U.S. DEPARTMENT OF ENERGY | Nuclear Energy

Office Of Nuclear Energy
Sensors and Instrumentation
Annual Review Meeting

REALIZING VERIFIABLE I&C AND EMBEDDED DIGITAL DEVICES FOR NUCLEAR POWER

Matt Gibson, Program PI, EPRI
Dr. Carl Elks, Co-PI, Virginia Commonwealth University
Rick Hite, PhD Candidate, Virginia Commonwealth University
Smitha Gautham, PhD Candidate ,Virginia Commonwealth University

DE-NE0008445
October 18, 2017

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Project Overview

- **Goal: Develop science-based technologies and approaches for NPP I&C systems that show the potential for:**
  - Reducing qualification burden of I&C systems
  - Reducing complexity to enhance V&V awareness
  - Address CCF issues associated with digital I&C systems.
- **Participants**
  - Matt Gibson, Program PI, Electric Power Research Institute
  - Dr. Carl Elks, PI, Virginia Commonwealth University
  - Rick Hite, PhD Candidate, Virginia Commonwealth University
- **Schedule**
  - 2017 – Complete Design and Verification of SymPle 1131
  - 2018- Fabricate and Test demonstration devices and develop a Commercial Grade Dedication prototype.

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Accomplishments

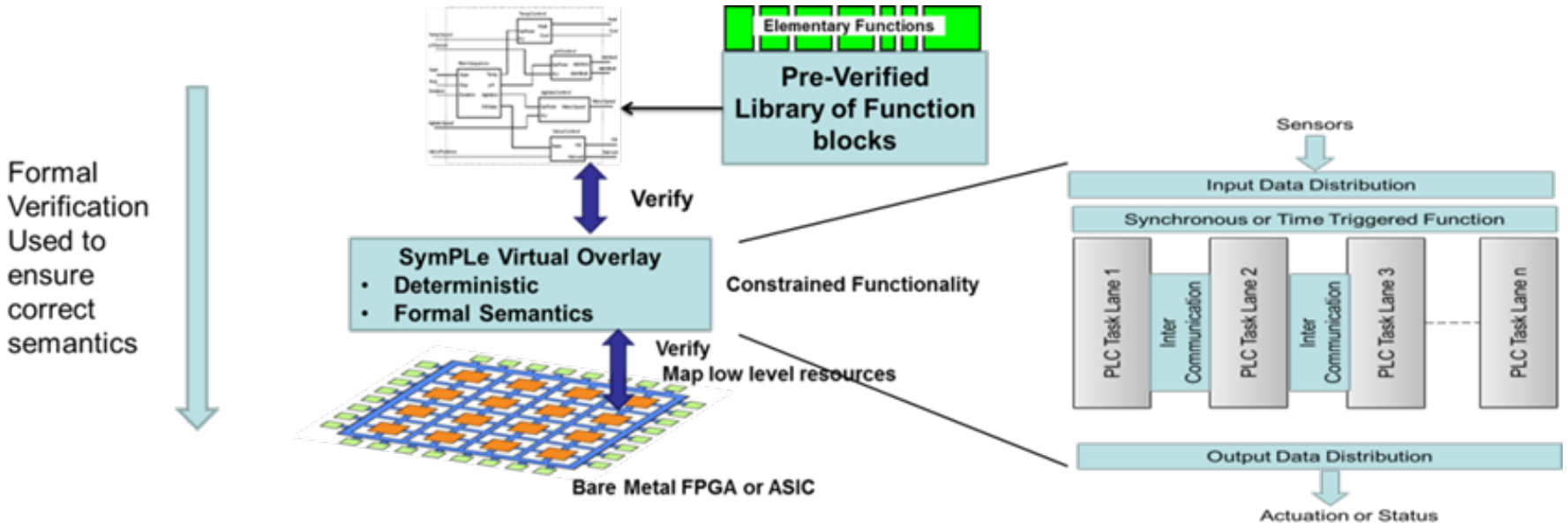
- M3CA-15-CA-EPRI-0703-0211 - Develop Test and Validation criteria for the final SymPLe 1131 Architectures
  - Description: Finalize SymPLe architecture,
  - Formal Verification of SymPLe,
  - Preliminary Investigation of Fault Tolerant SymPLe
  - Low-level (VHDL, Verilog) verification
  - Outcome: Reports, NPIC Papers, and Initial commercial interests
- M3CA-15-CA-EPRI-0703-0213 - Development and Verify Prototype Device Architecture -Part 2
  - End-to-end verification demonstration with Emergency Diesel Generator Startup Application.
  - Preliminary testing of EDG on Prototype
  - Preliminary study of Fault Tolerant SymPLe
  - Outcomes: NPIC Paper, Implementation data, exercised the entire development cycle with Simulink tools.

Research Perspective

- **Premise: Trend in NPP I&C migrating towards *SW intensive or SW based* digital I&C systems.**
  - So called *Change Enabled Systems and Technologies*
    - **Increasing complexity and flexibility in SW intensive systems exacerbates manifestation of SW failures, cyber-vulnerabilities and SW Common Cause Failures (SCCF)**
- Fundamental position we pose is that I&C systems in the context of nuclear power **may not need to be derivatives of software intensive systems** and by extension, not carrying the complexity associated with the SW intensive systems. .
- Our approach called **SymPLe** is to rethink digital I&C from a perspective of three views: Simplicity, Determinism and Verifiability.

