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, PI, Virginia Commonwealth University
Dr. Gary Atkinson, Co-PI, Virginia Commonwealth University
Dr. Tim Bakker, Co-PI, Virginia Commonwealth University

DE-NE0008445
October 12-13, 2016

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
  - Dr. Gary Atkinson, Co-PI, Virginia Commonwealth University
  - Dr. Tim Bakker, Co-PI, Virginia Commonwealth University
- **Schedule**
  - 2017 – Complete Design and Verification of SymPle 1131 and MEMs Relay devices
  - 2018- Fabricate and Test Demonstration Devices and Develop a Commercial Grade Dedication Example.

Accomplishments (1 of 2)

- **Develop Classification of Target Device use cases**
  - Milestone: M3CA-15-CA-EPRI-0703-022
  - Description: Classifies the various use cases for that drive embedded device performance requirements. Critical to proper bounding
  - Outcome: Report on Summary and Description of Classification Learnings and Discoveries

- **Develop SymPLe 1131 Architecture - Part 1**
  - Milestone: M2CA-15-CA-EPRI-0703-023
  - Description: Establishes the requirements and operational semantics needed to actualize the SymPLe 1131 Architecture
  - Outcome: Summary and Description of the SymPLe 1131 Architecture Objectives - Report

U.S. DEPARTMENT OF ENERGY

Nuclear Energy

Accomplishments (2 of 2)

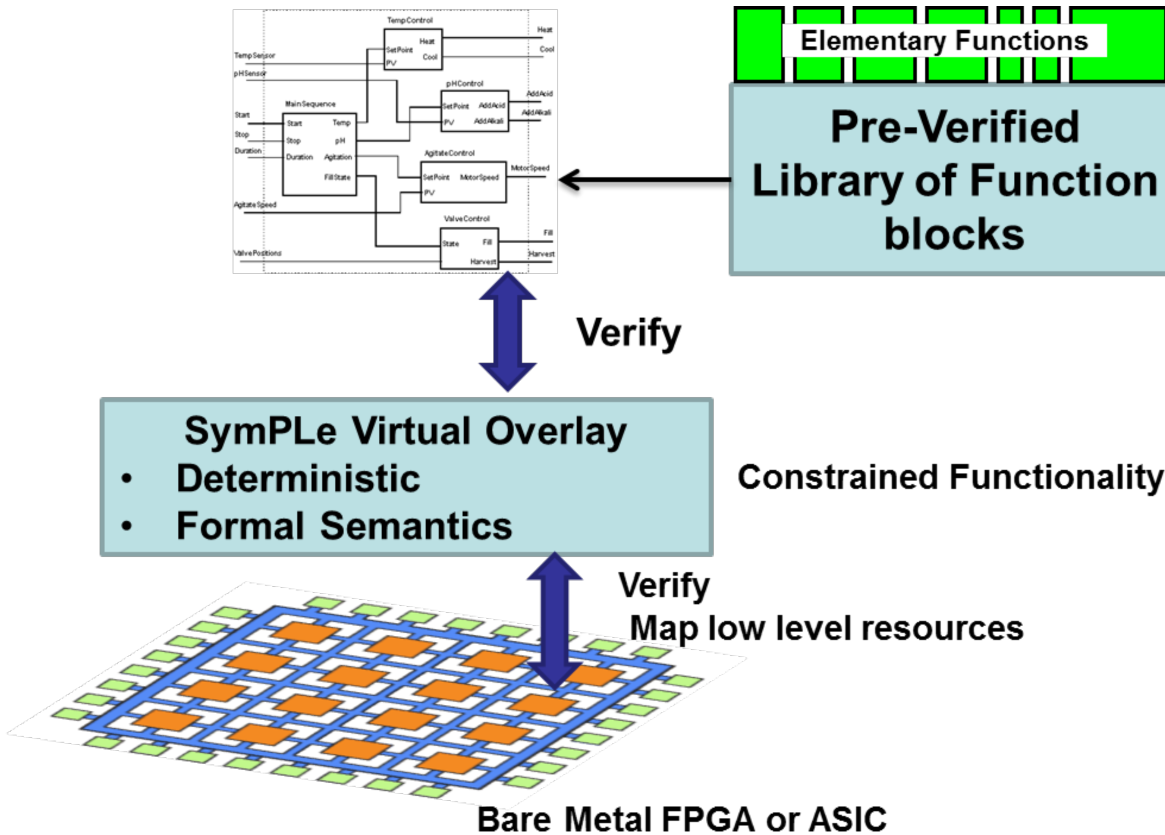
- **Identify or Develop Accessible Design/Verification & Validation Testing**
  - Milestone: M3CA-15-CA-EPRI-0703-024
  - Description: Establishes the tools and methods used provide V&V of the SymPLe designs
  - Outcome: Effective Methods and Tools for Architecture validation - Report

Research Perspective

- **<u>Premise</u>: Trend in NPP I&C migrating towards *SW intensive or SW based* digital I&C systems where software contributes essential influences to the design, implementation and evolution of the system.**
  - So called <u>*Change Enabled Systems and Technologies*</u>
    - **Increasing complexity and flexibility in SW intensive systems exacerbates manifestation of SW failures, cyber-vulnerabilities and SW Common Cause Failures (SCCF)**
    - **One example, a fielded commercial safety grade I&C system was found to have at least ~2000 SW functions, not including the application.**
- Fundamental position we pose is that I&C systems in the context of nuclear power **<u>may not need to be derivatives of software intensive systems</u>** 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.

