Safety Activities for Improving Safety-Critical Software Reliability

May 21th, 2008

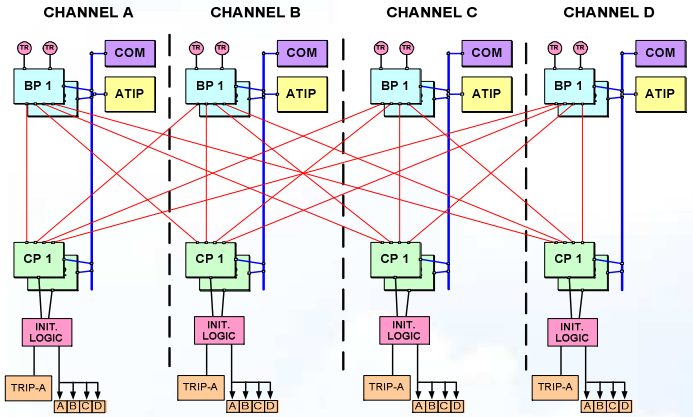
Gee-Yong Park* and Kee-Choon Kwon

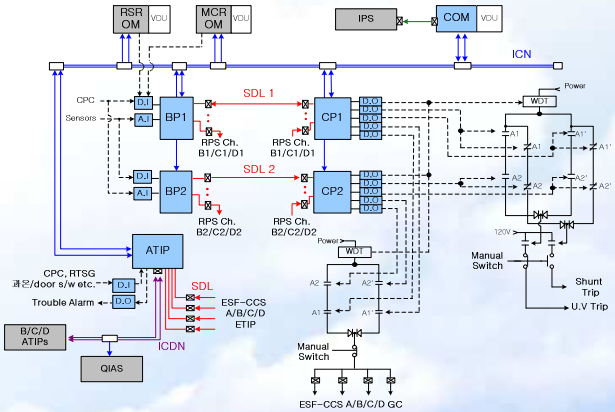
I&C and Human Factors Division
Korea Atomic Energy Research Institute

한국원자력연구원
Korea Atomic Energy Research Institute

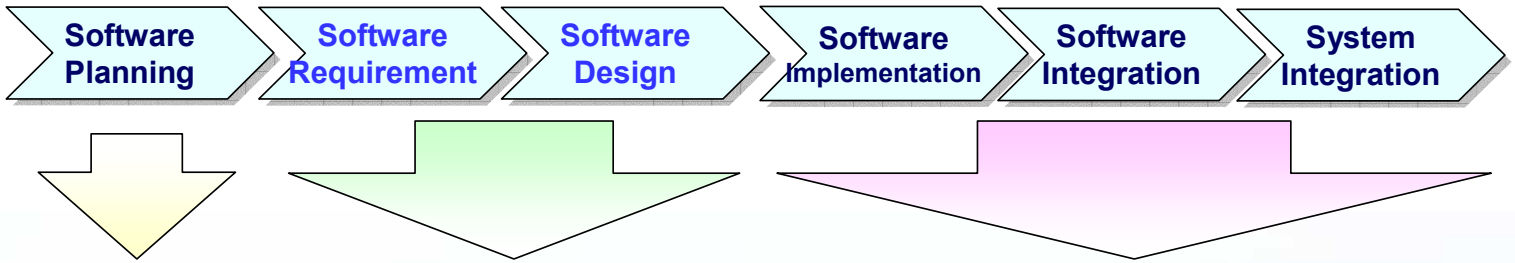
KNICS Reactor Protection System

- **Configuration of Single Channel in KNICS RPS**
  - Two Bistable Processors (BPs): Determine trip state by signal comparison, SC
  - Two Coincidence Processors (CPs): Generate trip signal by a 2/4(2/3) voting, SC
  - Automatic Test & Interface Processor (ATIP): Performs Tests(MT/MIAT/PT) & Interfaces with other ATIPs, SR
  - Cabinet Operator Module (COM): GUI + H/W (Ch. Bypass, Init. Circuit Reset)
  - Network Type: SDL (SC), ICN (SR), ICDN





S/W V/V Activities of KNICS RPS



- QA Plan
- V&V Plan
- CM Plan
- Safety Plan

Review of Plans

- Development Plan
- Management Plan
- Integration Plan
- Installation Plan
- Operation Plan
- Maintenance Plan
- Training Plan