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

SymPLe Concept

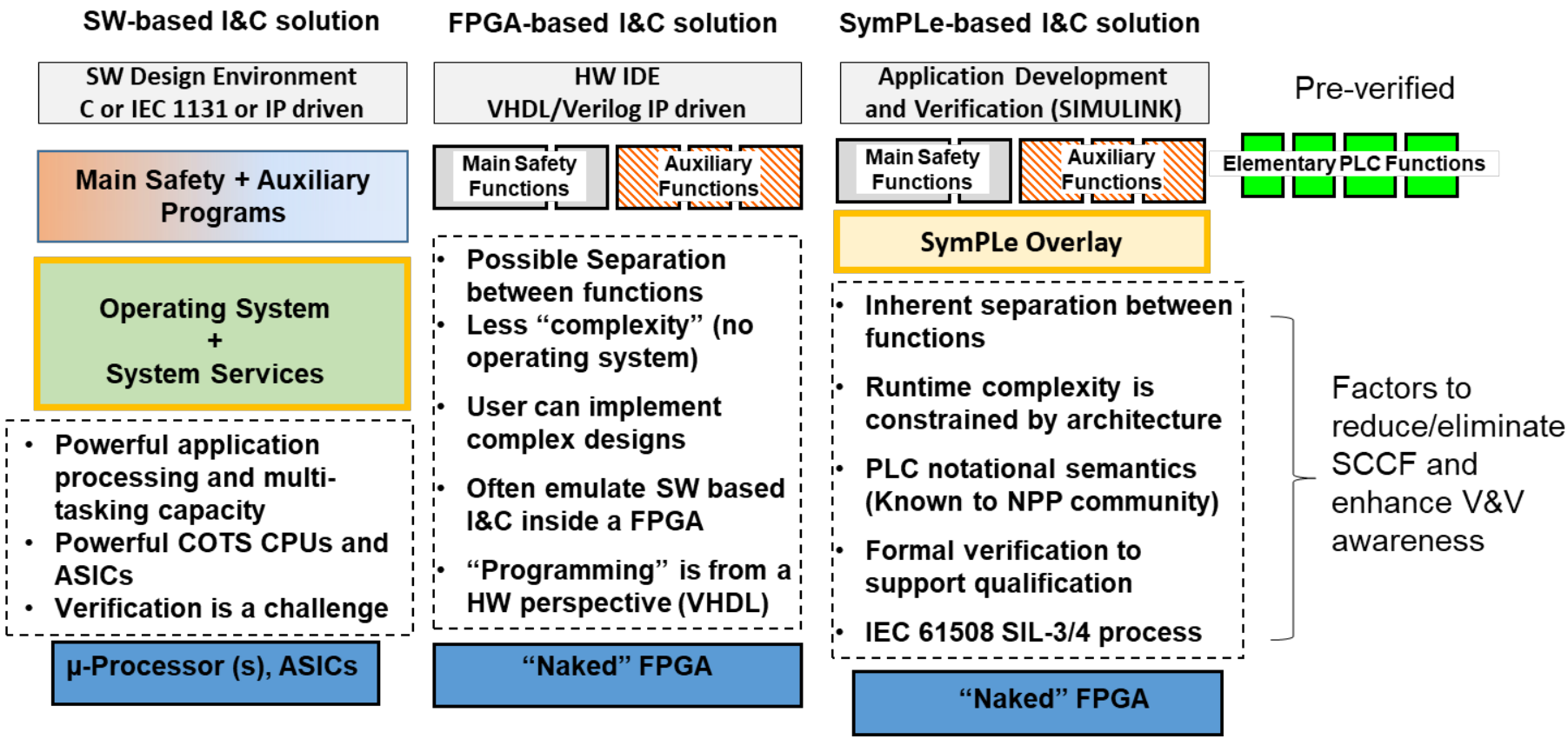


- SymPLe is a *virtual machine or overlay* constraining functionality
- Formal verification of operational semantics

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

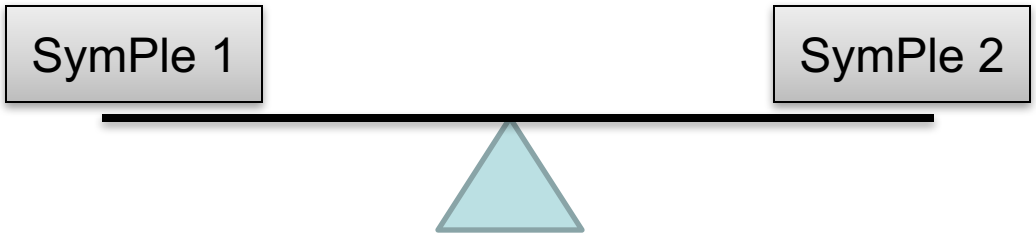
Comparative View of I&C "Stacks"

What's the difference: SW vs. FPGA vs. SymPLe based I&C



Application Domain of SymPLe

- The SymPLe Architecture has range and domain of applicability.
- Flexible, but requires trade-offs, and has a upper bound..



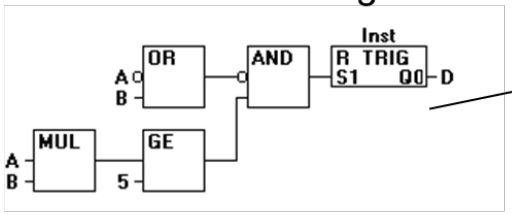
- SymPLe 1 – Significantly constrained processing, maximize "design for verification", limited reprogramability.
- SymPLe 2 – More processing power, More flexibility and programmability, more burden on verification.
- Upper Bound: SymPLe is not suited for I&C functions that require complex processing resources (DSPs, high performance CPUs, Graphic processing GPUs), database engines, heuristics engines, etc…

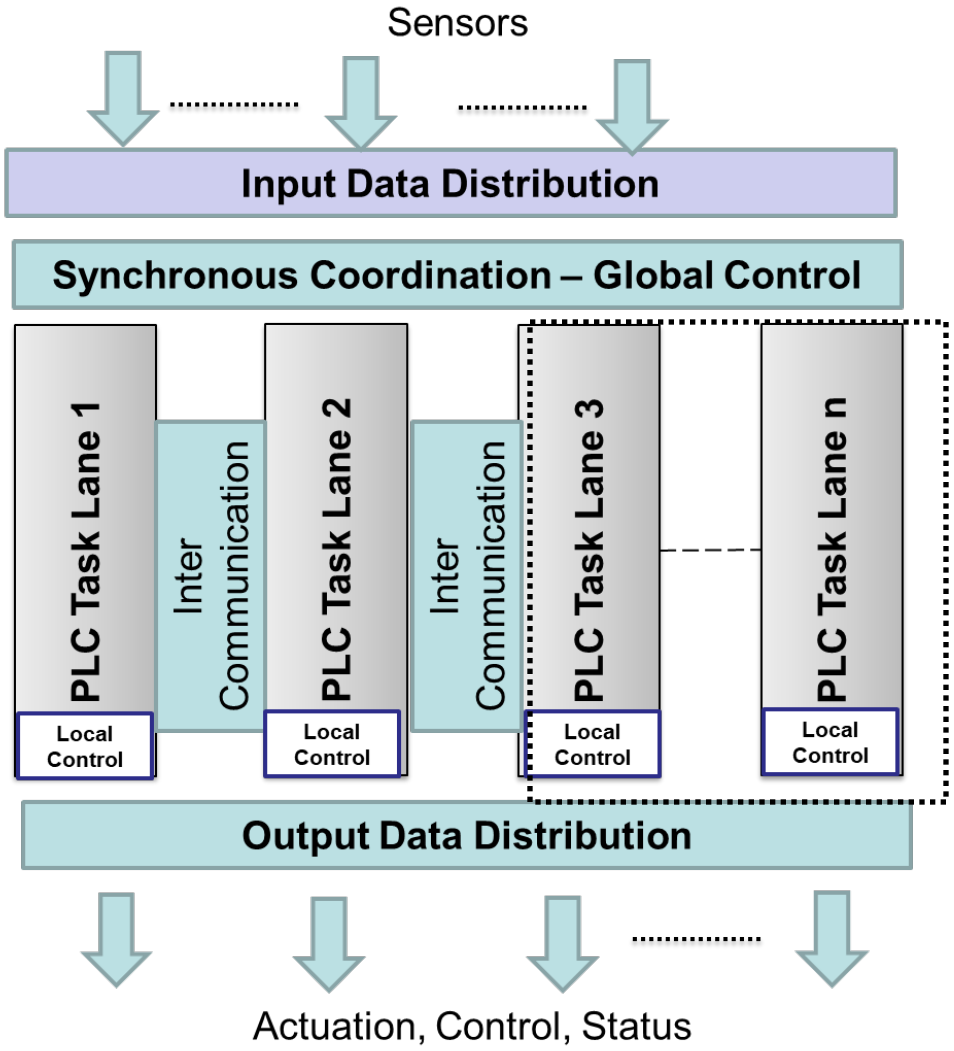
U.S. DEPARTMENT OF ENERGY
Nuclear Energy

