DEPENDABLE SOFTWARE LABORATORY

NuDE : Formal method based NPP system development and verification environment

KU KONKUK UNIVERSITY

Target Domain

Development institutions :
- Konkuk university, Korea
- Dependable software laboratory

Application domain :
- Software for safety-critical system in NPP
- RPS (Reactor Protection System)

Embedded hardware :
- FPGA (Field Programmable Gate Array)
- PLC (Programmable Logic Controller)

Programming language :
- PLC → FBD (Function Block Diagram, IEC 61131-3)
- FPGA → VHDL (VHSIC Hardware Description Language), Verilog

Tool-set :
- 26 tools (8 external tools)

NuDE Tool-Sets

Requirement Analysis

NuSRS	Editor for NuSCR formal language
NuSCRtoFBD	Translator for NuSCR to FBD
NuFTA	Analysis tool for NuSCR using Fault tree
Quick checker	Static analysis tool for NuSCR
NuSCRtoSMV	Translator for NuSCR to SMV input
Cadence SMV	Symbolic model checking tool

Design

FBD Editor	Editor for FBD program
FBDtoC	Translator for FBD to C
FBDtoVHDL	Translator for FBD to VHDL
FBDtoVerilog	Translator for FBD to Verilog
FBDFTA	Analysis tool for FBD using Fault tree
VIS	System for formal verification, synthesis, and simulation
Cadence SMV	Symbolic model checking tool
Scenario Generator	Simulation scenario generator for FBD simulator
FBD Simulator	Simulator for FBD with scenario
FBD Checker	Rule and coding style checker for FBD
FBD Tester	Tester for implemented FBD

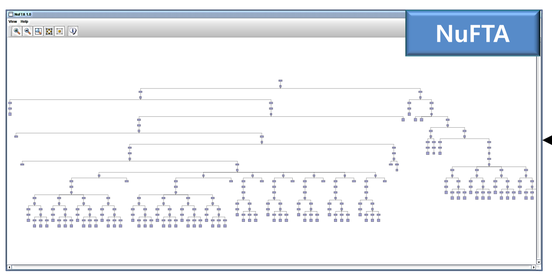
Implementation

C Compiler	Compiler for C code
FPGA Synthesis Tool	Synthesis tool for Verilog/VHDL code
Place & Route	Place and route tool for Netlist
EDIFtoBLIF-MV	Translator for EDIF to BLIF-MV
Vl2mv	Translator for Verilog to BLIF-MV
HW-CBMC	Bounded model checker for C/C++ program
C Simulator	Simulator for C program with scenario
FBD-Verilog Comparator	Comparator for FBD simulation result with Verilog simulation result
FBD-C Comparator	Comparator for FBD simulation result with C simulation result
VIS	System for formal verification, synthesis, and simulation
Modelsim	HDL simulator

