원자력발전소용 FPGA 기반 디지털 I&C 시스템 개발에 사용된 COTS 소프트웨어의 안전 카테고리 분류

- Safety Category Classification of COTS software for developing Digital I&C System of Nuclear Power Plants

Sejin Jung, Eui-Sub Kim, Junbeom Yoo, and Jong-Gyun Choi, JangYeol Kim

Dependable Software Laboratory

KONKUK University

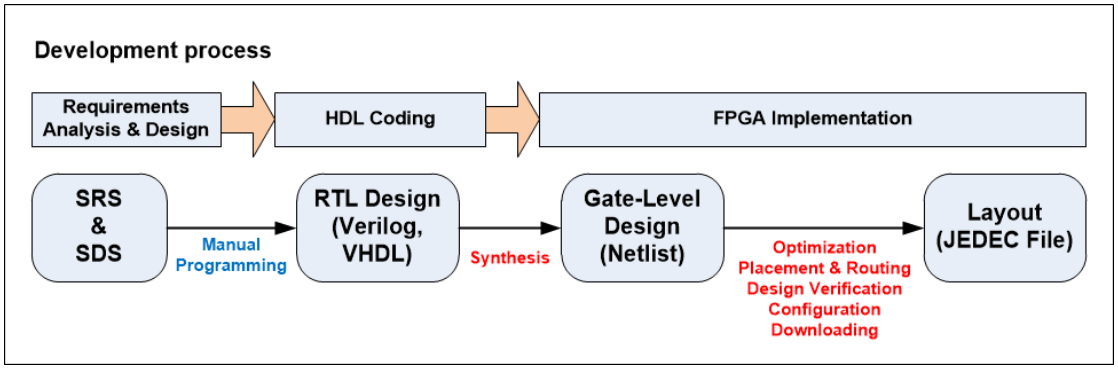
Korea Atomic Energy Research Institute

2015.06.26

Contents

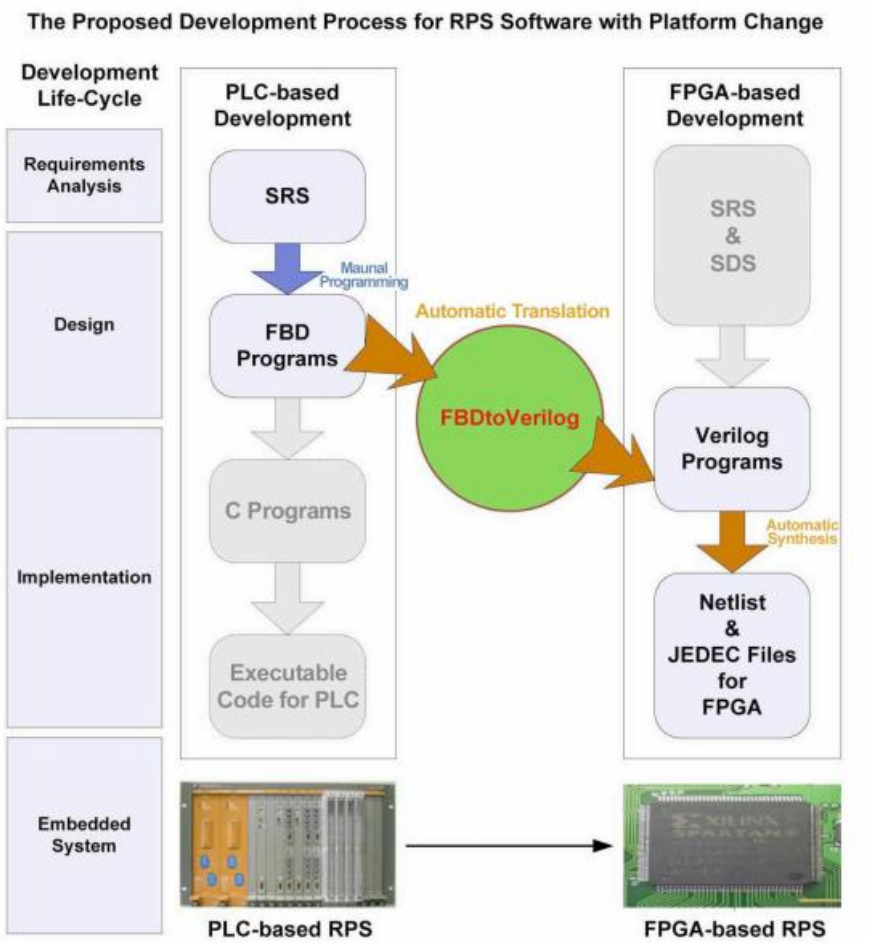
Introduction

- PLC(Programmable Logic Controller) has been used to implement I&Cs for decades
  - SW development on industrial computers (CPU & OS)
- Increasing maintenance cost about old nuclear plants
  - Request for alternative implementation platforms
- FPGA(Field Programmable Gate Array) is an alternative platform of PLC for I&Cs
  - Higher computation performance and stronger security
  - HW development
- Development of FPGA needs several software different from PLC
  - Like logic synthesis, P&R tools



Introduction

- The proposed development process with platform change



COTS(Commercial Off-The-Shelf) SW Dedication

- **Acceptance process**
  - Providing reasonable assurance that a CGI to be used as a basic component
  - Demonstrating correctness and safety of commercial software

- Standard guidelines for dedication
  - NUREG/CR-6421
  - NP-5652
  - TR-106439 based on NP-5652

Standards	Target	Process	Note
EPRI-NP5652 (EPRI TR-106439)	Commercial Grade Item (CGI) + Software-based equipments	Method 1 ~ 4	Focusing on Direct CGI
NUREG/CR-6421	Direct / Indirect COTS software	Processes for each safety category	Containing Indirect CGI

