPS). In this paper, we also present the result of sensitivity study which shows the effect of digital equipment to the probability of ATWS. For the base case of sensitivity study, the ATWS probability of the digital-protection-system-based KSNPP is quantified as 9.13×10^{-6} which is slightly higher value than that of analog-protection-system-based plant 8.40×10^{-6}. Main contributors to the ATWS which are related to the DPPS could be categorized as common cause failures (CCFs) of sensors, actuators, input modules, output modules and processing/watchdog modules which are combined with the failure of human operator or that of diverse protection systems.

1. Introduction

In the PSA of nuclear power plants, the anticipated transients without scram (ATWS) is considered as one of the most important initiating events. Actually, the ATWS is not an original initiating event, but rather is a faulted response to an event requiring control element

assemblies insertion for reactivity control. However, because of the significant impact that the ATWS has on plant response, it is included as a separate initiating event category. The ATWS is defined to an anticipated operational occurrence coupled with the subsequent failure to scram when the appropriate trip parameters are reached.

In this paper, we will address the quantification of the ATWS probability based on the fault tree analysis of Korea standard nuclear power plant (KSNPP) which includes the effect of digital equipment in digital plant protection system (DPPS) and digital engineered safety feature actuation system (DESFAS). The DESFAS would not affect the function of reactor trip, so only the digital equipment in the DPPS affect the probability of ATWS. The aim of this study is to investigate the effect of important features of digital equipment to the critical function, ATWS.

Microprocessors and software technologies make the digital system multi-functional. That is, a system performs several functions sequentially or conditionally. This multi-tasking feature would cause the risk concentration and deteriorate the reliability of the system. The designs of safety-critical systems such as nuclear power plants have adopted conservatism and have various functional redundancies through separated systems. In the case of digital systems, however, the software programs of these functions are executed by one processor and the redundancy is no more valid.

Different functions such as alarm generation, trip signal generation and safety-function-actuation signal generation are performed in DPPS. It will cause the risk concentration. The failure of alarm generation will deteriorate the human operator’s manual action which could play as a backup of automatic signal generation. Regarding the trip signal generation, multiple trip parameters are processed in DPPS. This also causes risk concentration. In this study, we will investigate the ATWS only, so the result of the study is expected to show only a part of risk concentration effect.

In section 2, we will describe the information of the target functions and modeling assumptions. In section 3 we will explain the fault tree modeling of the ATWS. And in section 4, we will show the quantification results and presents the result of simple sensitivity study which examines the effect of important factors of digital system on the ATWS probability.

2. System Description and Modeling Assumptions

A. Description of ATWS

The ATWS is potentially a severe event in which reactor coolant system (RCS) goes through a pressure excursion due to an imbalance between the core heat generation and RCS heat removal.

The ATWS is defined as an anticipated operational occurrence coupled with failure to insert negative reactivity via the control element assemblies, due either to electrical faults within the DPPS and diverse protection system (DPS) or mechanical binding of the CEAs themselves [1]. Since the primary ATWS concern is the peak RCS pressure, the ATWS initiators may be redefined as only the transients that tend to produce RCS pressure transients. However, all initiating events to be required a reactor trip are conservatively included in this study.

That is, ATWS occurs if the CEA insertion fails when an initiating event occurs. The reason of the CEA insertion failure could be grouped as signal failure or mechanical failure. For the signal failure, we consider three signal sources: the DPPS, the DPS and the manual initiation by human operator.

B. Description of DPPS

The purpose of the DPPS is an automatic generation of a trip signal for an emergency. In order to detect an emergency, it monitors various process parameters using independent instrumentation and processing channels. Many protection systems of nuclear power plants adopt a four-channel layout and the DPPS is one of them. Figure 1 shows the schematic diagram of a typical four-channel DPPS including a selective two-out-of-four voting logic.