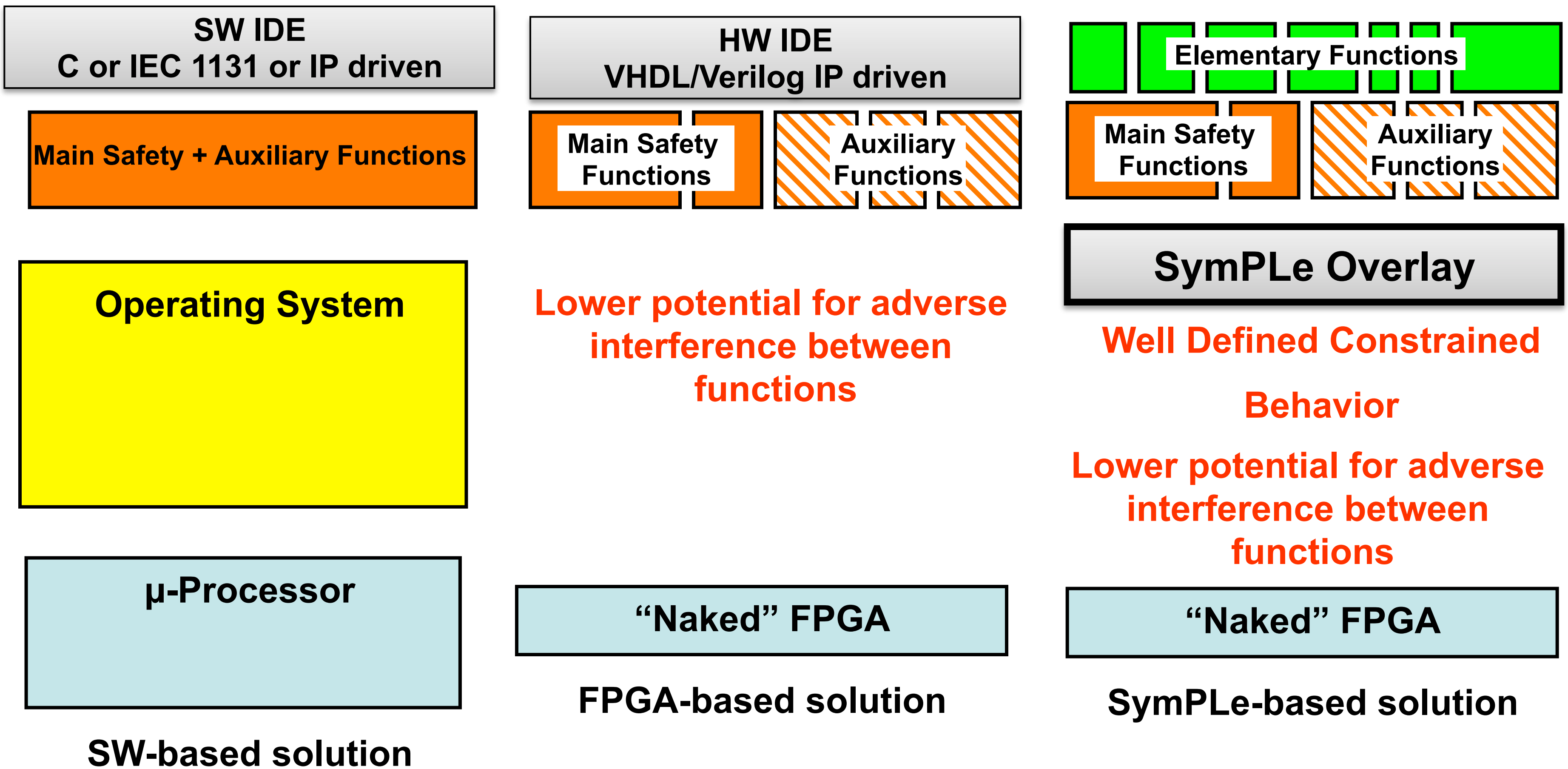
SymPLe Concept

- **SymPLe is an architectural concept that has it's foundations in:**
  - PLCs notational architectures (e.g. IEC 1131 and 11499)
  - FPGA overlay architectures or *FPGA Virtualization*.



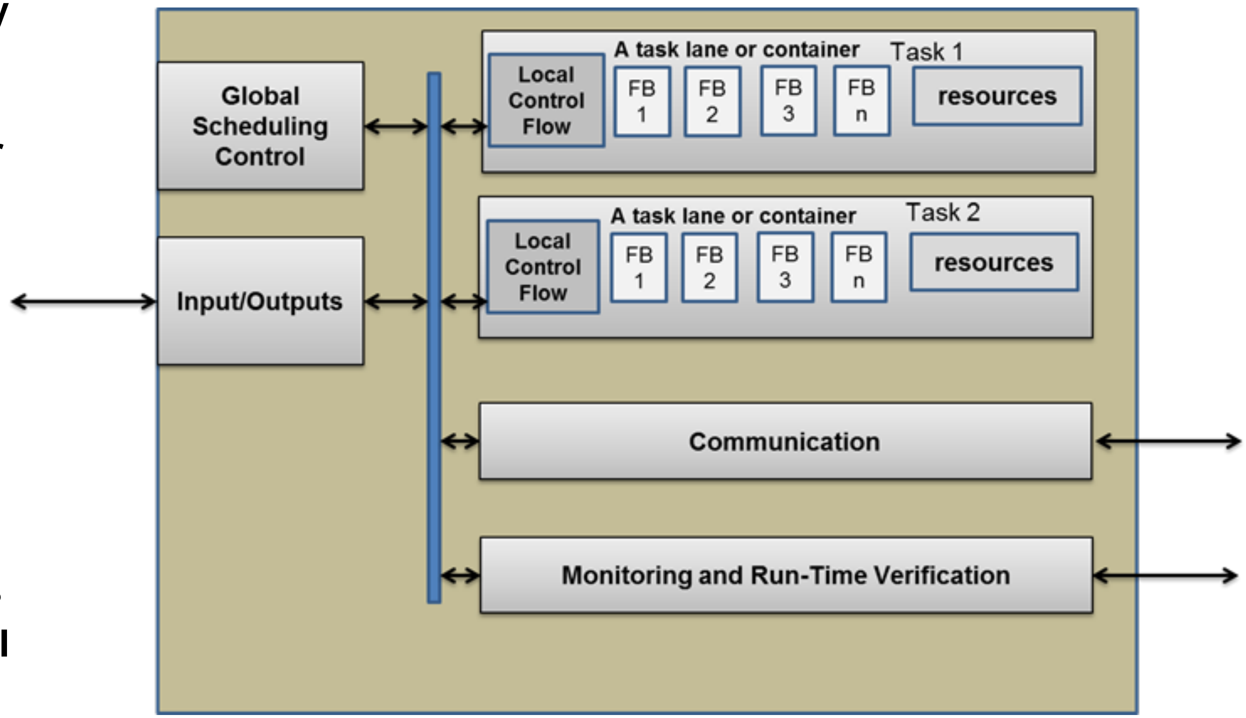
- **SymPLe is a *<u>virtual machine or overlay</u>* constraining functionality**
- **Formal verification of operational semantics**

