2008 대한임베디드공학회 추계학술대회

원자력발전소 디지털 제어기기를 위한 정형기법 기반의 소프트웨어 개발 방법론

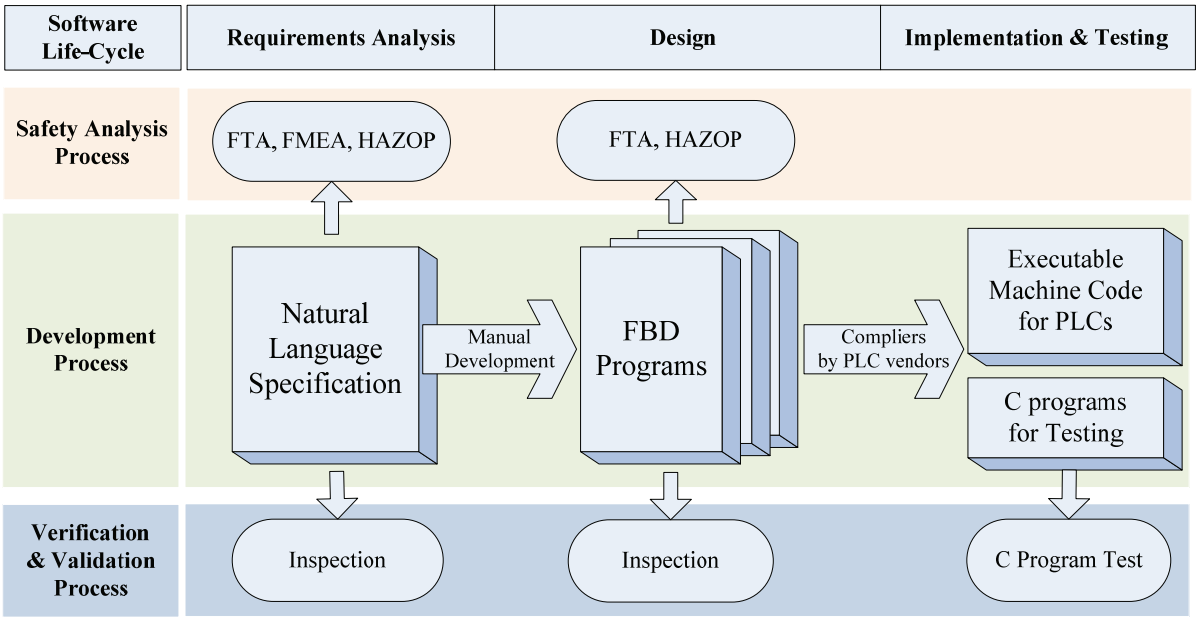
A Formal Methods based Software Development Methods for Digital Controllers in Nuclear Power Plants

유 준 범
건국대학교 컴퓨터공학부

Abstract: Software safety is an important issue for real-time embedded control systems such as PLCs (Programmable Logic Controllers) in nuclear power plants. Use of formal method to formally specify and verify software is strongly recommended by the most safety experts and government authorities. This paper introduces our experience in developing KNICS consortium's RPS (Reactor Protection System) software with support of formal methods in comparison with existing development methods.

Keywords: Software development method, formal methods, PLC, RPS, nuclear power plant'

1. 원자력발전소 원자로보호시스템 개발 프로세스 (월성, 울진 원자력발전소)



PLC (by POSCON)