High Level Architecture Model of SymPLe

MATLAB SIMULINK
SymPLe Tools

Function Block Diagram





1131 PU – Program unit

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

SymPLe Function Blocks

Elementary FBs

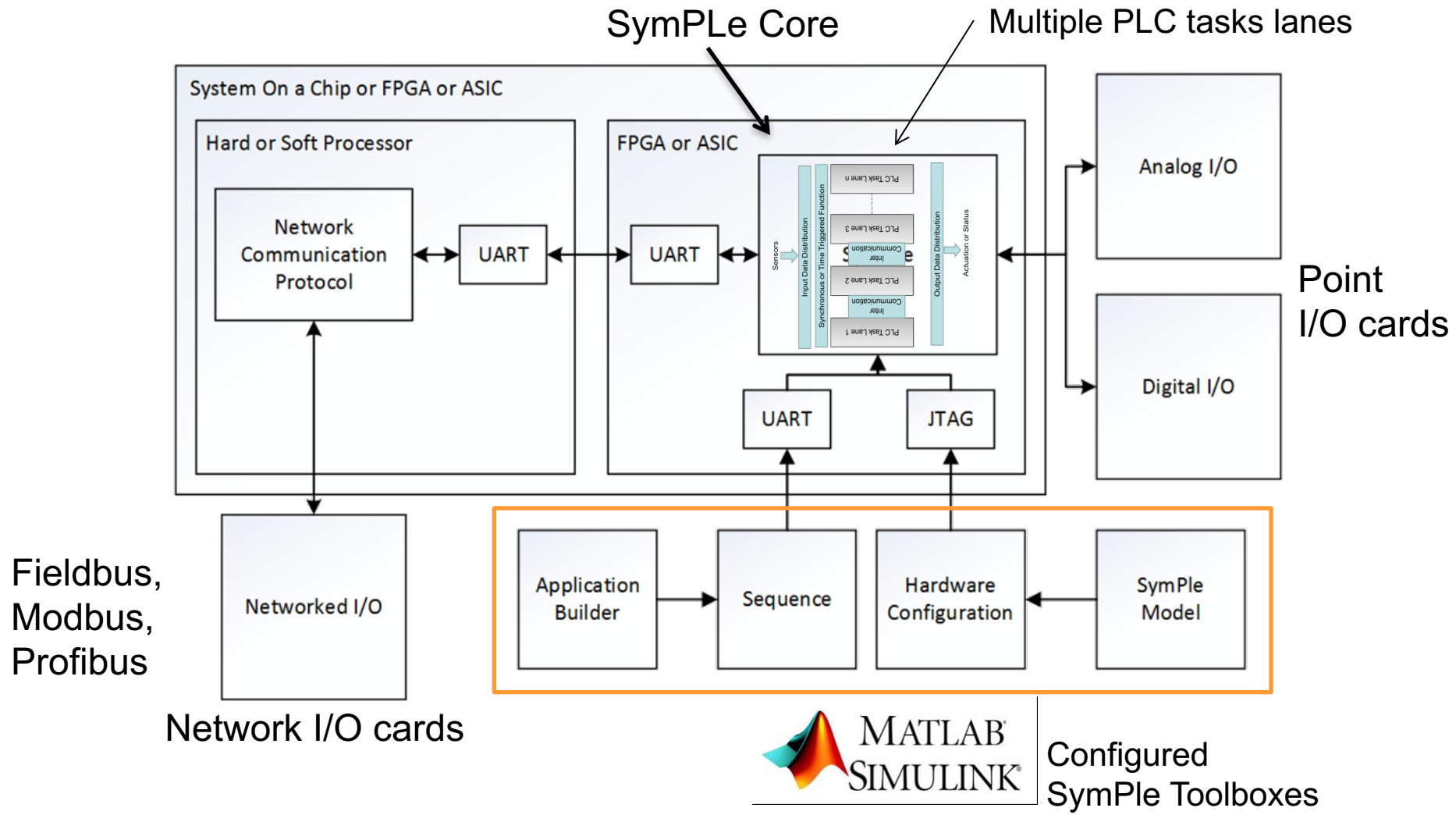
Instruction	Description
AND, OR, NOT, XOR, NAND, NOR	Logical Operators
AND, OR, NOT, XOR, NAND, NOR	Bitwise Logical Operators
MAX, MIN, MUX	Selection Operators
GT, GE, EQ, LT, LE, NE	Comparison Operators
ADD, SUB, MUL, DIV	Arithmetic Operators
SLL, SLR	Bit-shift Operators
MOVE	System Operators

Built-up FBs

Instruction	Description
PID	Control operator
TON, TOF	Timer operator
FXTOI, ITOFX	Data conversion operator
AVOTE	Analog voting
BVOTE	Digital voting
MEM	Memory operator
LOG	Logging operator

All Function blocks were formally proven, except PID. PID will be proven by end of quarter.

