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

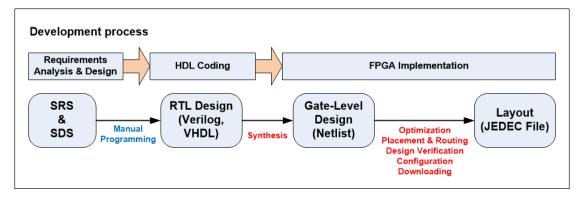
Contents

- 1. Introduction
- 2. COTS SW Dedication
- 3. Classification of Software
- 4. Conclusion and Future Work



Introduction

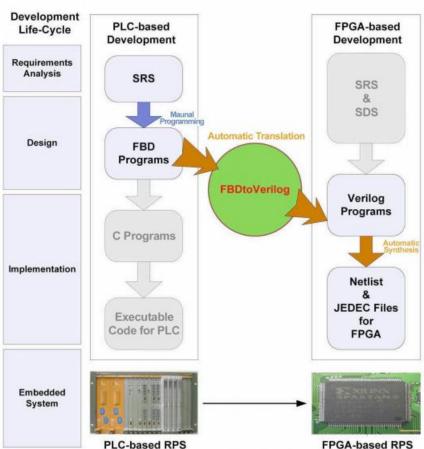
- PLC(Programmable Logic Controller) has been used to implement I&Cs for decades
 - SW development on industrial computers (CPU & OS)
- Increasing maintenance cost about old nuclear plants
 - Request for alternative implementation platforms
- FPGA(Field Programmable Gate Array) is an alternative platform 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



The Proposed Development Process for RPS Software 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 offthe-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

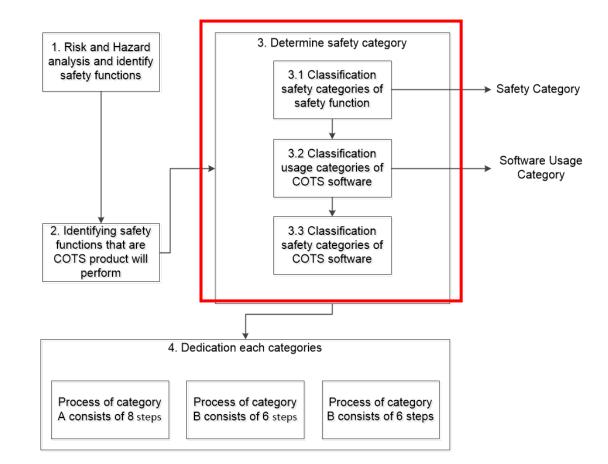
IEC 1226 Safety Category	Examples
A	원자로 보호 계통 시스템(RPS) / ESFAS 등
В	발전소 자동 제어 시스템 / 연료 재충전 시스템 등
С	알람 / 모니터링 시스템 등

• (+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

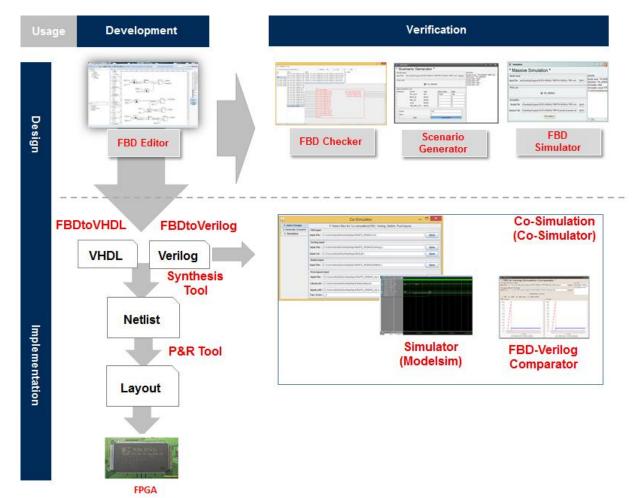
Usage Category	Description	IEC 1226 Category
Direct	Directly used in an A,B,C application	A, B, C
Indirect	Directly produces executable modules which are used in an A,B,C applications (e.g. compilers, linkers)	A, B, C, unclassified
Support	CASE systems, or support systems that indirectly assist in the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