NUREG/CR-6421

- **NUREG/CR-6421** is proposed acceptance process for commercial off-the-shelf software in reactor applications by NRC

- It is based on several standards about nuclear power plants systems
  - Quality Assurance
  - Validation & Verification
  - Etc

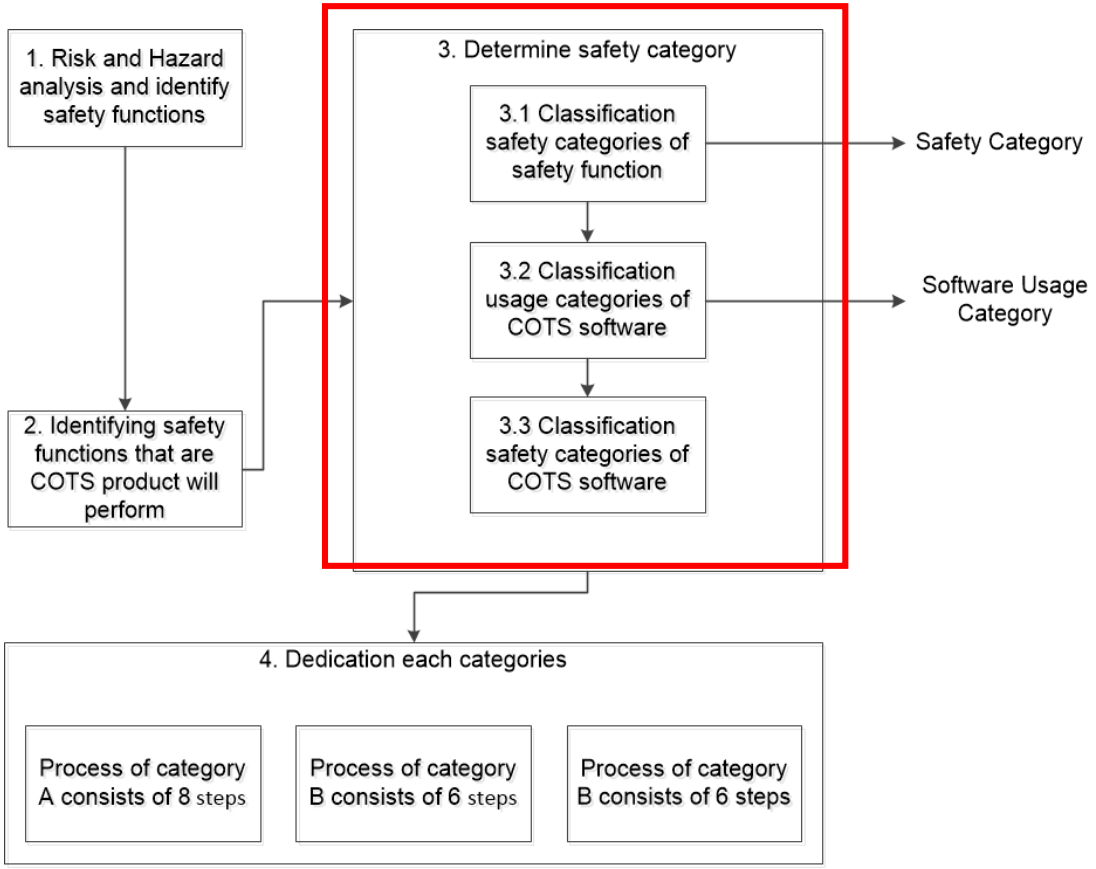
- Processes for each **safety category** which are used in IEC 1226
  - Applying **different criteria** accordance with safety categories

IEC 1226 Safety Category	Examples
A	원자로 보호 계통 시스템(RPS) / ESFAS 등
B	발전소 자동 제어 시스템 / 연료 재충전 시스템 등
C	알람 / 모니터링 시스템 등

  - (+unclassified)