Four redundant channels are provided to satisfy single failure criterion and improve plant availability. Each channel of the DPPS contains six microprocessor-based signal-

processing modules which are two bistable processors and four local-coincidence-logic processors. The bistable processor in each channel receives analog inputs from sensors through analog input modules. A bistable processor compares the input signals to the trip setpoints and transmits the results to local-coincidence-logic (LCL) processors.

A LCL processor performs two-out-of-four voting for each process input using the signals from the four bistable processors. It produces the output signal using a dedicated digital output module. Its stall will result in a loss of its heart beat output signal to a watchdog timer, then the watchdog timer will force the DPPS trip and initiate trip signal. Figure 2 shows the structure of a selective 2-out-of-four logic which initiates the interposing relay. More detailed description of the DPPS is available in reference [2] and [3].

C. Modeling Scope and Assumptions

The Risk Monitor, fault trees for the KSNPP developed by Integrated Safety Assessment team in KAERI, is used to model the general plant risk. It consists of about 2500 basic events and 3500 logical gates.

The aim of this fault tree modeling is to analyze the effect of digital safety-critical systems on the ATWS probability. We do not focus on the DPS which is categorized in non-safety-critical system. Therefore, the DPS failure is not modeled based on elementary modules and we treat one DPS processing channel as one basic event.

The DPPS failure is modeled based on elementary modules' failure in a detailed manner. The modeling assumptions for the DPPS fault trees are as follows:

- Since we don't have enough information about failure modes of digital systems, all failure modes are assumed to be hazardous.
- Watchdog timers monitor the status of local-coincidence-logic processors and local-coincidence-logic processors monitor the status of bistable processors. Generally, the coverage of timer-to-processor monitoring is much lower than that of processor-to-processor monitoring because the processor-to-processor monitoring method uses much more sophisticated algorithms. We assume that the fault coverage of processor-to-processor monitoring as 0.99. The coverage of timer-to-processor monitoring is

treated as a variable of sensitivity study. And for the simplicity, we also assume that watchdog timers could detect software failures with the same coverage in the case of hardware failures.

– We assume that every processor contains the identical software program and the software failure induces the CCF of processors.
– We ignore the fail-to-hazard probability of the network or serial communications.
– We ignore the fail-to-hazard probability of the inter-system data bus and the back plane of PLC.
– We assume that the components are tested at least once per month. That is, the periodic test interval (T) is 730 hours. Component unavailability (Q) is the half of the product of failure rate (λ) and periodic test interval: $Q=\lambda T/2$.

As shown in Table 1, the ATWS condition depends on the occurrence of initiating event. In consideration that the trip signal from the DPS is initiated only by high pressurizer pressure and high containment pressure, the DPS availability could be assumed as in Table 1. Since in case of LSL, HSL, LSP, and LSF, the trip signals are initiated by sensing the cooling loop's status, we have to consider that there are two cooling loop.

The failure probability of the manual initiation signal by an operator must be calculated considering the available alarms, training, experience, time limitation, and plant situation. We treat this failure probability as the variable of sensitivity study.

3. Fault Trees for ATWS

Figure 3 shows the schematic fault tree for the ATWS initiating event. It consists of all initiating events listed in Table 1. The system unavailability varies along with the plant situation because different plant abnormalities initiate different trip parameters.

For the convenience of explanation, we will explain only the case of LOFW. Figure 4 shows a fault tree in the case of LOFW. The reasons of reactor trip failure in LOFW are mechanical failure of CEAs and the trip signal failure. The trip signal could be generated by the DPPS or the DPS. The DPPS would generate trip signal based on three trip parameters:

HPP, LSL1, and LSL2. In each case of trip parameters, the system for generating trip signal is modeled in a separate manner.

Figure 5 shows the fault tree for modeling under-voltage (UV) signal failure for the parameter of LSL1. The reasons of UV signal failure could be the failure of UV element itself, the failure of human operator manual initiation, or the failure of the DPPS output. The explanation of the other parts of the DPPS model is available in reference [2] and [3].