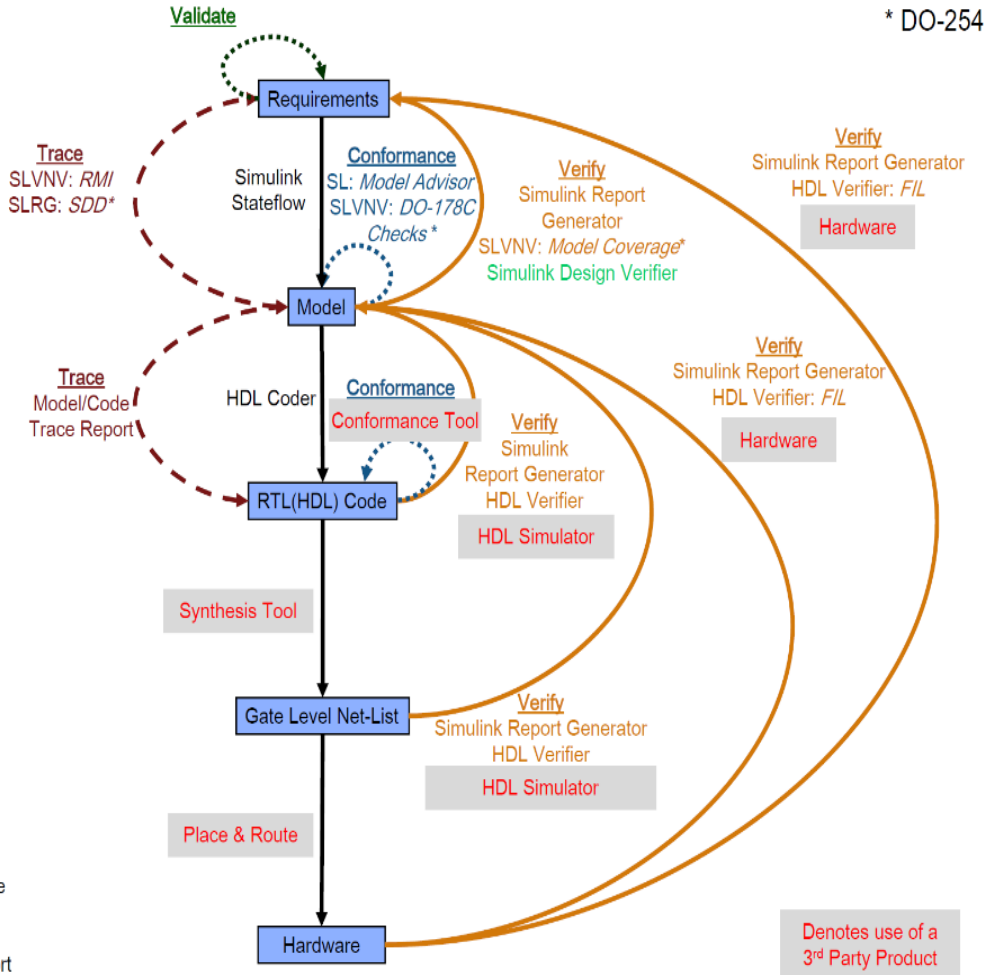
Complete SymPLe System



U.S. DEPARTMENT OF ENERGY
Nuclear Energy

SymPLe Development and Design Assurance Workflow

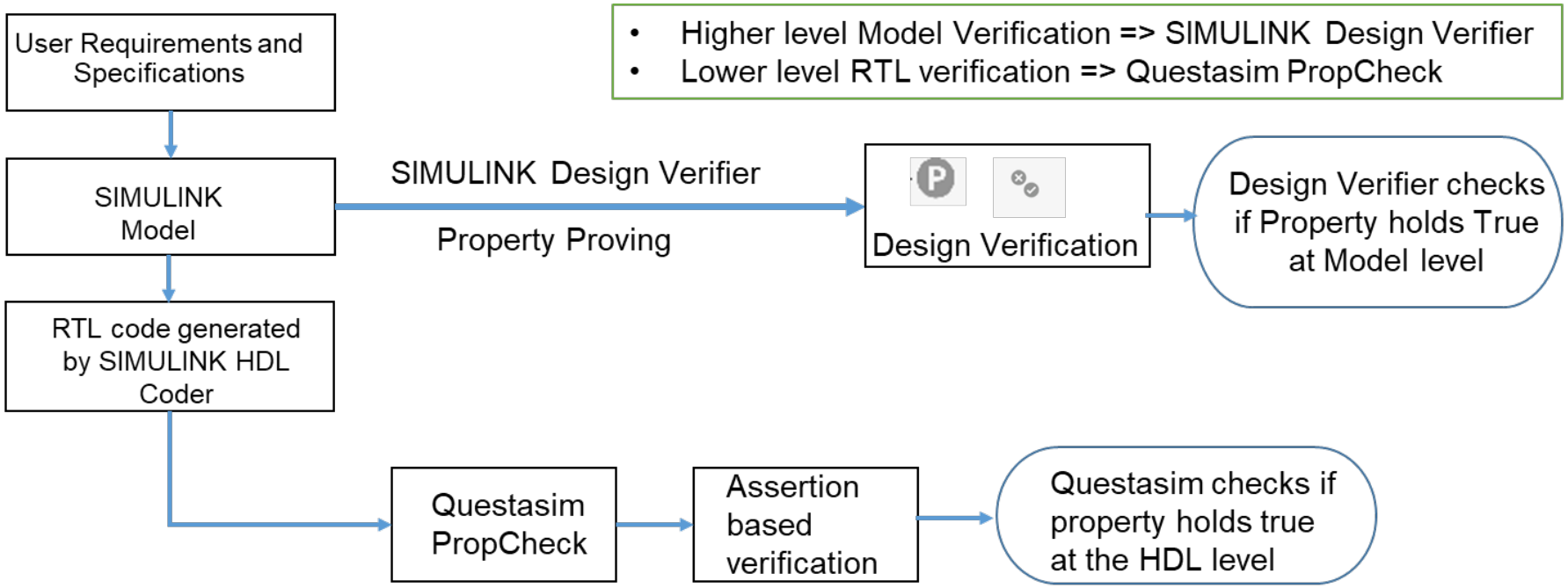
- **Verification at each step from requirements to implementation**
- **Math works Tools used throughout V&V workflow**
  - Prevents gaps in V&V from oversight or misinterpretation
- **Third party software used to complete, supplement, and diversify primary software V&V tools**
- **IEC 61508 certified**



Abbreviations
SL: Simulink
SLVNV: Simulink Verification and Validation
RMI: Requirements Management Interface
SDD: System Design Description
SLRG: Simulink Report Generator
FIL: FPGA-in-the-Loop

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

End-to-End Property Verification using MATLAB and MENTOR GRAPHICS Questasim

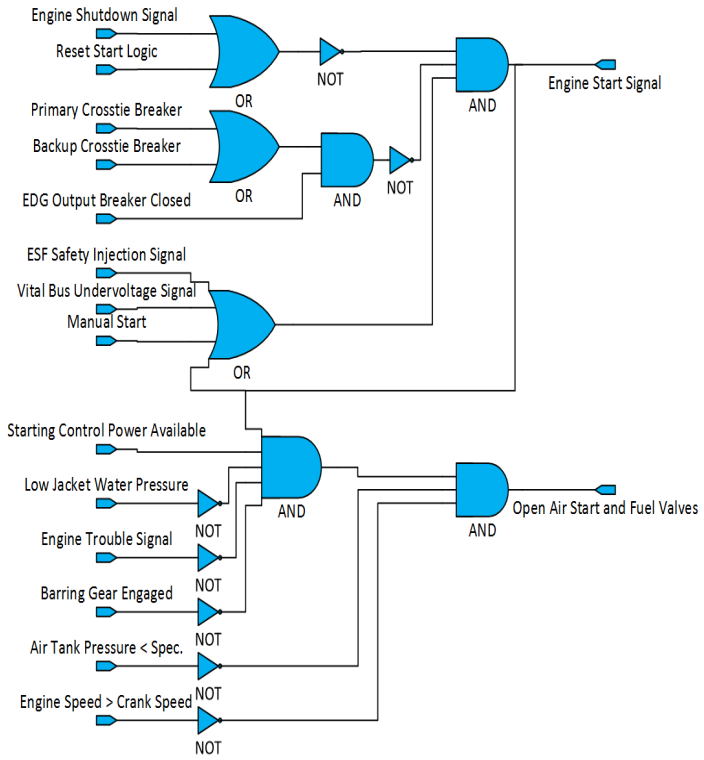


24

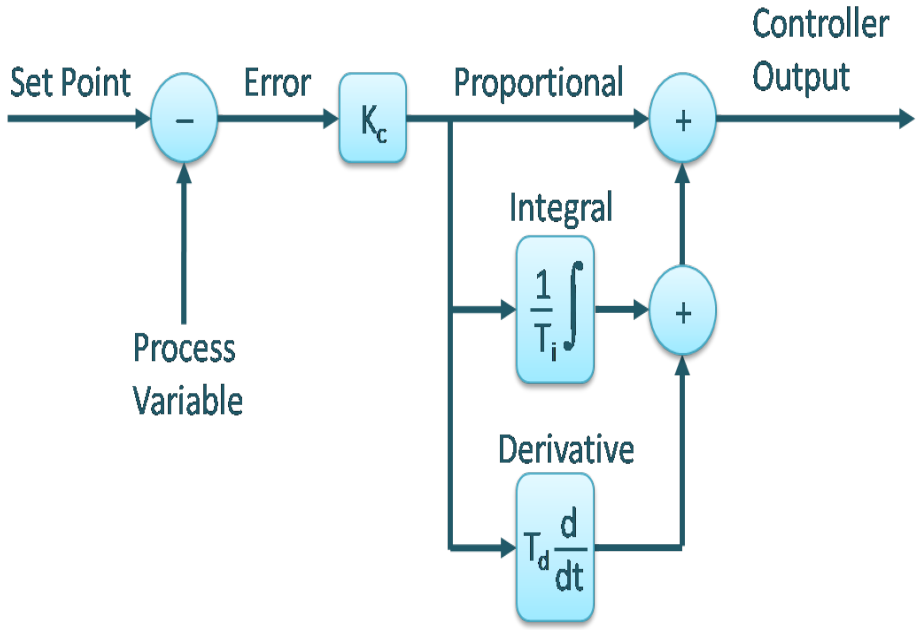
Check that actual SymPLe HW has inherited the proven property of models