Dedication Process in NUREG/CR-6421

- Dedication Process



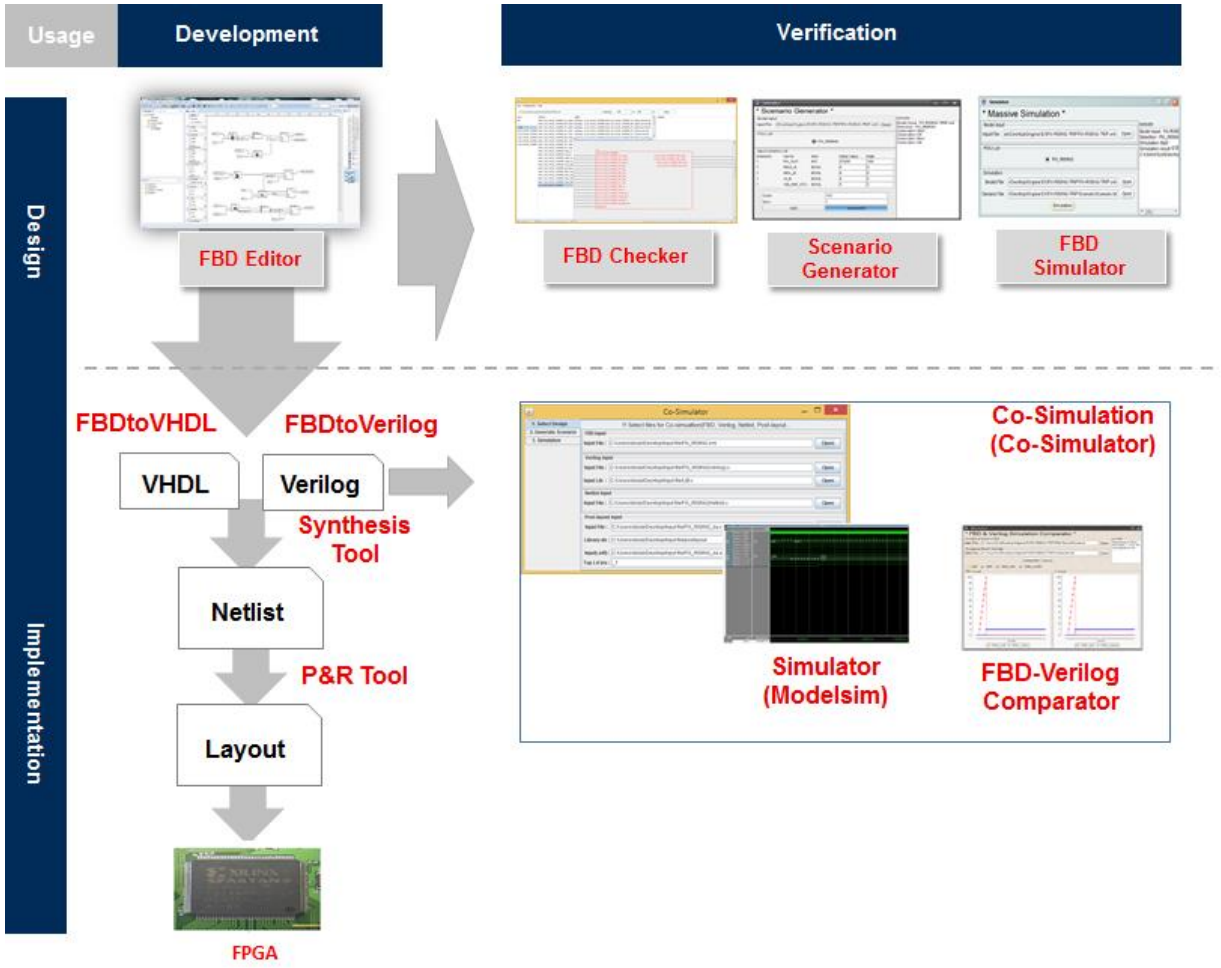
Usage Category & Safety Category

- **Based on usage of software**
  - Safety category is decided to use usage category and safety category of safety function
  - Especially, indirect software is decided to target module and possibility of verification

Usage Category	Description	IEC 1226 Category
Direct	Directly used in an A,B,C application	A, B, C
Indirect	Directly produces executable modules which are used in an A,B,C applications (e.g. compilers, linkers)	A, B, C, unclassified
Support	CASE systems, or support systems that indirectly assist in the production of A,B,C applications	unclassified
Unrelated	Software which has no impact	unclassified

Target Software

- **FPGA development process**
  - Changing in the hardware platform from PLC to FPGA before
  - Developing tools and using several commercial software also