4. Quantification Result

Using KwTree [5], which is the fault-tree analysis software package produced by Korea Atomic Energy Research Institute, we perform the quantification of the ATWS fault tree. For the base case, we assume the value of three important factors: the human failure probability, the software failure probability, and the watchdog timer coverage. They are assumed as 0.05, 0.00, and 0.7, respectively. The result of quantification shows that the ATWS initiating event probability is 9.13E-6 which is slightly higher value than that of analog-protection-system-based plant 8.40E-6.

Main contributors to the ATWS which are related to the DPPS could be categorized as common cause failures (CCFs) of sensors, actuators, input modules, output modules and processing/watchdog modules which are combined with the failure of human operator or that of diverse protection systems.

In order to quantify the effect of above three important factors, we perform sensitivity study. For the simplicity of study, we change the values of important factors one by one. That is, from the base case mentioned above, we change the value of a factor.

Regarding the human failure probability, we use 1E-10, 0.05, 0.5, and 1.0. The results are 8.43E-06, 9.13E-6, 1.55E-05 and 2.25E-05, respectively. The last case is for representing the case of no human action.

Regarding the software failure probability, in this analysis, we examine the effect of the software of LCL processor modules only. We use 0, 1E-4 and 1E-3 as the software probability. The results are 9.13E-6, 1.01E-05 and 1.13E-05, respectively. We roughly

assume that the watchdog timer could detect the failure of software with the same coverage as in case of hardware failure.

Regarding the watchdog timer coverage, we use 0.3, 0.7, and 0.9. The results are 9.21E-06, 9.13E-6, and 9.09E-06, respectively. Since the base-case assumptions are zero software failure and highly credible operator backup, the effect of watchdog timer seems relatively small. However as shown in references [2] and [6], the watchdog timer coverage plays critical role to decide the system unavailability when we assume the realistic values for software failure and human failure.

5. Concluding Remarks

The aim of this study is the quantification of probability of ATWS and the examination of the effect of important factors of the DPPS modeling. In this study, we consider three important factors; the human failure probability, the software failure probability, and the watchdog timer coverage.

In the case of base study, the ATWS probability of the digital protection system-based KSNPP is quantified as 9.13×10^{-6} which is slightly higher value than that of analog protection system-based plant 8.40×10^{-6}. And the results of sensitivity study show that the three important factors could change the ATWS probability from 8.43E-06 to 2.25E-05. If we consider the combinatory effect of the factors, the range of result would be much larger.

The study gives a hint to address the effect of risk concentration induced by digital equipment. In this study, we investigate the ATWS only, so the result of the study shows only a part of risk concentration effect. The further study to investigate the core damage frequency based on further researches on the human failure probability and input dependencies is strongly recommended in order to see the total risk concentration effect.

Acknowledgement

This work has been carried out under the Nuclear R&D Program supported by MOST

Reference

[1] KEPCO, Full scope level 2 PSA for Ulchin unit 3&4: Internal event analysis, 1998.

[2] Kang, H.G., et al., Reliability Study: Digital Reactor Protection System of Korean Standard Nuclear Power Plant, KAERI/TR-2419/2003, Korea Atomic Energy Research Institute, 2003.

[3] Kang, H.G. and Sung, T., An analysis of safety-critical digital systems for risk-informed design, Reliability Engineering and Systems Safety, Vol. 78, 2002.

[4] 장승철 외, 표준원전 위험도 감시용 PSA 모델 개발, KAERI/TR, To be published, 2003.

[5] Sang Hoon Han, et al., “User’s Manual for KIRAP (KAERI Integrated Reliability Analysis code Package) Release 2.0,” KAERI/TR-361/93, 1993.

[6] Kang, H.G., Jang, S.C. & Ha, J.J., Evaluation of the Impact of the Digital Safety-Critical I&C Systems on the Plant Risk, Proceeding of ISOFIC 2002, Seoul, Korea.