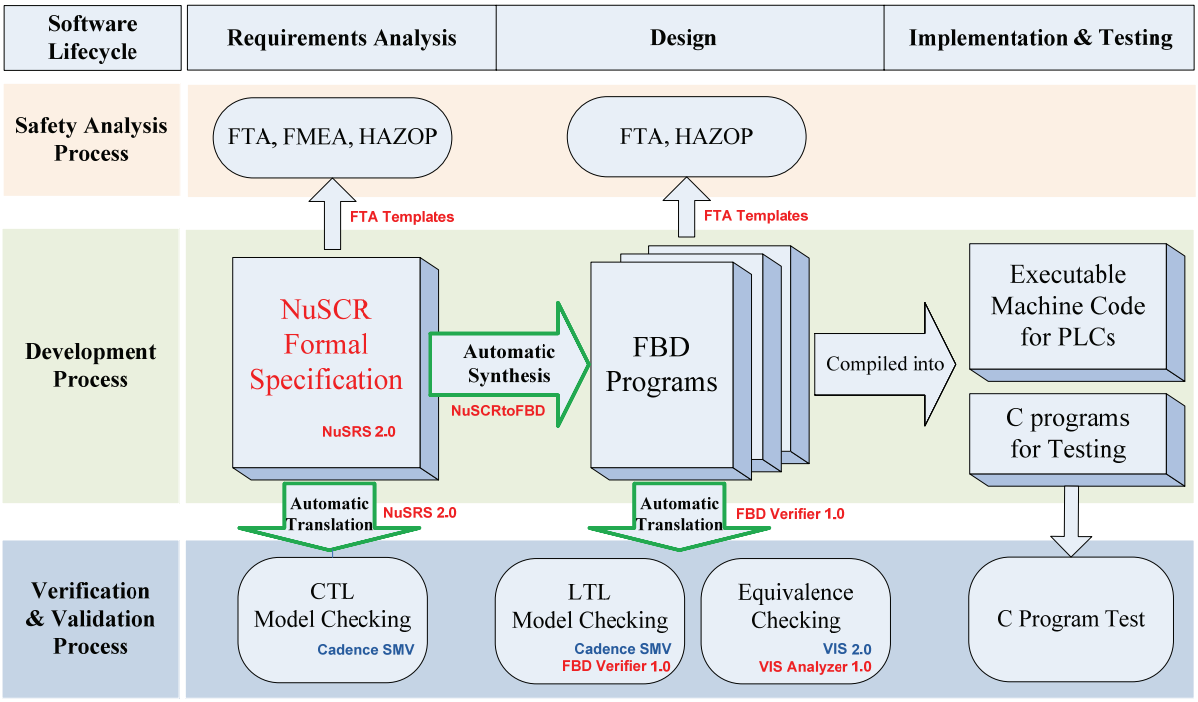
a. **3 Parallel Processes가 독립적으로 진행됨**
   - ① **Development process**
   - ② **Verification & Validation process**
   - ③ **Safety Analysis process**

b. **Development process**
   - ① 자연어 요구사항 명세서
   - ② FBD 프로그래밍 [1] (수동)
   - ③ 임시로 생성된 C 프로그램을 이용한 테스트

c. **Verification & Validation process**
   - ① Document inspection
   - ② FBD code inspection

d. **Safety Analysis process**
   - ① FTA (Fault Tree Analysis)
   - ② FMEA (Failure Mode and Effect Analysis)
   - ③ HAZOP (Hazard and Operability)
   - ④ 수동으로 수행됨.

2. 정형기법 기반의 개발 프로세스 (APR-1400 신형 원자로)



a. 정형기법을 사용하여 소프트웨어의 Safety [2]를 증진함.

① **Formal Specification (정형명세)**

② **Formal Verification (정형검증)**

b. Development process

① NuSCR 정형명세 기법 사용 [3]

② NuSRS 2.0 : NuSCR 정형명세 지원 도구

③ NuSCRtoFBD 1.0 : NuSCR 정형명세를 FBD 프로그램으로 자동 변환하는 도구 [4]

c. Verification & Validation process

① SMV Model Checking (CTL) for NuSCR 명세 [5]

② NuSRS 2.0 : NuSCR 명세로부터 SMV input program을 자동 생성 [6]

③ FBD 프로그램을 위한 SMV Model Checking 및 VIS Equivalence Checking 기능

④ FBD Verifier 1.0 : FBD 프로그램을 Verilog 로 변환

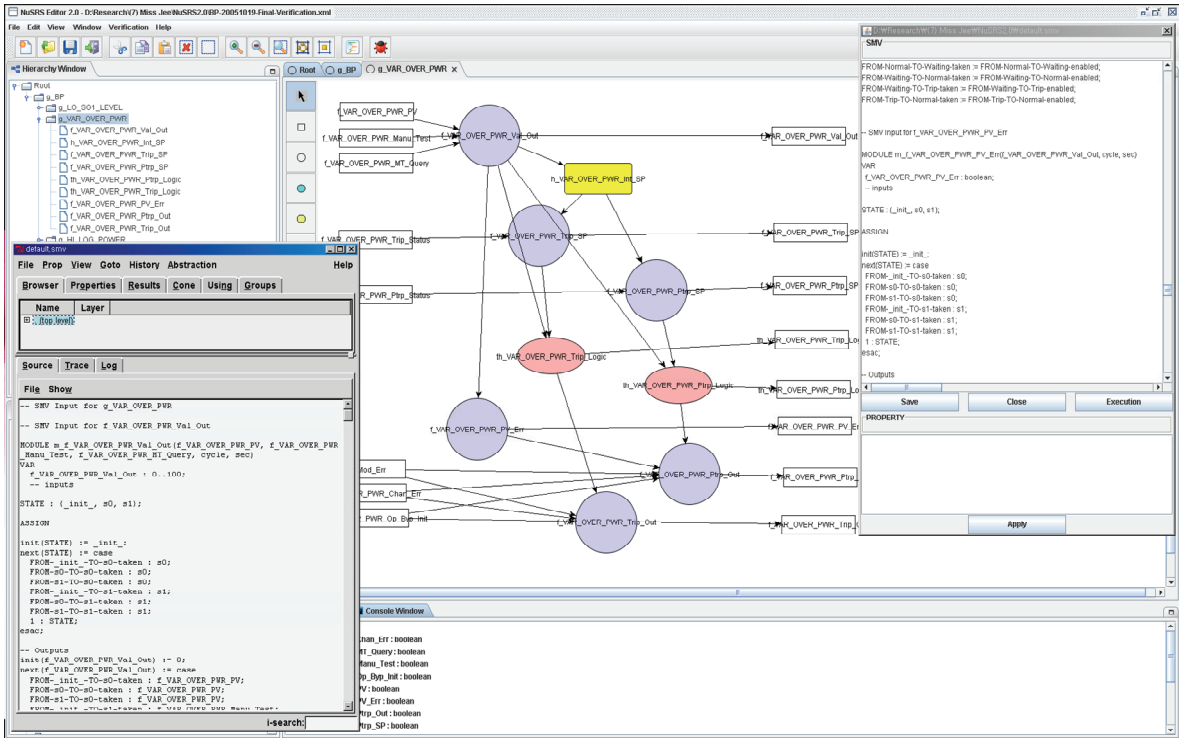
⑤ VIS Analyzer 1.0 : VIS 검증 결과를 분석하고 Visualization 제공 [7]