Licensing Suitability

Fagan Inspection

Traceability Evaluation

Formal Verification

Test Preparation

Testing

Static Analysis

- Inspection
- Traceability

Software Safety Analysis

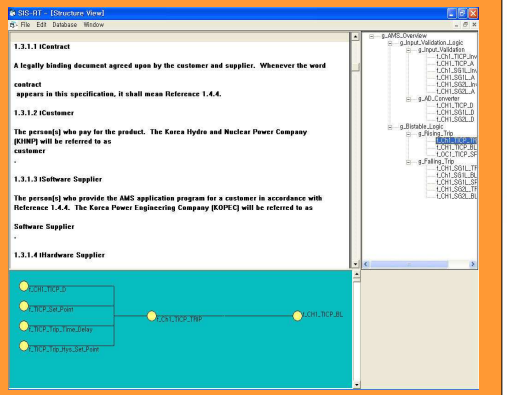
Software Configuration Management

Type & Methods for S/W Dependability

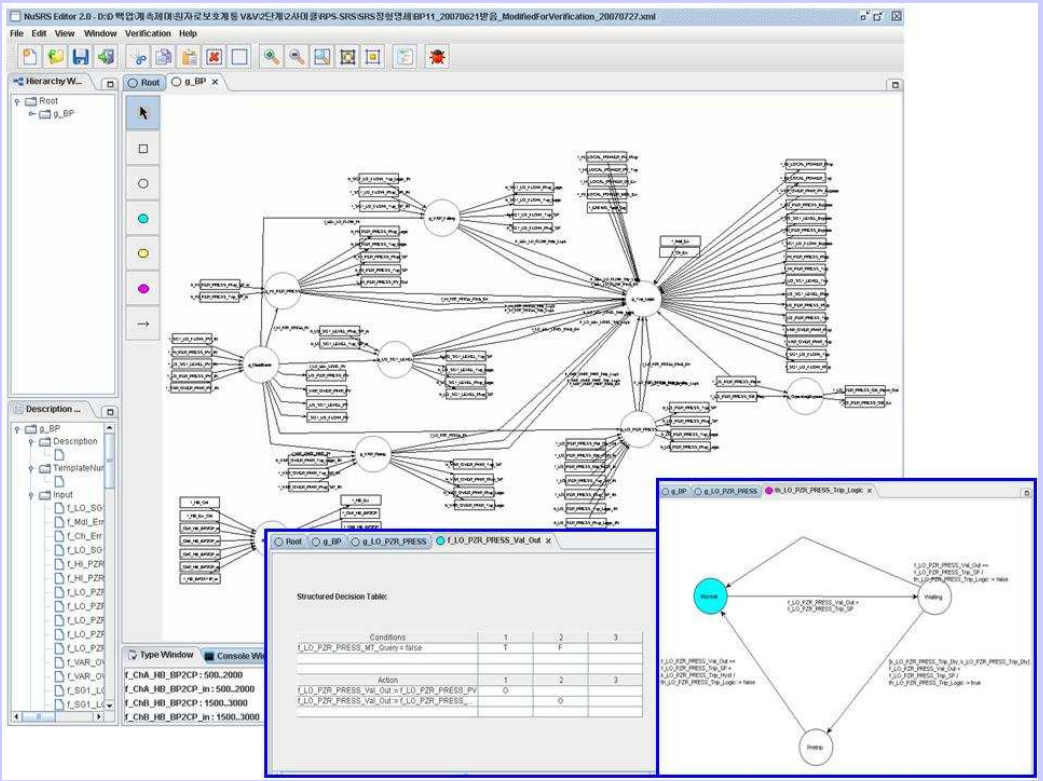
- **Fault Prevention**
  - It is a means for preventing a fault occurrence that is mainly due to software developers.
  - Formal Modularization, Formal Specifications, Design/Coding Guidelines
- **Fault Removal**
  - It is a means for reducing the presence of faults.
  - Verification & Validation Activities, Software Safety Analysis, Formal Verification, and Testing

CASE Tools for KNICS RPS S/W

Formal Modularization



Formal Specifications

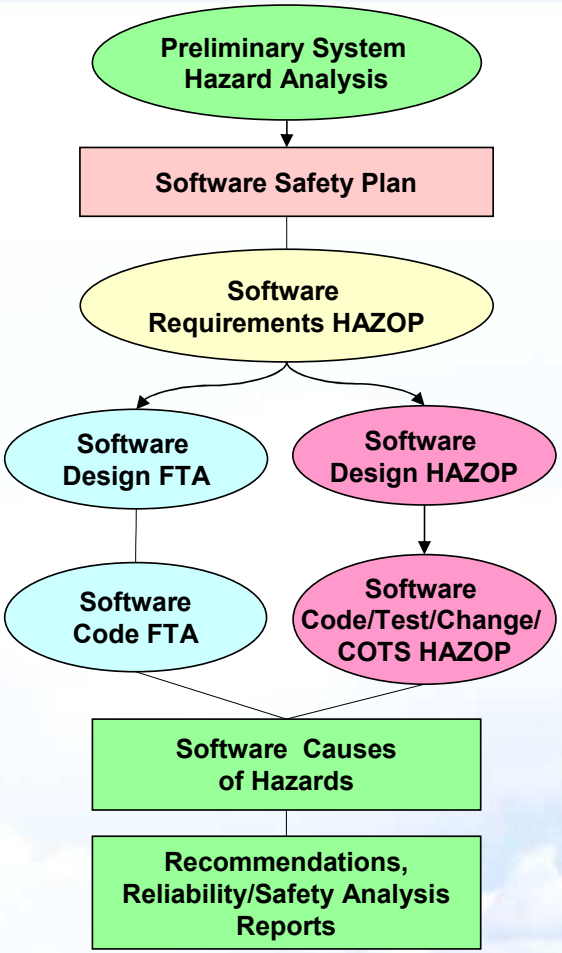


Type & Methods for S/W Dependability

- **Fault Tolerance**
  - It is for ensuring a service capable of fulfilling a system's function in the presence of faults.
  - Watchdog Timers in RPS
- **Fault Prediction**
  - It is about how to estimate the present number, future incidence, and consequences of faults.
  - There are few standard methods with an inter-disciplinary consensus which are applicable to a rare failure event.

