SAND2013-4159C

Digital Systems Analysis for Assessing Trust of Critical Information Systems

Joe Ruthruff

Computer & Information Sciences External Review Panel
Sandia National Laboratories

May 22, 2013

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

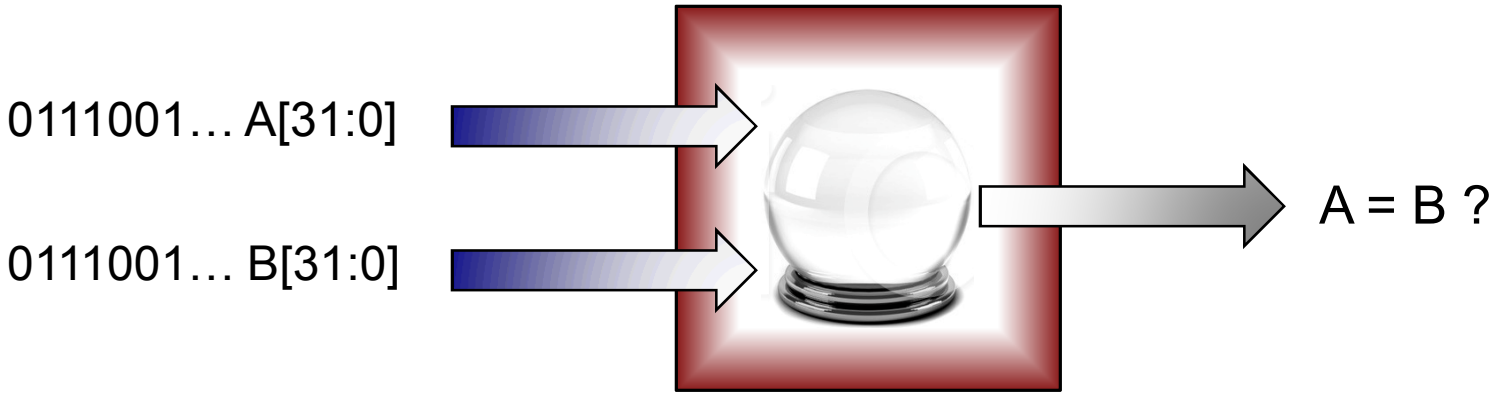
NNSA National Nuclear Security Administration

Sandia National Laboratories

Problem Space

Information Systems are Digital Systems, and Verifying Digital Systems is Intractable

- **Inherent limitations of simulation:**



- **How long is needed to exhaustively verify this using simulation?**
  - **2^{64} input vectors x 1 nanosecond per evaluation = more than 580 years**

- **A digital design with 300 state variables has more possible states than the number of protons in the universe (10^{80})**

?>

Sandia National Laboratories

Why is it Hard to "Trust" an Information System in a Cyber Security Context?

Answer: Cyber Security Is Especially Asymmetric

- **Developer, user, *and attacker* cannot predict where vulnerabilities are (undecidable)**
  - **But, even one vulnerability can compromise an entire system (asymmetry)**
- **Worse, attackers in control of design specifications have knowledge**
  - **Even worse, attackers with system access (e.g., supply chain) may plant a vulnerability**
- **For trusted information systems:**
  - **Strict operational requirements exacerbate issues**
  - **Situational awareness strains mitigation strategies**
  - **Supply chain causes increased risk**

CIS Strategic Plan: Demonstrate a Basis for Assessing Trust in Information Systems

Assertion of this work: Any solution must navigate the asymmetric cyber security challenges in the context of information systems

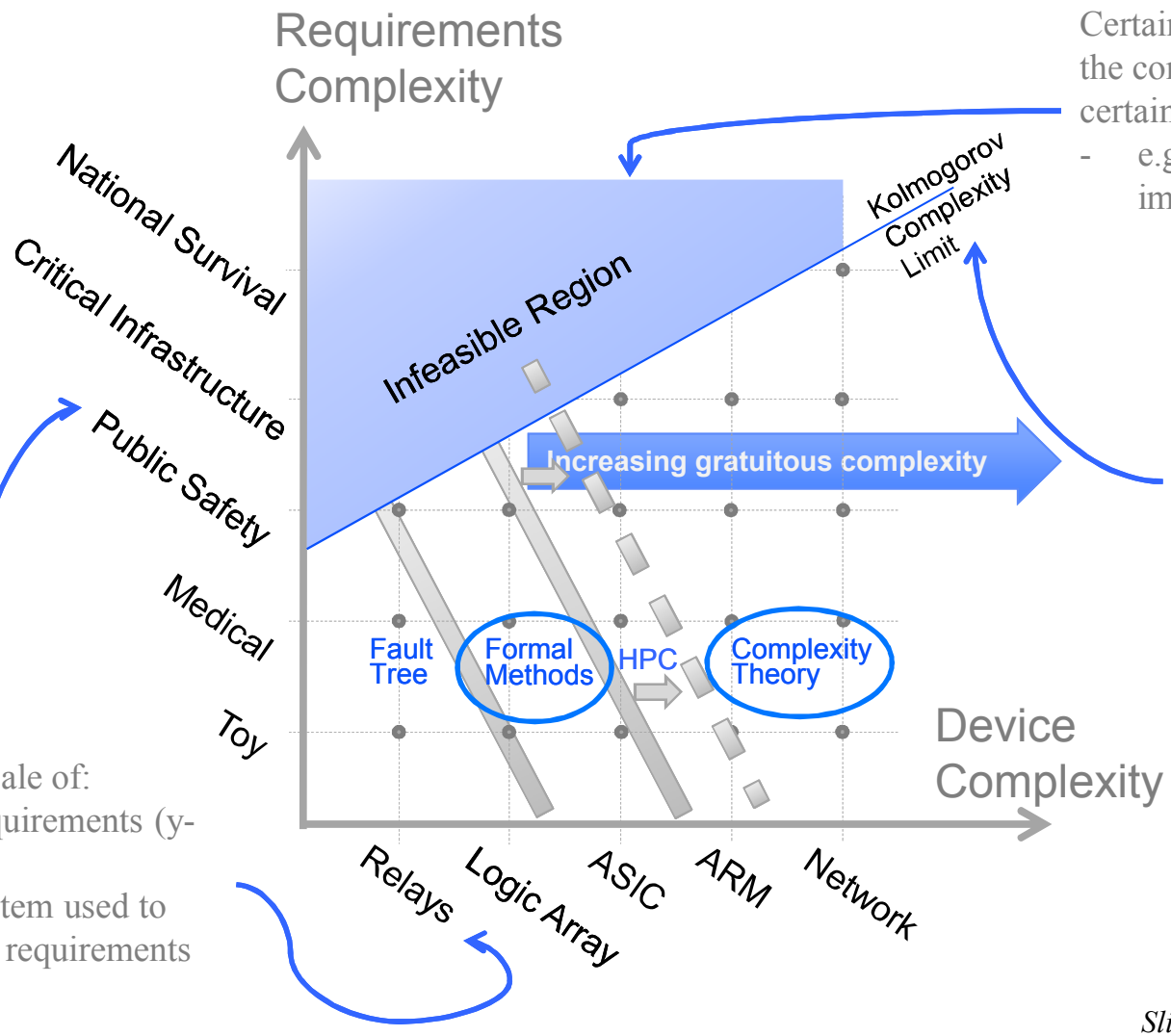
- **Embracing Asymmetry:**
  - **Need to guard against vulnerabilities everywhere? Then search everywhere.**
  - **(Yes, I just said this is intractable for digital systems in general.)**

- **Ameliorate Knowledge or Access by Adversaries:**
  - **Worried about an unwanted behavior? Then:**
    - **Mathematically prove your system cannot do that, or**
    - **Assess and quantify risk probabilistically.**

Formal Verification and Complex Systems Analysis

One Part of the Necessary Solution Space

Methods and Tradeoffs for Analyzing and Establishing Trust in Information Systems



Certain devices inherently lack the complexity needed for certain tasks

- e.g., a relay cannot implement a power grid

A device needs only a given amount of design complexity to implement a set of requirements

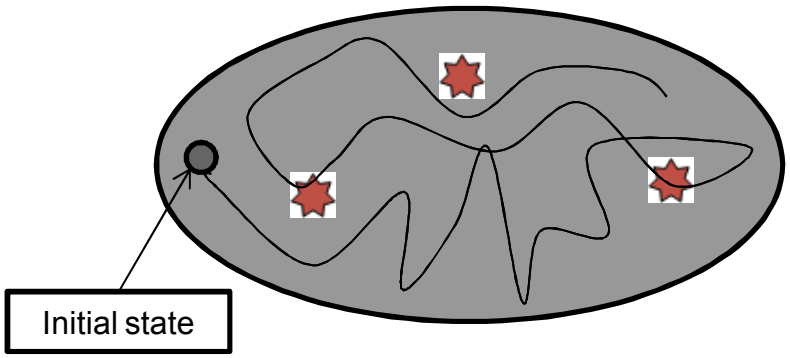
Logarithmic scale of:

- System requirements (y-axis)
- Device/system used to implement requirements (x-axis)

Comparing Solutions to This Problem Space

- **Testing and simulation**
  - **Historical ties with ASC/V&V**

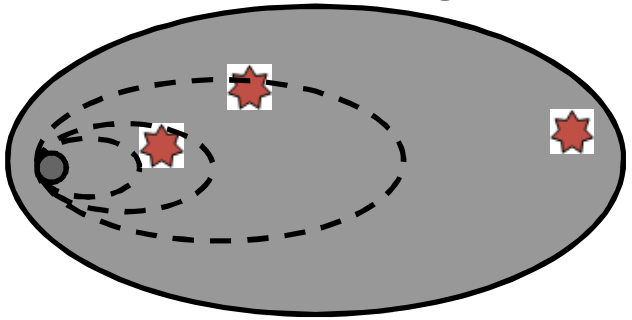
- **Not exhaustive**



- **Ensures function (for provided stimulus)**
  - **Does not ensure absence of failure!**
- **Does not scale to digital state spaces**
  - **Individual depth-first paths**

- **Formal verification**
  - **Analyzes mathematical models**

- **Complete coverage**



- **Ensures correct function for all stimuli**
  - **Can ensure absence of specific failures**
- **Scales to modest digital state spaces**
  - **Exhaustively breadth-first**

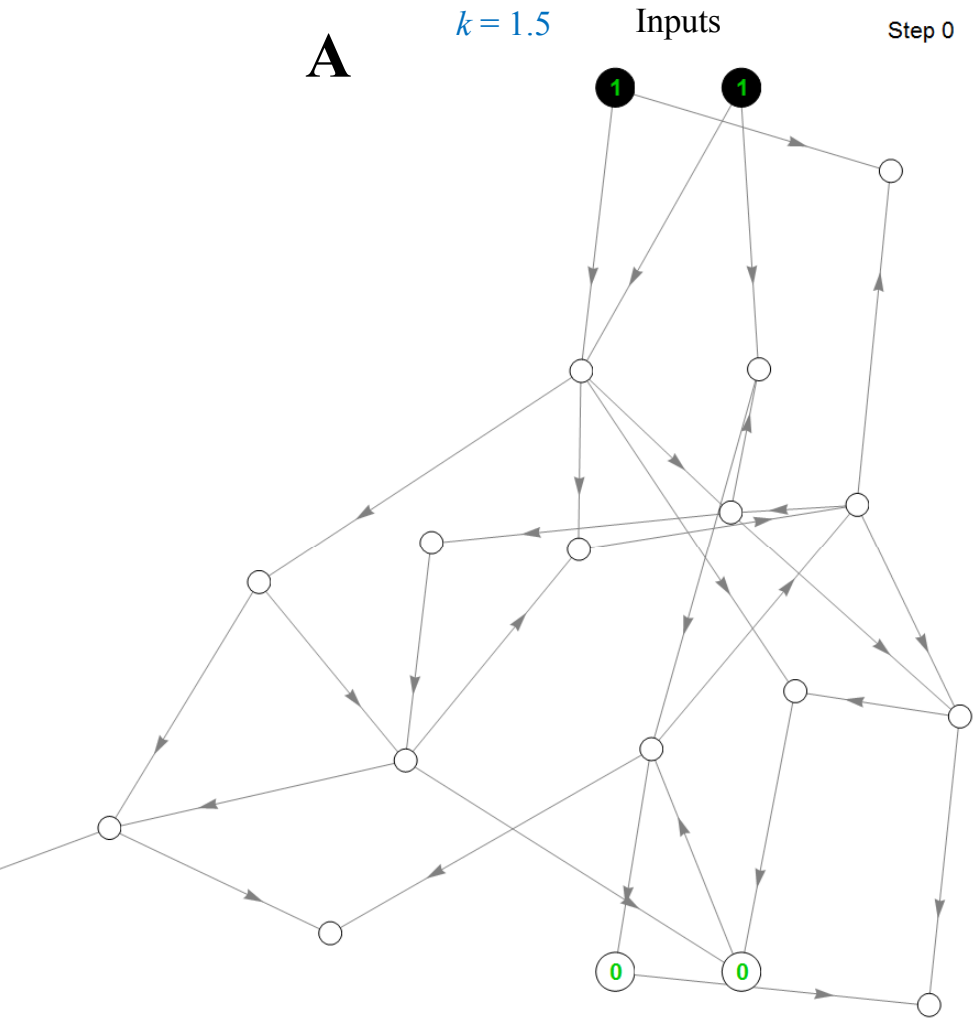
What Formal Methods Can Mean For Trusted Information Systems

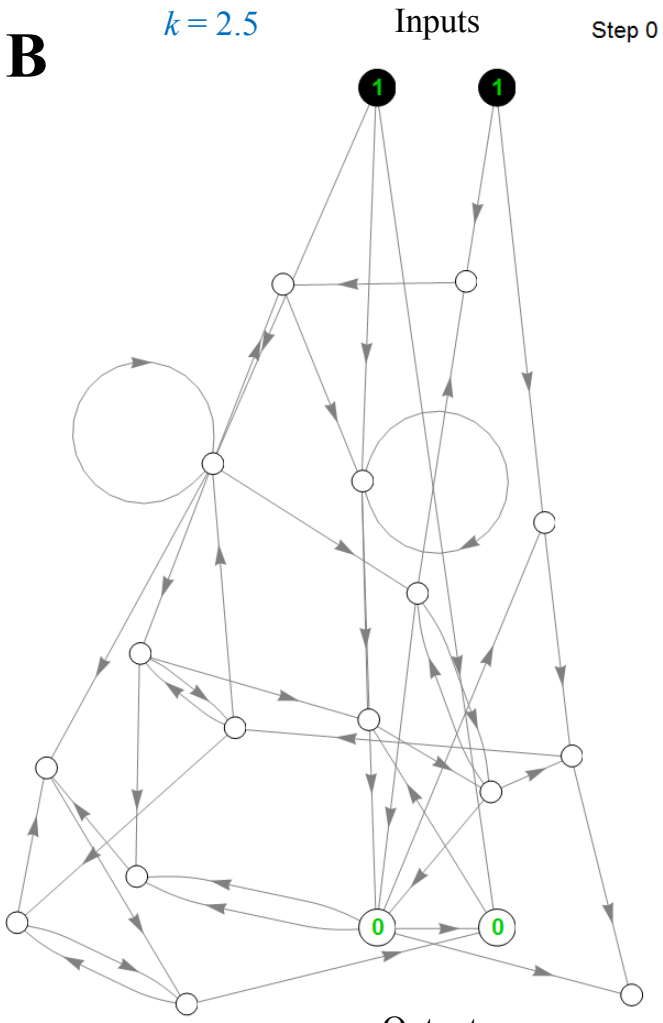
- Mathematically prove certain properties are built into system…
  - … or can never be performed by a system
- Computationally ensure those properties exist everywhere…
  - … or no where at all

- For trusted information systems, this means:
  - Trust properties can be mathematically verified

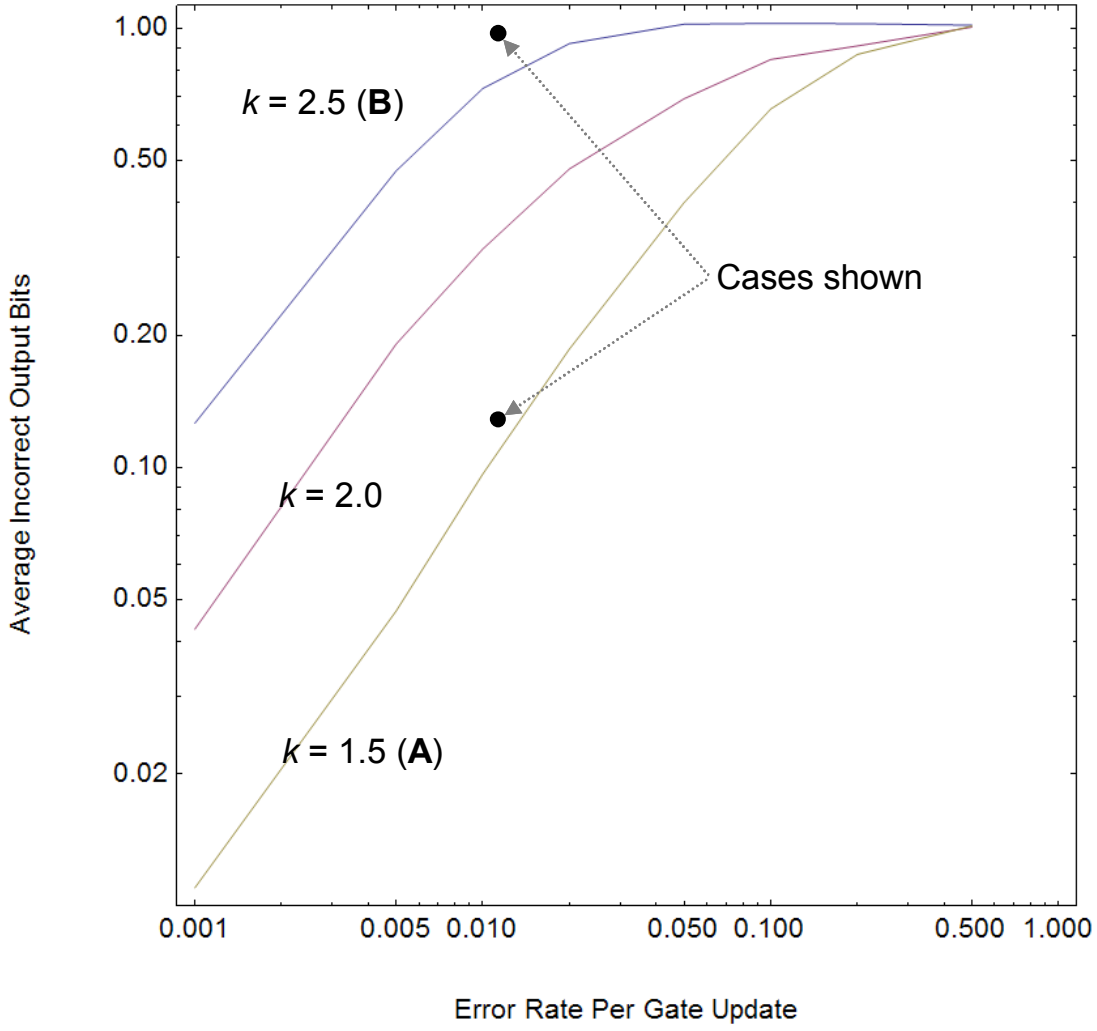
"Trust, but Verify."