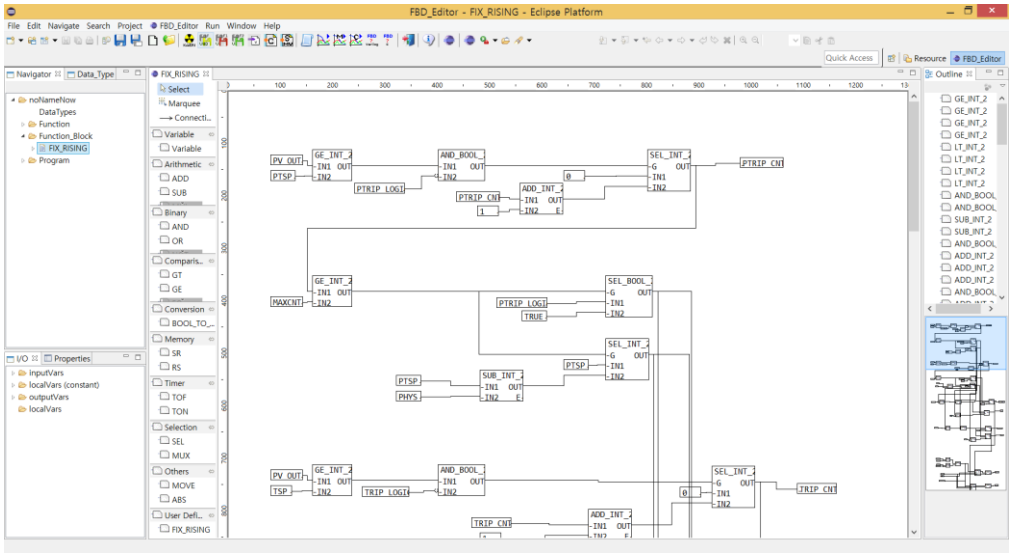


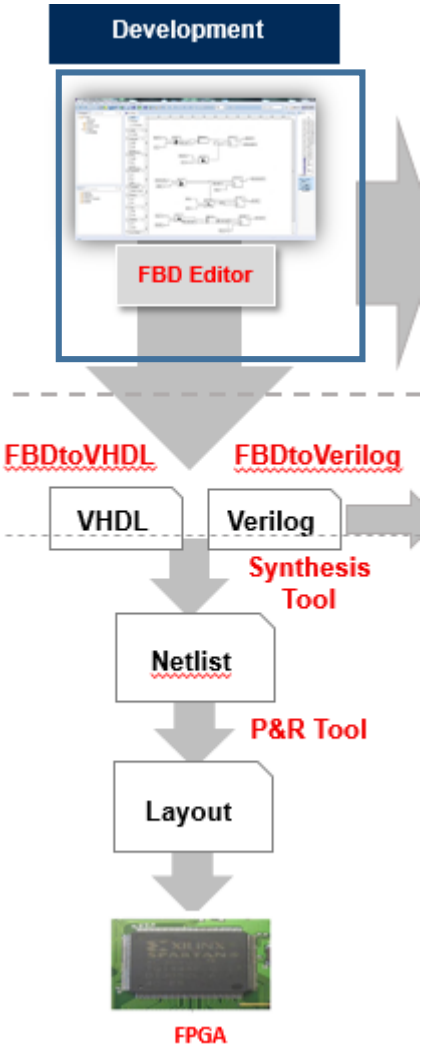
Usage Category of Target Software

- **Development Software**
  - FBD Editor

- FBD Editor supports to design FBD

  - Possible to classify usage category of **support**



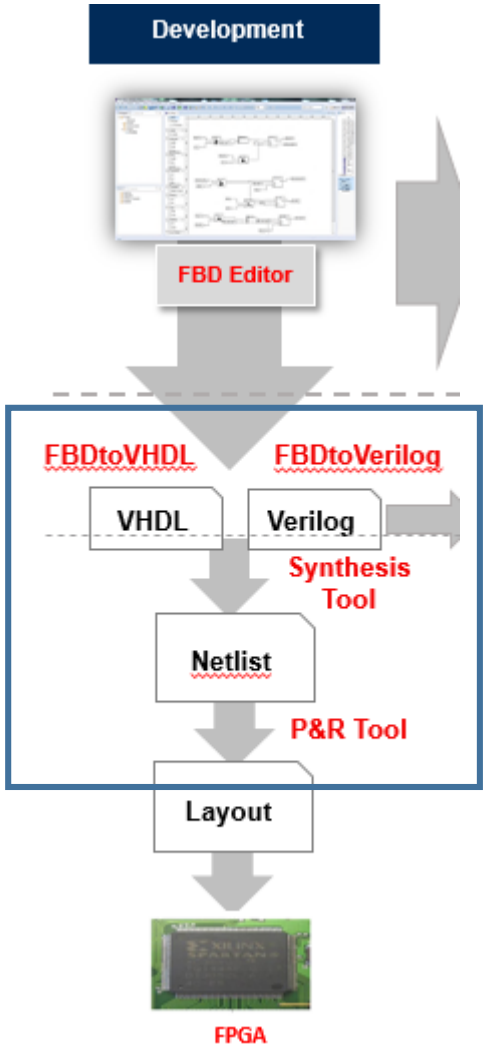


Usage Category of Target Software

- **Development Software**
  - FBDtoVerilog
  - FBDtoVHDL
  - Synthesis Tool
  - P&R Tool

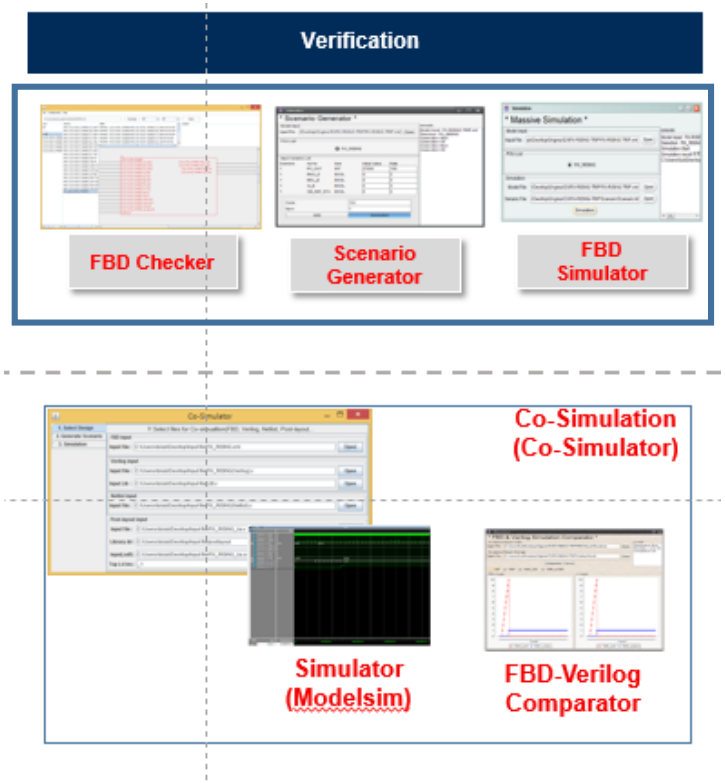
- Tools are translated, synthesis
  - They have an effect on design
  - Producing modules which are used in applications

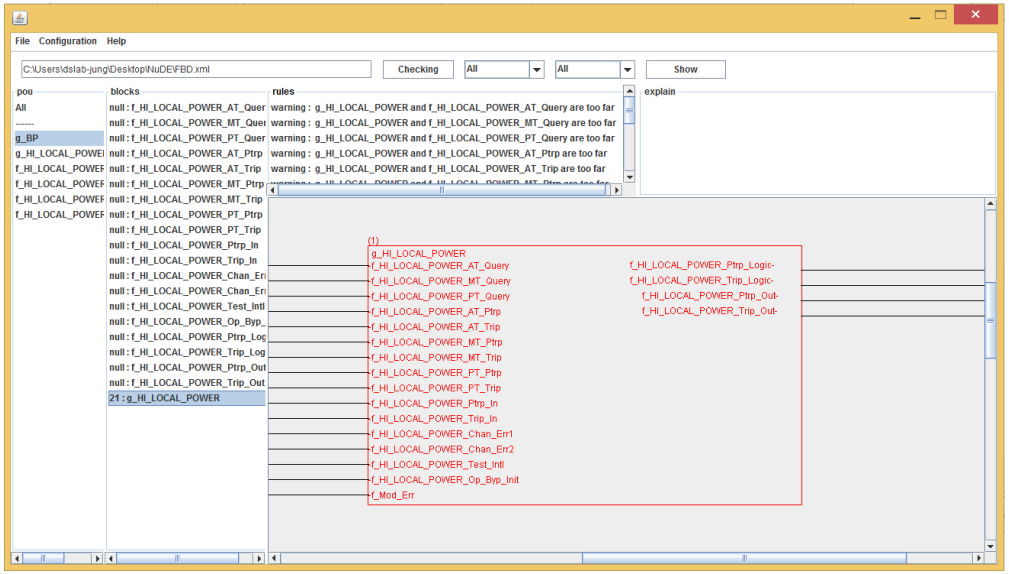
  - Possible to classify usage category of **indirect**