- **All activities for RPS S/W are for improving S/W quality of safety and correctness and for achieving highly reliable software.**

S/W Safety Analysis Process of KNICS Digital Systems (RPS + PLC)



HAZOP: Hazard and Operability,
FTA: Fault Tree Analysis
COTS: Commercial-Off-The-Shelf

S/W Safety Analysis at Design Phase

❑ Safety Activity

- ➢ Hazard Analysis for Functional Characteristics

❑ S/W Safety Analysis for DD by Function Block Diagram

- ➢ Scope: All Safety-Critical Software Modules/Functions
- ➢ Method: Software HAZOP + Software FTA
- ➢ Strategy:
  - ✓ Preparation of Software-Contributable System Hazards
  - ✓ HAZOP is applied to all the S/W modules to identify a S/W hazard that can induce a system hazard, considering the system safety and availability
  - ✓ Software FTA is applied to only S/W modules that the S/W HAZOP indicated some critical hazards residing in those modules. And its top node is only related with the most safety-critical hazard.
  - ✓ Software FTA is composed of fault tree templates for function blocks used in FBD (function block diagram).

Characteristics of Analysis Techniques

Software HAZOP	Software FTA
•All Design Specifications (Documents + DD by FBD) •All SW Contributable Hazards •Forward, Broad-Thinking Analysis •Brainstorming by HAZOP Members	•Defective SW Module •Most Critical Hazard •Backward, Local Systematic Analysis •Fault Tree by an Individual Analyst
•Deviation Quantity: Qualitative Functional Characteristics •Guide Phrases (Rather Than Guide Words)	•Based on Fault Tree Templates for Function Blocks •Logical Operation in Fault Event
•Need Discussion Skills	•Difficult to Apply to All Scope

Software-Contributable System Hazards

❑ Software-Contributable System Hazards for KNICS RPS

No	Hazard	Criticality Level
1	RPS cannot generate a trip signal when a trip condition for a process variable is satisfied.	4
2	RPS generates a trip signal when it should not generate a trip signal.	3
3	RPS cannot send qualified information of its operating status to the main control room.	2

Criticality Level 4 - The most significant hazard that can drive a plant to an accident,
Criticality Level 3 - A hazard that impacts significantly on the system operation but does not lead to an accident
Criticality Level 2 - A hazard that can affect more or less the system operation
Criticality Level 1 - An insignificant hazard that seldom affects the system availability

Software HAZOP

❑ HAZOP Definition

- A HAZOP study is for the identification of a hazard in a target system by investigating a plausible deviation of a quantity or attribute and then seeking out the cause that is capable of inducing this deviation and consequences resulting from this deviation.

❑ Basic Components of HAZOP

- Deviation Quantity: (Quantitative) Temp., Press., Valve Openings
- Guide Words: More, Less, Equal, etc.

❑ Distinguishing Features of Software HAZOP

- Deviation Quantity: S/W Functional Characteristics (Qualitative)
  - ✓ Functional Characteristics: Accuracy, Capacity, Functionality, Reliability, Robustness, Security, Safety
- Guide Phrases: For Application to All S/W Lifecycles

Guide Phrases and Deviation Checklist

- **Among guide phrases devised and collected, appropriate guide phrases and their associated deviation checklist suitable for KNICS RPS S/W design are extracted and arranged for S/W functional characterisitics.**