SW vs. FPGA vs. SymPLe



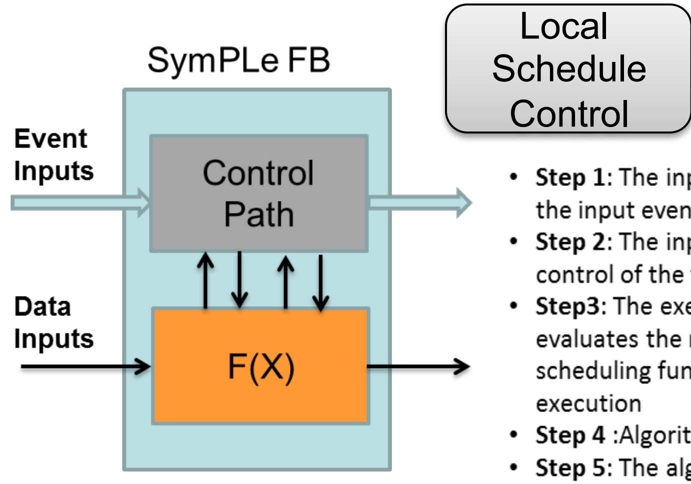
SymPLe Architectural Overlay

- **Function Blocks – elementary functions used to create safety I&C functions.**
- **Local Control-responsible for dispatching:**
  - the sequence of FB execution
  - marshaling inputs and outputs
  - and managing local state.
- **global controller - provides global coordination and synchronization of task lanes**
- **Runtime Verification – Formal checking of executions, I/O, and non-interference.**
- **True Concurrency between Lanes**



Function Block Architecture

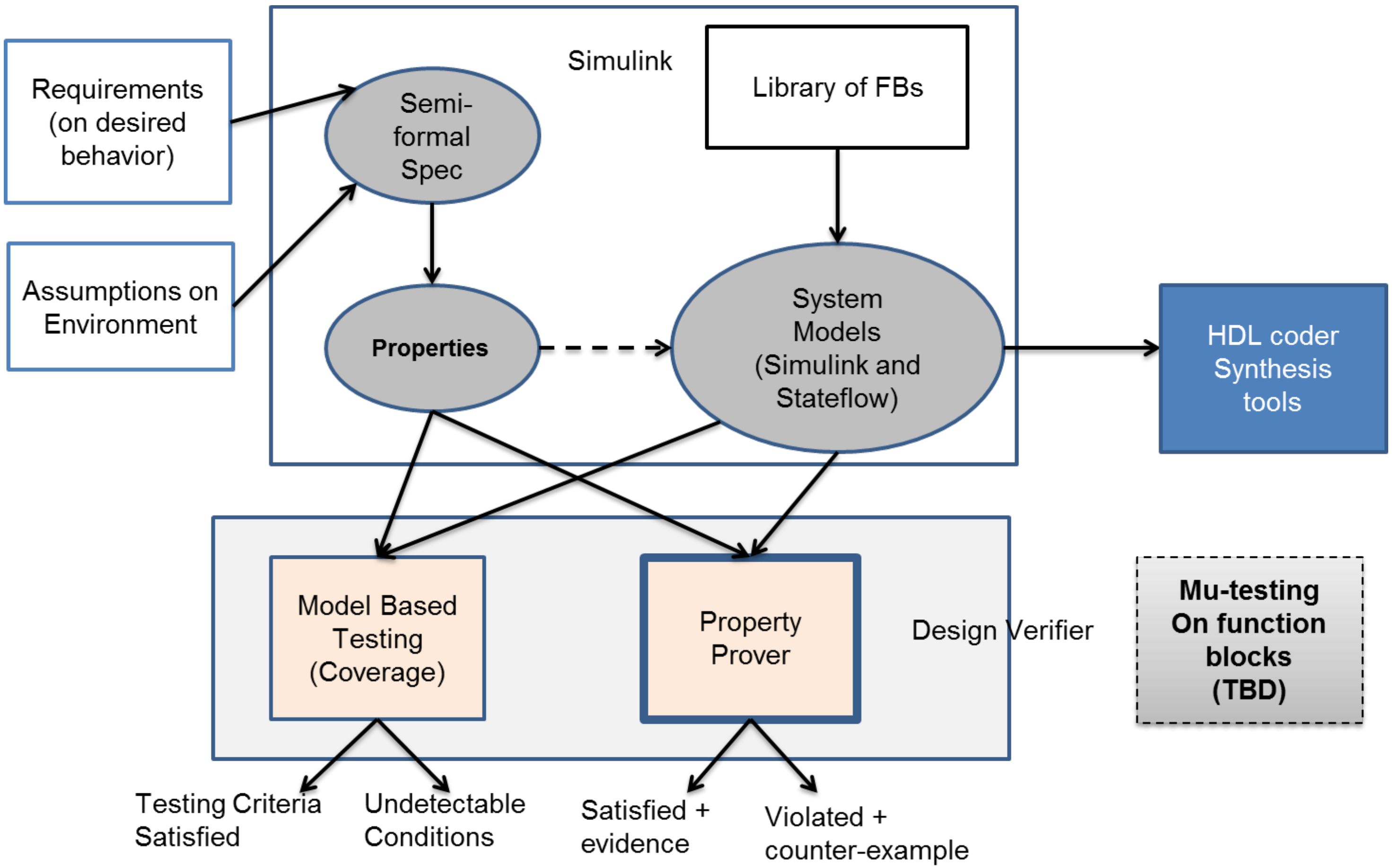
- **Common architecture for all SymPLe function blocks**
  - Separation of control and dataflow with clear and defined interconnections
  - Formal Semantics
  - Inspired by IEC-61499
- **SymPLe architecture variants differ in the control path of the generic function block**
  - Autonomous Function Block
  - Lite Function Block