Usage Category of Target Software

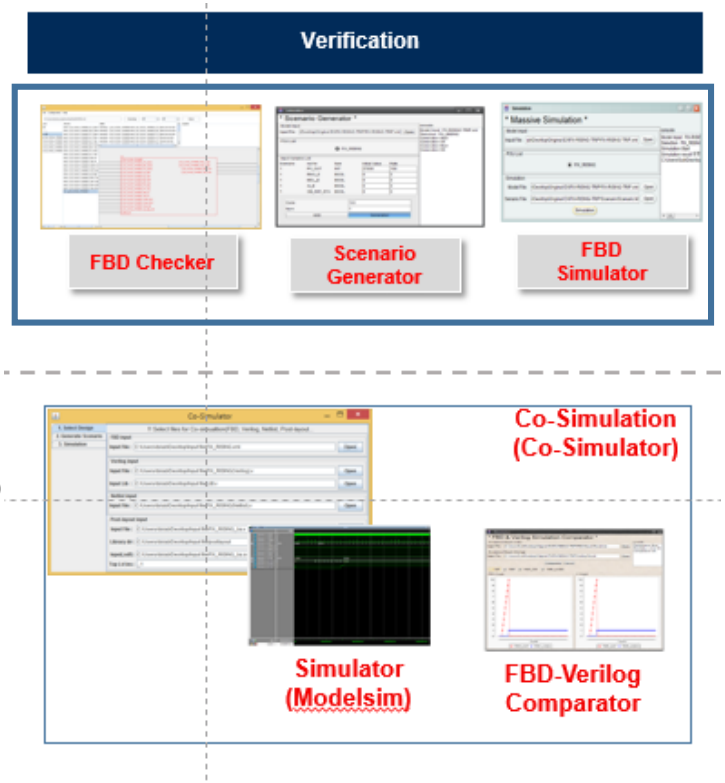
- **Verification Software**
  - FBD
    - FBD Checker
    - Scenario Generator
    - FBD Simulator
  - FBD Checker
    - FBD Rule Checking
    - based on NUREG/CR-6463

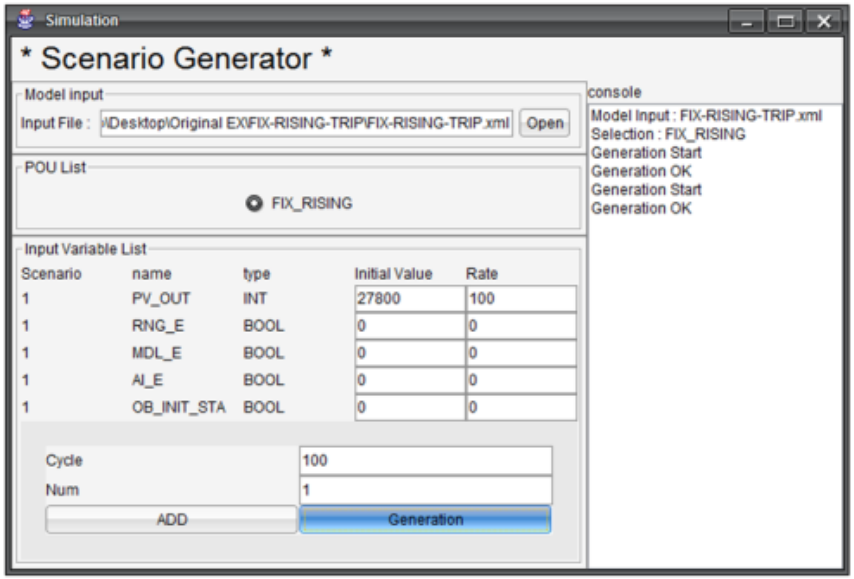




Usage Category of Target Software

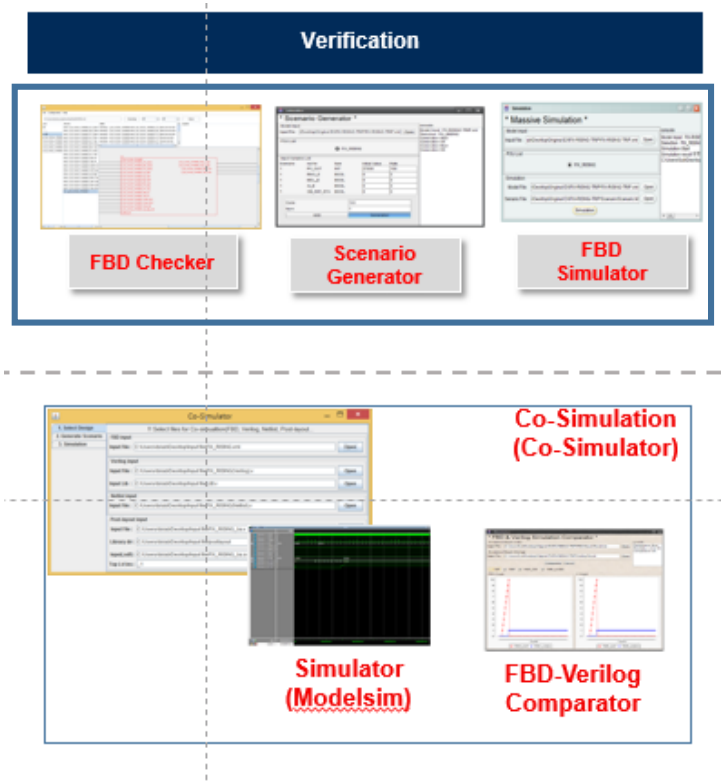
- **Verification Software**
  - FBD
    - FBD Checker
    - Scenario Generator
    - FBD Simulator
  - Scenario Generator
    - Generating scenario for simulation using FBD