Motivating Example: Probabilistic Bit-errors in a Trusted Digital Circuit





Complex Systems Analysis: Probabilistic Analysis of Emergent Behavior in a System



- **Results for these half-adder circuits could be obtained by brute-force simulation**
  - Can you wait a really long time?
- **Complex system analysis enables probabilistically assessment of rare cascading failures**
  - **Applicable to designs too large for verification**
  - **Quantify various properties for trusted information systems**

Sandia National Laboratories

Research Applications in Computing and Information Sciences at Sandia

Outside World is Not Sufficiently Directing its Work at Trusted Information Systems

- Formal methods increasingly common place in industry, academia

- What the outside parties do:
  - Verify reliability
- What they don't do much of:
  - Verify security
  - Assess trust in engineering
  - Address complex scenarios (e.g., situational awareness, cascading failures)

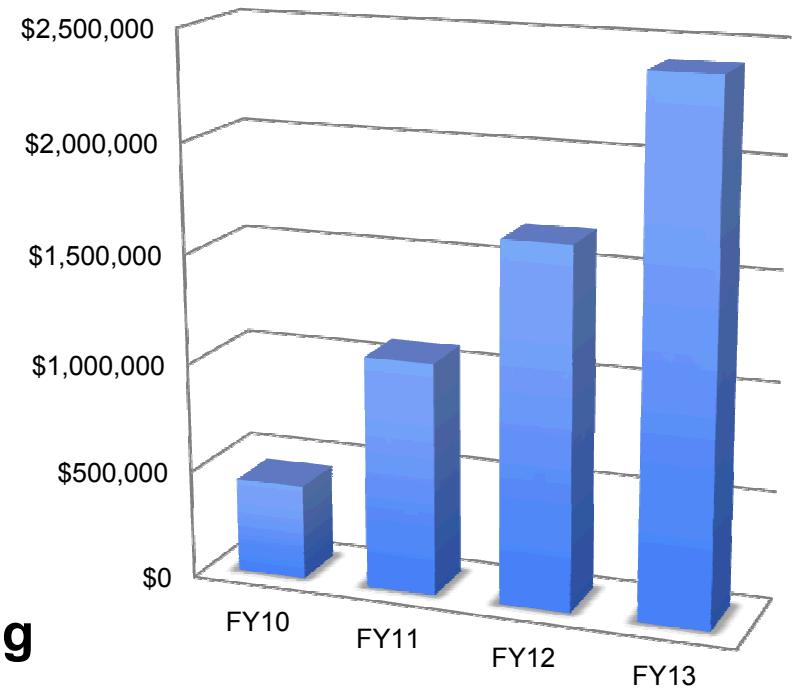
- Complex systems theory has been sparingly applied to engineered digital systems

- Sandia is uniquely capable of impacting this area

Sandia Investments in Research Capabilities

- **Research – Over $5 million thru last four FYs, including:**
  - **ASC CSRF/CSAR: ~$2.7M, FY10-13**
  - **Cyber S&T LDRD: ~$1.5M, FY11-13**
  - **Early Career LDRD: ~$850K, FY11-13**
- **Building capability, particularly with applications to security problems and engineered trust**
- **Increasing scalability, seeking to leverage high-performance computing**
- **Current contributing staff:**
  - **15 staff in 8900, 2 staff in 1400**
  - **3 staff in other centers**

Total Research Funding

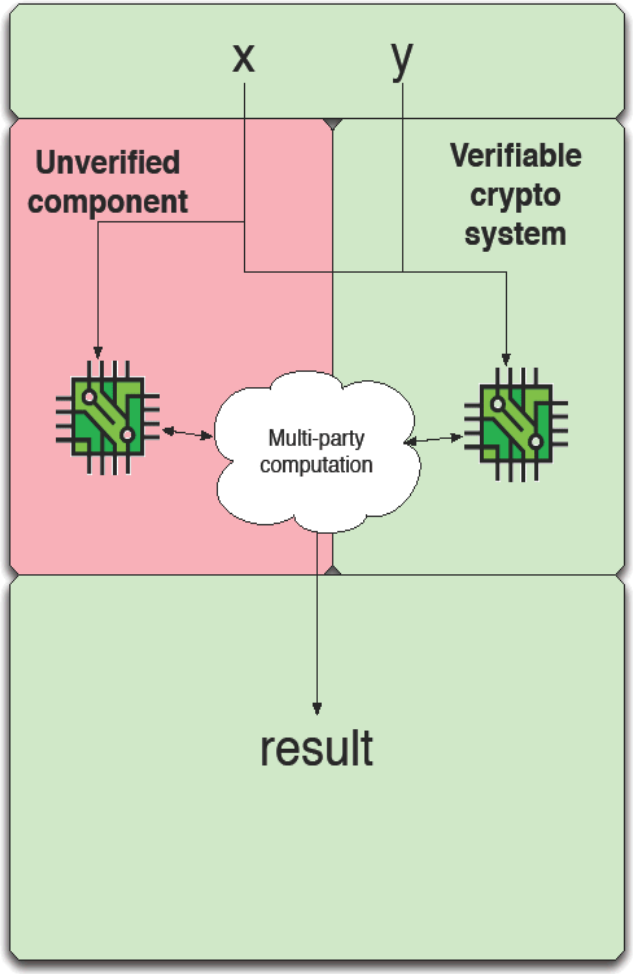


	FY10	FY11	FY12	FY13
Total Funding	$435,000	$1,070,000	$1,650,000	$2,405,000

Sandia National Laboratories

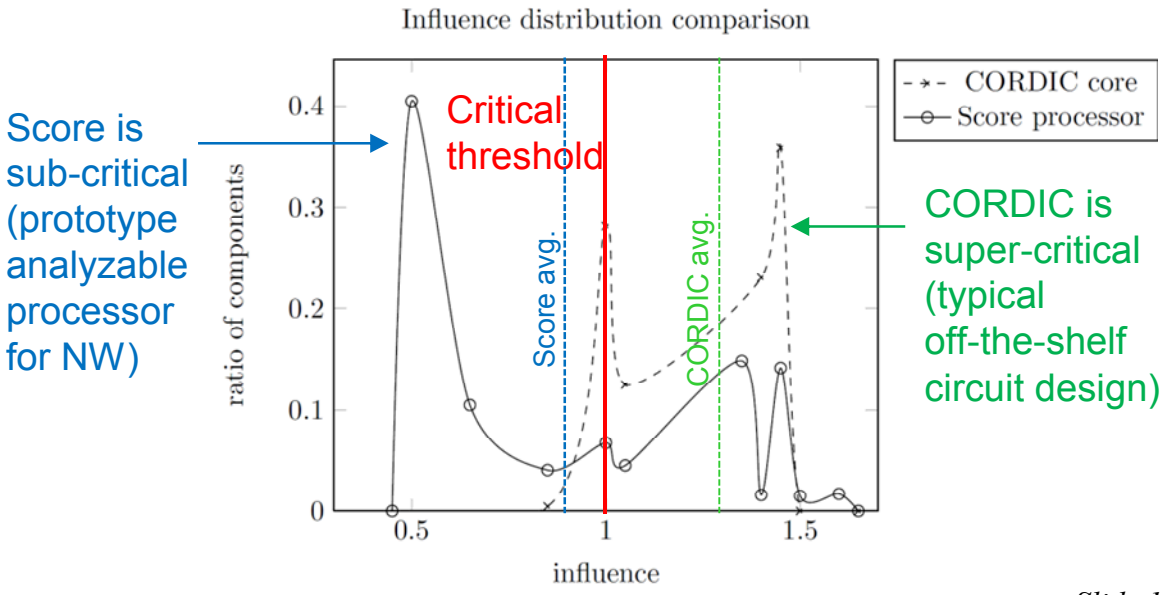
Framework for Designing Trusted Systems from Untrusted Components