d. Safety Analysis process

① FTA templates for NuSCR 제공 [9]

② FTA templates for FBD program 제공 [8]

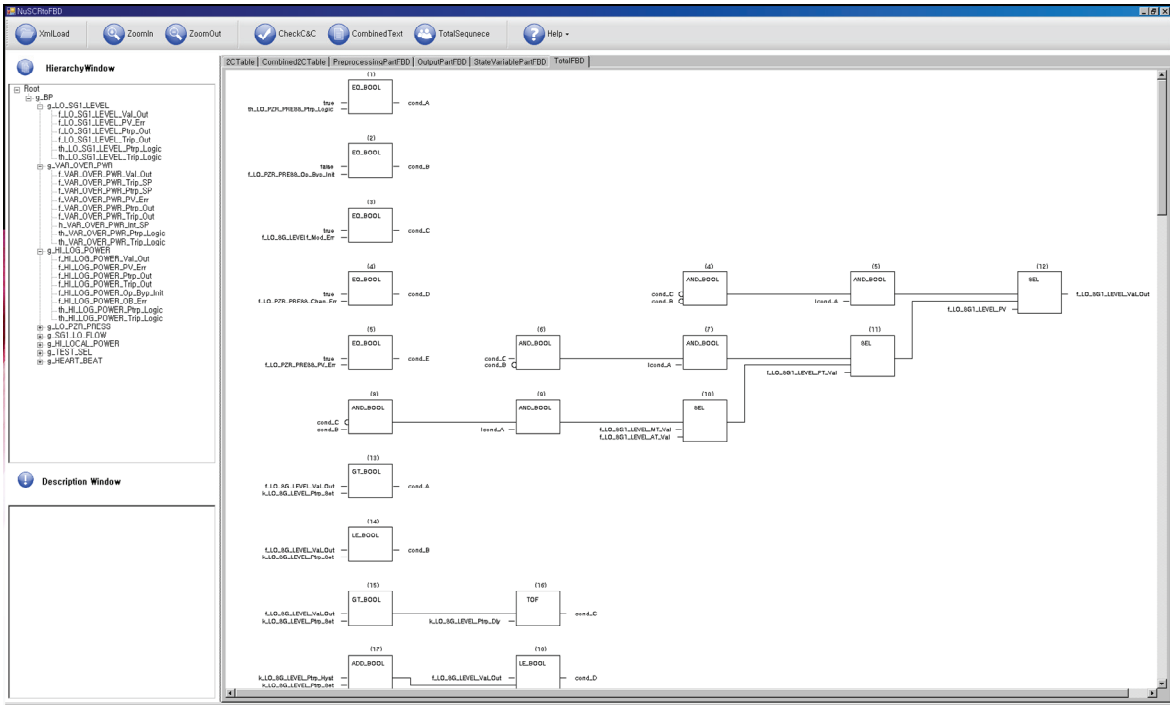
3. Development Process



NuSRS 2.0

1. Read XML format file for NuSCR specification

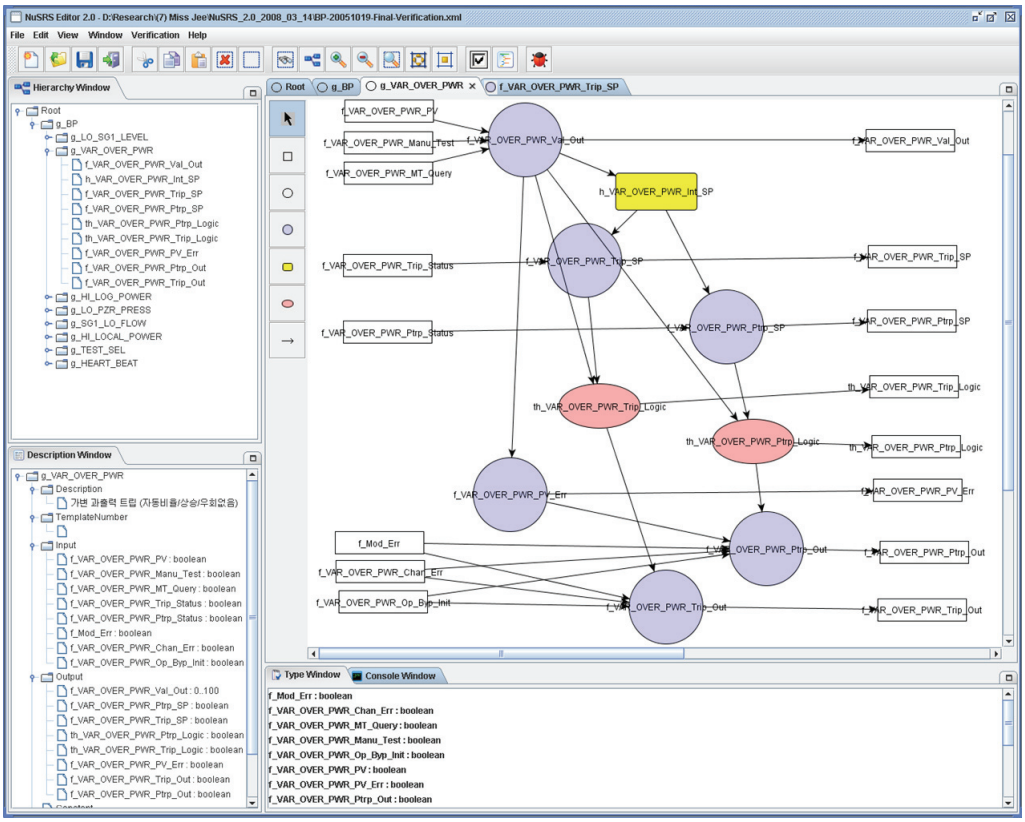
2. Synthesize FBD programs automatically