Applications Ported to SymPLe to Date

Emergency Diesel Generator Startup Controller



Proportional, Integral, and Differential Controller



U.S. DEPARTMENT OF ENERGY
Nuclear Energy

SYMPLE HOSTED ON THE KINTEX-7 FPGA – METRICS ON RESOURCE UTILIZATION

Name	Slice LUTs (203800)	Slice Registers (407600)	Slice (50950)	LUT as Logic (203800)	LUT as Memory (64000)	LUT Flip Flop Pairs (203800)	Block RAM Tile (445)	Bonded IOB (500)	BUFGCTRL (32)	MMCME2_ADV (10)
design_1_wrapper	1043	1928	528	1010	33	518	64	179	2	1
design_1_i (design_1)	1043	1928	528	1010	33	518	64	0	2	1
clk_wiz (design_1_...	0	0	0	0	0	0	0	0	2	1
rst_clk_wiz_100M (...	15	25	9	14	1	12	0	0	0	0
single_task_0 (desi...	1028	1903	520	996	32	505	64	0	0	0

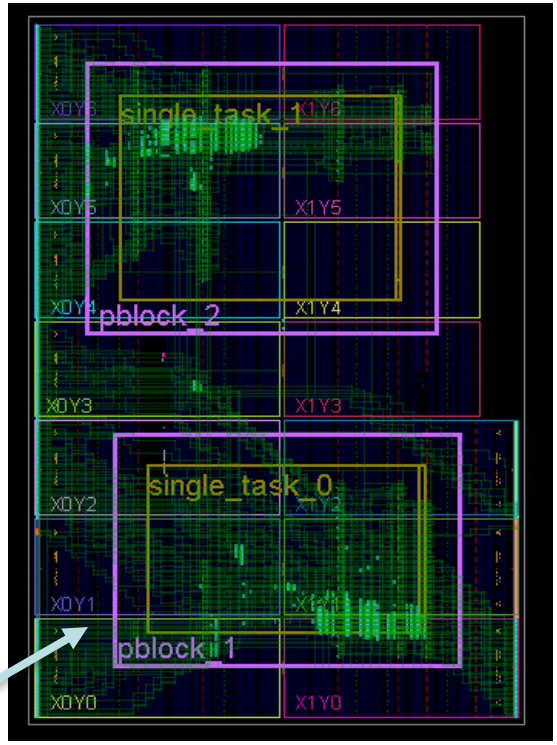
Resource utilization for a single task after Implementation

- LUT (Slice LUTs), LUTRAM (LUT as Memory), FF (flip flops or slice registers) : less than 0.5% of available resources on Kintex 7.
- The Block RAM tiles and MMCM : less than 10% of the available resources.
- The I/O pins: 35% of the resources on Kintex 7 (not optimized)
- A Kintex 7 can host about a SymPLe architecture with 10 task lanes.

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Implementation of DMR: Place and route for enhanced reliability

- To use SymPLe in safety critical applications or applications where high availability/reliability are needed – fault tolerance is needed..
- Fault tolerance in FPGA's is tricky.. Lot's of places where coupling can occur – clock tree's…
- We developed a methodology and workflow to design FT SymPLe architectures - conducted a preliminary study.
- One of the important design tools is the Xilinx Isolation Design Flow (IDF).
- IDF helps define fault containment regions in FPGA during place and route.
- IDF is IEC 61508 certified and verifies that the isolated regions meets SIL 3 safety requirements.
- The isolated regions are defined by drawing regions called Pblocks around them.
- Constraints were defined to isolate the Pblocks.



Implemented design: Dual modular redundancy

Two Task Lanes as a DMR

2017 Summary and Take Away

- **Have designed and realized a practical verifiable PLC Instantiable architecture that addresses CGD and SCCF via:**
  - Constrained architecture operations
  - Formal deterministic FB semantics
  - Extensive use of model based design and analysis
  - Complementary Formal verification and Testing
- **Have developed and exercised a design and V&V workflow for SymPLe**
- **Have Demonstrated SymPLe concept with Basic Emergency Diesel Generator (EDG) start controller**
- **Have Implemented SymPLe and EDG on actual HW**
- **Developed preliminary tools and methods for FT versions of SyMPLe**
- **Presented two papers at ANS NPIC 2017, more papers in preparation for IEEE Journal on Control Systems Technology.**
- **Developing interest for SymPLe from industry Rockwell Collins/Allen Bradley, Mathworks**

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

2018 planned activities

- **Conduct IEC 61508 (Sil-3)Commercial Grade Dedication (CGD) Exercise with Paragon Energy Solutions Nuclear and EPRI.**
- **Use Model Based Tools to provide CGD data to Paragon for CGD review.**
- **VCU purchased IEC 61508 tools from Mathworks**
- **Continue refining architecture, complete critical review of Property Proving with Mathworks experts**
- **Complete design and testing of I/O architecture**
- **Select a new "more complex" application to port and test on SymPLe**
  - Richard Vilim NSSC Control Rod ..?
- **More HW testing, and more HW testing….**
- **Document final project findings and results**