Usage Category of Target Software

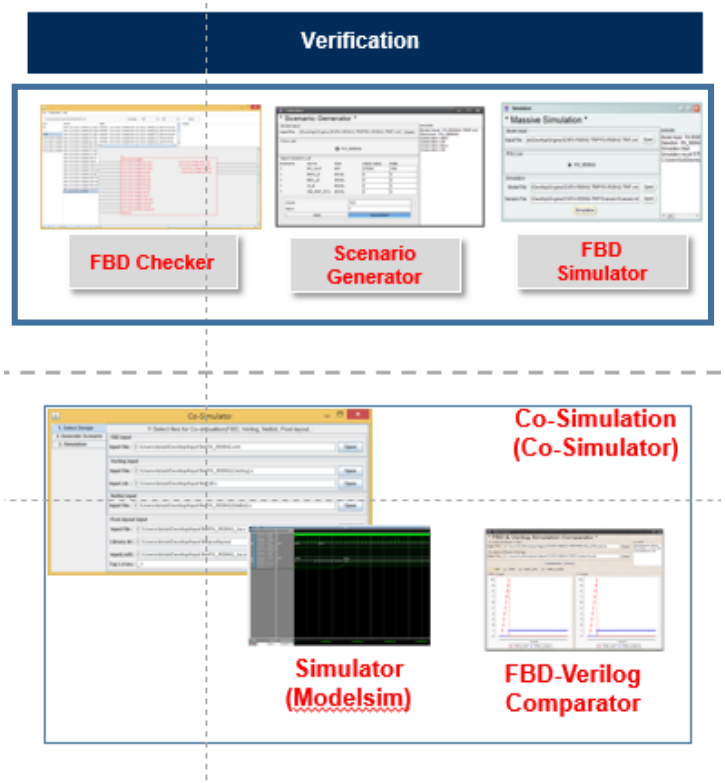
- **Verification Software**
  - FBD
    - FBD Checker
    - Scenario Generator
    - FBD Simulator
  - FBD Simulator
    - Simulation FBD using scenario



Usage Category of Target Software

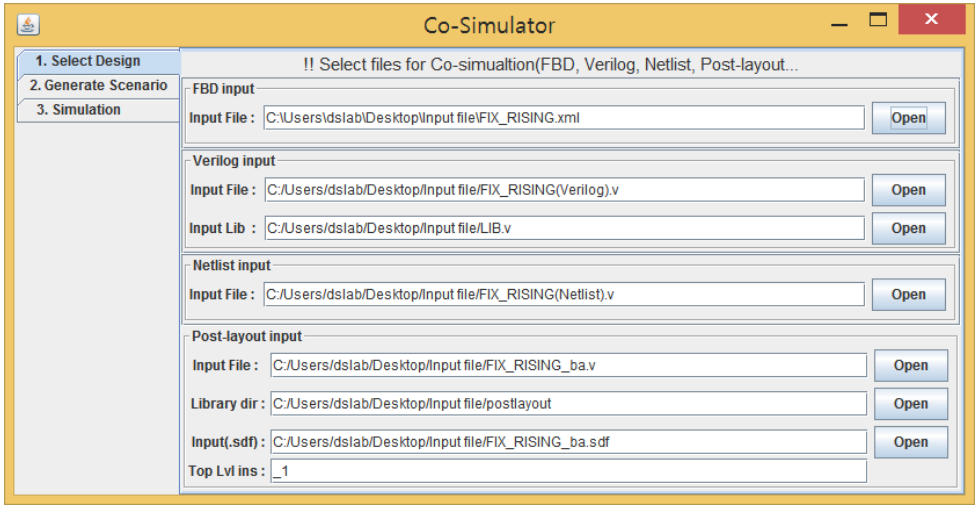
- **Verification Software**
  - FBD
    - FBD Checker
    - Scenario Generator
    - FBD Simulator

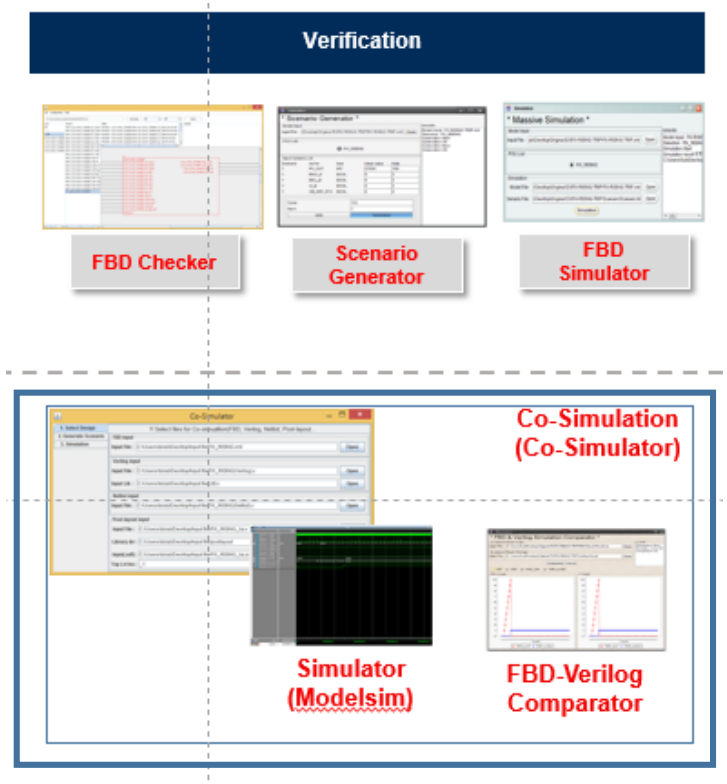
  - Verification software for FBD is classified as unrelated category