- **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.

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

Composability of Function Block Diagrams: Verification Workflow



Abstract the formal domain with a verified library of operations and components (at various levels of abstraction and targeting specific 1131 types of FBS) from which designers can specify their designs.

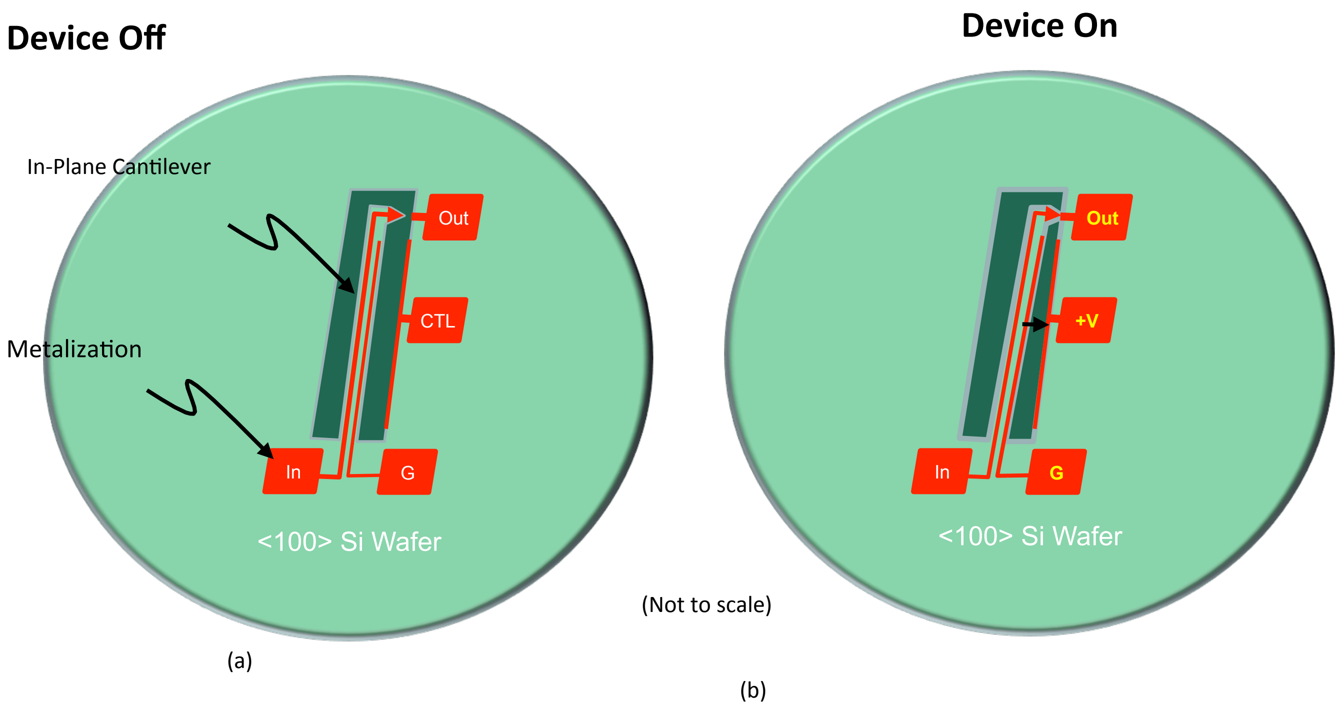
Project Overview: MEMs based Relays Tasks

- **Resilient In-Plane Silicon Micro-relays for NPP Applications**
- **Goal and Objectives**
  - Feasibility Study
    - Microfabrication considerations and process design
      - How do we build it?
  - Preliminary Process and Device Design
    - DRIE Process Development
      - High resolution, high aspect ratio patterning / etching technique
    - Analytical Modeling
      - Can we design relays with reasonable fabrication dimensions and operating characteristics?
- **Participants**
  - Dr. Gary M. Atkinson, Department of ECE, VCU School of Engineering
- **Schedule**
  - Micro-Technology Review / Selection (Fall 15)
  - Device Concepts and Analytical Model Development (Spr 16)
  - Process and Device Development (Sum 16)