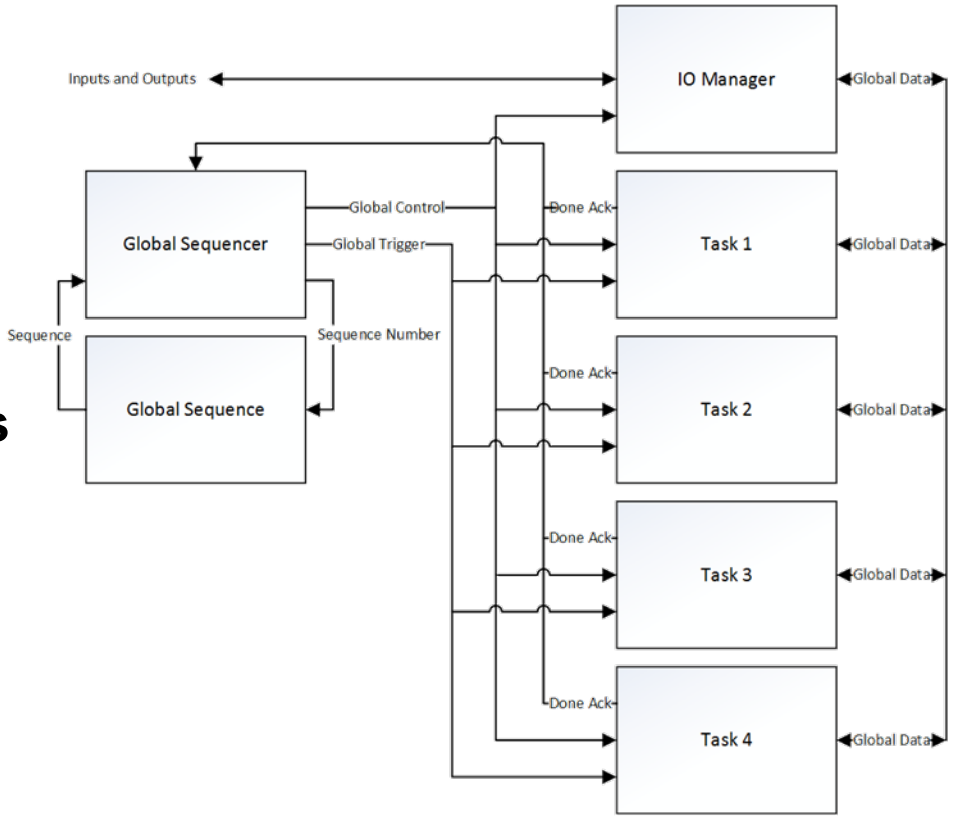
U.S. DEPARTMENT OF ENERGY

Nuclear Energy

Extras

Tasking in SymPLe

- PLC applications in SymPLe execute in Task Lanes.
- Task Lanes are independent
- Application FBDs assigned to a task lane are scheduled via a fixed, deterministic sequence of task executions.
- Tasks have a *cycle time* that is repeating (e.g. every 50ms the execution repeats)
- Cycle time can be set by user.
- The state of the task lane is managed by sequencer function

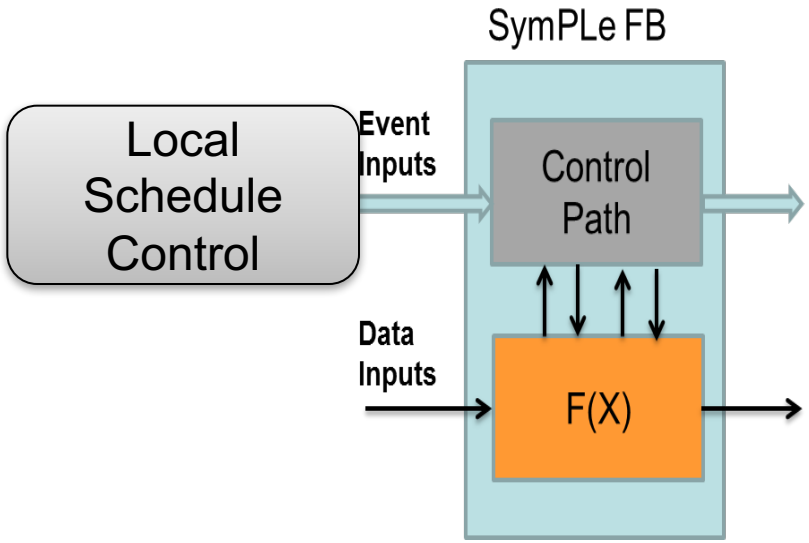


U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Function Block Architecture

Common architecture for all SymPLe function blocks

- **Inspired by IEC 61499**
- **Deterministic, synchronous behavior.**
- **Separation of control and dataflow with clear and defined interconnections**
- **Formal semantics**



Function Block Semantics

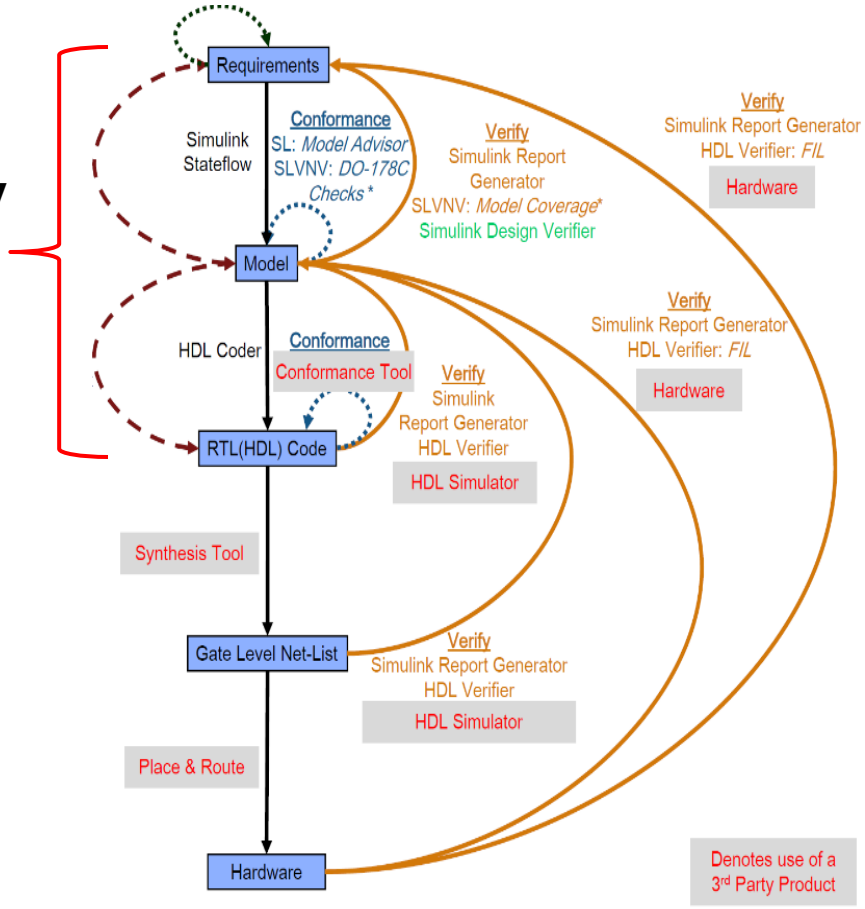
- **Step 1**: The input variable values relevant to the input event are registered and available.
- **Step 2**: The input event occurs, the execution control of the function block is triggered
- **Step3**: The execution control function evaluates the request and notifies the scheduling function to schedule algorithm for execution
- **Step 4** :Algorithm execution begins.
- **Step 5**: The algorithm completes the establishment of values for the output variables associated with the event output by the WITH qualifier
- **Step 6**: The resource scheduling function is notified that algorithm execution has ended.
- **Step 7**: The scheduling function invokes the execution control function.
- **Step 8**: The execution control function signals event at the event output.