Characteristic	Guide Phrase	Deviation Checklist
Accuracy	Below minimum range	What is the consequence if the sensor value is below its minimum range?
Accuracy	Above maximum range	What is the consequence if the sensor value is above its maximum range?
Accuracy	Within range, but wrong	What is the consequence if the sensor value is within its physical range but incorrect?
Accuracy	Incorrect physical units	What is the consequence if the input has an incorrect physical unit?
Accuracy	Wrong data type or data size	What is the consequence if the input has a wrong data type or data size?
Accuracy	Wrong physical address	What is the consequence if the input variable is allocated to a wrong physical address?
Accuracy	Correct physical address, but wrong variable	What is the consequence if a wrong input variable is allocated to a correct physical address?
Accuracy	Wrong variable type or name	What is the consequence if wrong type or name for an input /output/internal variable is used in the FBD module?
Accuracy	Incorrect variable initialization	What is the consequence if the input/output/ internal variables are initialized incorrectly?
Accuracy	Wong constant value	What is the consequence if the internal constant is given a wrong value?
Accuracy	Incorrect update of history variables	What is the consequence if the variable is updated incorrectly?
Accuracy	Wrong setpoint calculation	What is the consequence if the procedure for calculating a setpoint is incorrect?
Capacity	Erroneous communication data	What is the consequence if there is an error in the ICN data?
Capacity	Erroneous communication data	What is the consequence if there is an error in the SDL data?
Capacity	Unexpected input signal	What is the consequence when an unexpected input signal is arrived?
Capacity	Untimely operator action	What is the consequence if the operator commences a setpoint reset or an operating bypass function untimely?
Functionality	Function is not carried out as specified	What is the consequence if some portions in the FBD module have a defect or cannot perform the intended behavior?
Reliability	Data is passed to incorrect process	What is the consequence if the data is passed to an incorrect process?
Robustness	Incorrect selection of test mode	What is the consequence if the test mode is selected or changed unexpectedly?
Robustness	Incorrect input selection	What is the consequence if the input selection is incorrect?

A Result of Software HAZOP

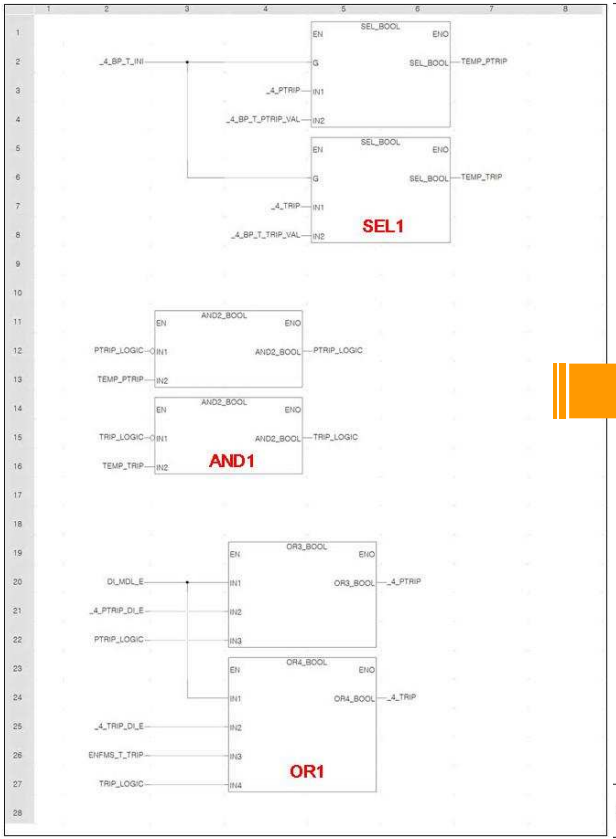
❑ Software HAZOP for SG1_FLW_Lo Trip FBD Module