- **Secure Multi-party Computation**
  - Cryptographic scheme allowing multiple parties to jointly evaluate a function without revealing individual inputs
- **Key Concept:**
  - Incorporate MPC into untrusted operation/functionality
  - System designer has full knowledge of inputs: untrusted and (trusted) MPC components
  - Cryptographically verify component output to detect subversion attempts



Complexity Analysis Provides Insight on Real-world Circuits

- "Influence" measure is a more precise generalization of "inputs per node"
  - If Avg. Influence > 1 (super-critical), network is unstable
  - If Avg. Influence < 1 (sub-critical), network is stable
- Example: Score processor shows signs of enhanced resilience – consistent with its goals of analyzability and predictability



Sandia National Laboratories

Summary of Digital Systems Analysis Research at Sandia

- Sandia has active and growing R&D in this area
  - Building new capability
  - Increasing existing scalability
- Increasingly active presence in research community
- Key capability for analyzing and verifying trust properties in information systems

- R. C. Armstrong, J. R. Mayo. Leveraging Complexity in Software for Cybersecurity. Conference Paper, Cyber Security and Information Intelligence Research Workshop, 2009.
- C. Seshadhri, Y. Vorobeychik, J. R. Mayo, R. C. Armstrong, J. R. Ruthruff. Influence and Dynamic Behavior in Random Boolean Networks. Physical Review Letters 107:108701, 2011.
- Y. Vorobeychik, J. R. Mayo, R. C. Armstrong, J. R. Ruthruff. Noncooperatively Optimized Tolerance: Decentralized Strategic Optimization in Complex Systems. Physical Review Letters 107:108702, 2011.
- J. R. Mayo, R. C. Armstrong. Tradeoffs in Targeted Fuzzing of Cyber Systems by Defenders and Attackers. Conference Paper, Cyber Security and Information Intelligence Research Workshop, 2011.
- J. Letchford, Y. Vorobeychik. Computing Optimal Security Strategies in Networked Domains: A Cost-Benefit Approach. Conference Paper, International Conference on Autonomous Agents and Multiagent Systems, 2012.
- J. Letchford, Y. Vorobeychik. Optimal Interdiction of Attack Plans. Conference Paper, to appear in International Conference on Autonomous Agents and Multiagent Systems, 2013.
- A. Smith, Y. Vorobeychik, J. Letchford. Multi-Defender Security Games on Networks. Conference Paper, to appear in Workshop on Pricing and Incentives in Networks and Systems, 2013.

- 7 separate Sandia Technical Reports between 2008-2013
- 5 separate invited presentations between 2009-2013

Acknowledgments (8900 and 1400 in color)

- **Contributing Technical Staff:**
  - Ben Allen (8961), Rob Armstrong (8961), Bob Carr (1465), Richard Chen (8954), Fred Chyan (8135), Sesh Comandur (8966), Brian Gestner (8136), Yalin Hu (8136), Geoff Hulette (8961), Kevin Hulin (8136), Akshat Kumar (8961), Jacques Kvam (8229), Jackson Mayo (8953), Cindy Phillips (1465), Ratish Punnoose (8229), Joe Ruthruff (8954), Andrew Smith (8953), John Solis (8961), Eugene Vorobeychik (8953), Matthew Wong (8953)

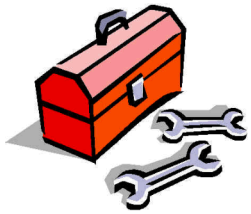
- **Program Sponsors (S&T and Application):**
  - Robert Clay (8953), Bruce Hendrickson (1420), David Womble (1540)
  - Bill Hart (1464)
  - Phil Bryson (8242)
- **Other Notable Senior Management Champions:**
  - Jim Costa (8950), Mary Gonzales (8250), Mike Hardwick (8240), Bob Hutchinson (8960)

Supplemental Slides

Tiers of Formal Methods

- **Mathematically-based techniques to specify, verify, and design digital systems (hardware and software) using abstract models**
  - **Prove properties about systems ("it does what I want, when I want")**

- **Tier 0: System specification**
  - **Building formal models reveals inconsistencies, ambiguities, incompleteness**

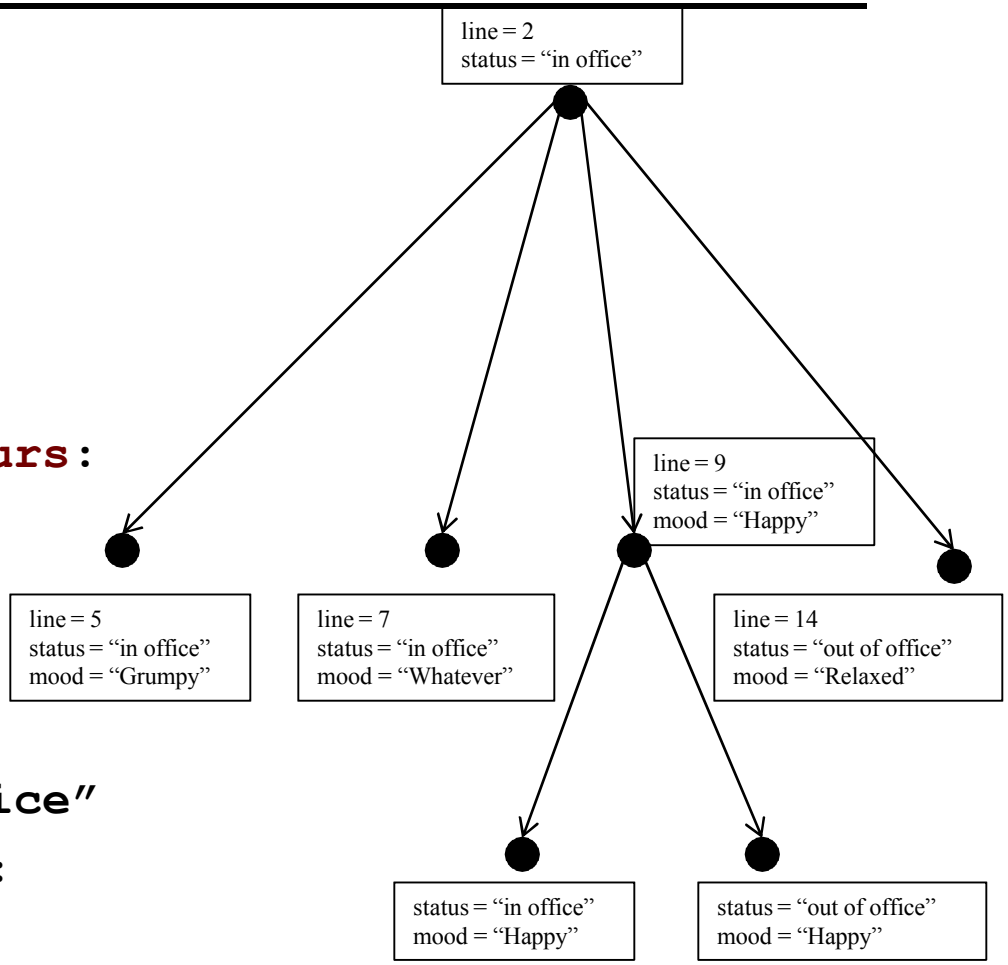


- **Tier 1: Proofs by Exhaustive Analysis**
  - **Using tools to exhaustively explore a model**
- **Tier 2: Fully formal machine-checked proofs**
  - **A human creates a mathematical proof using a tool**

- **Tier 3: Design and implementation**
  - **Create provably correct systems from models**

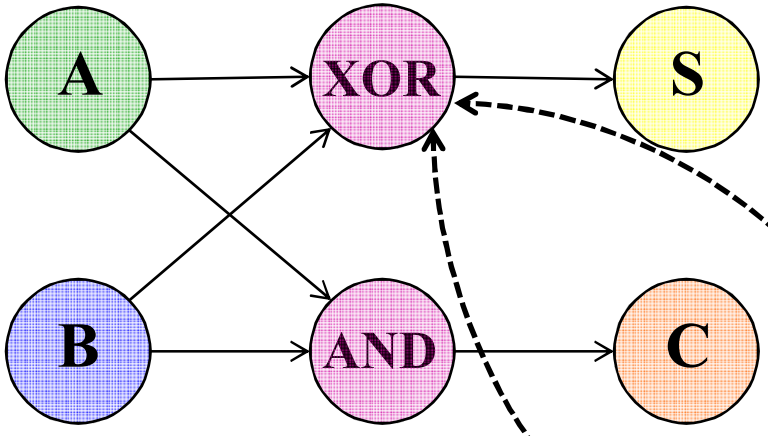
Mapping State Spaces in Software Designs