Target Software

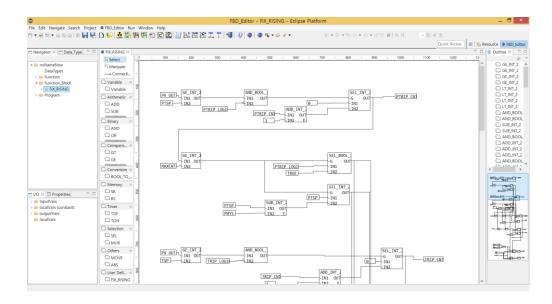
FPGA development process

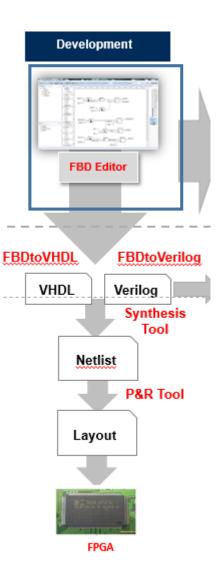
- Changing in the hardware platform from PLC to FPGA before
- Developing tools and using several commercial software also





- Development Software
 - FBD Editor
- FBD Editor supports to design FBD
 - Possible to classify usage category of support

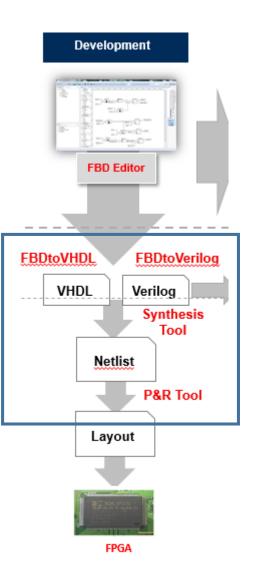






Development Software

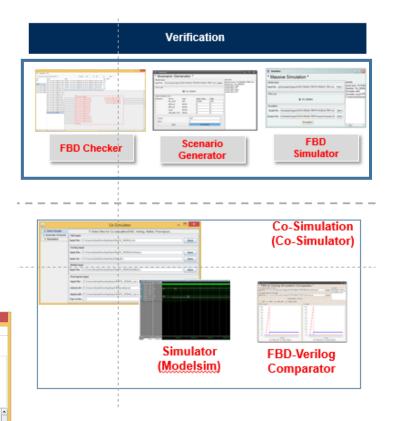
- FBDtoVerilog
- FBDtoVHDL
- Synthesis Tool
- P&R Tool
- Tools are translated, synthesis
 - They have an effect on design
 - Producing modules which are used in applications
 - Possible to classify usage category of indirect





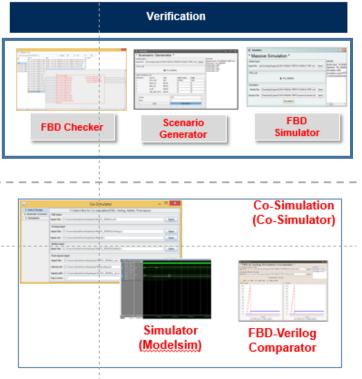
- FBD
 - FBD Checker
 - Scenario Generator
 - FBD Simulator
- FBD Checker
 - FBD Rule Checking
 - based on NUREG/CR-6463

File Configuration						_		
	g\Desktop\NuDE\FBD.xml		Checking	All	▼ All	-	Show	
f_HI_LOCAL_POWER	blocks null:f_H_LOCAL_POWER_AT_Quer null:f_HL_LOCAL_POWER_MT_Quer null:f_HL_LOCAL_POWER_PT_Quer null:f_HL_LOCAL_POWER_AT_Trip 6 null:f_HL_LOCAL_POWER_AT_Trip 6 null:f_HL_LOCAL_POWER_MT_Ptrp 6 null:f_HL_LOCAL_POWER_MT_Trip	warning : g_HI_LOCAL warning : g_HI_LOCAL warning : g_HI_LOCAL warning : g_HI_LOCAL	_POWER and f_HI_ _POWER and f_HI_ _POWER and f_HI_	LOCAL_POWER LOCAL_POWER LOCAL_POWER	MT_Query are too PT_Query are too f AT_Ptrp are too fa	far 🛄 ar r	explain	
	IIII: JULIOAL POWER JP. IMP IIII: JULIOAL POWER JP. IMP IIII: JULIOAL POWER JP. IMP IIII: JULIOAL POWER JP. IMP IIII: JULIOAL POWER Chan En IIII: JULIOAL POWER Chan En IIII: JULIOAL POWER Chan En IIII: JULIOAL POWER TEN IIII IIII: JULIOAL POWER TEN IIIII IIII: JULIOAL POWER TEN IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		() (), H, LOGAL, POW (H, LOGAL, POW)	ER_AT_Query ER_MT_Query ER_PT_Query ER_AT_Trip ER_AT_Trip ER_MT_Ptrp ER_MT_Ptrp ER_PT_Ptrp ER_PT_pin ER_Ptrp_in ER_Trip_in ER_Chan_Err1 ER_Chan_Err2 ER_Tes_Intl		Ē	HLLOCAL_POWER_Ptrp_Logic HLLOCAL_POWER_Trip_Logic (HLLOCAL_POWER_Ptrp_Out (HLLOCAL_POWER_Trip_Out	