MEMS Accomplishments

- **Milestones / Deliverables / Outcomes for FY 16**
  - Developed a new single wafer, in-plane, single crystal micro-relay device concept
    - Single crystal construction offers high reliability, reproducibility
  - Developed a new high resolution shadow mask fabrication technique
    - Simplifies the fabrication process
  - Developed a first order analytical modeling tool
    - Expected mechanical / electrostatic response of the proposed micro-relays
  - Designed a preliminary process flow
    - Shadow mask process flow using a new DRIE tool
    - Micro-Relay process flow using the high res shadow mask technique
  - Installed a new DRIE Etching System in the VCU Microelectronics Center
  - Developed a preliminary set of micro-relay device designs
    - Relay dimensions for fabrication of relays for a range of 24V – 300V

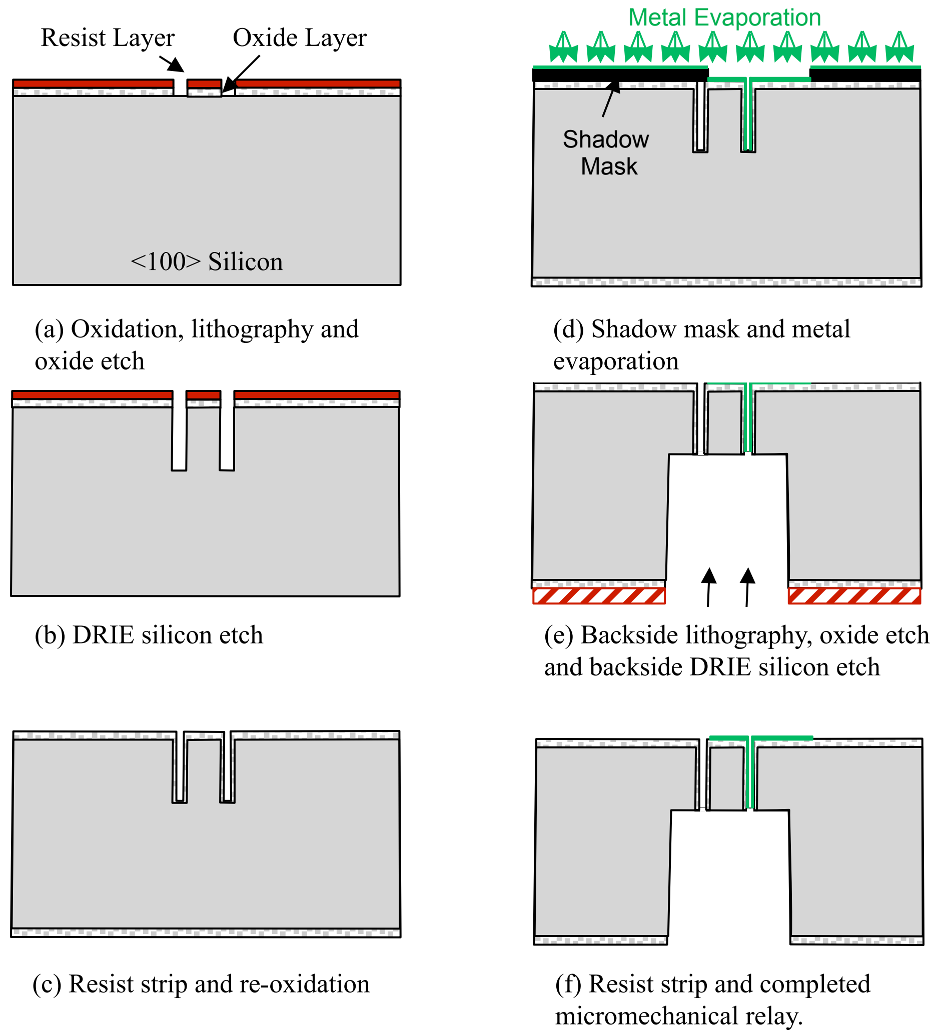
In-Plane Micromachined Si Relay



- **(a) Conceptual schematic of an in-plane micromechanical relay in the off or open position and (b) the micromechanical relay with a voltage applied in the closed position.**

In-plane silicon micro-machined relay fabrication process.

- **Single-Crystal Relay Components**
- **Single wafer construction**
- **New High Resolution Shadow Mask Technology**