Usage Category of Target Software

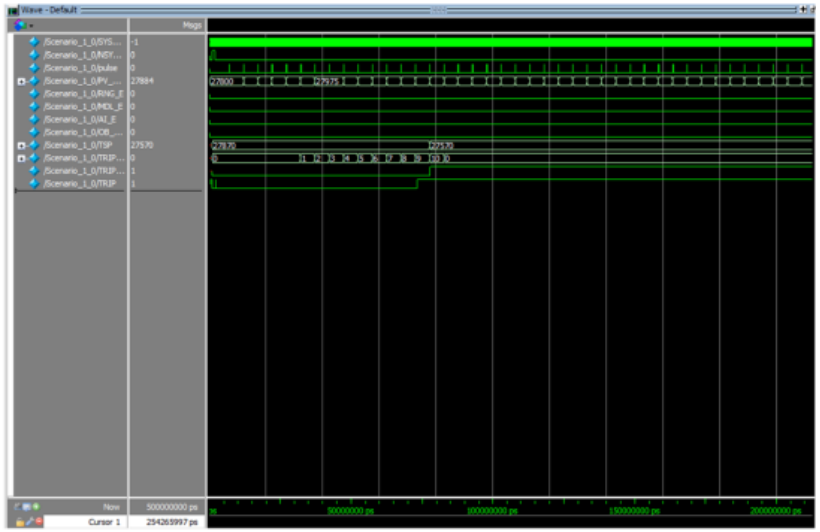
- **Verification Software**
  - Verilog
    - Co-Simulator (Contains VHDL)
    - Modelsim
    - FBD-Verilog Comparator
  - Co-Simulator
    - Providing Simulation environment
      - Verilog, VHDL

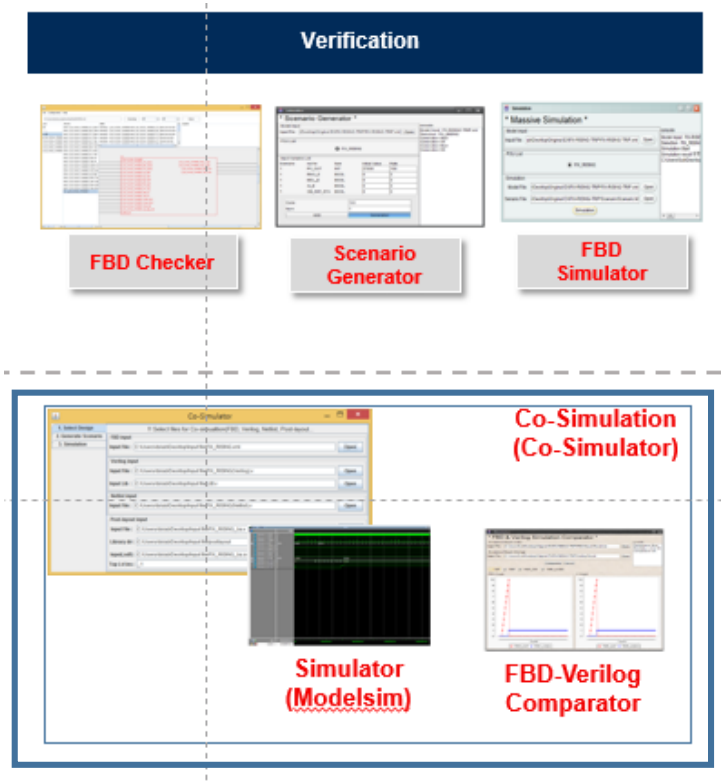




Usage Category of Target Software

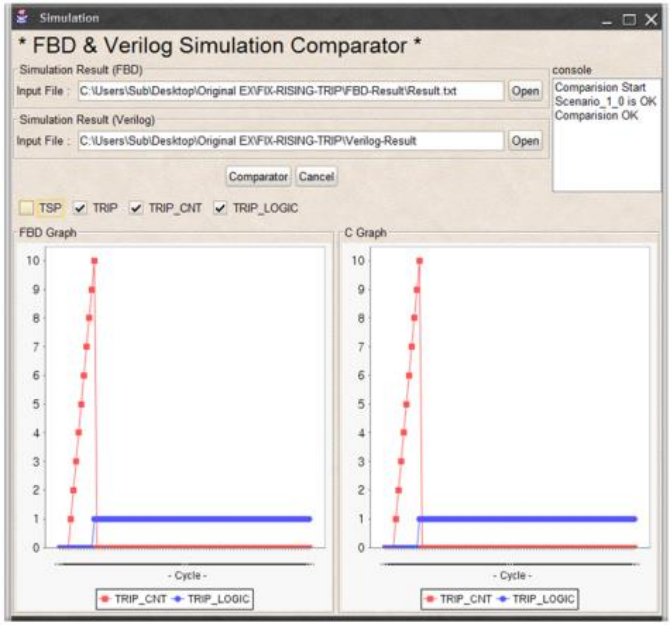
- **Verification Software**
  - Verilog
    - Co-Simulator (Contains VHDL)
    - Modelsim
    - FBD-Verilog Comparator
  - Simulator (Modelsim)
    - Simulation Verilog, VHDL