Table 1. ATWS occurrence condition

Initiating Event	DPPS Variables	DPS Availability
SLOCA	DNB LPP HCP	X
SGTR	HSL DNB	X
LSSB	LSP VOPT LSL LPP DNB	X
LOFW	LSL HPP	O
LOCV	HPP	O
LOCCW	LSF DNB	O
LOKV	LSF DNB	O
LODC	HPP DNB HSL	O
LOOP	DNB LSF	O
GTRN	HPP DNB	O

Abbreviations:

SLOCA	Small Loss of Coolant Accident
SGTR	Steam Generator Tube Rupture
LSSB	Large Secondary Side Break
LOFW	Loss of Feed Water
LOCV	Loss of Condenser Vacuum
LOCCW	Loss of Component Cooling Water
LOKV	Loss of 4.16KV AC bus
LODC	Loss of 125V DC bus
LOOP	Loss of Offsite Power
GTRN	General Transient
VOP	Variable Overpower
HPL	High Logarithmic Power Level
HLD	High Local Power Density
DNB	Low Departure from Nucleate Boiling Ratio
HPP	High Pressurizer Pressure
LPP	Low Pressurizer Pressure
LSL	Low Steam Generator Water Level
HSL	High Steam Generator Water Level
LSP	Low Steam Generator Pressure
LSF	Low Steam Generator Reactor Coolant Flow
HCP	High Containment Pressure