(a) Oxidation, lithography and oxide etch

(b) DRIE silicon etch

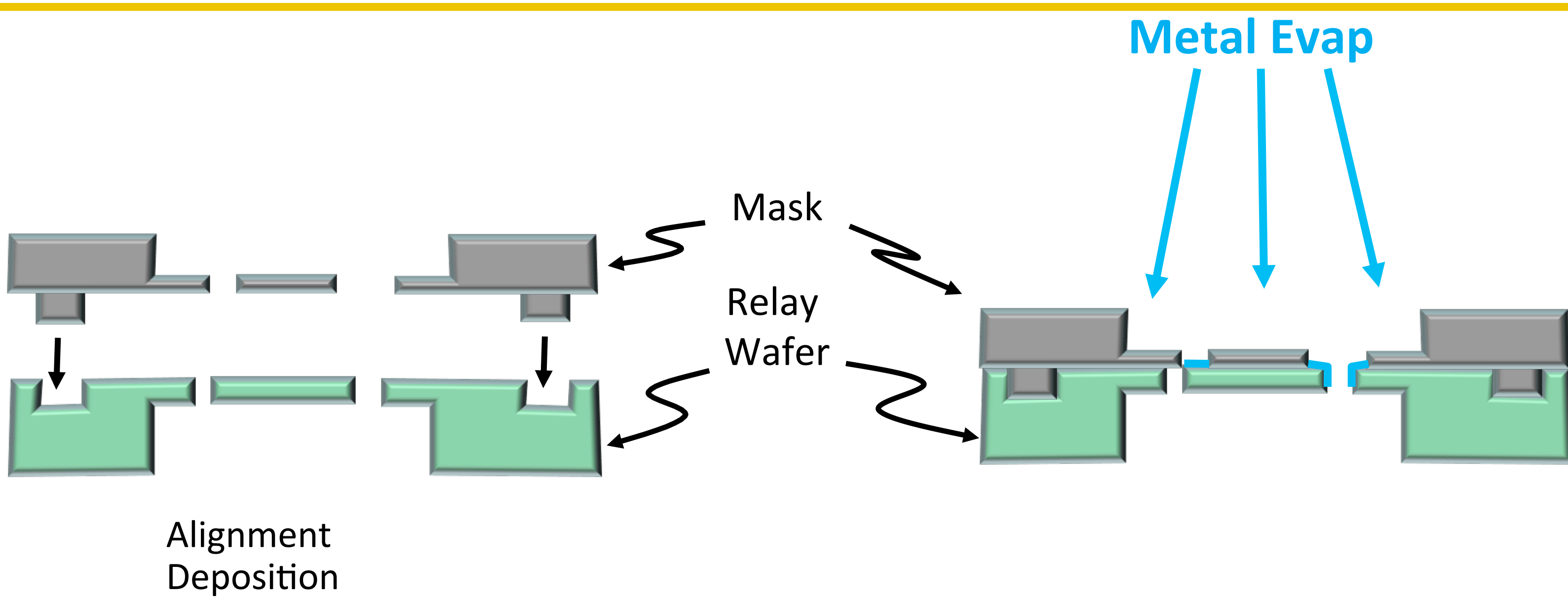
(c) Resist strip and re-oxidation

(d) Shadow mask and metal evaporation

(e) Backside lithography, oxide etch and backside DRIE silicon etch

(f) Resist strip and completed micromechanical relay.

High-Resolution Shadow Mask



- **High-Resolution Shadow Mask Technology being developed at VCU. The silicon shadow mask is fabricated from a standard silicon wafer using DRIE. The arrows show were the alignment posts and holes connect.**

Technology Impact

- ***The Micro-Relay technology being developed here offers a high reliability control system technology not subject traditional failure modes of microelectronic components***
  - *Radiation Tolerance, SW flaws, Malicious Coding /Hacking or EM Interference*
- ***Simple micro-relay control system are highly verifiable***
- ***The Micro-Relay technology can potentially be integrated with other microelectronic control circuitry for improved fault tolerance***
- ***The low-cost microfabrication provides lowers system cost, and allows additional fault tolerance / redundancy in nuclear control systems***
- ***The overall impact is to provide a control circuit technology that is immune to SCCF susceptibility and enhances verifiability***

MEMs Conclusion

- ***Developing a new micro-relay technology for application in the NE Industry***

- ***Developing a new fabrication process technology to simplify and lower the cost of relay fabrication***

- ***Currently have demonstrated that this technology appears feasible in terms of the microfabrication process technology required and the expected device performance.***

SymPLe Conclusions

- **Development of SymPle is a novel approach to I&C**
  - Emphasizes effective verifiability and transparency for classes of I&C functions, at the expense of more complex I&C functionality.
  - We have developed two variant SymPLe architecture models (in SimuLink) – evaluating tradeoffs now.
  - Library based verification approaches and strategies are being evaluated
  - SymPLe formal operational semantics (well-formedness conditions) derived.
  - Functionally complete set of 25 generic function blocks - some FB properties proven
  - EPRI Emergency Diesel Generator specification being used as application driver.
- **Effective methods and tools for architecture validation**
  - Several tools and methods evaluated (Model checkers → theorem Provers)
  - MathWorks SimuLink tool chain and DV selected for initial design and verification environment

Questions?

Application Domain of SymPLe

- **Assumption: A separation of concerns – Simple I&C versus Complex I&C.**
  - A significant portion of NPP I&C functions are not computationally or algorithmically complex.
  - Typically characterized by logic, comparison, conversions, simple control flow, timing, arithmetic – Elementary IEC 1131 functions..
- **SymPLe is targeted for I&C functions that <u>do not</u> require complex processing resources (DSPs, high performance CPUs)**
- **<u>Not SymPLe</u>: Communication Protocol chips (Profibus), HMI(Graphic processing GPUs), database engines, heuristics engines, etc…**