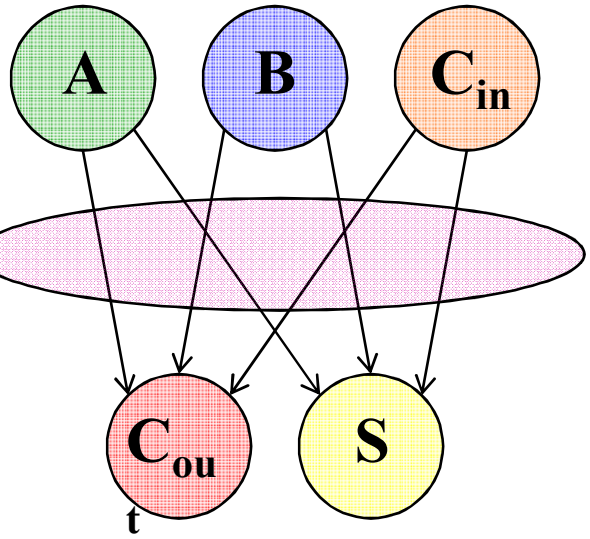
```
1.  Function WhatDayIsToday?:
2.     status = "In Office"
3.
4.     if Today is Monday:
5.        mood = "Grumpy"
6.     else if Today is Tues-Thurs:
7.        mood = "Whatever"
8.     else if Today is Friday:
9.        mood = "Happy"
10.       if Schedule is 9/80:
11.          status = "Out of Office"
12.    else if Today is Weekend:
13.       mood = "Relaxed"
14.       status = "Out of Office"
```

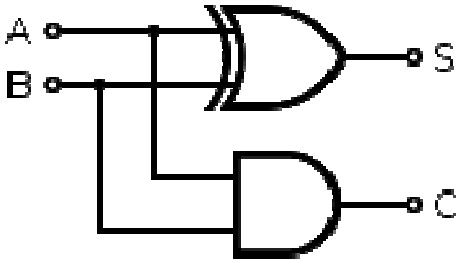


Sandia National Laboratories

State Diagrams for Hardware Designs

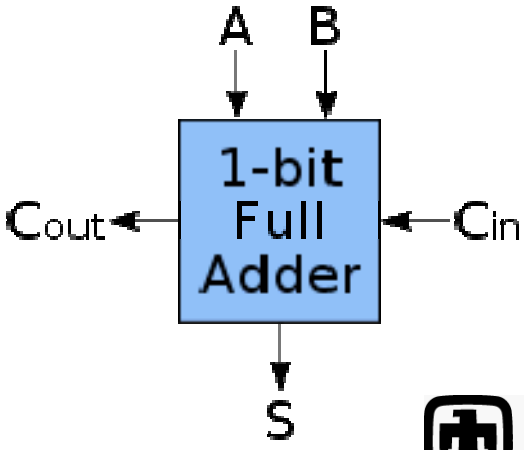




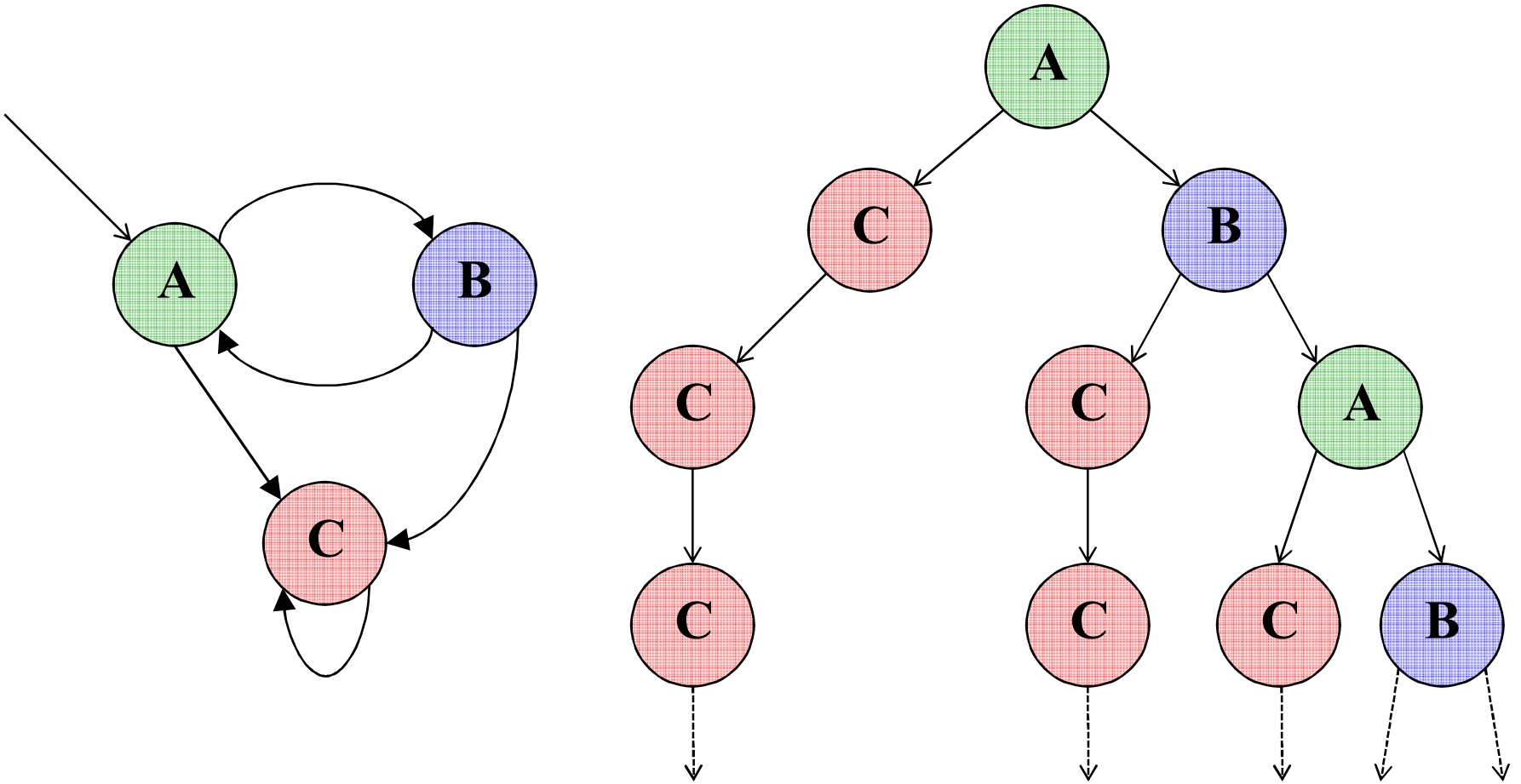


Operations Present

Operations Abstracted Away



Unrolling State Transition Diagrams



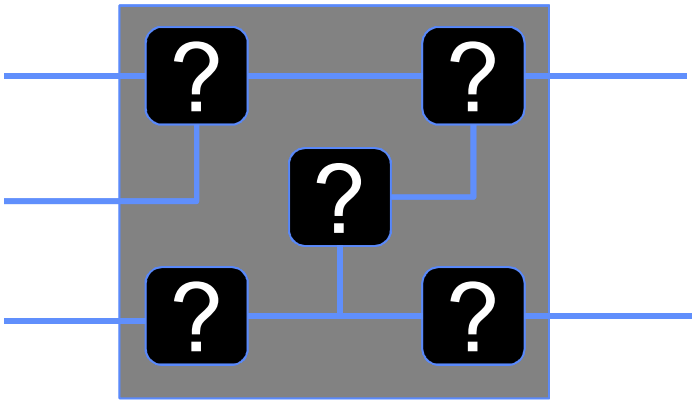
Complexity theory can address system-level resilience

- **Resilience of a digital model to bit errors:**
  - Characterized via growth or damping of perturbations
  - Bit errors can represent breakdown of digital idealization, or effect of untested states within the digital space
  - Networks transition from quiescent (stable) to chaotic (unstable) based on connectivity and transfer functions
- **Next slide shows simple example using half-adders**
  - Cascading errors are outlined in red
- **Circuit A has much less error in final output (greater resilience) than circuit B**
  - Here, average inputs per node (*k*) makes the difference
- **We have applied such metrics in realistic NW circuits**