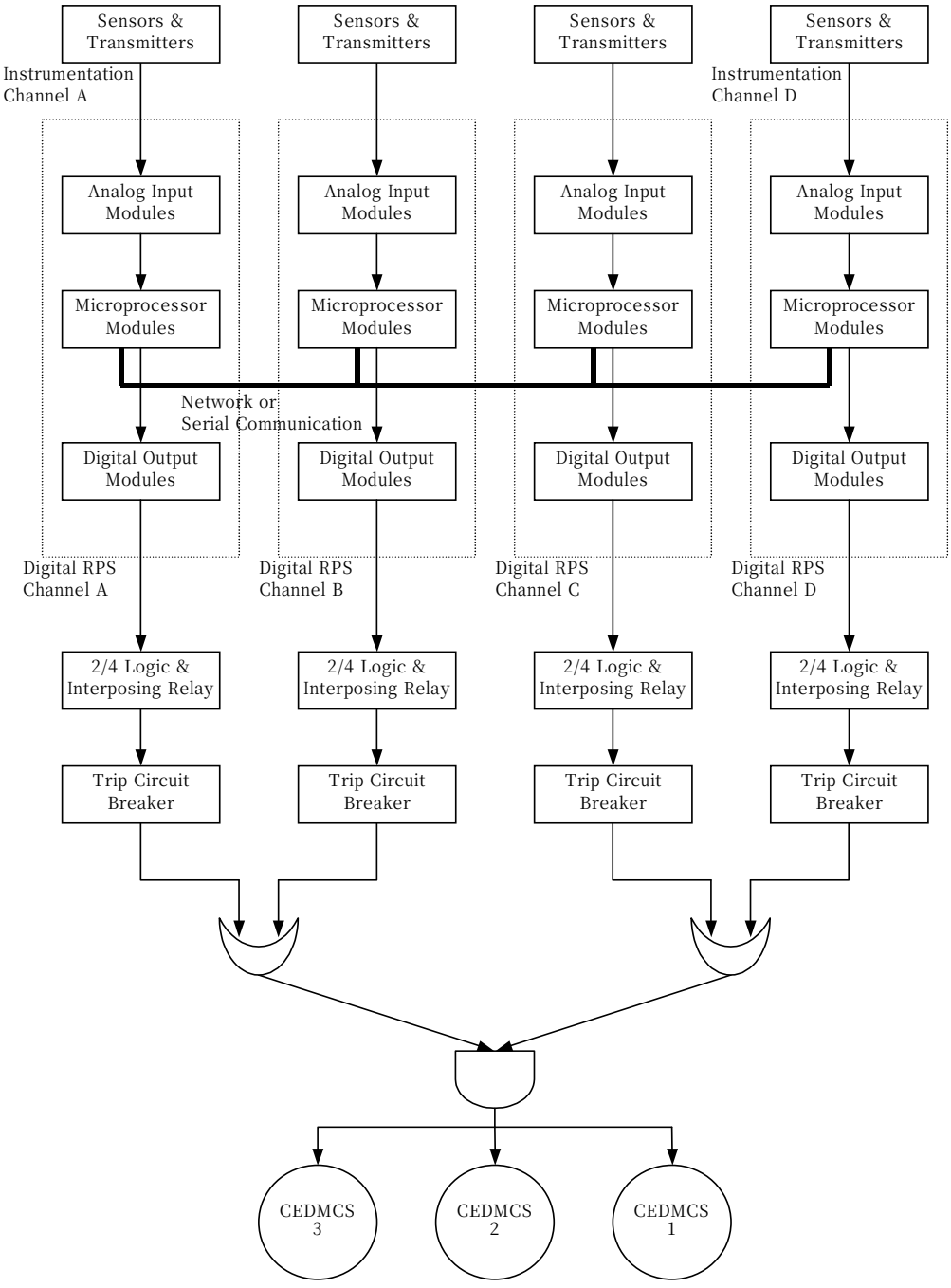

Figure 1. The schematic diagram of a typical four- channel DPPS

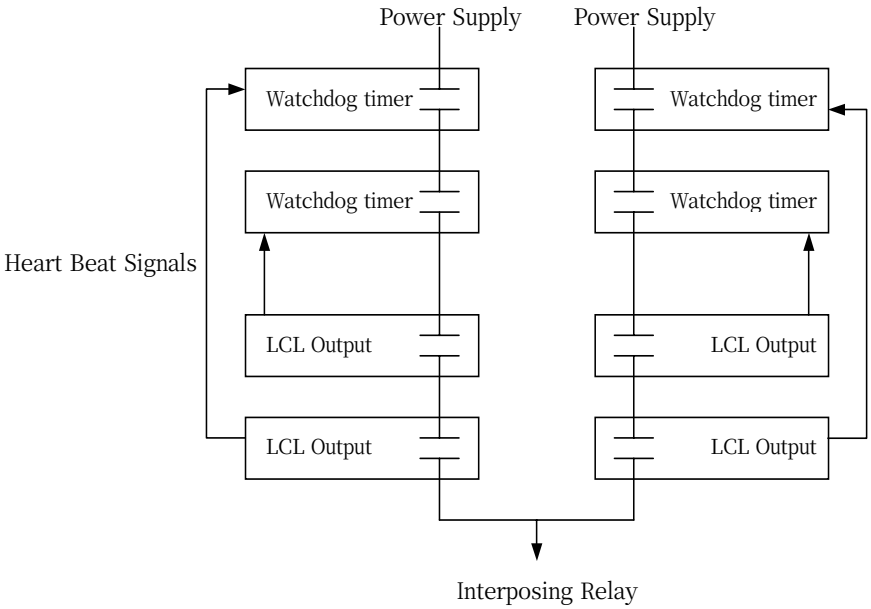

Figure 2. The detailed diagram of a selective 2-out-of-four logic which initiates the interposing relay