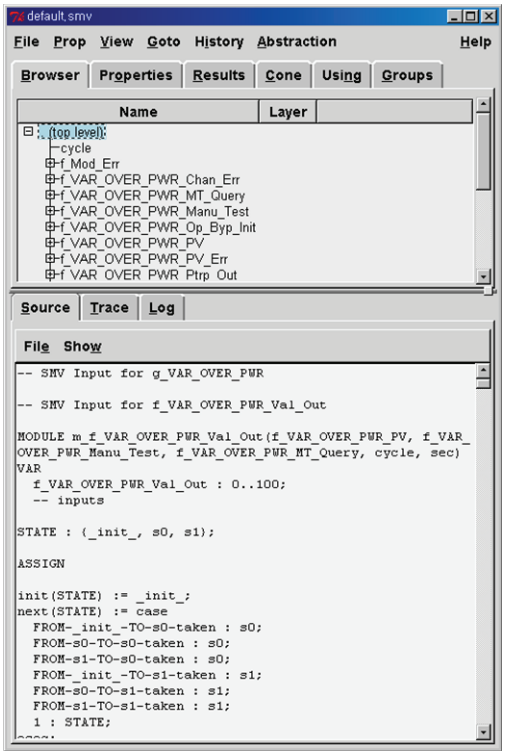


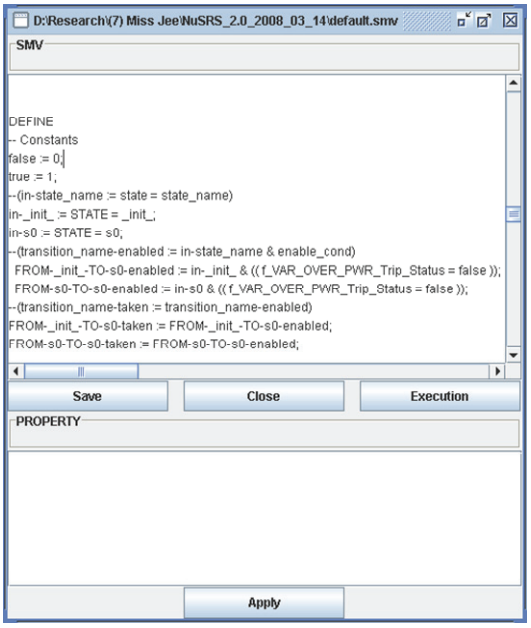
NuSCRtoFBD 1.0

4. Verification & Validation Process

4.1 SMV Model Checking for NuSCR Specification (CTL)



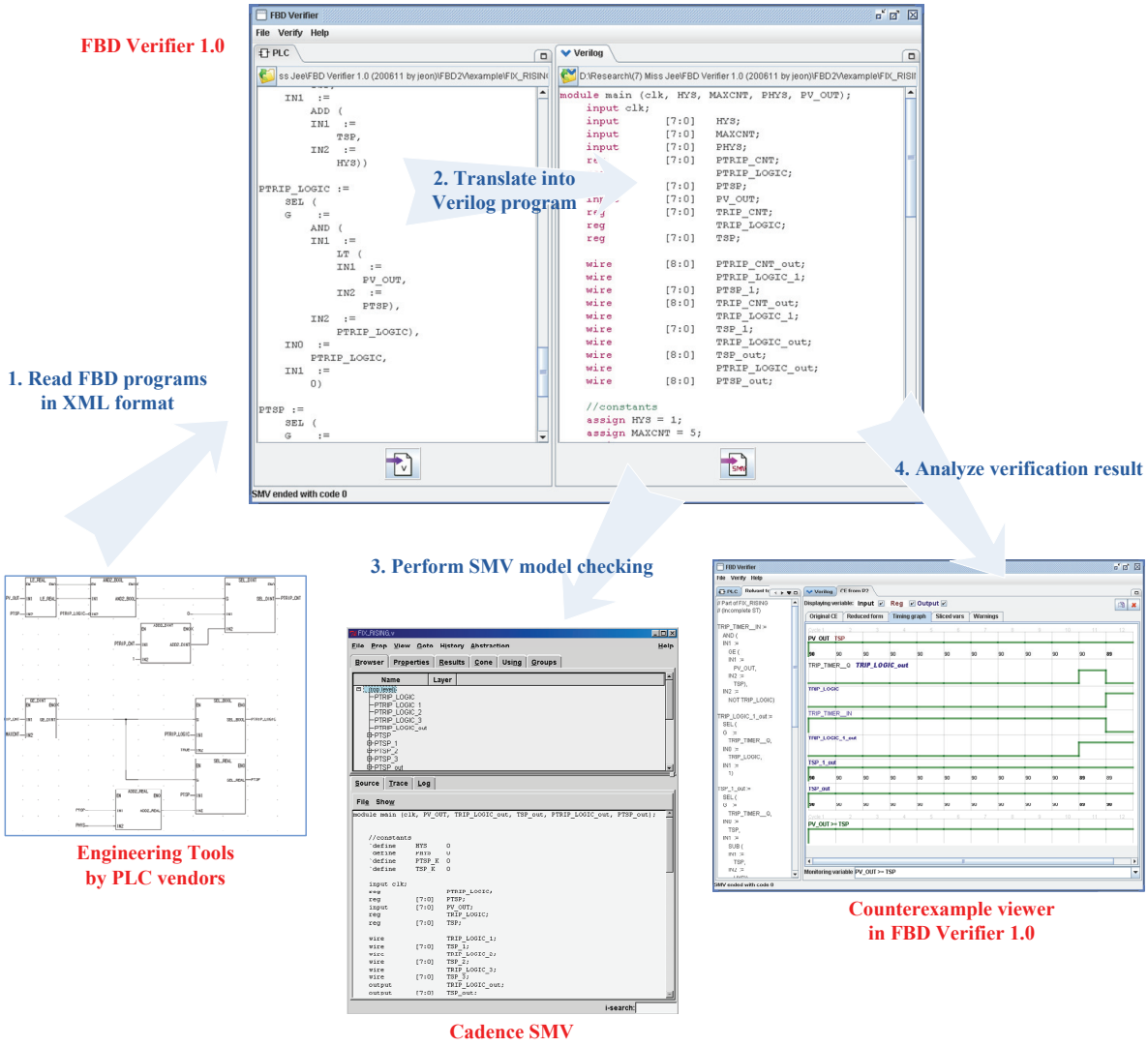




Cadence SMV Model Checker

4. Verification & Validation Process

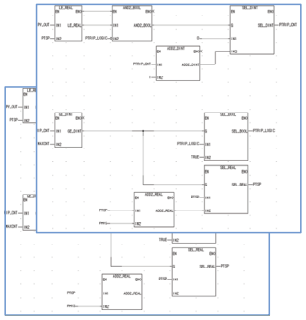
4.2 SMV Model Checking for FBD Programs (LTL)