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

SymPLe V&V- Traceability

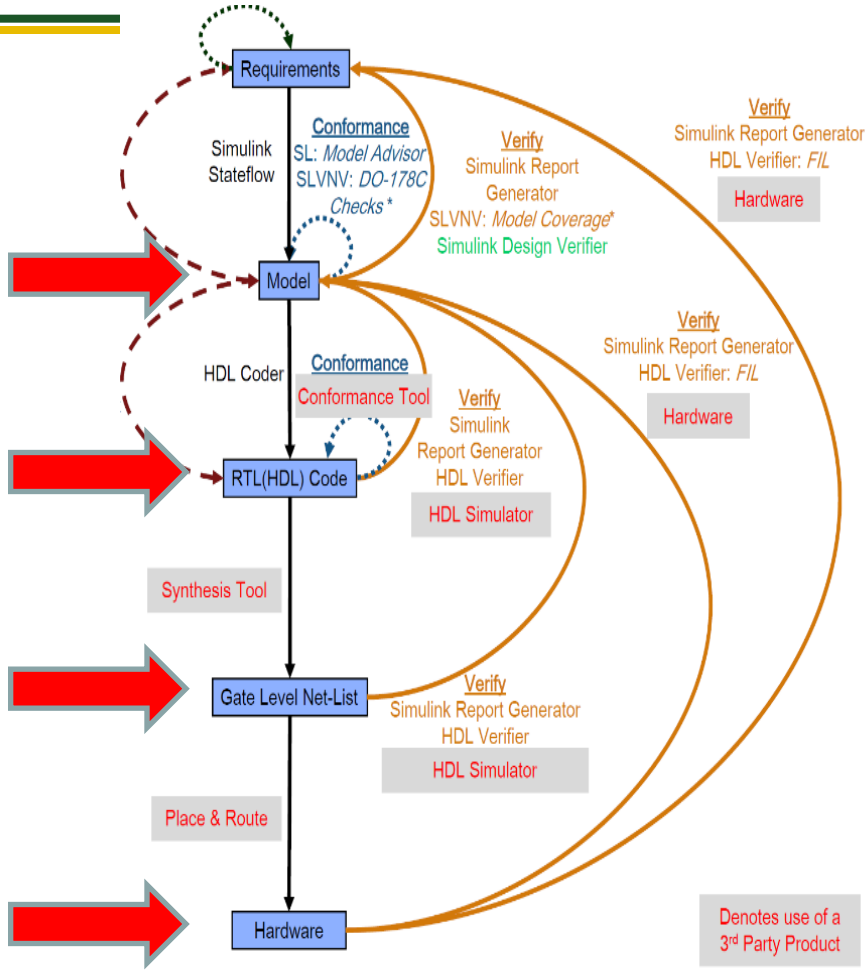
- **Software used: Simulink Verification and Validation**
- **Provides traceability from**
  - Requirements to
    - Contained in Word document
    - Hyperlinked to Simulink model component
  - Model to
    - Hyperlinked back to Word requirements document
  - HDL code
    - Requirement embedded in code
    - Hyperlinked in HTML version of code
- **Traceability report**
  - Documents requirements chain
  - Identify components lacking requirements

Traceability



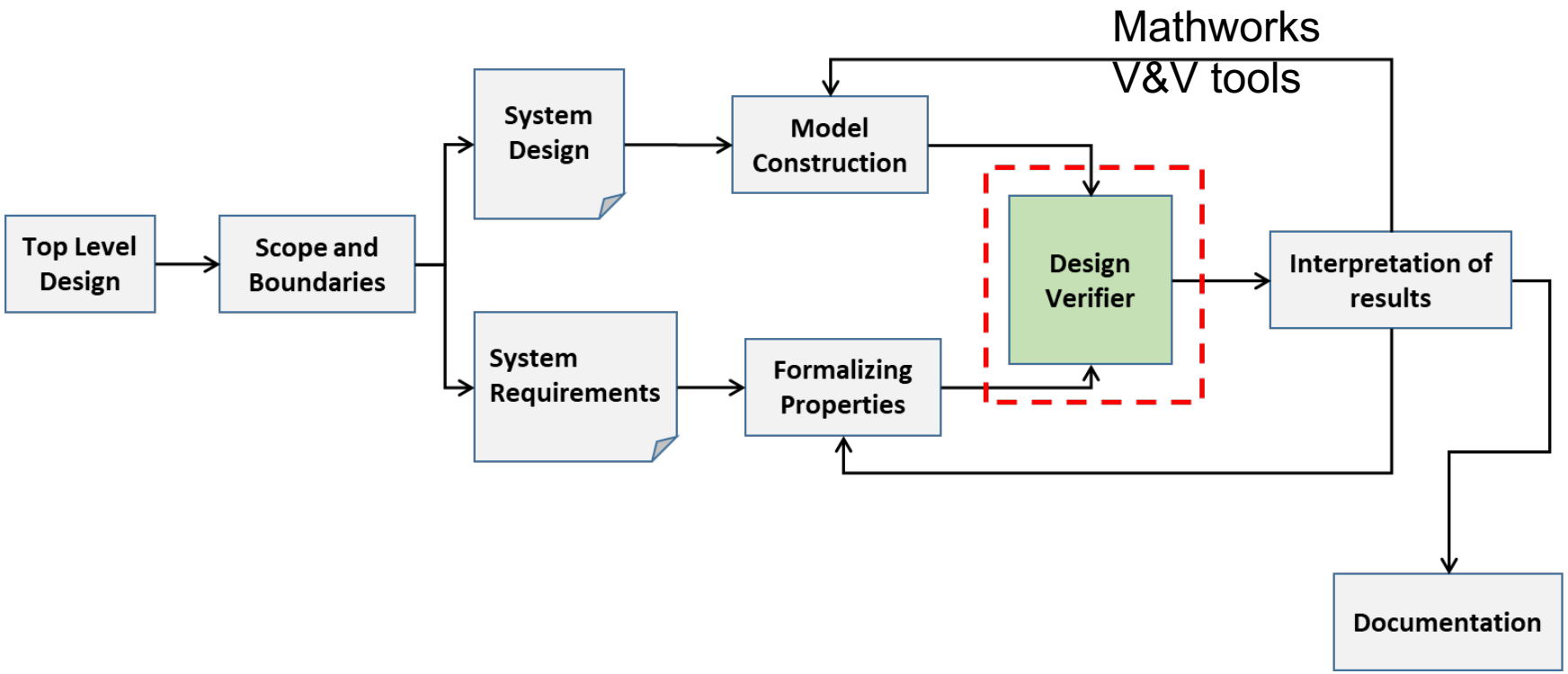
SymPLe V&V - Test Case Generation

- **Why?: Formal verification needs to be balanced with test cases - generate corner cases.**
- **Bridges gaps in formal methods**
- **Develop specific test cases for:**
  - Execution sequences
  - Edge cases
    - Errors commonly found here
  - Mid range cases
    - Verify normal operation



