Software Test-based Reliability Assessment Framework for Nuclear Power Plant Safety-critical Software

Probabilistic Safety Assessment and Management (PSAM 14),
September 17-21, 2018, Los Angeles, CA.

Sang Hun LEE[1], Seung Jun LEE[2], Jinkyun Park[3], Eun-chan LEE[4], Hyun Gook KANG[1*]

[1] Department of Mechanical, Aerospace, and Nuclear Engineering, Rensselaer Polytechnic Institute (RPI), Troy, NY, USA

[2] School of Mechanical and Nuclear Engineering, Ulsan National Institute of Science and Technology (UNIST), Ulsan, ROK

[3] Integrated Safety Assessment Division, Korea Atomic Energy Research Institute (KAERI), ROK

[4] Korea Hydro & Nuclear Power (KHNP) Co., Ltd., ROK

Contents

- **Introduction**
  - Research background/scope
  - Previous research on QSRMs
- **Proposed Framework:**

  <Simulation-based NPP safety SW testing & reliability quantification>
  - Safety-critical PLC SW Test-bed development
  - Operational-profile-based SW test case generation
- **Application to KNICS IDiPS-RPS BP trip logic software**
  - Development of SW test case for BP trip signal generation
  - Test procedure and results of BP trip logic using SW test-bed
  - Software failure probability quantification from BP trip logic test results
- **Conclusion**
- **Reference**

Research Background

- Reliability assessment of safety-critical software used in NPP has been one of the important issues in PRA of digital I&C system.
  - The failure of the safety-critical software failure can induce the common cause failure (CCF) of processor modules in NPP digital I&C system.
  - In order to model the software failure in the PRA of digitalized NPP, the quantification/verification of a very low software failure probability is crucial.

Digital System Failure Events Reported in LERs (1990-1993) [AEOD/T94-03]

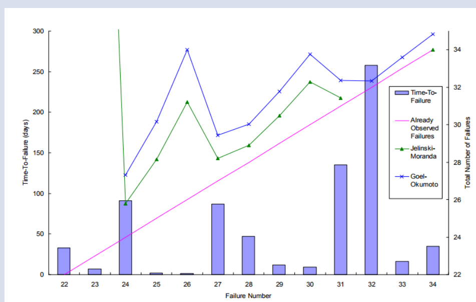
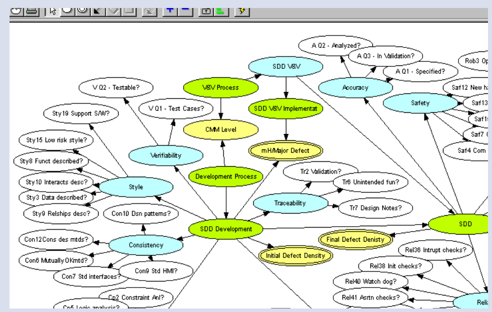
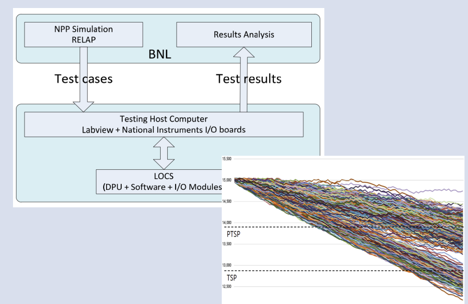
Category	Number of Event
Software error	30
HMI error	25
EM interference	15
Component random failure	9
Total	79

Standards on the Safety issues related to Software used in Digitalized Nuclear Power Plant

Previous Research on QSRMs

- Due to limitations of available QSRMs in nuclear field, existing approaches are inappropriate to quantify/verify very low SFP (~10^{-5} failure/demand).
  - Therefore, a practical SW testing framework is needed in order to effectively ass ure low NPP safety SW reliability and prove error-freeness of SW functionality.

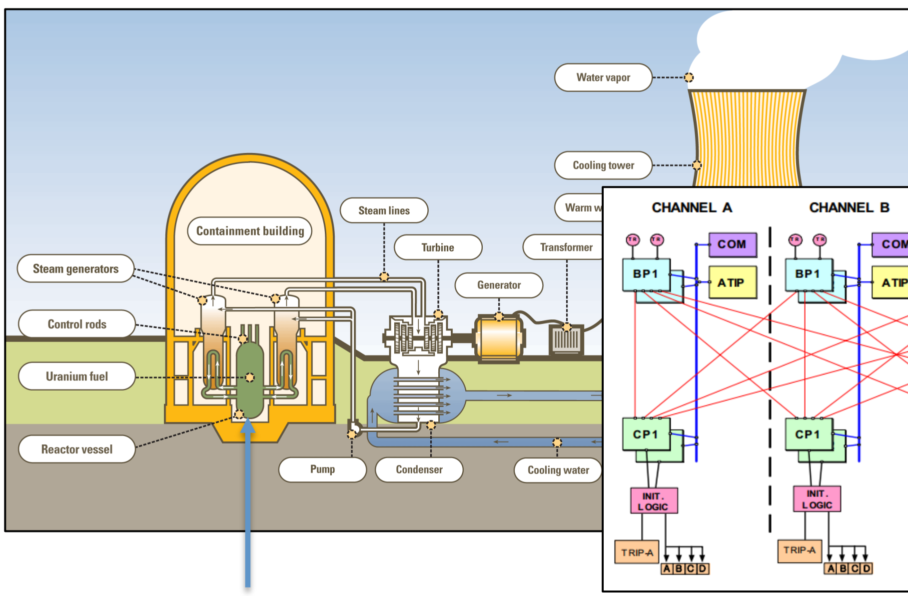
Representative examples of existing quantitative software reliability methods (QSRMs)

Representative existing QSRMs	Software Reliability Growth Model (SRGM) (Kim, 2007; 2012)	Bayesian Belief Network (BBN) model (Eom, 2013)	Black-box test-based method (Chu, 2016; Li 2016)
Description	 - Using available software testing results or failure histories, the software reliability is estimated.	 - By aggregating disparate inform ation on the software (failure data , quality of SDLC), the SFP is esti mated.	 - Without knowledge on software internal structure, random sample s from SW input space are selected and tested.
Limitations	• Lack of software failure data • Model estimate is sensitive to software time-to-failure data	• Uncertainty in SFP estimates due to parameter uncertainty. • Model is often requires software-specific evidence.	• Difficulty in addressing input coverage • Long test execution time per test case • Large number of test set required to demonstrate low SFP

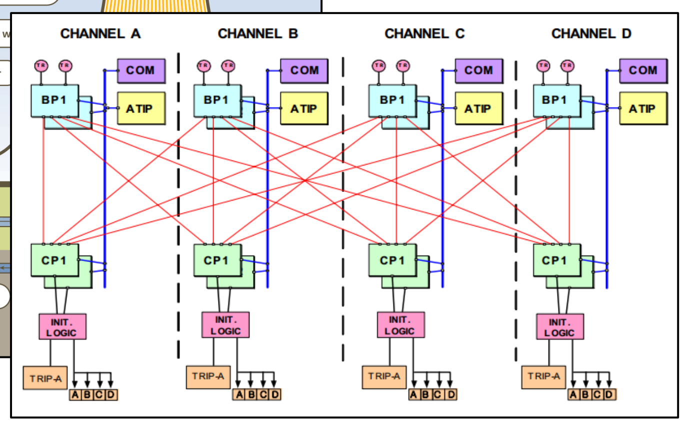
Research Scope

- Software failure probability of NPP safety SW is defined as:
  - probability of failure on demand (here, demand = plant condition that requires act uation of safety systems) - e.g. a failure to generate a Rx trip signal.