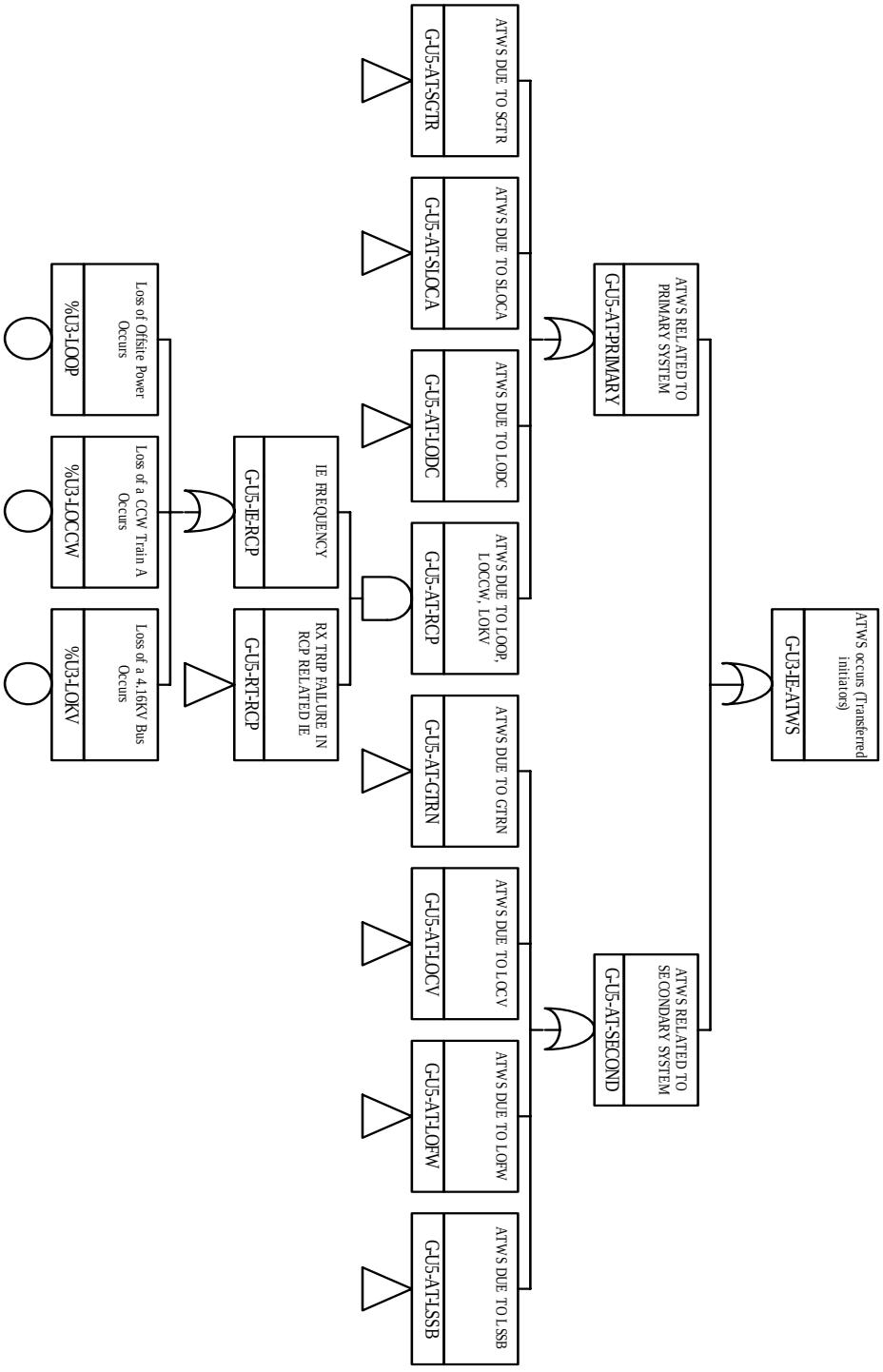

Figure 3. The structure of ATWS initiating event