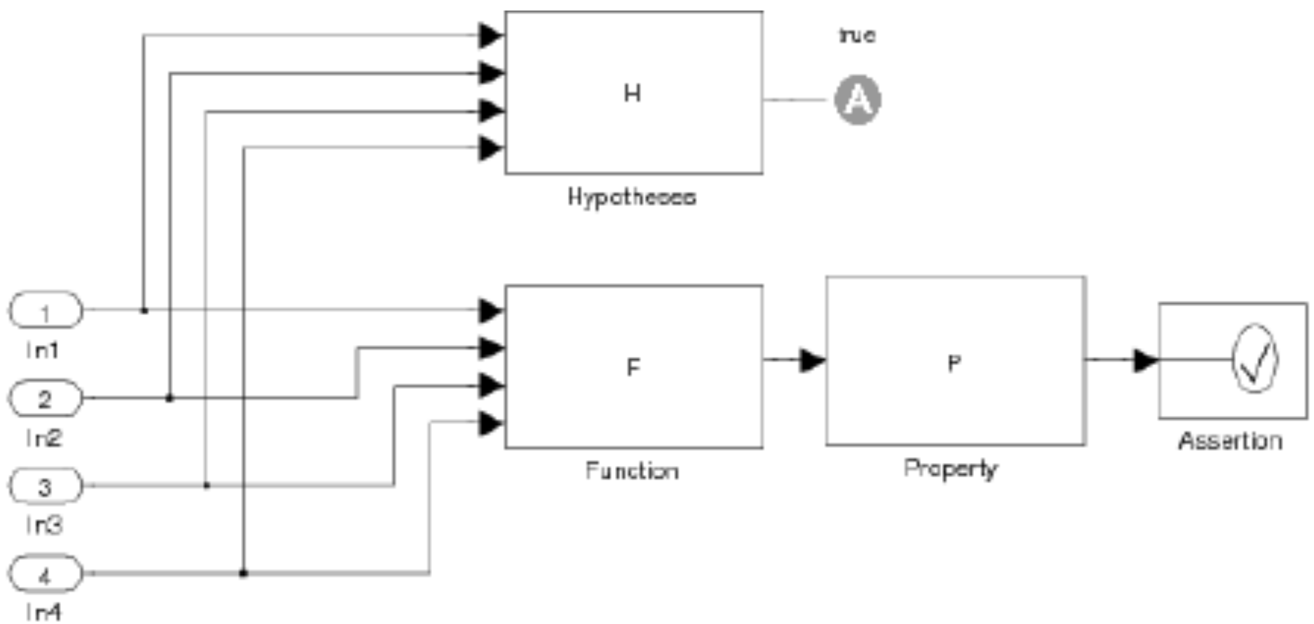
U.S. DEPARTMENT OF ENERGY

Nuclear Energy

Function Blocks Verification

- **Example of Property Verification using MathWorks Design Verifier**

General Proof Structure

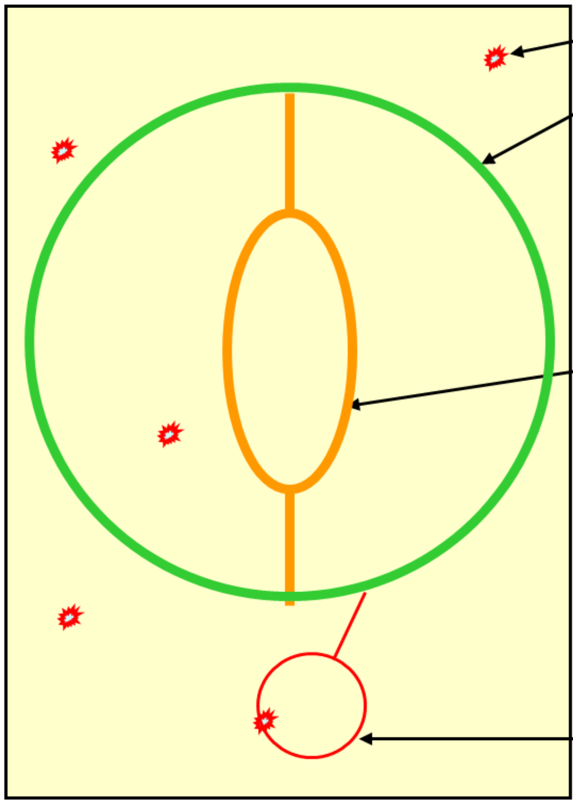


All proof obligations and counter-examples are exported as reports and traces to support "evidence" based verification.

Problem Perspective

Software Driven Architectures

Cyclic Behavior with Non-Deterministic Characteristics



Complete domain of behavior
May contain residual digital faults

Path exercised continuously in normal situations
Influence factors during continuous operation:
- normal process inputs (validated before use)
- short-term memory (as little as possible)
- clock interrupts (thorough verification)
- *(process-related interrupts: none)*
- *(resource management: static)*

Path exercised in occasional but tested situations
Influence factors that could disrupt cyclic behavior:
- initialization (only once)
- operator requests (single channel)
- hardware failures (single channel)
- exceptions (very simple)
- *(particular dates & times: avoided)*
- plant transients: affect all channels

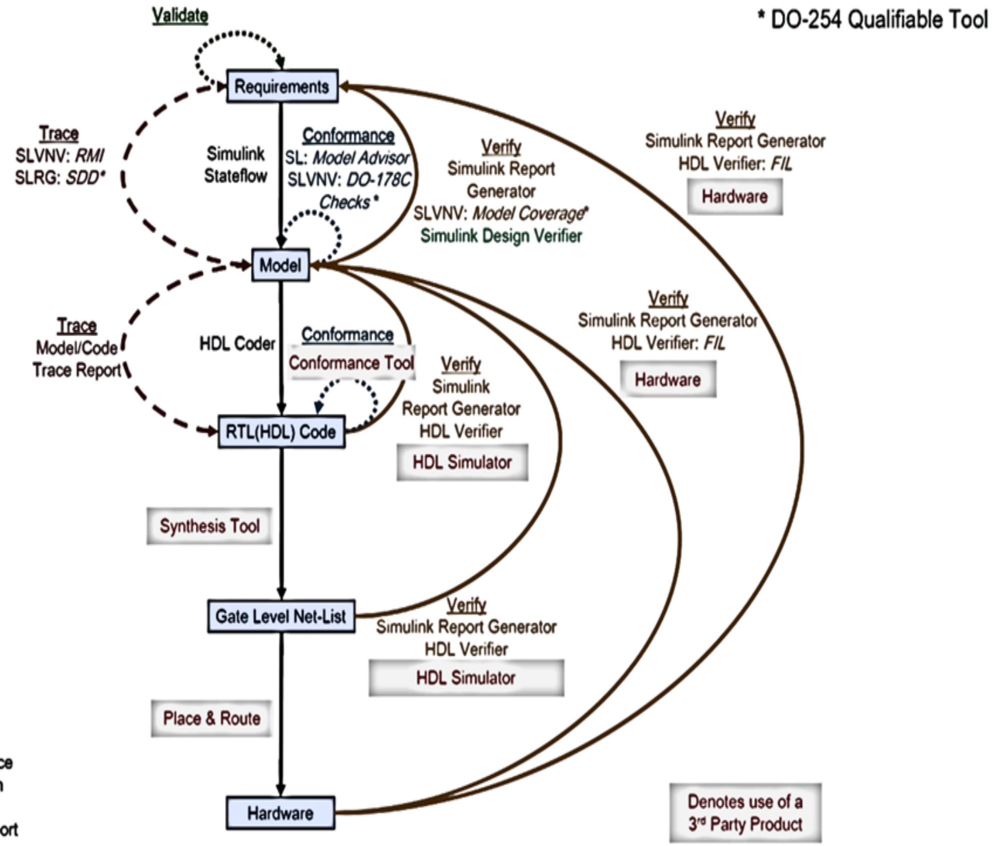
Path exercised in unanticipated or untested situations