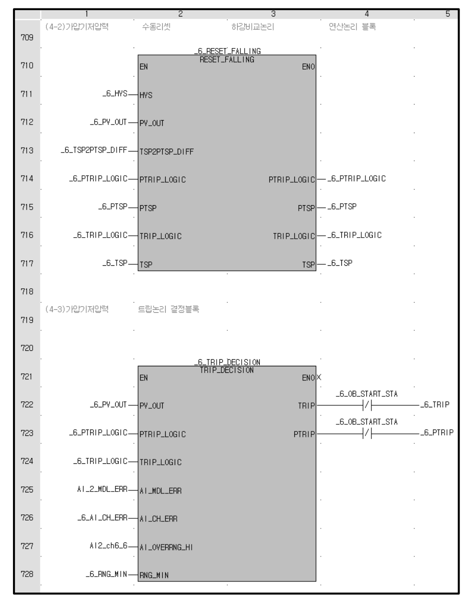
- The scope of this study is focused on:
  - 1) develop a software testing framework for NPP safety software failures to gener ate its dedicated safety signal.
  - 2) quantify the SFP based on software test results using simulation-based SW te st-bed in consideration of the operational profile of SW test cases.



If trip signal is generated by RPS, the reactor is safely shutdown.

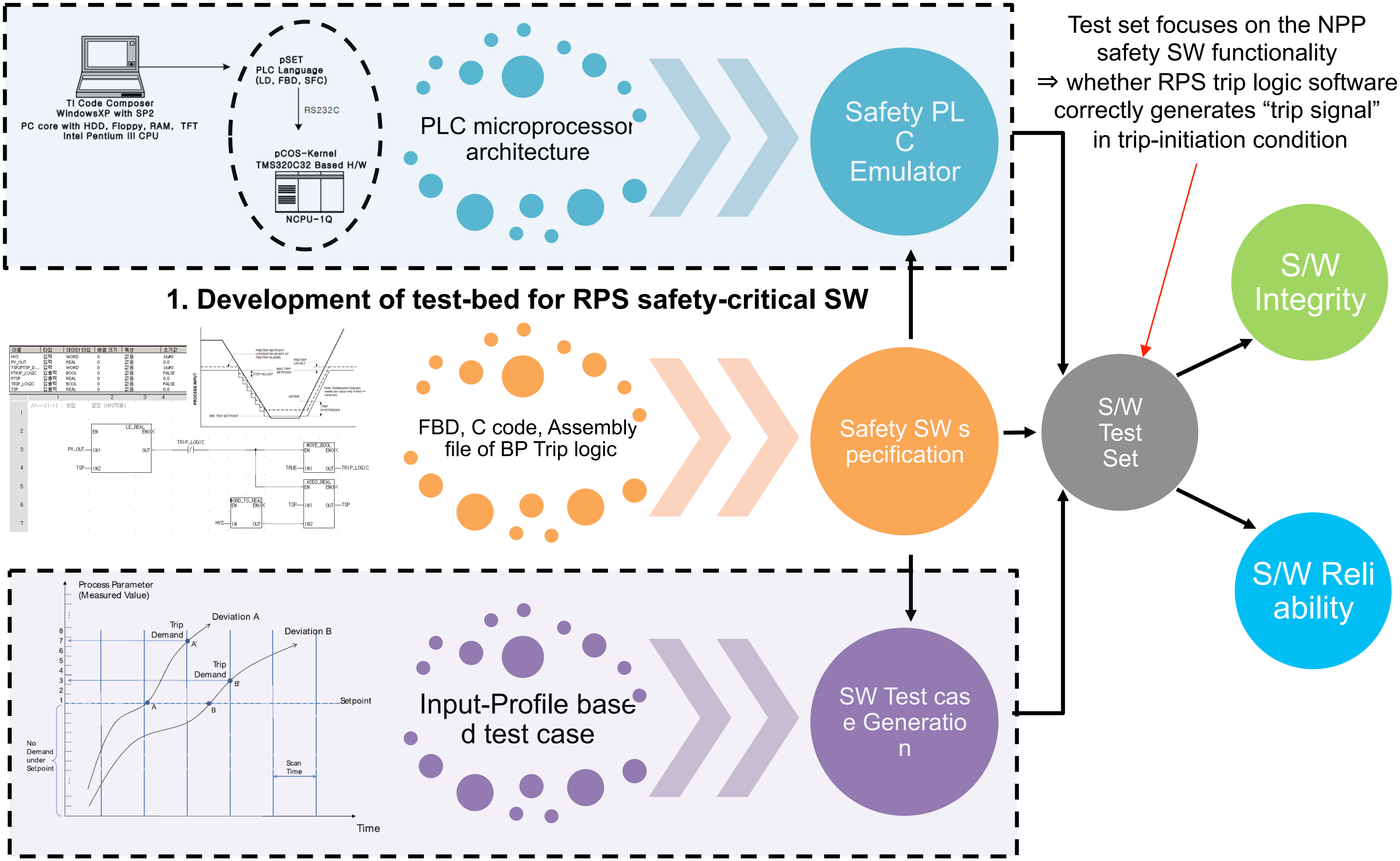


Configuration of 2-out-4 Reactor Protection System in NPP



Example of Rx Trip Logic Software

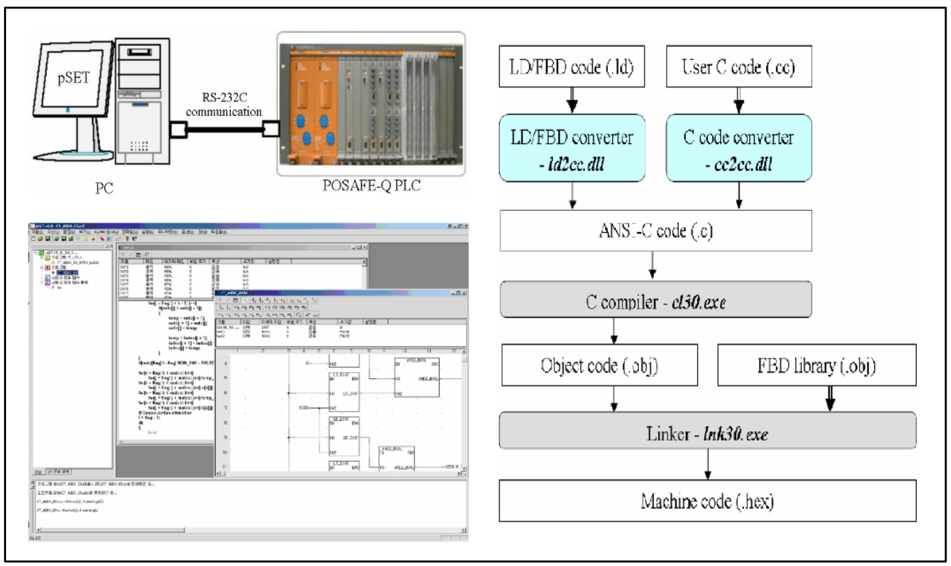
Overall Framework



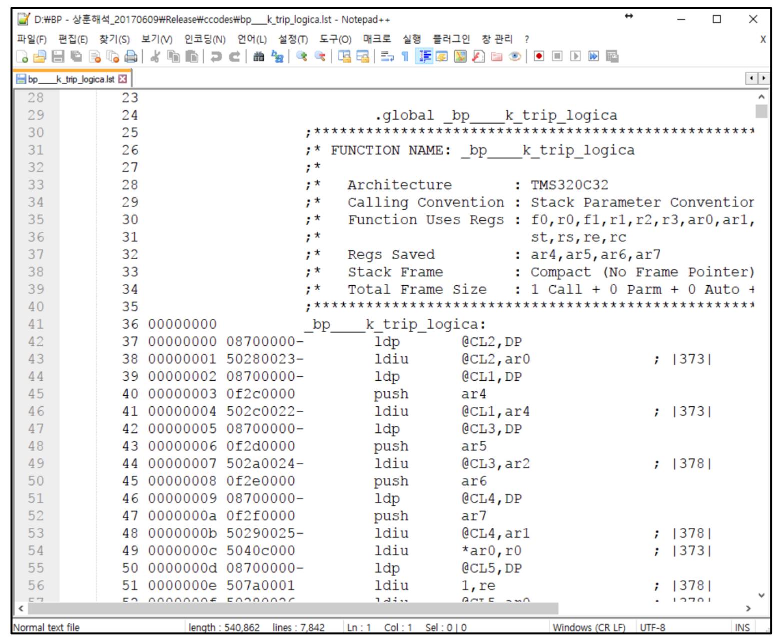
2. Development of SW test cases (input/internal) for RPS safety-critical SW

Safety-critical PLC SW Test-bed development

- PLC widely used in NPP control system consists of various modules, such as process or, communication, and I/O modules.
  - Especially, the processor module uses a programmable memory to store program instructions and to implement functions as a binary form.
- PLC executes a compiled machine code (from FBD/LD and C code), thus test-bed can be developed by capturing PLC microprocessor architecture, such as:
  - CPU registers, Memory
  - Machine instructions, etc.