4. Verification & Validation Process

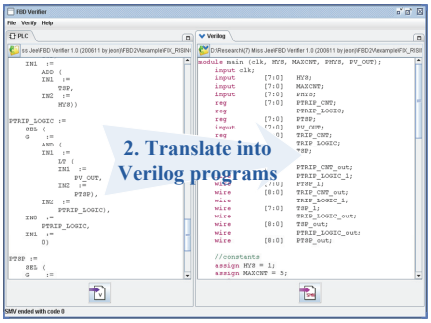
4.3 VIS Equivalence Checking for FBD Programs

Engineering Tools
by PLC vendors



1. Read two FBD programs
in XML format

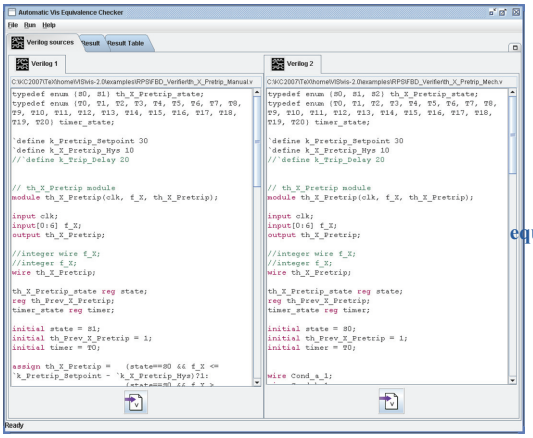
FBD Verifier 1.0



2. Translate into
Verilog programs

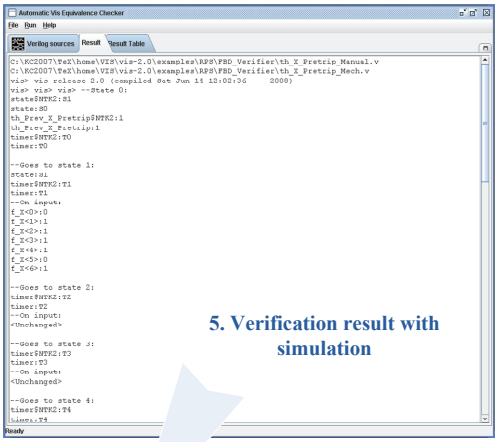
3. Read two Verilog programs

VIS Analyzer 1.0 (Source)



4. Perform VIS
equivalence checking

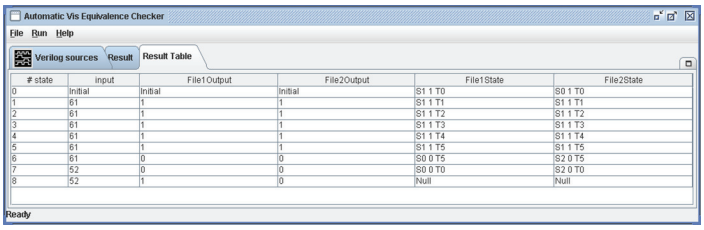
VIS Analyzer 1.0 (Result)



5. Verification result with
simulation

6. Complete traces

VIS Analyzer 1.0 (Result Table)