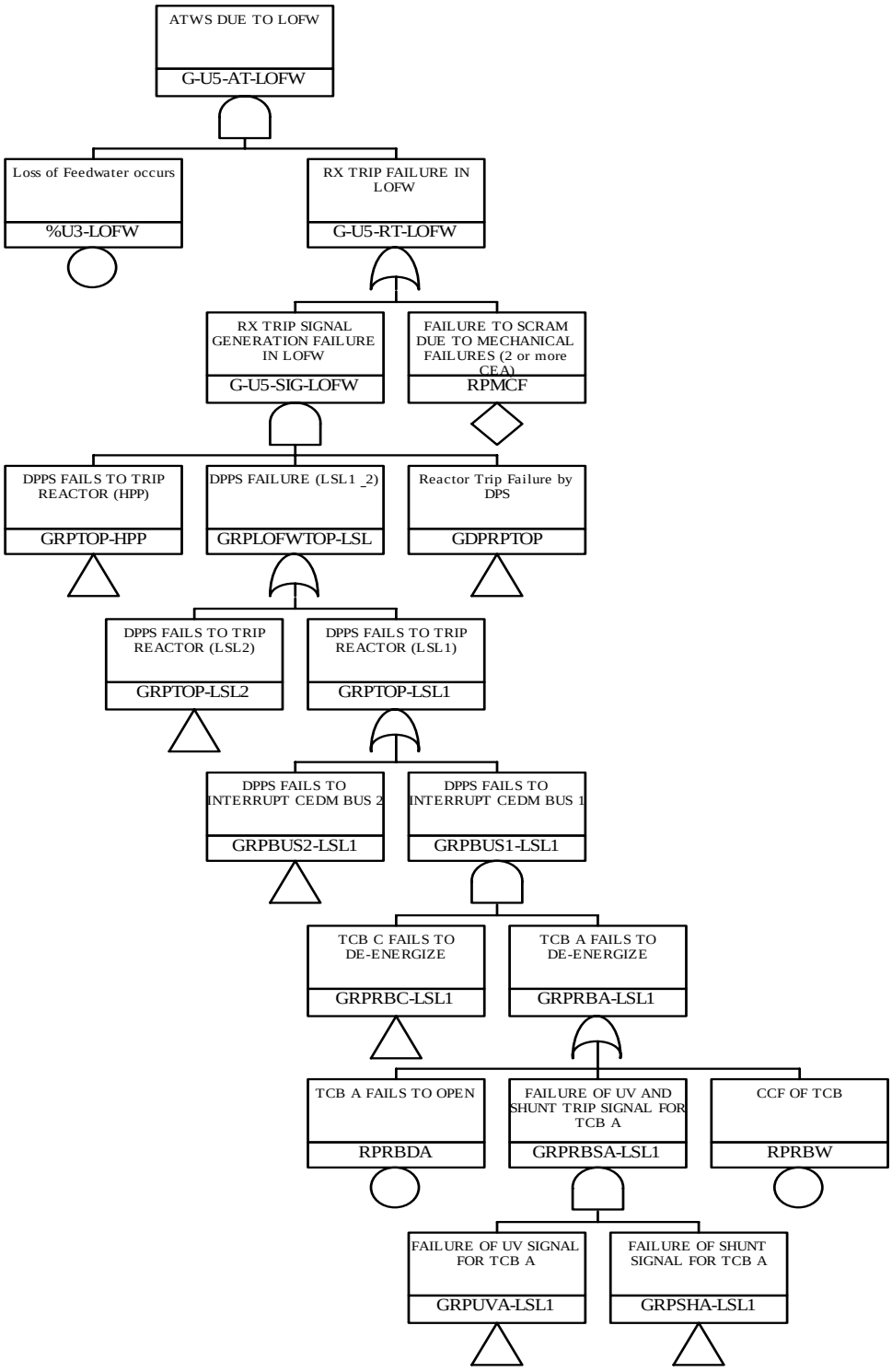

Figure 4. The fault tree for modeling the ATWS in case of LOFW

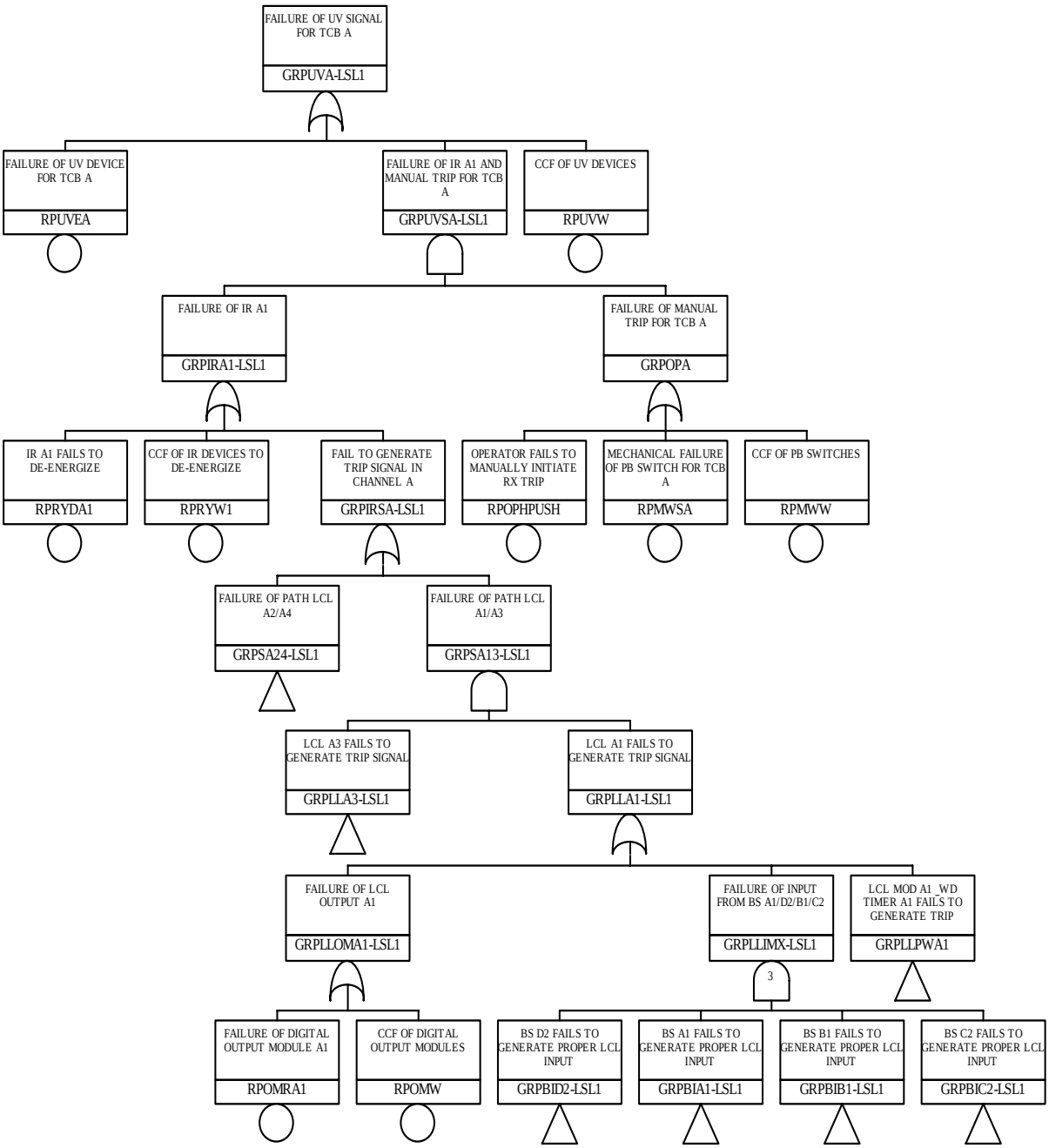

Figure 5. The fault tree for modeling under-voltage signal failure for the parameter of LSL1