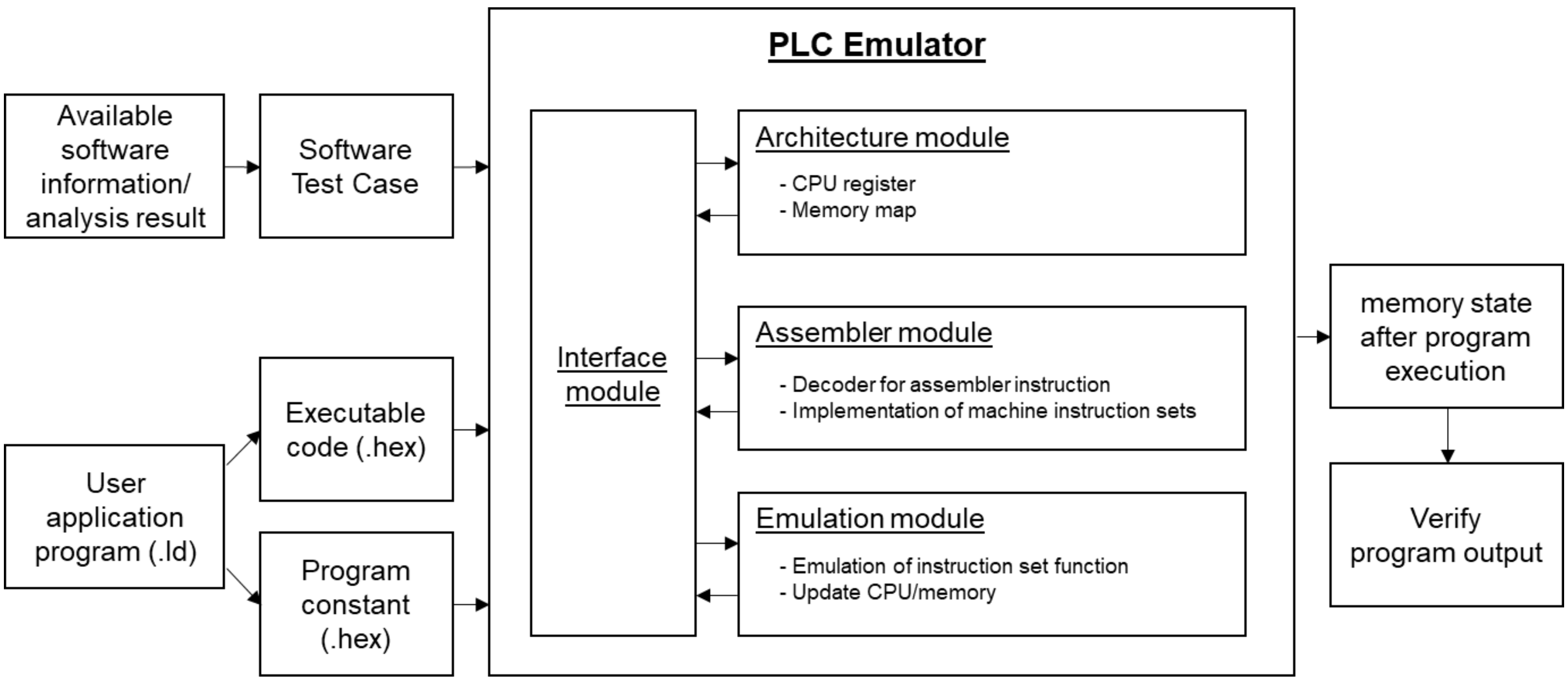
Software engineering tool of NPP safety PLC and its compile procedure for safety programs



Example of compiled BP software from LD/FBD

Safety-critical PLC SW Test-bed development

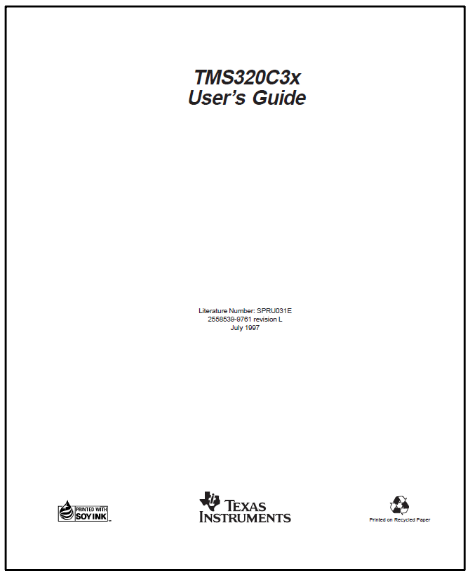
- Components of safety PLC SW test-bed [Lee et al., 2018]:
  - **1) Architecture module**: CPU registers, Memory map (16Mbyte; 0x000000 ~ 0x00FFFFFF)
  - **2) Assembler module**: Instruction sets of PLC microprocessor (113 instructions)
  - **3) Emulation module**: Emulation of operation of PLC microprocessor instruction sets
  - **4) Interface module**: Interface between each module
    - Instruction set decoded from Assembler module is transferred to Emulation module to conduct its spec ific operation.
    - Result of instruction set execution by Emulation module is updated to the CPU/memory emulated in Ar chitecture module.



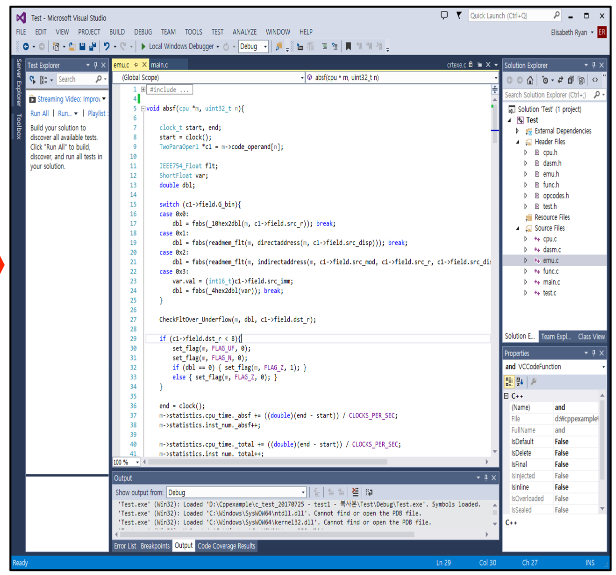
An overview of the simulation-based test-bed for safety-critical PLC software testing