Automatic Vis Equivalence Checker

File Run Help

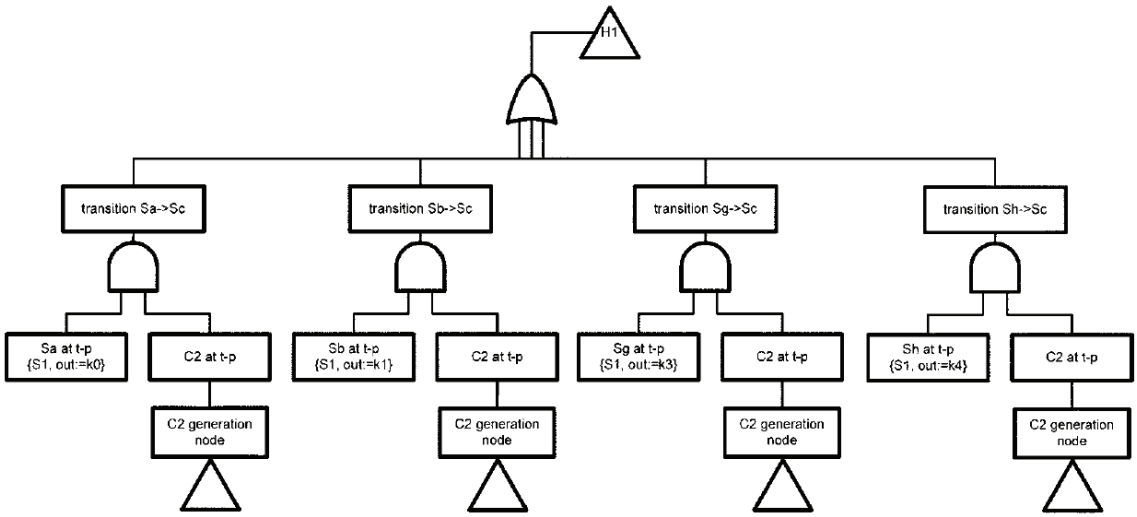
Verilog sources | Result | Result Table

# state	input	File1 Output	File2 Output	File1 State	File2 State
0	Initial	Initial	Initial	S1 1 T0	S0 1 T0
1	61	1	1	S1 1 T1	S1 1 T1
2	61	1	1	S1 1 T2	S1 1 T2
3	61	1	1	S1 1 T3	S1 1 T3
4	61	1	1	S1 1 T4	S1 1 T4
5	61	1	1	S1 1 T5	S1 1 T5
6	61	0	0	S0 0 T5	S2 0 T5
7	52	0	0	S0 0 T0	S2 0 T0
8	52	1	0	Null	Null