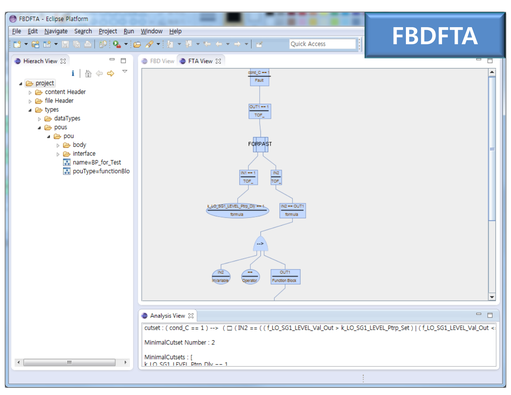
External | Developed

Safety Analysis

NuFTA

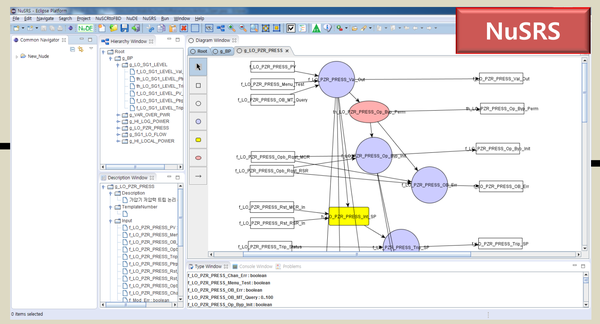


FBDFTA



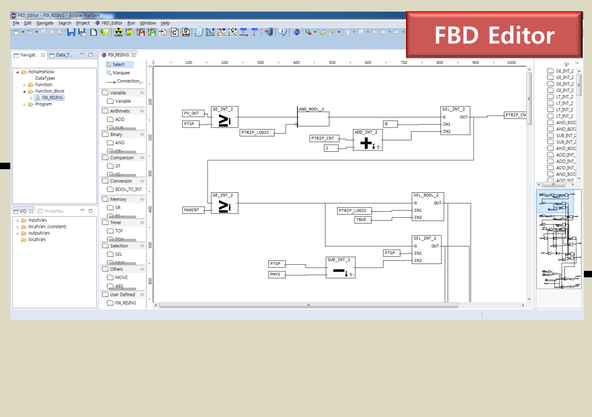
Development

NuSRS



NuSCRtoFBD

FBD Editor



FBDtoC
FBDtoVerilog

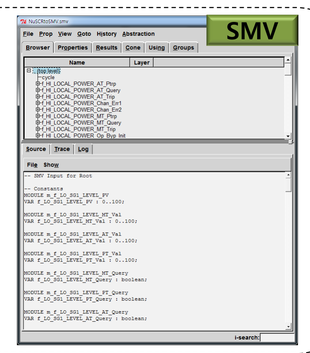
FBDtoVHDL
FBDtoVerilog

Verification

Model checking

NuSCRtoSMV

SMV



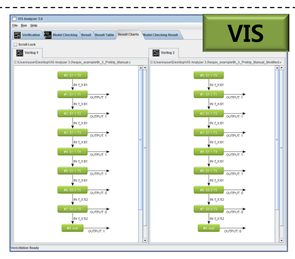
Rule checking

Quick Checker

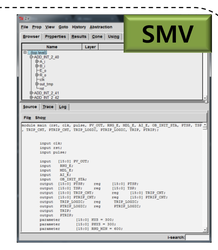
Model checking

FBDtoVerilog

VIS



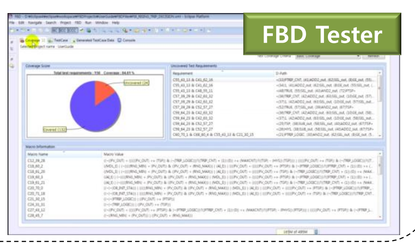
SMV



Rule checking

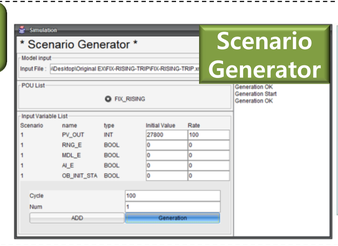
FBD Checker

FBD Tester

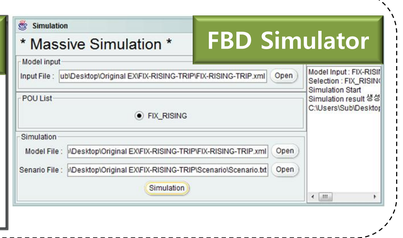


Co-Simulation

Scenario Generator



FBD Simulator



Scenario & FBD Simulation Result

Model Checking

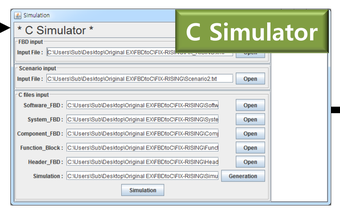
HW-CBMC

Verilog

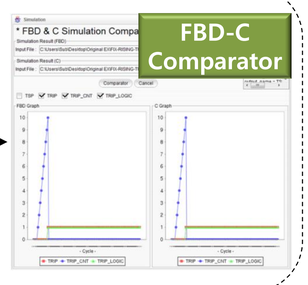
C Program

Co-Simulation

C Simulator



FBD-C Comparator



C Compiler

Executable Code for PLC

Load

PLC

VHDL

Verilog

FPGA Synthesis Tool

Netlist (EDIF)

Place & Route

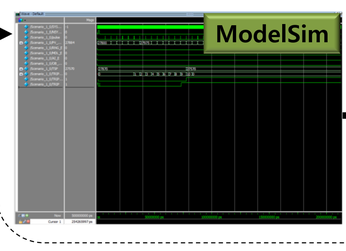
JEDEC File

Load

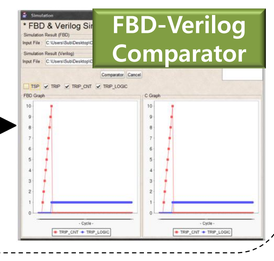
FPGA

Co-Simulation

ModelSim



FBD-Verilog Comparator



Equivalence Checking

vl2mv

BLIF-MV

VIS

EDIFtoBLIF-MV

BLIF-MV

Requirement Analysis

Design

Implementation

COTS

PLC Implementation

COTS

FPGA Implementation

Safety analysis | Development | Verification | File

External | Developed

→ : Input : Automatic Translation