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

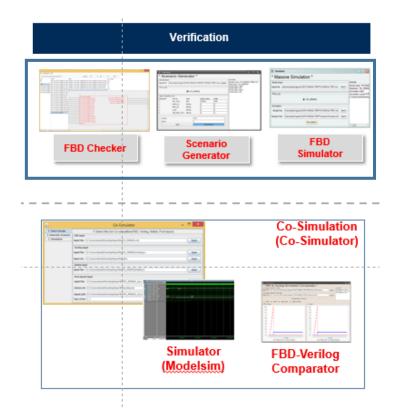
\$	Simulation	n			_	- = ×
*:	Scen	ario Gen	erato	or *		
	del input ut File : N	Desktop\Original E	-TRIP.xml Open	console Model Input : FIX-RISING-TRIP.xml Selection : FIX_RISING		
PO	U List			Generation Start Generation OK Generation Start Generation OK		
Inp	ut Variable	List				1
Sce	enario	name	type	Initial Value	Rate	
1		PV_OUT	INT	27800	100	
1		RNG_E	BOOL	0	0	
1		MDL_E	BOOL	0	0	
1		AI_E	BOOL	0	0	
1		OB_INIT_STA	BOOL	0	0	
	Cycle			100		
	Num			1		
	ADD			Generati	on	
	<u> </u>			~		





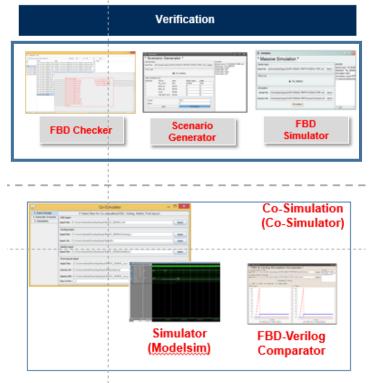
- FBD
 - FBD Checker
 - Scenario Generator
 - FBD Simulator
- FBD Simulator
 - Simulation FBD using scenario

👻 Simulatio			
* Mass	sive Simulation *		
Model input			console
Input File : u	b\Desktop\Original EX\FIX-RISING-TRIP\FIX-RISING-TRIP.xml	Open	Model Input : FIX-RISI Selection : FIX_RISIN Simulation Start
POU List	FIX_RISING		Simulation result 생설 C:\Users\Sub\Deskto
Simulation			
Model File :	VDesktop\Original EX\FIX-RISING-TRIP\FIX-RISING-TRIP.xml	Open	
Senario File :	Desktop/Original EX/FIX-RISING-TRIP/Scenario/Scenario.bt	Open	
	Simulation		<





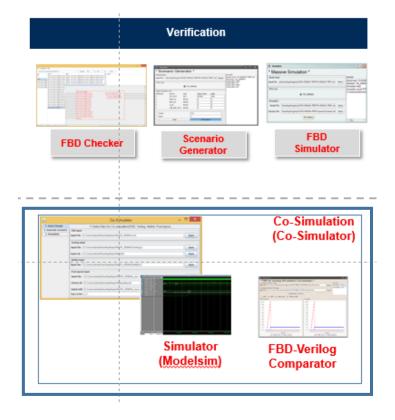
- Verification Software
 - FBD
 - FBD Checker
 - Scenario Generator
 - FBD Simulator
 - Verification software for FBD is classified as unrelated category





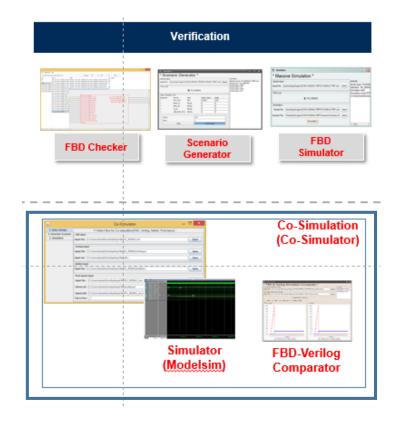
- Verilog
 - Co-Simulator (Contains VHDL)
 - Modelsim
 - FBD-Verilog Comparator
- Co-Simulator
 - Providing Simulation environment
 - Verilog, VHDL