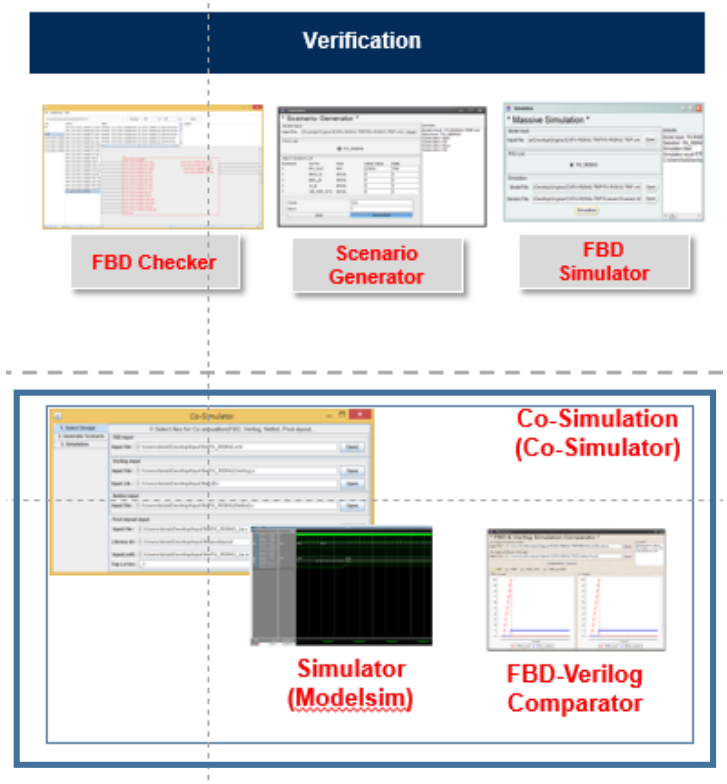




Usage Category of Target Software

- **Verification Software**
  - Verilog
    - Co-Simulator (Contains VHDL)
    - Modelsim
    - FBD-Verilog Comparator
  - FBD-Verilog Comparator
    - Comparing simulation results

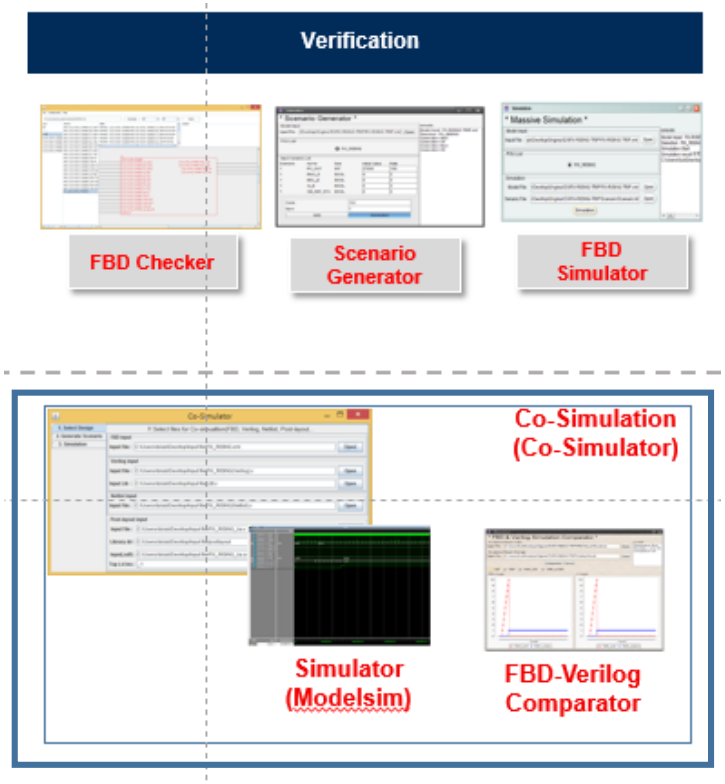




Usage Category of Target Software

- **Verification Software**
  - Verilog
    - Co-Simulator (Contains VHDL)
    - Modelsim
    - FBD-Verilog Comparator

  - Verification software for FBD is classified as unrelated category



Usage Category of Target Software

- Tables about results of usage category
  - Indirect
  - Support
  - Unrelated

Usage Category	COTS Software in FPGA based I&C development environment	Uses
Indirect	FBDtoVerilog / FBDtoVHDL / Synthesis Tool / P&R Tool	Development
Support	FBD Editor	Development
Unrelated	FBD Checker Scenario Generator / FBD Simulator / FBD-Verilog Comparator / ModelSim / Co-Simulator	Verification

Safety Category of Software

- Usage category of **Support** and **Unrelated**
  - Classifying **unclassified** category by standards

- Usage category of **Indirect**
  - Classifying **B** category by standards
  - If the results are able to verify another methods

Tools	Results format	Verification Method
FBDtoVerilog	Verilog Design	Model Checking, Simulation
FBDtoVHDL	VHDL Design	Simulation
Synthesis Tool	Gate-Level Design (netlist)	Simulation
P&R Tool	Layout (EDIF)	Simulation

Safety Category of Software

- Usage category of **Support** and **Unrelated**
  - Classifying **unclassified** category by standards

- Usage category of **Indirect**
  - Classifying **B** category by standards
  - If the results are able to verify another methods

Safety category	COTS Software in FPGA based I&C development environment
A	N/A
B	FBDtoVerilog / FBDtoVHDL / Synthesis Tool / P&R Tool
C	N/A
Unclassified	FBD Editor / FBD FTA / FBD Checker / Scenario Generator / FBD Simulator / FBD-Verilog Comparator / ModelSim / Co-Simulator

Conclusion and Future Work

- We classify safety categories of software which are used in FPGA development process researched before for dedication

- Verification tools in development process is classified as unclassified category
  - Confirming relationship about standards functional safety certification

- However, NP-5652/TR-106439 is accepted in Korea by KINS/RG-N17.12 “안전성관련품목 대체사용을 위한 일반규격품의 품질검증”

- We are researching about relationship between NP-5652 and NUREG/CR-6421

END