Safety-critical PLC SW Test-bed development

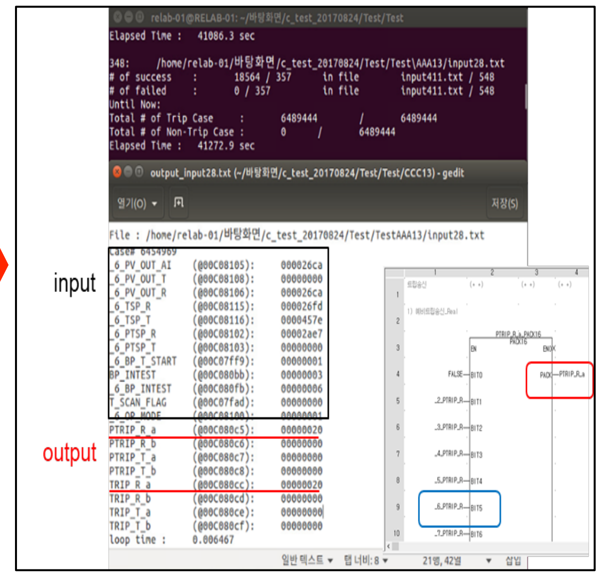
- KNICS IDiPS-RPS BP processor module – TI C32 DSP CPU (TMS320C3x)



Target microprocessor assembly (TMS320C3x)



Developed BP Software Test-bed (emulate the behavior of the microprocessor given SW program)

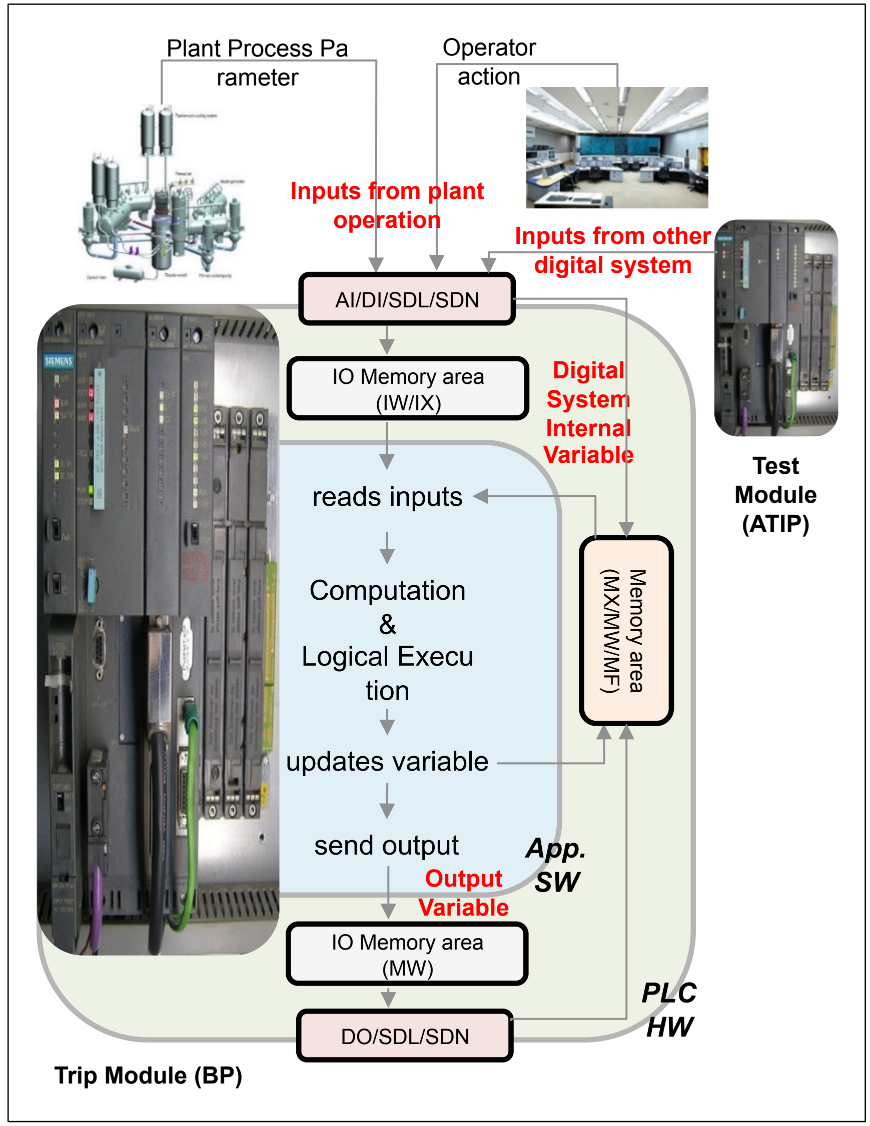


Check the final state of PLC microprocessor after SW program execution

Operational-profile based SW Test Case Generation

- PLC operation is characterized b y its cyclic operation mode:
  - CPU checks
  - I/O checks
  - Input scan
    - copy physical input values into it s memory
  - Logic execution
    - executes a program based on a memory map
  - Output scan
  - updates output

- By deriving the combination of p ossible SW input/internal space, it is possible to test a software by verifying the output for each test case (sets of input/internal varia bles states).



Operating Mechanism of a Typical NPP safety PLC

Operational-profile based SW Test Case Generation

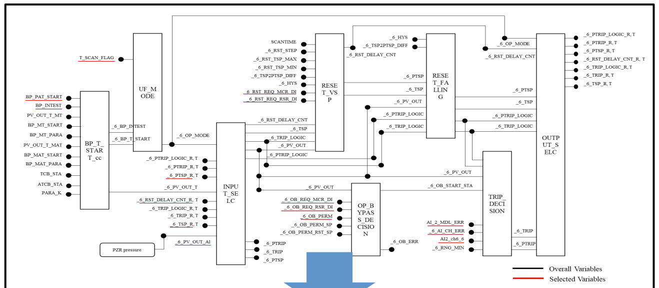
Reliability

Software test case generation
(considering SW logic/input/internal variable)

+

Operational Profile of SW Test Case
(Plant Behavior + Operator action)

SW logic/SRS/SDS

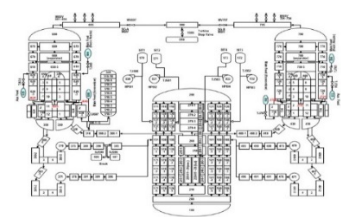


Software test cases

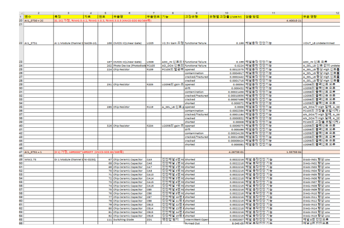
ID	Input, internal variable state of test case*	Description of test case
1	AI_2_MDL_ERR = 0x1, …	Trip generated due to error signal from analog input module
4	_6_PV_OUT_AI = 0x256, …	Process variable is below its minimum range
5	_6_PV_OUT_AI = 0x454B, _6_TSP_R = 0x457E, _6_OB_REQ_MCR_DI = 0x1, …	Operator requested the trip bypass signal, but not is permitted. Trip signal is generated since process variable is below the trip set-point
…	…	…

(in total of 705,892,684 test cases)

Plant Behavior/Spec docs/etc.

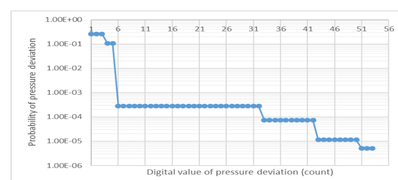


T-H analysis

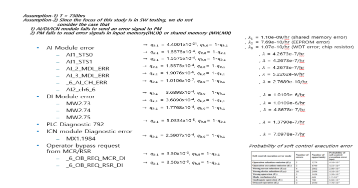


PLC FMEA data

Derive the profile of Input/Internal Variable



Profile of plant process variable



Profile of PLC status variables.