System *constrained* to well-understood and tested trajectories

Formal Verification: Mathworks Simulink Design Verifier

- Unlike other formal verification tools, works directly on the Simulink models..not an abstract specification or abstract model.
- Possible to automate the proof integration process. Easier for Engineers to use.
- Downside: Requires careful development of model/proof strategies – else state explosion…

Work Flow and Traceability



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

Office Of Nuclear Energy Sensors and Instrumentation Annual Review Meeting

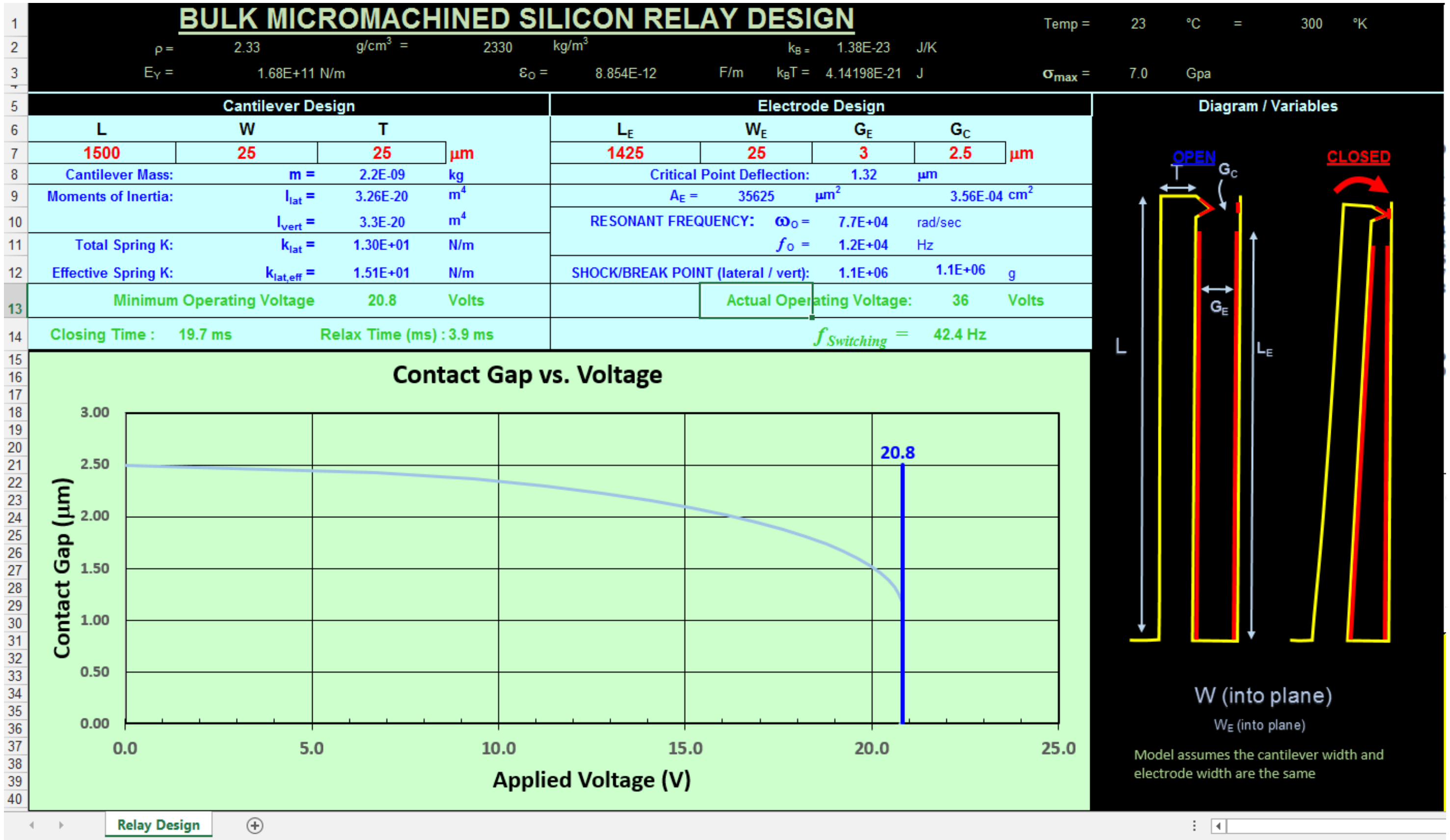
Resilent In-Plane Silicon Microrelays for NPP Applications

Gary M. Atkinson
Virginia Commonwealth University

Nuclear Qualification Demonstration Of a Cost Effective Common Cause Failure Mitigation in Embedded Digital Devices

October 12-13, 2016

Analytical Modeling Tool



■ **Screen shot of the silicon relay modeling tool using first order analytical models. The chart shows the contact gap at the end of the cantilever vs. voltage, with a marker at the instability point where it closes.**