\$	Co-Simulator -	- 🗆	x				
1. Select Design	!! Select files for Co-simualtion(FBD, Verilog, Netlist, Post-layout						
2. Generate Scenario	FBD input						
3. Simulation	Input File: C:\Users\dslab\Desktop\Input file\FIX_RISING.xml	Оре	'n				
	- Verilog input						
	Input File: C:/Users/dslab/Desktop/Input file/FIX_RISING(Verilog).v	Оре	n				
	Input Lib: C:/Users/dslab/Desktop/Input file/LIB.v	Оре	n				
	Netlist input						
	Input File: C:/Users/dslab/Desktop/Input file/FIX_RISING(Netlist).v	Оре	n				
	Post-layout input						
	Input File : C:/Users/dslab/Desktop/Input file/FIX_RISING_ba.v	Ор	en				
	Library dir : C/Users/dslab/Desktop/Input file/postlayout	Ope	en				
	Input(.sdf): C:/Users/dslab/Desktop/Input file/FIX_RISING_ba.sdf	Ope	en				
	Top Lvl ins : _1						



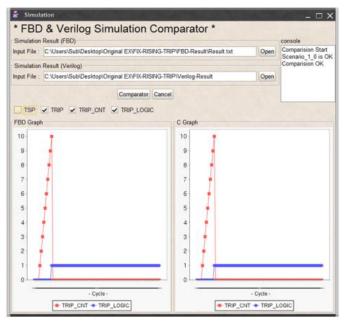
- Verilog
 - Co-Simulator (Contains VHDL)
 - Modelsim
 - FBD-Verilog Comparator
- Simulator (Modelsim)
 - Simulation Verilog, VHDL

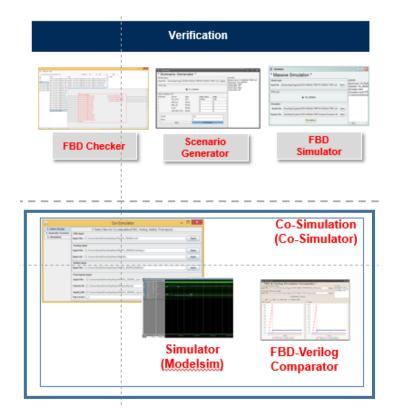
Wave - Default								 	 	
\$.	Mags									
/Scenario_1_0/SYS1	1					_	_		 	
/Scenario_1_0/NSY 0										
 /Scenario_1_0/pulse /Scenario_1_0/PV 		27800 I I		79751 I I					TTTT	
/Scenario_1_0/RNG_E_0								 	 	
/Scenario_1_0/MDL_E 0										
/Scenario_1_0/AI_E 0										
/Scenario_1_0/08 0 0.4 /Scenario_1_0/TSP 2		07870			—,	2757.0				
5cenario_1_0/TRIP 0		0	11 12	3 14 15 18		0.0				
/Scenario_1_0/TRJP 1		_								
/Scenario_1_0/TRJP 1										
CER Nov	500000000 ps		1	50000000 26			0000 ps	 150000000 ps	 200000	
Cursor 1	254265997 ps	*		5000000 ps		10000	6000 ps	190000000 ps	200000	uto pe





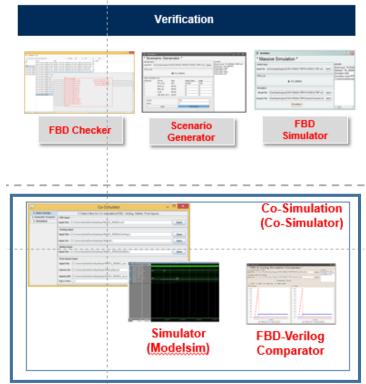
- Verilog
 - Co-Simulator (Contains VHDL)
 - Modelsim
 - FBD-Verilog Comparator
- FBD-Verilog Comparator
 - Comparing simulation results







- Verification Software
 - Verilog
 - Co-Simulator (Contains VHDL)
 - Modelsim
 - FBD-Verilog Comparator
 - Verification software for FBD is classified as unrelated category





- 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
Α	N/A
В	FBDtoVerilog / FBDtoVHDL / Synthesis Tool / P&R Tool
С	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