Building Secure Designs from Black-box Components

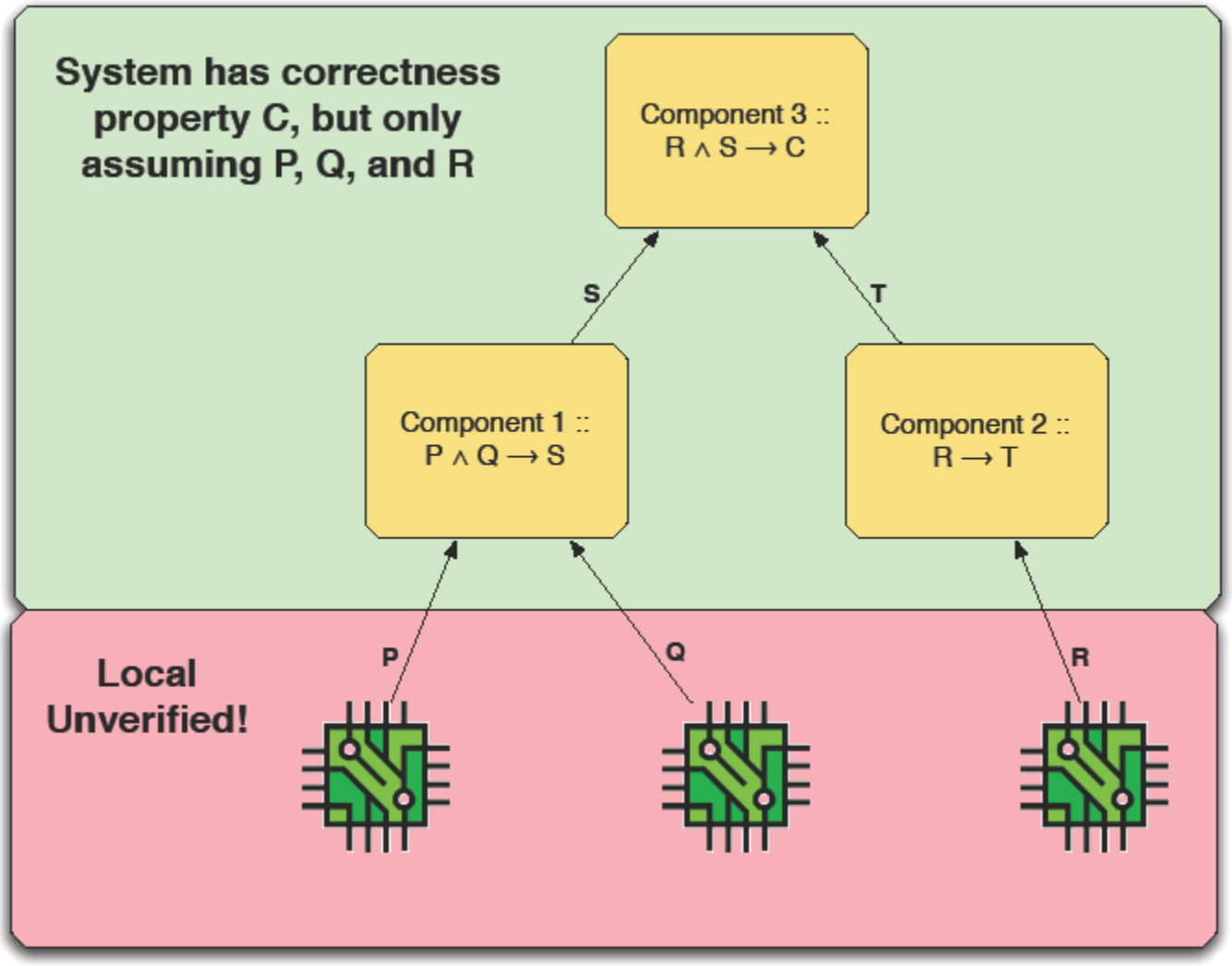
- **Motivation:**
  - Large systems use several hardware components, often manufactured by multiple foundries
  - Individual components can cause system-level failures (reliability) or subversion (adversarial)

- **Problem Summary:**
  - How do we build trusted and verifiable secure systems out of black-box components?



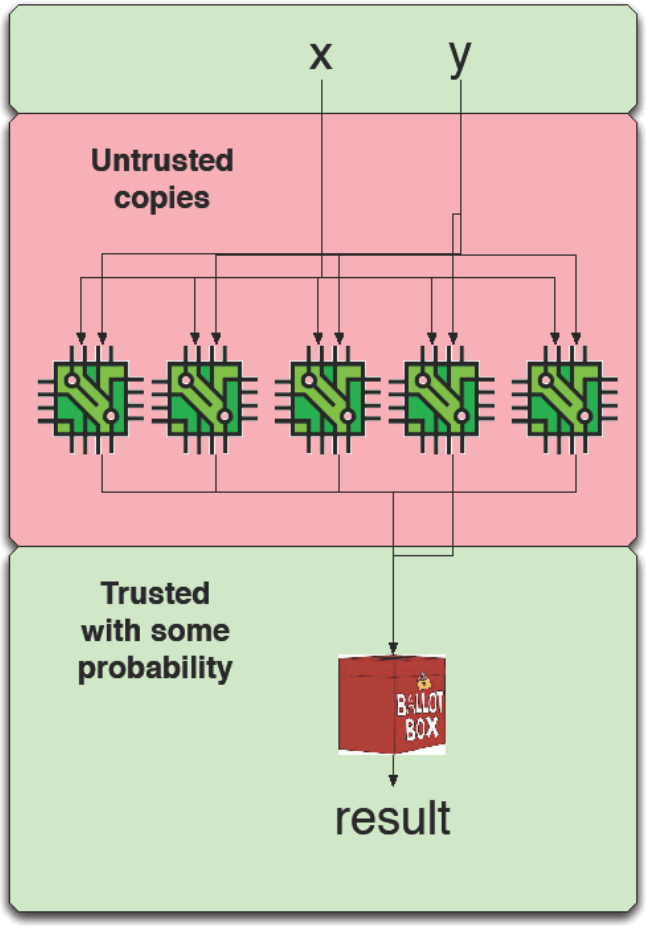
- **Approach: Divide-and-conquer, underpinned by formal verification**
  - Global scope: System-level verification
  - Local scope: Component-level verification

Global vs. Local Scope



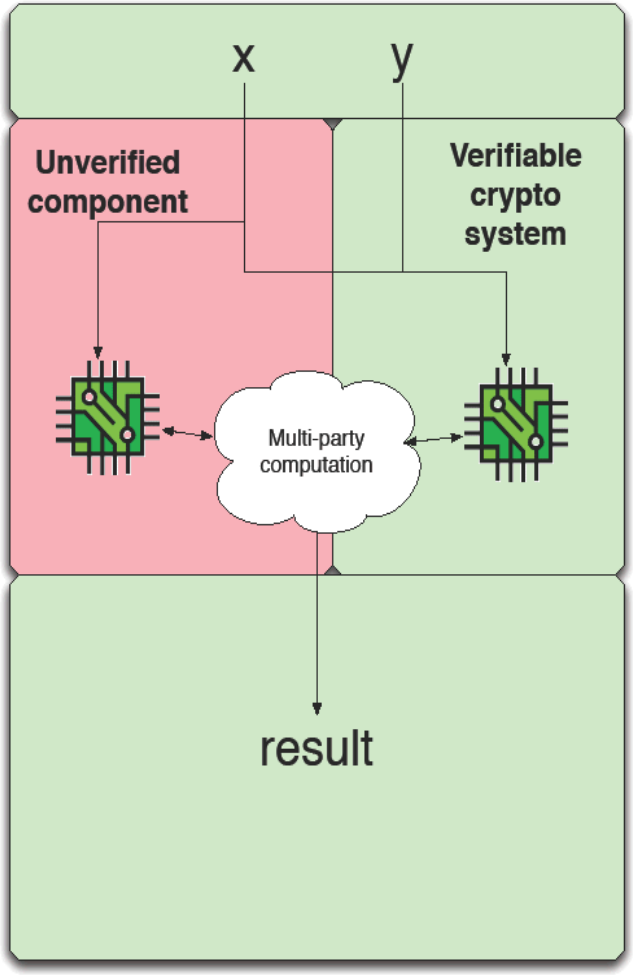
Local Scope : Voting Scheme

- Naive approach
  - Send inputs to several duplicate components
  - Return most frequent output as final result
  - Manufactured by multiple foundries to reduce collusion possibility
- Robust: up to ½ can fail
- Expensive
  - Increased cost
  - Increased board area
- How can we do better?