U.S. DEPARTMENT OF ENERGY
Nuclear Energy

SymPLe Verification Workflow



U.S. DEPARTMENT OF ENERGY
Nuclear Energy

SYMPLE HOSTED ON THE KINTEX-7 FPGA – METRICS ON RESOURCE UTILIZATION

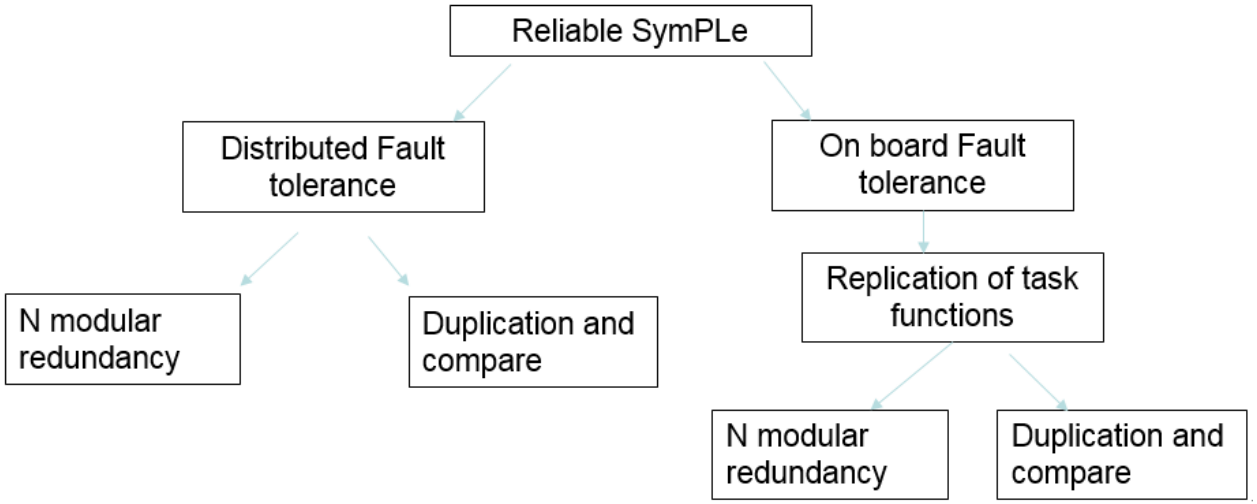
- SymPLe architecture was implemented on a Kintex 7 Evaluation board on the xc7k325tffg900-2 device family
- Synthesis : Vivado tool generates gate level netlist for the RTL code.
- Implementation : tool places and routes gates level netlist on FPGA.
- Global optimization, register duplication, logic optimization and other attributes cause slight variations in the FPGA resource utilization during Synthesis and Implementation

Name	Slice LUTs (203800)	Slice Registers (407600)	Block RAM Tile (445)	Bonded IOB (500)	BUFGCTRL (32)	MMCME2_ADV (10)
design_1_wrapper	1110	1943	64	216	2	1
design_1_i (design_1)	1110	1943	64	0	2	1
clk_wiz (design_1_...	0	0	0	0	2	1
rst_clk_wiz_100M (...	19	40	0	0	0	0
single_task_0 (desi...	1091	1903	64	0	0	0

Resource utilization for a single task after Synthesis

Fault Tolerant SymPLe

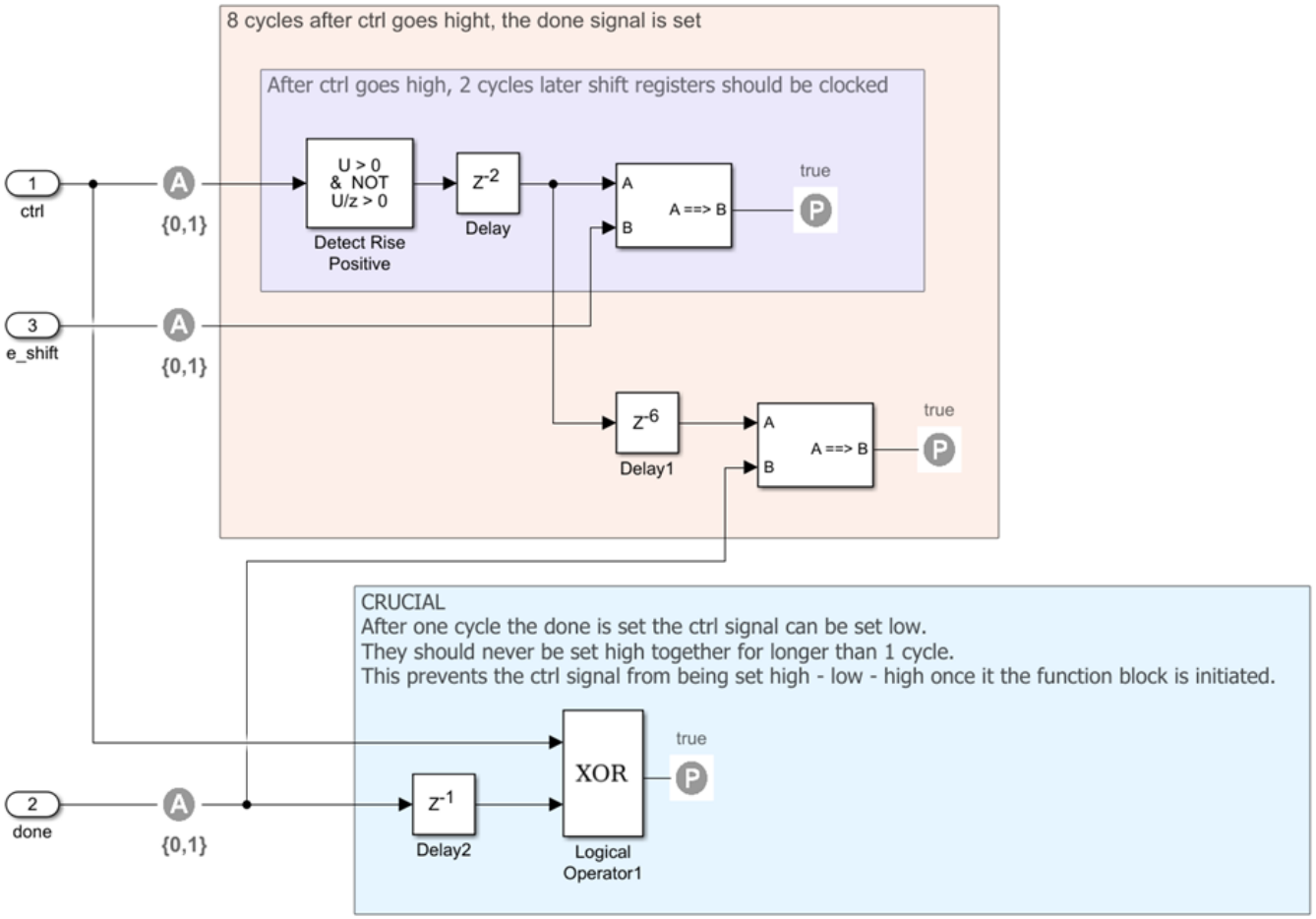
- To use SymPLe in safety critical applications or applications where high availability/reliability are needed – fault tolerance is needed..
- Fault tolerance can be achieved by (1)distributed fault tolerance where redundancy is implemented on two different FPGAs or (2) on board fault tolerance where redundancy is implemented on the same FPGA or combinations of both
- Replication at the task level ensures reliability at the application level.



Approaches to Fault Tolerance on SymPLe

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Example of Property Proving in Simulink Design Verifier



U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Commercial Grade Dedication Exercise for SymPLe

- **2017 we began pre-staging for CGD "demo" exercise for SymPLe.**
- **Principle CGD consultant is Argo-Turbo, with EPRI and VCU as support.**
- **July 2017 meeting. Decided that IEC 61508 was the best route to take for CGD exercise.**
  - An established standard that is applicable, tool support exits, and Nuclear Industry is interested in 61508
- **VCU purchased Mathworks certified 61508 toolboxes**
- **We have begun to familiarize ourselves with the tools.**
- **November 2017 we start CGD activity.**