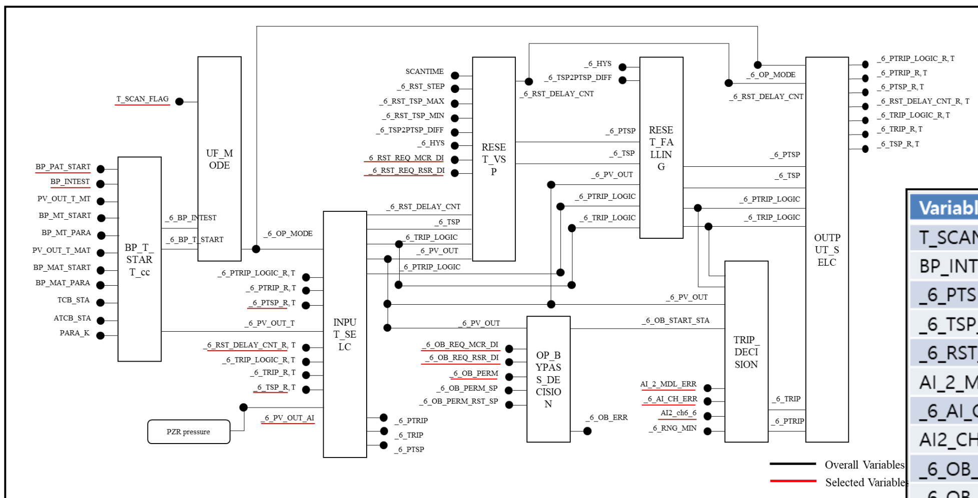
→ Based on SW test result, software failure probability is estimated as:

$\hat{\theta}_t$: estimated software failure probability,
$\hat{\theta}_i$: software failure probability for test case i,
p_i: operational (explicit) profile of each test case

Application: IDiPS-RPS BP Trip logic SW

Reliability

- IDiPS-RPS BP Trip Logic SW - Test Case Generation
  - **Target Trip logic**: PZR_PR_LO Trip (Manual-Reset Variable Trip-setpoint)
  - **Target Case**: Trip-initiation condition
    (test input/internal variables' states that will generate Rx trip signal)
  - **Target scenario**: Double-ended guillotine break accident (30 inch x 2)



An overview of the BP PZR_PR_LO trip logic♪

Variable	Description	Format	Type*
T_SCAN_FLAG	Flag for PLC scan operation (operation/test)	BOOL	SV
BP_INTEST	BP test status	BOOL	SV
_6_PTSP_R	PZR_PR_LO pre-trip set-point	WORD	SV
_6_TSP_R	PZR_PR_LO trip set-point	WORD	SV
_6_RST_DELAY_CNT_R	PZR_PR_LO reset delay count	WORD	SV
AI_2_MDL_ERR	Analog Input module error signal	BOOL	IV
_6_AI_CH_ERR	Analog Input channel error signal	BOOL	IV
AI2_CH6_6	Analog Input channel high over range error signal	BOOL	IV
_6_OB_PERM	Operator trip bypass permission	BOOL	IV
_6_OB_REQ_MCR_DI	Operator trip bypass request (from MCR)	BOOL	IV
_6_OB_REQ_RSR_DI	Operator trip bypass request (from RSR)	BOOL	IV
_6_RST_REQ_MCR_DI	Trip set-point reset signal (from MCR)	BOOL	IV
_6_RST_REQ_RSR_DI	Trip set-point reset signal (from RSR)	BOOL	IV
BP_PAT_START	Periodic automatic test start signal	WORD	IV
_6_PV_OUT_AI	PZR_PR_LO process parameter (PZR pressure)	WORD	IV

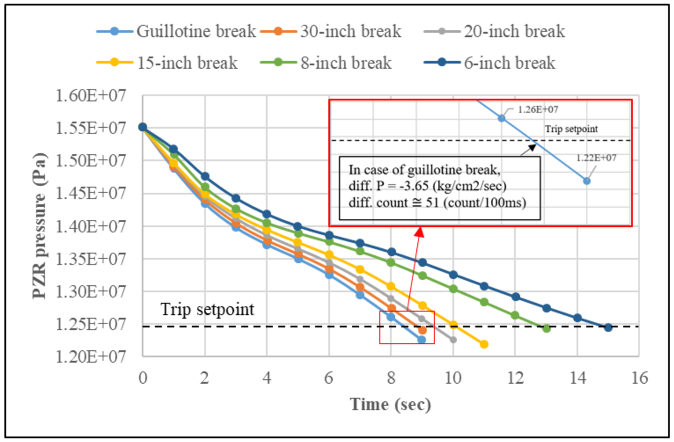
*SV: State (or internal) variable; IV: Input Variable.

Summarized variables for PZR_PR_LO (_6_) trip logic test case generation♪

Application: IDiPS-RPS BP Trip logic SW

IDiPS-RPS BP Trip Logic SW - Test Case Generation

- Number of test sets: 705,892,684 cases
  - Pressurizer pressure: 17738 ~ 22503 (TSP: 17790, full power 15.5MPa: 22503)
    - D_{max} (maximum i-th digital value below trip set-point) at Double-ended guillotine break = 53

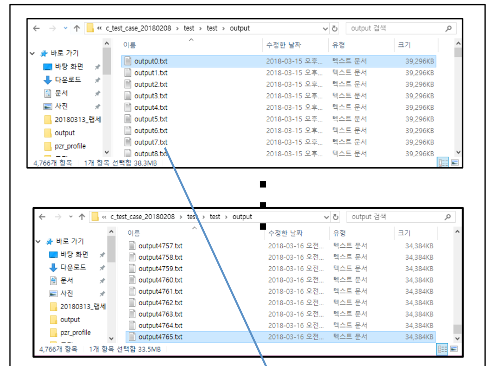


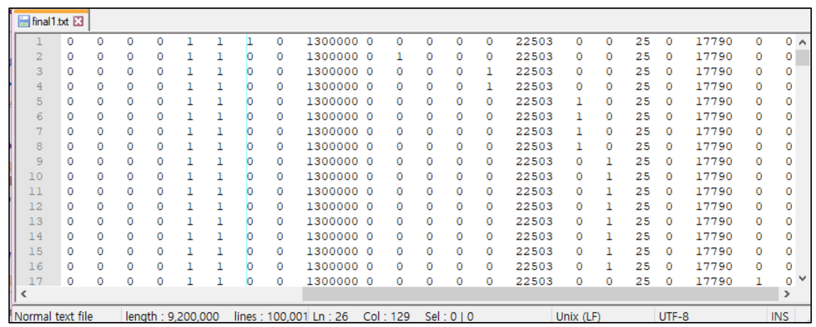
Obtained profile of PZR pressure for various LOCA groups from T-H analysis of target NPP using MARS code.♪

D_{max} of the PZR pressure (_6_PV_OUT_AI) for various LOCA categories

ID	Effective diameter (in.)	D_{max} (count)	Frequency	Fraction
1	0.50	1	1.46E-03	7.78E-01
2	1.625	4	4.02E-04	2.14E-01
3	3.0	6	1.42E-05	7.54E-03
4	7.0	33	1.37E-06	7.29E-04
5	14.0	43	1.71E-07	9.10E-05
6	31.0	51	2.90E-09	1.54E-05
	30.0 * 2	53		