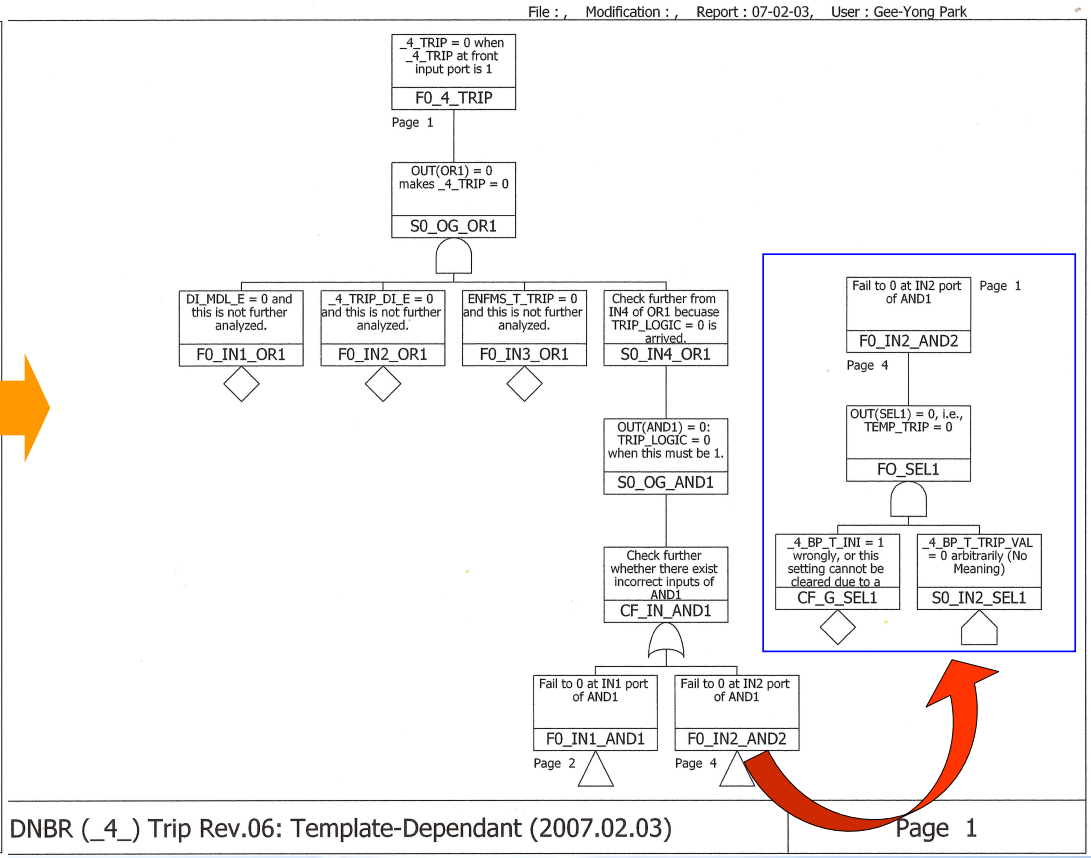
Fun. Charac.	Deviation Checklist	Cause	Analysis	Effect	C	Suggestion
Accuracy	What is the consequence if the sensor value is below its minimum range?	Sensor Failure	The TRIP_DECISION sub-module handles properly an out-of-range value, but it is carried out after all logical operations are done.	No effect on safety, but operability is poor.	2	It is desirable that a trip signal occurs at the front when an out-of-range sensor input value exists.
Accuracy	What is the consequence if the sensor value is above its maximum range?	Sensor Failure				
Accuracy	What is the consequence if the sensor value is within its physical range but incorrect?	Sensor Failure or, Input Conditioner Malfunction	This is the problem at input conditioning processor.	Severe effect on safety	4	Measures should be provided at input processor.
Accuracy	What is the consequence if the internal constant is given a wrong value?	Wong constant value allocation	If MAXCNT is set to 0, the trip signal is always ON regardless of the trip condition status.	Poor Operability	3	Need careful attention when assigning a value.
			If MAXCNT is too large, the trip signal is generated at much later time.	Violating the system response time	4	
Capacity	What is the consequence when an unexpected input signal is arrived?	ATIP Error	No part performs an exceptional handling when ATIP sets up an erroneous test operation.	Wrong test execution	1	Augment test mode selection.
Functionality	What is the consequence if some portions in the FBD module have a defect or cannot perform its intended behavior?	Error in Logic Operation	Pretrip is cancelled whenever it is triggered at the pretrip sub-module.	Pretrip is never functioning	3	Modify a pretrip logic.
			The hysterisis is not reflected in the trip logic sub-module because of using 19th previous value.	Inducing a trip malfunction	4	Modify trip logic.

- **The software module with criticality level 4 (mostly in Functionality) is the target module for the application of software FTA**
- **Defective Modules in BP: SG1_FLW_Lo Trip, PZR_PR_Lo Trip, VA_OVR_PWR_Hi Trip, DNBR_Lo Trip**