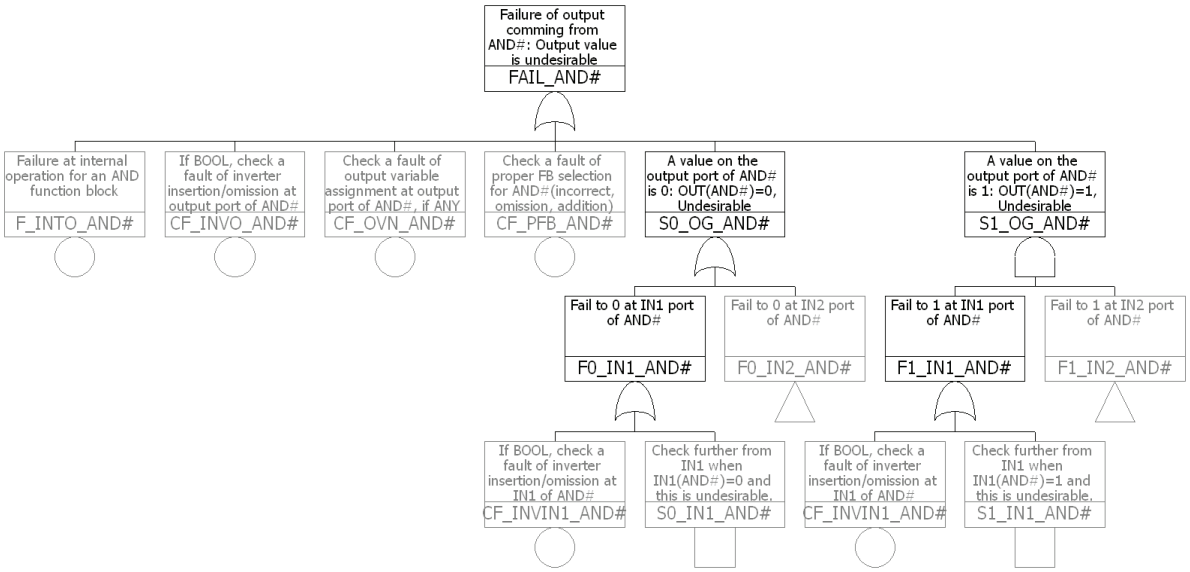
Ready

5. Safety Analysis Process

5.1 Templates for FTA of NuSCR Formal Specification



5.2 Templates for FTA of FBD Programs

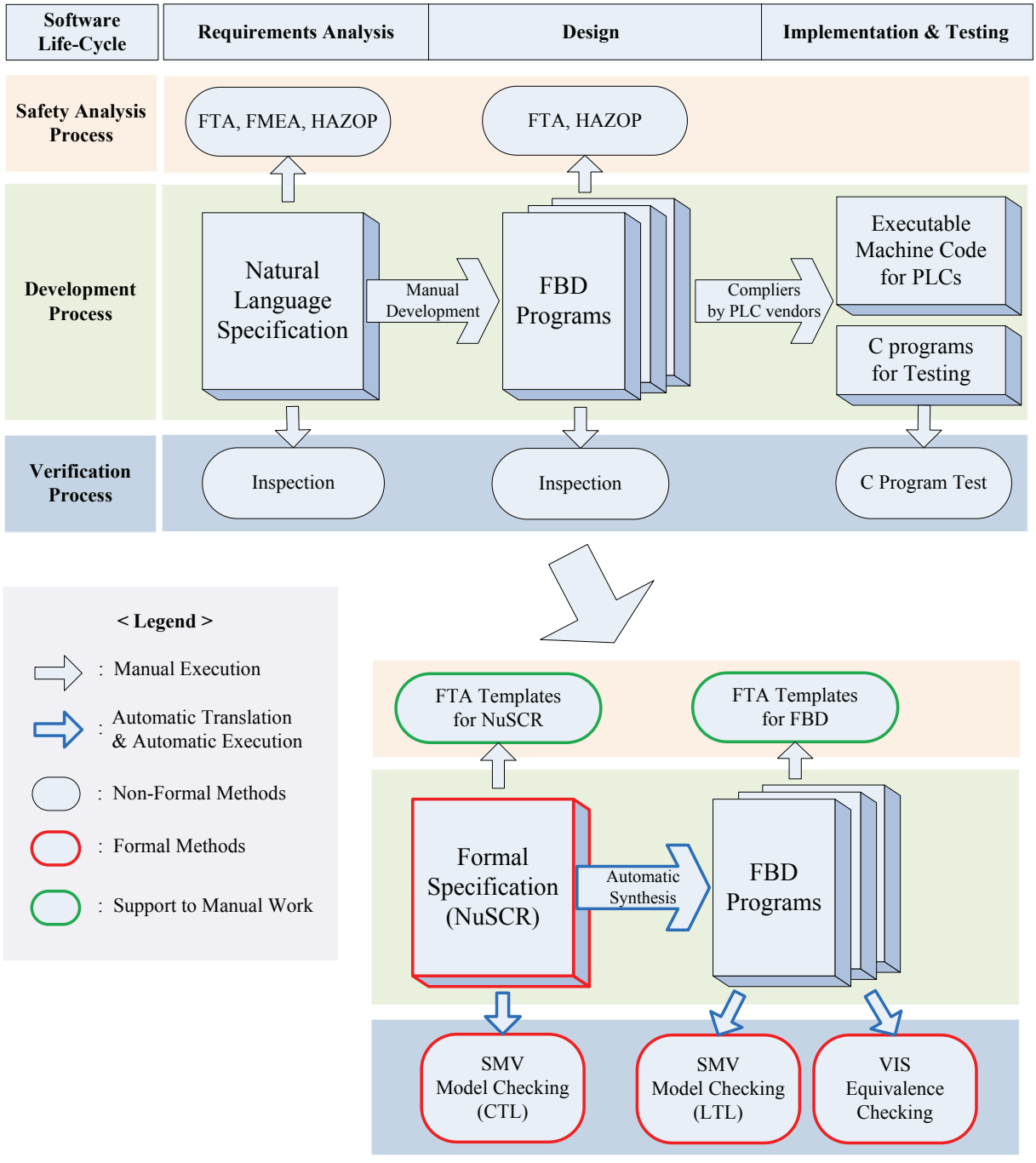


6. Summary

정형기법 기반의 원자력발전소 제어시스템 소프트웨어 개발 방법론

→ 정형기법을 사용하여 소프트웨어의 안전성을 증진

→ 전체 Software Lifecycle 에 대한 체계적인 방법론을 제안



References

[1] IEC (International Electrotechnical Commission). International standard for programmable controllers: Programming languages, part 3, 1993.

[2] N.G. Leveson. SAFEWARE, System Safety and Computers. Addison Wesley, 1995.

[3] Junbeom Yoo, Taihyo Kim, Sungdeok Cha, Jang-Su Lee, Han Seong Son, "A Formal Software Requirements Specification Method for Digital Nuclear Plants Protection Systems," Journal of Systems and Software, Vol.74, No.1, pp73-83, 2005.

[4] Junbeom Yoo, Sungdeok Cha, Chang Hwoi Kim, Duck Yong Song, "Synthesis of FBD-based PLC Design from NuSCR Formal Specification," Reliability Engineering and System Safety, Vol.87, No.2, pp287-294, 2005.