Generated test set files

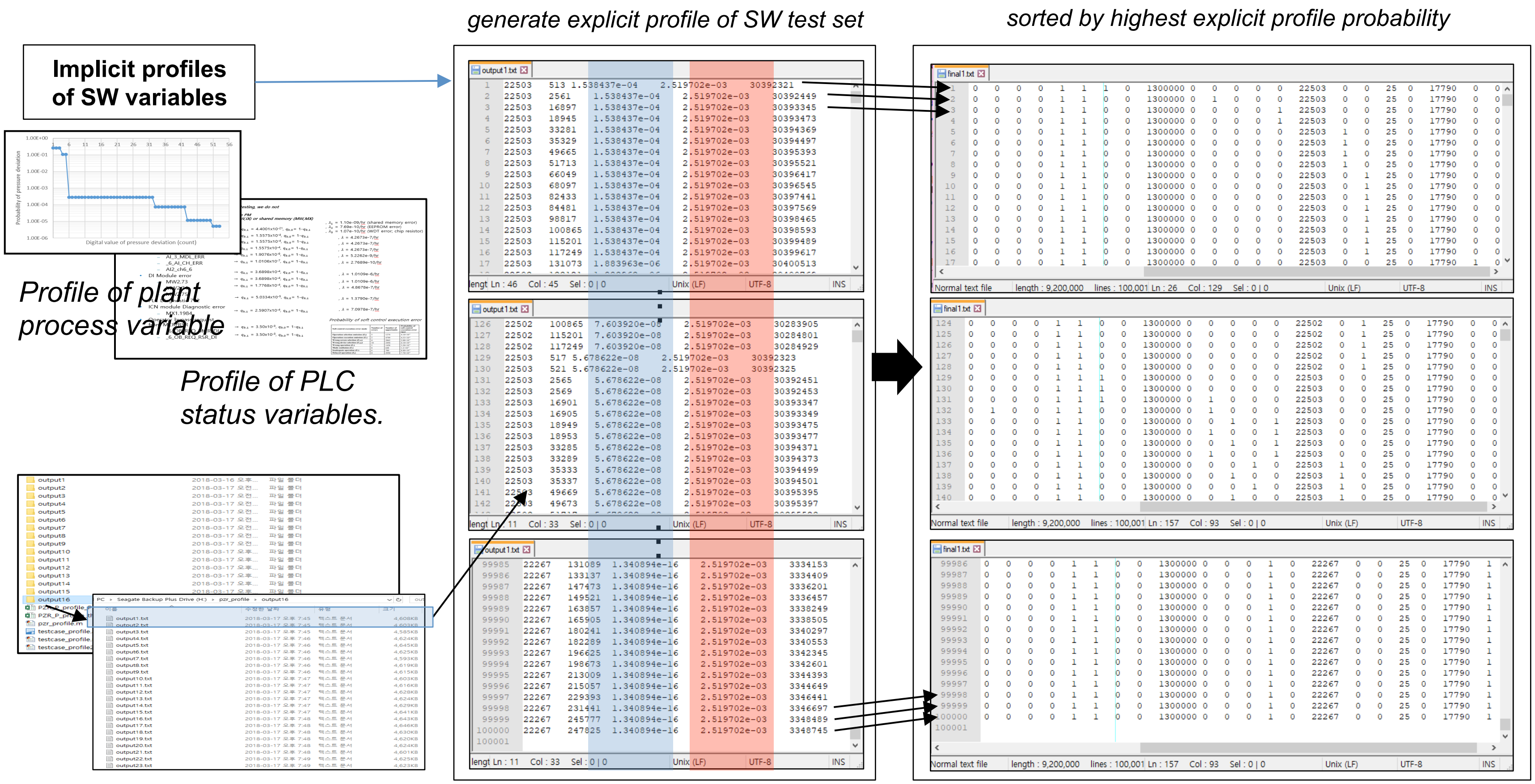




Example of generated test set file for BP PZR_PR_LO trip logic

Application: IDiPS-RPS BP Trip logic SW

- IDiPS-RPS BP Trip Logic SW – Derive Profile of Test Case
  - **Target logic**: KNICS RPS BP trip logic - pressurizer-pressure-low trip (PZR_PR_LO_Trip)
  - **Target scenario**: NPP full power operation
  - **Assumption**: No test module(ATIP) heartbeat error
    PLC error (AI/DI/ICN/diagnostics error) are considered.
  - **Pressurizer pressure**: 17738 ~ 22503 (TSP: 17790, full power 15.5MPa: 22503)



Application: IDiPS-RPS BP Trip logic SW

- IDiPS-RPS BP Trip Logic SW – Number of SW test set to assure low SW PFD:
  - Software failure probability after the success of the first test:
  - Based on the derived explicit profile for the SW test set, the number of test sets to assure low S W PFD can be derived quantitatively.
  - A low software failure probability can be verified with minimum effort by running the SW test set having highest probability to lowest probability.

From Highest Probability						
ID	folder	test case		Prob.	Fraction	SW failure prob.
1	16	22503	513	1.54E-04	6.05E-02	9.39E-01
2	16	22503	2561	1.54E-04	6.05E-02	8.79E-01
3	16	22503	16897	1.54E-04	6.05E-02	8.18E-01
4	16	22503	18945	1.54E-04	6.05E-02	7.58E-01
5	16	22503	33281	1.54E-04	6.05E-02	6.97E-01
6	16	22503	35329	1.54E-04	6.05E-02	6.37E-01
7	16	22503	49665	1.54E-04	6.05E-02	5.76E-01
8	16	22503	51713	1.54E-04	6.05E-02	5.16E-01
9	16	22503	66049	1.54E-04	6.05E-02	4.55E-01
10	16	22503	68097	1.54E-04	6.05E-02	3.95E-01
11	16	22503	82433	1.54E-04	6.05E-02	3.34E-01
12	16	22503	84481	1.54E-04	6.05E-02	2.74E-01
13	16	22503	98817	1.54E-04	6.05E-02	2.13E-01
14	16	22503	100865	1.54E-04	6.05E-02	1.52E-01
15	16	22503	115201	1.54E-04	6.05E-02	9.20E-02
16	16	22503	117249	1.54E-04	6.05E-02	3.14E-02
17	16	22503	131073	1.88E-06	7.41E-04	3.07E-02
18	16	22503	133121	1.88E-06	7.41E-04	2.99E-02
19	16	22503	147457	1.88E-06	7.41E-04	2.92E-02
20	16	22503	149505	1.88E-06	7.41E-04	2.85E-02
21	16	22503	163841	1.88E-06	7.41E-04	2.77E-02
22	16	22503	165889	1.88E-06	7.41E-04	2.70E-02
23	16	22503	180225	1.88E-06	7.41E-04	2.62E-02
24	16	22503	182273	1.88E-06	7.41E-04	2.55E-02
25	16	22503	196609	1.88E-06	7.41E-04	2.48E-02
26	16	22503	198657	1.88E-06	7.41E-04	2.40E-02
27	16	22503	212993	1.88E-06	7.41E-04	2.33E-02
28	16	22503	215041	1.88E-06	7.41E-04	2.25E-02
29	16	22503	229377	1.88E-06	7.41E-04	2.18E-02
30	16	22503	231425	1.88E-06	7.41E-04	2.10E-02
31	16	22503	245761	1.88E-06	7.41E-04	2.03E-02
32	16	22503	247809	1.88E-06	7.41E-04	1.96E-02
33	16	22503	4609	5.40E-07	2.13E-04	1.94E-02
34	16	22503	6657	5.40E-07	2.13E-04	1.91E-02
35	16	22503	8705	5.40E-07	2.13E-04	1.89E-02
36	16	22503	10753	5.40E-07	2.13E-04	1.87E-02
37	16	22503	20993	5.40E-07	2.13E-04	1.85E-02
38	16	22503	23041	5.40E-07	2.13E-04	1.83E-02