Local Scope : MPC

- **Secure Multi-party Computation**
  - **Cryptographic scheme that allows multiple parties to jointly evaluate a function without revealing their individual inputs**
- **Key Concept**
  - **Incorporate MPC into unverified operation/functionality**
  - **System designer has full knowledge of inputs: untrusted and (trusted) MPC components**
  - **Verify component output by inverting/removing MPC input**
- **Single trusted component**

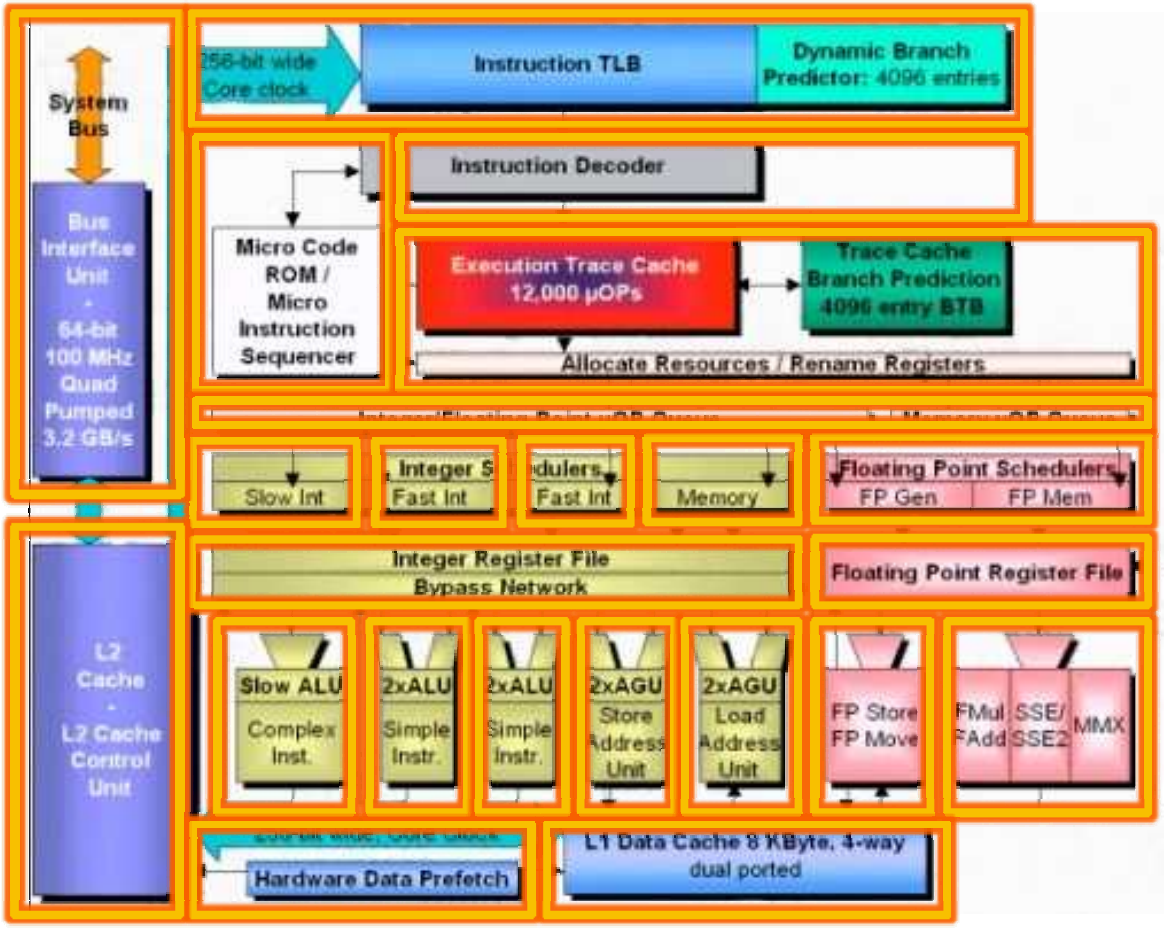


Research Questions

- **Global Scope**
  - **How much dynamic analysis is required?**
  - **How do we compose multiple systems and retain provable properties?**
  - **Can analysis of the global system reduce the input space at the local scope?**

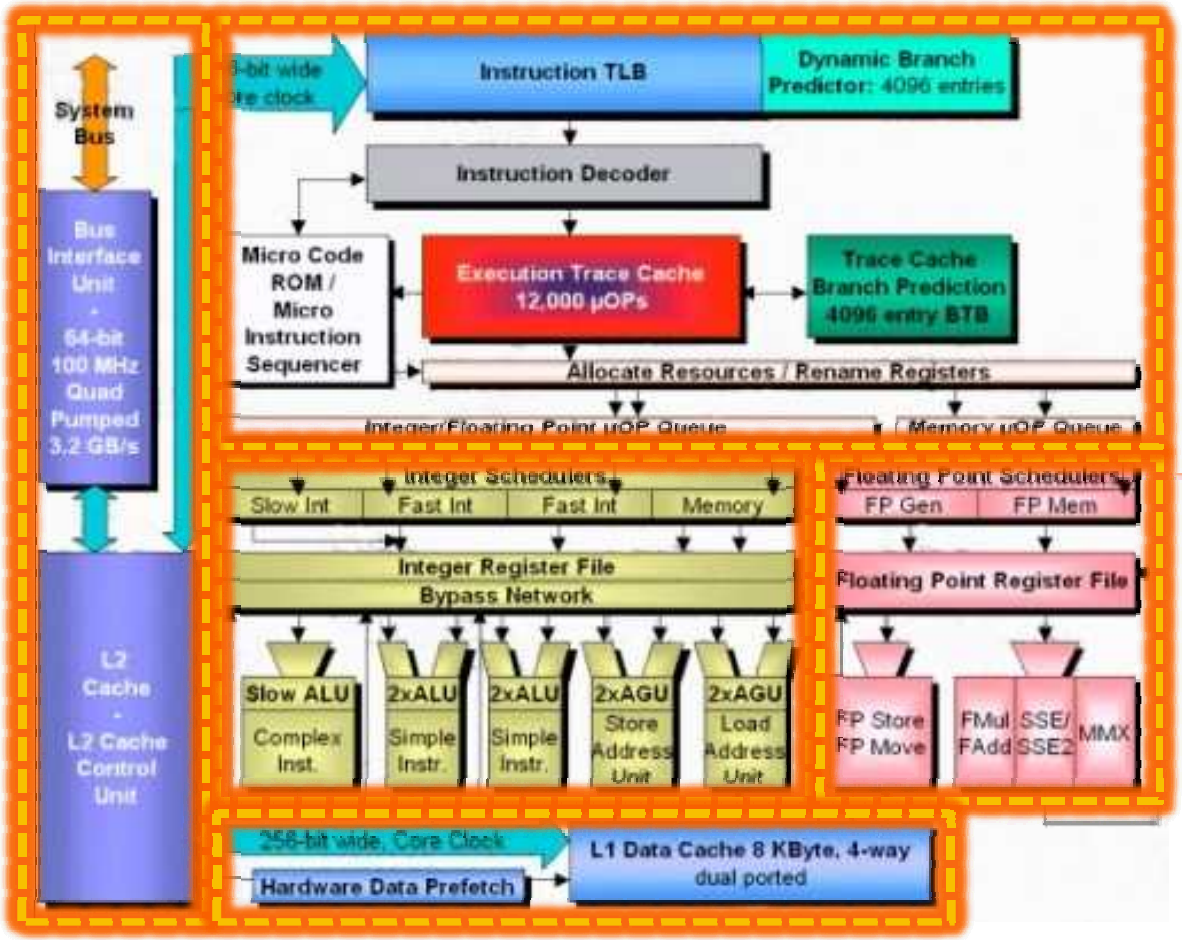
- **Local Scope**
  - **How do we couple untrusted components with trusted sandbox?**
    - **Voting scheme : simple, straightforward, but many duplicates needed**
    - **Secure multi-party computation: complex, interactive protocol, but only a single trusted component needed**
  - **How many couplings are required for a given circuit?**
  - **Which class of boolean circuits are amenable to coupling?**