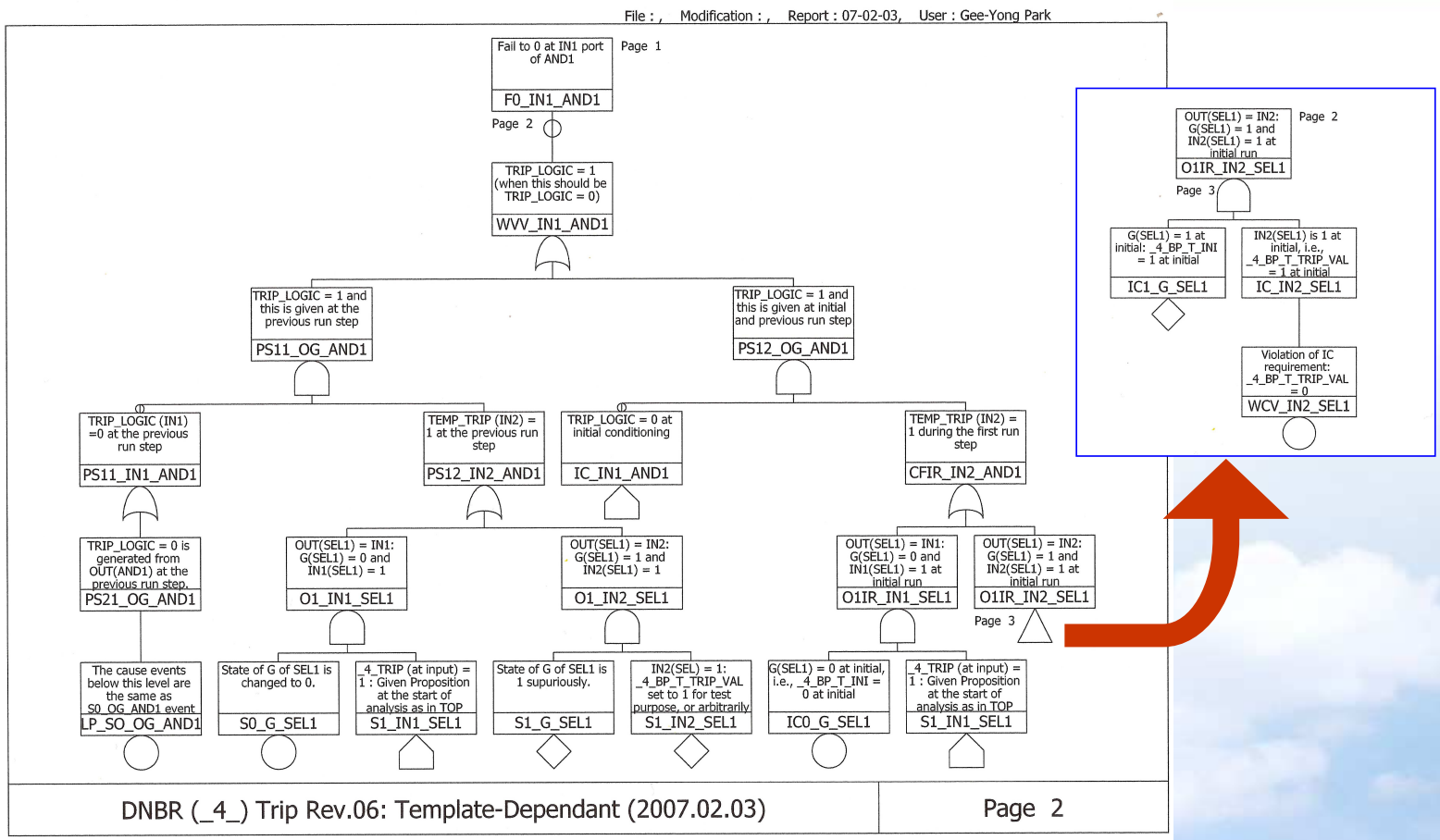
Software FTA for DNBR_LO Trip

FBD Module for DNBR_Lo Trip



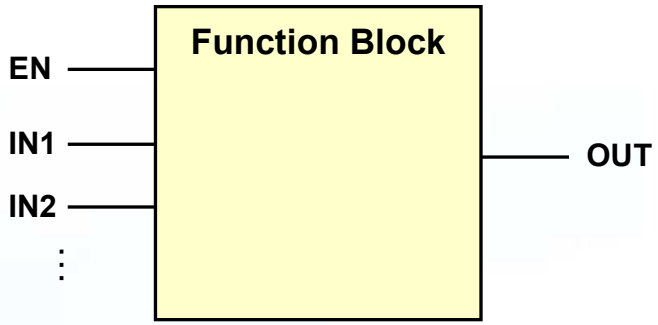


Software FTA for DNBR_LO Trip

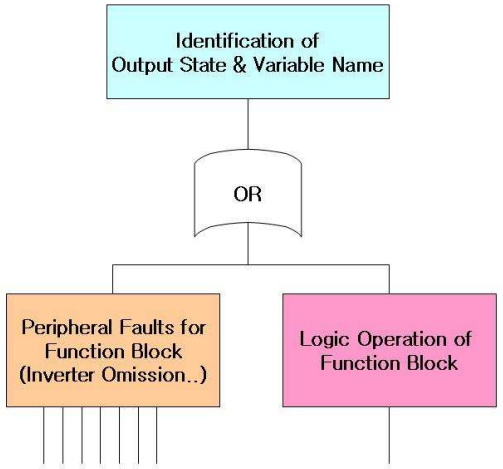


Fault Tree Template for Function Blocks

❑ Principle of Deriving Failure Mode for A FB Fault Tree Template



Typical Function Block

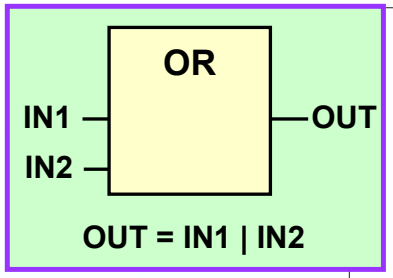


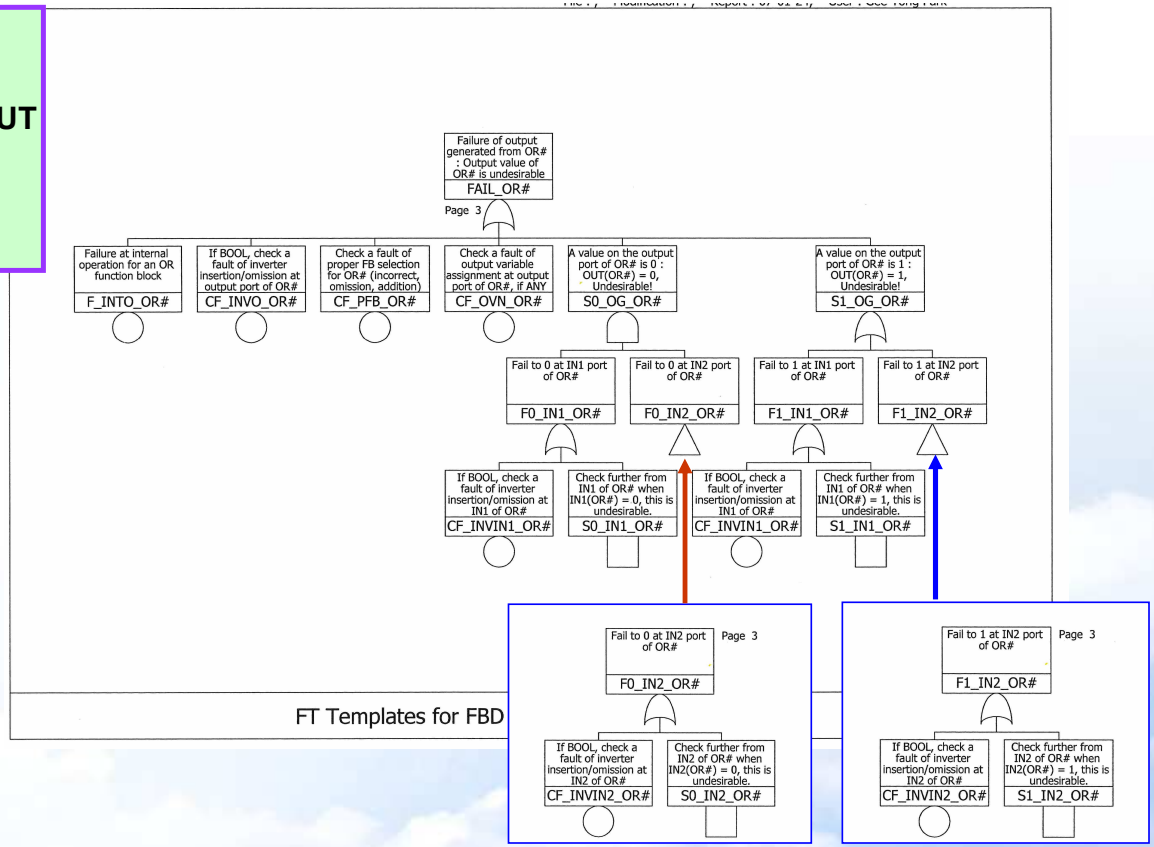
Procedure of FT Template

- It is first to identify the expected value and variable name at OUT.
- It is then to identify the fault type for a particular FB. (At this time, overall behavior for an FBD is understood clearly and the type of function blocks and their expected outputs are followed by an analyst.)
- It is finally to identify the expected value and variable name at INPUT.
- When there is no problem, go down to lower level through FB Logic Operation.

Software Fault Tree Templates for FBs

❑ Fault Tree Template for OR Function Block





Conclusions

- For KNICS RPS S/W, various rigorous methods such as formal specification, formal verification, and SSA are provided in order to achieve reliable software.
- For the SSA, two complementary methods (Software HAZOP + SFTA) are employed.
- Because of a different viewpoint, software HAZOP + SFTA can obtain some faults that have not been found from formal V&V.