From Highest Probability						
ID	folder	test case		Prob.	Fraction	SW failure prob.
37	16	22503	20993	5.40E-07	2.13E-04	1.85E-02
38	16	22503	23041	5.40E-07	2.13E-04	1.83E-02
39	16	22503	25089	5.40E-07	2.13E-04	1.81E-02
40	16	22503	27137	5.40E-07	2.13E-04	1.79E-02
41	16	22503	37377	5.40E-07	2.13E-04	1.77E-02
42	16	22503	39425	5.40E-07	2.13E-04	1.74E-02
43	16	22503	41473	5.40E-07	2.13E-04	1.72E-02
44	16	22503	43521	5.40E-07	2.13E-04	1.70E-02
45	16	22503	53761	5.40E-07	2.13E-04	1.68E-02
46	16	22503	55809	5.40E-07	2.13E-04	1.66E-02
47	16	22503	57857	5.40E-07	2.13E-04	1.64E-02
48	16	22503	59905	5.40E-07	2.13E-04	1.62E-02
49	16	22503	70145	5.40E-07	2.13E-04	1.59E-02
50	16	22503	72193	5.40E-07	2.13E-04	1.57E-02
51	16	22503	74241	5.40E-07	2.13E-04	1.55E-02
52	16	22503	76289	5.40E-07	2.13E-04	1.53E-02
53	16	22503	86529	5.40E-07	2.13E-04	1.51E-02
54	16	22503	88577	5.40E-07	2.13E-04	1.49E-02
55	16	22503	90625	5.40E-07	2.13E-04	1.47E-02
56	16	22503	92673	5.40E-07	2.13E-04	1.45E-02
57	16	22503	102913	5.40E-07	2.13E-04	1.42E-02
58	16	22503	104961	5.40E-07	2.13E-04	1.40E-02
59	16	22503	107009	5.40E-07	2.13E-04	1.38E-02
60	16	22503	109057	5.40E-07	2.13E-04	1.36E-02
61	16	22503	119297	5.40E-07	2.13E-04	1.34E-02
62	16	22503	121345	5.40E-07	2.13E-04	1.32E-02
63	16	22503	123393	5.40E-07	2.13E-04	1.30E-02
64	16	22503	125441	5.40E-07	2.13E-04	1.28E-02
65	1	17790	1	3.96E-07	1.56E-04	1.26E-02
66	1	17790	2049	3.96E-07	1.56E-04	1.24E-02
67	1	17790	16385	3.96E-07	1.56E-04	1.23E-02
68	1	17790	18433	3.96E-07	1.56E-04	1.21E-02
69	1	17790	32769	3.96E-07	1.56E-04	1.20E-02
70	1	17790	34817	3.96E-07	1.56E-04	1.18E-02
71	1	17790	49153	3.96E-07	1.56E-04	1.17E-02
72	1	17790	51201	3.96E-07	1.56E-04	1.15E-02
73	1	17790	65537	3.96E-07	1.56E-04	1.14E-02
74	1	17790	67585	3.96E-07	1.56E-04	1.12E-02

Summarized explicit profile of SW test set for PZR_PR_LO trip logic
(sorted by highest prob. to lowest prob.)

From Highest Probability						
ID	folder	test case		Prob.	Fraction	SW failure prob.
75402	16	22334	68097	6.16E-11	2.42E-08	1.00E-04
75403	16	22334	82433	6.16E-11	2.42E-08	1.00E-04
75404	16	22334	84481	6.16E-11	2.42E-08	1.00E-04
75405	16	22334	98817	6.16E-11	2.42E-08	1.00E-04
75406	16	22334	100865	6.16E-11	2.42E-08	9.99E-05
75407	16	22334	115201	6.16E-11	2.42E-08	9.99E-05
75408	16	22334	117249	6.16E-11	2.42E-08	9.99E-05

SW PFD ~ 10^{-4}

From Highest Probability						
ID	folder	test case		Prob.	Fraction	SW failure prob.
246551	10	20474	25089	2.16E-13	8.52E-11	1.00E-05
246552	10	20474	27137	2.16E-13	8.52E-11	1.00E-05
246553	10	20474	37377	2.16E-13	8.52E-11	1.00E-05
246554	10	20474	39425	2.16E-13	8.52E-11	9.99E-06
246555	10	20474	41473	2.16E-13	8.52E-11	9.99E-06
246556	10	20474	43521	2.16E-13	8.52E-11	9.99E-06
246557	10	20474	53761	2.16E-13	8.52E-11	9.99E-06

SW PFD ~ 10^{-5}

From Highest Probability						
ID	folder	test case		Prob.	Fraction	SW failure prob.
706346	2	18115	34305	9.60E-15	3.78E-12	1.00E-06
706347	2	18115	35331	9.60E-15	3.78E-12	1.00E-06
706348	2	18115	36353	9.60E-15	3.78E-12	1.00E-06
706349	2	18115	49667	9.60E-15	3.78E-12	9.99E-07
706350	2	18115	50689	9.60E-15	3.78E-12	9.99E-07
706351	2	18115	51715	9.60E-15	3.78E-12	9.99E-07
706352	2	18115	52737	9.60E-15	3.78E-12	9.99E-07
706353	2	18115	66051	9.60E-15	3.78E-12	9.99E-07

SW PFD ~ 10^{-6}

Number of SW test set for some SW failure probability
(SIL-4 level: 10^{-4} ~ 10^{-6})

Application - KNICS-RPS BP Trip Logic SW

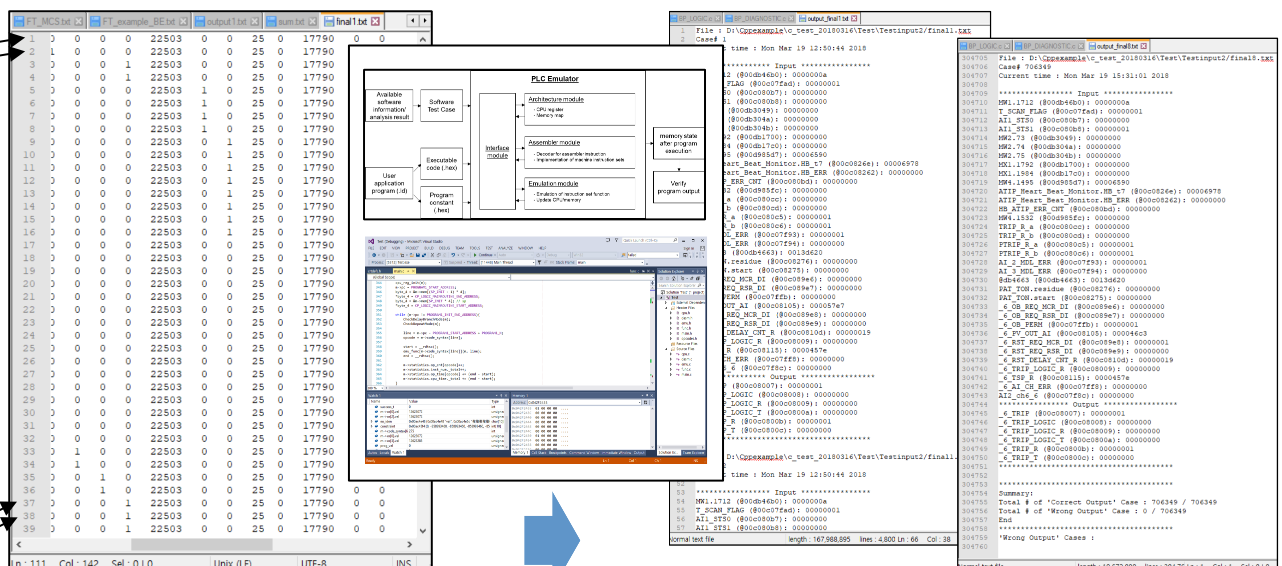
IDiPS-RPS BP Trip Logic SW - Test Result

- In previous section, we derived the number of test set to achieve 10^{-4}-10^{-6} SW pfd.
  - Number of test set to achieve SW pfd ~ 10^{-4} = 75,406 test sets
  - Number of test set to achieve SW pfd ~ 10^{-5} = 246,554 test sets
  - Number of test set to achieve SW pfd ~ 10^{-6} = 706,349 test sets

- By testing the test sets having high profile and confirming whether it generates correct SW out put, we can assure low SW PFD with minimum effort compared to previous studies:
  - 1) Functionality of the NPP safety SW can be proven without uncertainties compared to conventional bla ck-box which uses test cases randomly sampled from operational profile, and
  - 2) Software testing time per test case can be effectively reduced by using simulation-based test-bed.