[5] Jaemyung Cho, Junbeom Yoo, Sungdeok Cha, "NuEditor – A Tool Suite for Specification and Verification of NuSCR," In proceeding of Second ACIS International Conference on Software Engineering Research, Management and Applications(SERA2004), pp298-304, LA, USA, May5-7, 2004.

[6] Junbeom Yoo, Sungdeok Cha, and Eunkyoung Jee, "A Verification Framework for FBD based Software in Nuclear Power Plants," In the proceeding of 15th Asia Pacific Software Engineering Conference(APSEC), Beijing, China, Dec. 3~5, 2008.

[7] Junbeom Yoo, Sungdeok Cha, and Eunkyoung Jee, "Verification of PLC Programs written in FBD with VIS," Nuclear Engineering and Technology,Accepted.

[8] Younju Oh, Junbeom Yoo, Sungdeok Cha, Han Seong Son, "Software Safety Analysis of Function Block Diagrams using Fault Trees," Reliability Engineering and System Safety, Vol.88, No.3, pp215-228, 2005.

[9] Taeho Kim, Junbeom Yoo, Sungdeok Cha, "A Synthesis Method of Software Fault Tree from NuSCR Formal Specification using Templates," Journal of Korea Institute of Information Scientists and Engineers, SE Vol.32, No.12, 2005.