Hypothetical Intel Verification Approach for i7 Core Processor



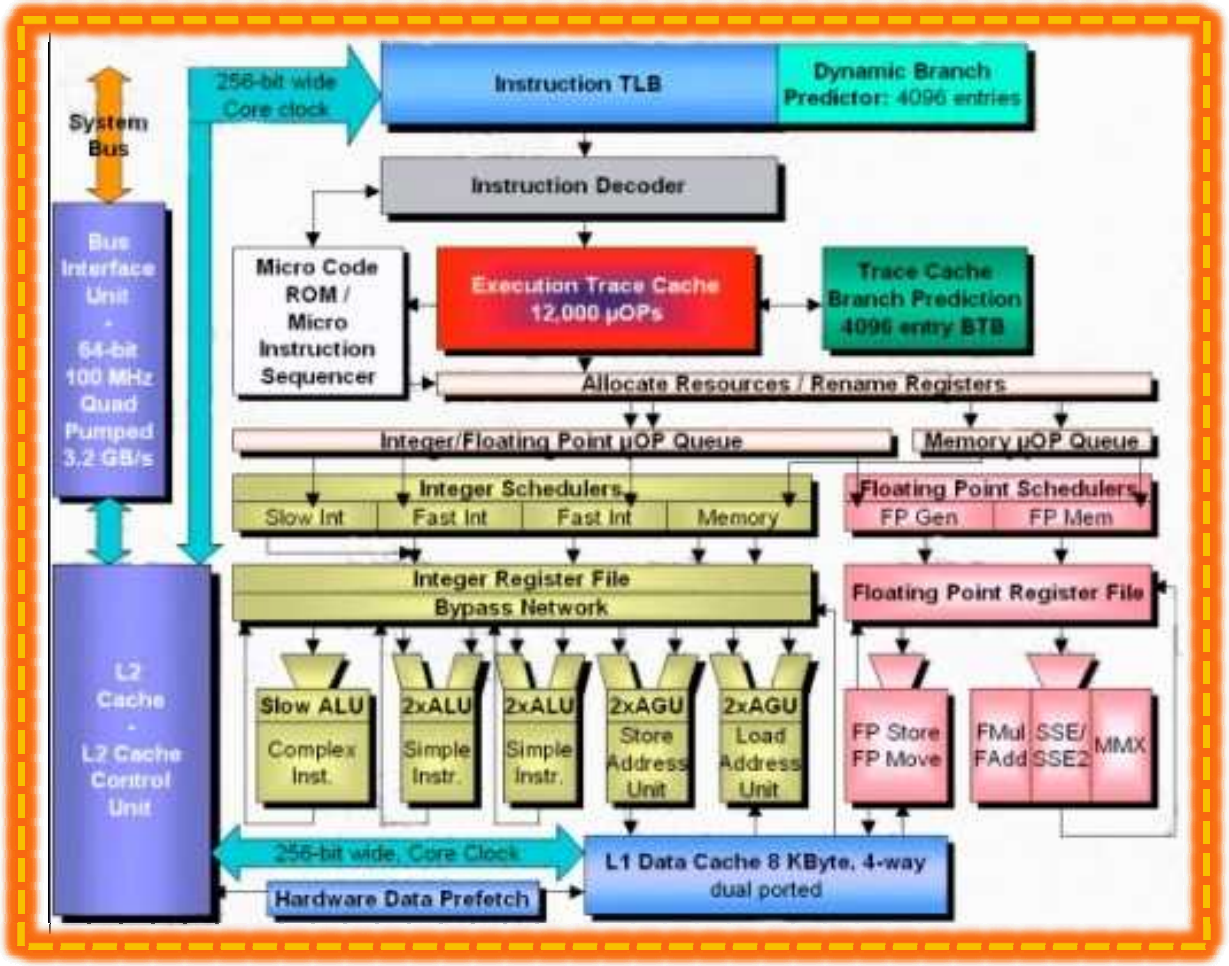
Verification of the pieces does not guarantee verification of the whole!

Reasoning About Ever-larger Portions of a System?



Sandia National Laboratories

System-level Verification: Difficult if not Impossible



Sandia National Laboratories

What did the White House National Science and Technology Council say about this?

- **This research goal specified in Cyber Security R&D strategic plan issued by Executive Office of the President:**

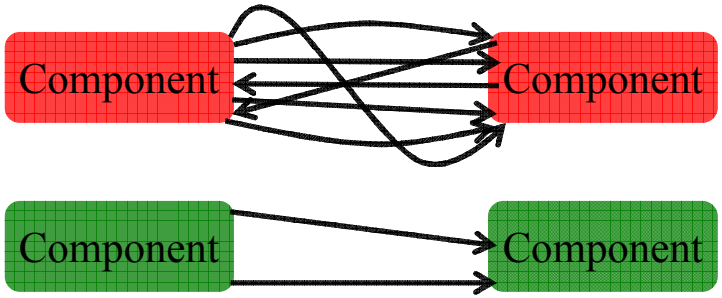
  The research challenges of this theme include:

  - ***Mathematically sound techniques to support combination of models and composition of results from separate components*** **(emphasis mine)**

- **National Science and Technology Council, "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program," Executive Office of the President, December 2011.**

Composition of Computation – Composition of Proof Certifications

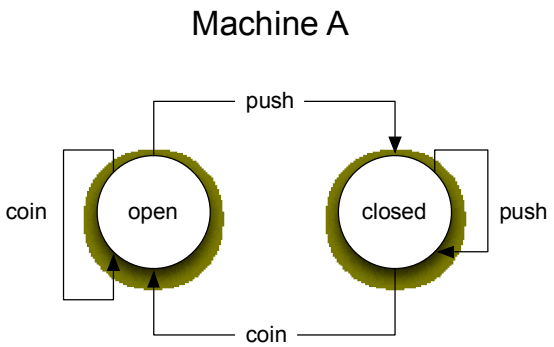
- **Certification of proofs should be composable, similar to computation, providing system-wide guarantees of correctness**



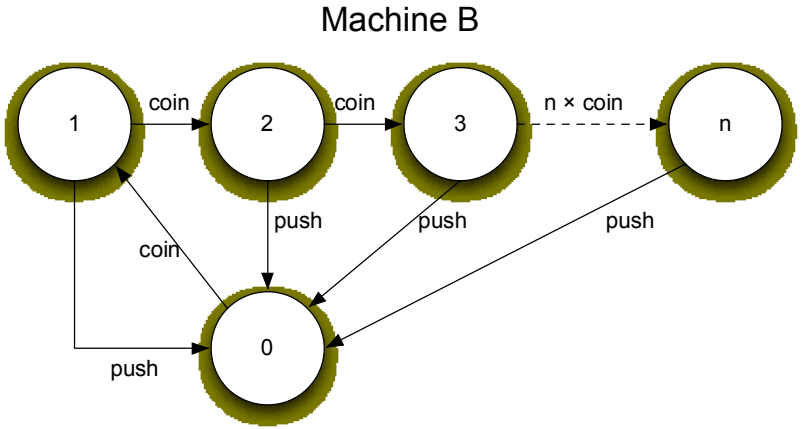
- **Construct cases where composition is less difficult**
  - Exploring many levels of formal verification (design specification, propositional logic, satisfiability)

Results To Date

- **Demonstrated composition of formal properties on small example (turnstile)**
  - **Theorem prover**
  - **Structured proof system**
- **Informs research paths and mitigates risk**
- **Near-term Work: Expand examples**
  - **Temporal logic, problem size**
  - **Explore security property verification**



Goal
Ensure that for any given n > 0, and starting from (close,0), the machine will never transition into (closed,n).



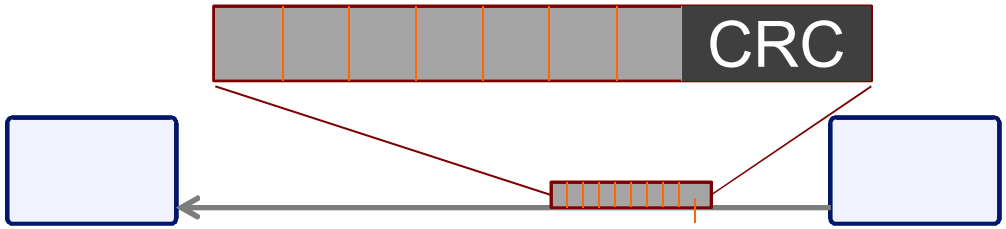
Sandia National Laboratories

Investments in Application to Problem Areas

- Over $750k thru last two FYs from customers in SNL mission areas
  - Sequestration has stalled growth this FY
  - Over $1 million expected in FY14 alone
- Applying capabilities developed by research projects to the benefit of core mission areas
  - Identified and resolved several issues in system design spaces
- Contributing technical staff (including design-team partnerships):
  - 6 staff in 8900
  - 6 staff in other centers

Sanitized Example from One Success Story

- **A communication bus expected to be resilient to single-bit errors**
  - **Enforced by CRCs that are provably one-bit safe**



- **Counter-example identified due to concurrent use of bit-stuffing**
  - Event prevalence (given a bit-error) formally quantified; design fixed

All zero/one pattern

0	1	1	1	1	1	p0	p1	p2	p3	– – – – – – – – ·	– – – – – – – – ·	pN	CRC (C bits)

Bit stuffing

0	1	1	1	1	1	0	p0	p1	p2	p3 – – – – – – – – ·	– – – – – – – – ·	pN	CRC bits

Error after bit stuffing. Stuffed bit is treated as data.

0	1	0	1	1	1	0	p0	p1	p2	p – – – – – – – – ·	– – – – – – – –	pN	CRC bits

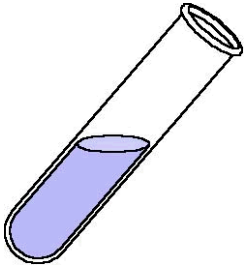
Sandia is Uniquely Capable of Impacting this Problem Area

- Responsibilities in existing mission areas (e.g., Nuclear Weapons and cyber security work) gives Sandia unique expertise in this area
  - Background in engineering and assessing trusted information systems
  - Experience building and deploying capability to address technology gaps

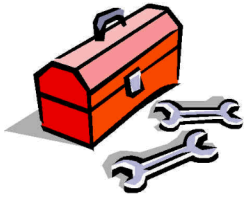
- Sandia has built a very high competence in cyber defense in order to safeguard its own enterprise-level networks
  - Effective understanding of complex scenarios regarding trusted systems

Summary of Formal Methods at Sandia

- **Research**: Sandia has active and growing R&D and analysis capabilities rooted in formal methods
  - Building capability, particularly with applications to security problems and engineered trust
  - Increasing scalability, seeking to leverage HPC



- **Capability**: Sandia is applying these capabilities and related tools to the benefit of core mission areas
  - Identified and resolved issues in system design spaces



- Key technical capability for analyzing and proving properties pertaining to trust in digital systems