가장 높은 probability부터 정리						
ID	folder	test case		Prob.	Fraction	SW failure prob.
1	16	22503	513	0.000153844	6.05E-02	9.39E-01
2	16	22503	2561	0.000153844	6.05E-02	8.79E-01
3	16	22503	16897	0.000153844	6.05E-02	8.18E-01
4	16	22503	18945	0.000153844	6.05E-02	7.58E-01
5	16	22503	33281	0.000153844	6.05E-02	6.97E-01
6	16	22503	35329	0.000153844	6.05E-02	6.37E-01
7	16	22503	49665	0.000153844	6.05E-02	5.76E-01
8	16	22503	51713	0.000153844	6.05E-02	5.16E-01
9	16	22503	66049	0.000153844	6.05E-02	4.55E-01
10	16	22503	68097	0.000153844	6.05E-02	3.95E-01
11	16	22503	82433	0.000153844	6.05E-02	3.34E-01
12	16	22503	84481	0.000153844	6.05E-02	2.74E-01
13	16	22503	98817	0.000153844	6.05E-02	2.13E-01
14	16	22503	100865	0.000153844	6.05E-02	1.52E-01
15	16	22503	115201	0.000153844	6.05E-02	9.20E-02
16	16	22503	117249	0.000153844	6.05E-02	3.14E-02
17	16	22503	131073	1.88396E-06	7.41E-04	3.07E-02
18	16	22503	133121	1.88396E-06	7.41E-04	2.99E-02
19	16	22503	147457	1.88396E-06	7.41E-04	2.92E-02
20	16	22503	149505	1.88396E-06	7.41E-04	2.85E-02
21	16	22503	163841	1.88396E-06	7.41E-04	2.77E-02
22	16	22503	165889	1.88396E-06	7.41E-04	2.70E-02
23	16	22503	180225	1.88396E-06	7.41E-04	2.62E-02
24	16	22503	182273	1.88396E-06	7.41E-04	2.55E-02
25	16	22503	196609	1.88396E-06	7.41E-04	2.48E-02
26	16	22503	198657	1.88396E-06	7.41E-04	2.40E-02
27	16	22503	212993	1.88396E-06	7.41E-04	2.33E-02
28	16	22503	215041	1.88396E-06	7.41E-04	2.25E-02
29	16	22503	229377	1.88396E-06	7.41E-04	2.18E-02
30	16	22503	231425	1.88396E-06	7.41E-04	2.10E-02
31	16	22503	245761	1.88396E-06	7.41E-04	2.03E-02
32	16	22503	247809	1.88396E-06	7.41E-04	1.96E-02
33	16	22503	4609	5.40344E-07	2.13E-04	1.94E-02
34	16	22503	6657	5.40344E-07	2.13E-04	1.91E-02
35	16	22503	8705	5.40344E-07	2.13E-04	1.89E-02
36	16	22503	10753	5.40344E-07	2.13E-04	1.87E-02
37	16	22503	20993	5.40344E-07	2.13E-04	1.85E-02
38	16	22503	23041	5.40344E-07	2.13E-04	1.83E-02

Explicit profile of SW test set (sorted by highest prob. to lowest prob.)



Format of SW test set (input to emulator)

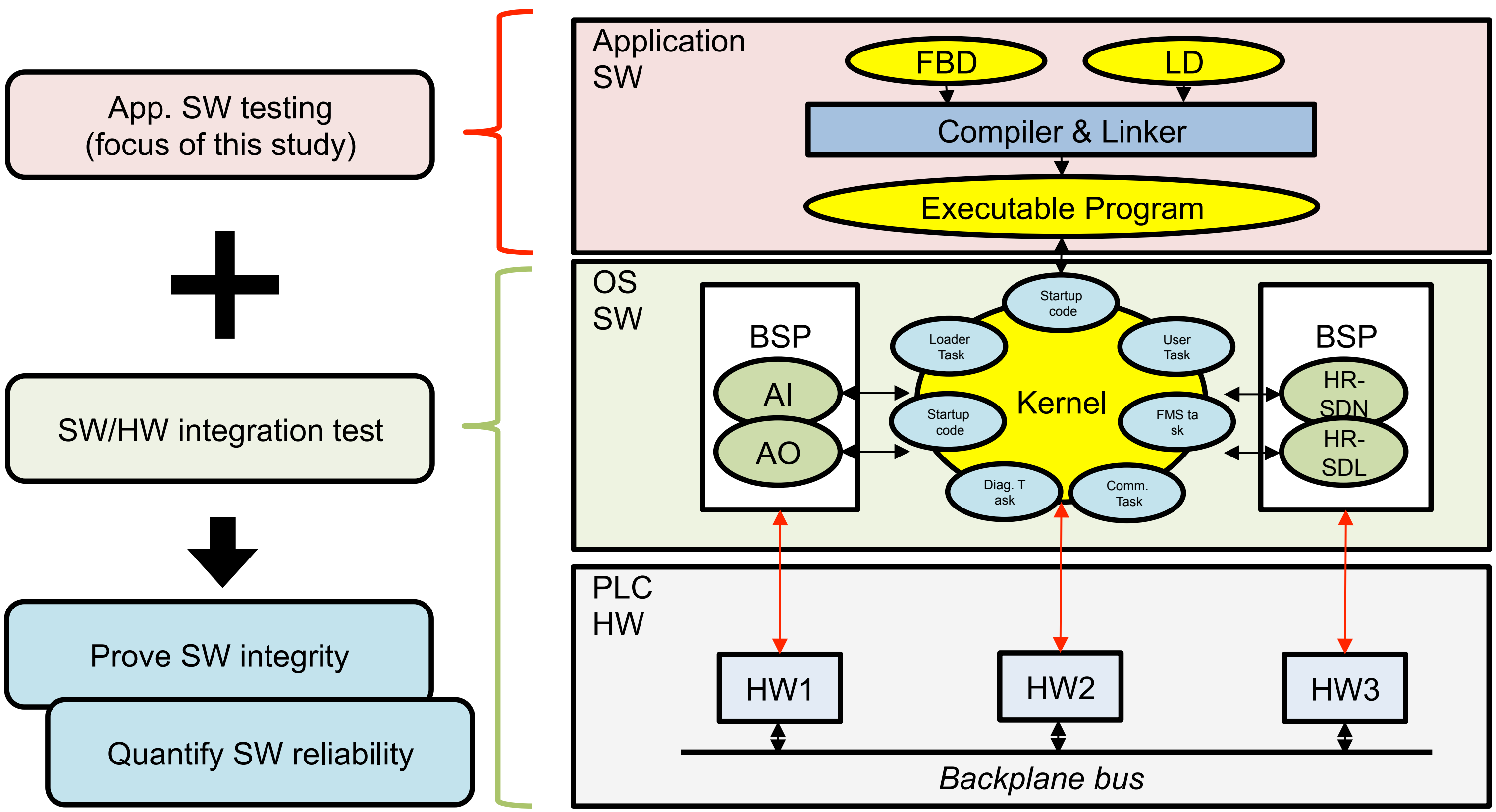
Run SW test set

Output of emulator for given SW test set (706,349 test sets; all correct output)

Conclusion & Future Works

- In this study, a software test framework for a QSRM of NPP SW utilizing simulation-based software test-bed with operational-profile-based test cases was proposed.

- The test results for application software of NPP safety-critical system combined with the SW/HW integration test result can be used for software reliability quantification.



Hierarchy structure of SW/HW components of typical PLC used in NPP

Acknowledgement

- This work was supported by the project of 'Evaluation of human error probabilities and safety software reliabilities in digital environment (L16S092000),' which was funded by the Central Research Institute (CRI) of the Korea Hydro and Nuclear Power (KHNP) company.

Thank you for your attention

Q&A