- The rigorous approach for SSA and V&V activities will improve S/W quality.

Identification of Interface Points

❑ FBD Modules for BP Software

NO	Module		Description
1	Receive_Signal		HW/SDL/ICN Receive Module
2	PAT_Scheduler		Automatic Test Scheduler
3	Test_Selection		Test Selection Module
4	Trip_ Logic	PZR_PR_Hi Trip	Pressurizer Hi Pressure Trip
		SG1_LVL_Lo_RPS Trip	SG-1 Low Level Trip
		SG1_LVL_Lo_ESF Trip	SG-1 Low Level Trip for ESF
		SG1_LVL_Hi Trip	SG-1 Hi Level Trip
		SG1_PR_Lo Trip	SG-1 Low Pressure Trip
		CMT_PR_Hi Trip	Containment Hi Pressure Trip
		CMT_PR_HH Trip	Containment Hi-Hi Pressure Trip
		SG1_FLW_Lo Trip	SG-1 Low Coolant Flow Trip
		PZR_PR_Lo Trip	Pressurizer Low Pressure Trip
		VA_OVR_PWR_Hi Trip	Variable Over Power Hi Trip
		SG2_LVL_Lo_RPS Trip	SG-2 Low Level Trip
		SG2_LVL_Lo_ESF Trip	SG-2 Low Level Trip for ESF
		SG2_LVL_Hi Trip	SG-2 Hi Level Trip
		SG2_PR_Lo Trip	SG-2 Low Pressure Trip
		SG2_FLW_Lo Trip	SG-2 Low Coolant Flow Trip
		LOG_PWR_Hi Trip	Log Reactor Power Hi Trip
		DNBR_Lo Trip	Low DNBR Trip
		LPD_Hi Trip	Hi LPD Trip
		CPC_CWP Trip	CPC CWP
5	Test_Results_Handler		Test Results Handling Module
6	HB_MONITORING		Heartbeat Monitoring Module
7	HB_Gen		Heartbeat Generation Module
8	Ch_Bypass_Send_Receive		Channel Bypass Transfer Module
9	Send_Signal		HW/SDL/ICN Sending Module

- **Interface Points between FBD Modules and Hazards**
  - **Trip modules in no.4 (except CPC_CWP) affect the hazard item 1 and 2.**
  - **Some S/W in FBD Module no.1 & 2 affect the hazard item 1 and 2 through Trip_Logic (no.4).**
  - **FBD modules of no.5,8, & 9 affect hazard item 3.**

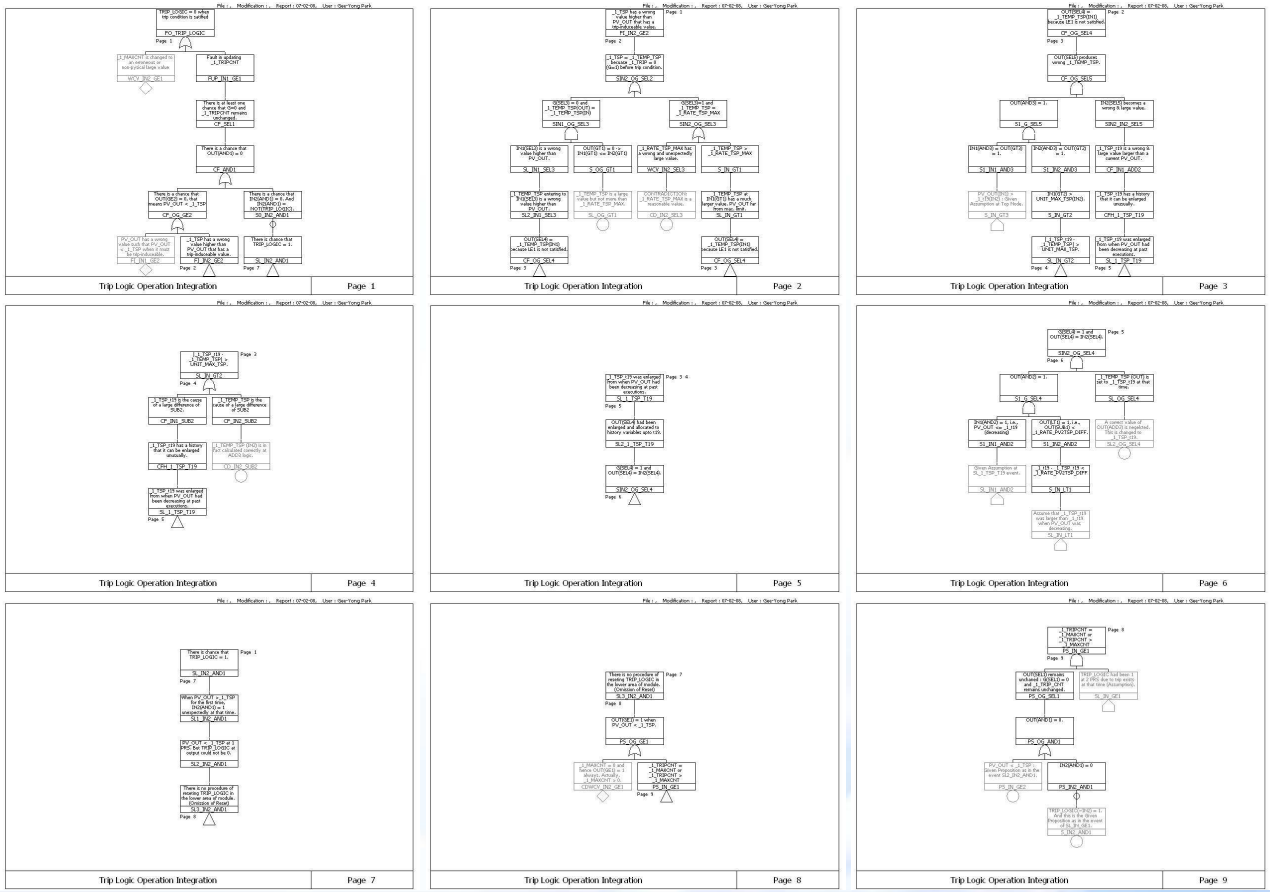
Software Fault Tree Analysis (SFTA)

❑ Analysis Concept of SFTA

- In the SFTA, it is hypothesized that the software has produced an unsafe output and it is shown that this could not happen because the hypothesis leads to a contradiction.
- If a path is found through the software and out into the controlled system or its environment that does not contain a logical contradiction, SFTA reveals the input conditions necessary for this hazard to occur.

Software FTA for VA_OVR_PWR_Hi

❑ SFTA for Variable Over Power High Trip (for Trip_Operation module ONLY)



•비율제한가변설정치

FB Module for VA_OVR_PWR_Hi