SAND2023-05373C

Sandia National Laboratories

Exceptional service in the national interest

AUTOMATED REASONING TECHNOLOGIES WILL ENABLE A CORRECT-BY-CONSTRUCTION APPROACH TO SYSTEMS ENGINEERING

Raheel S. Mahmood

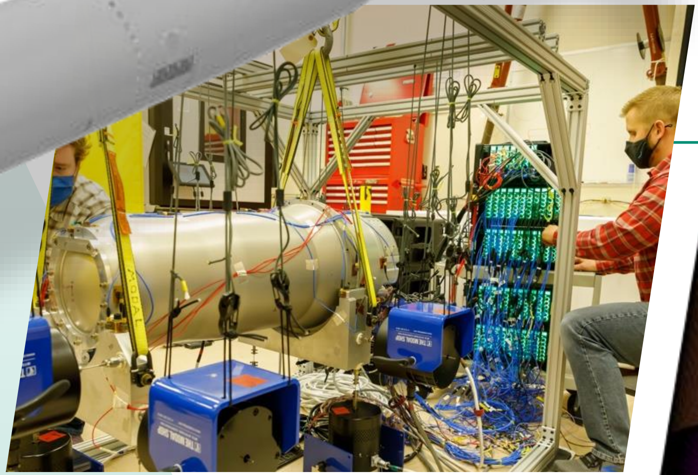
Principal Defense Systems Cybersecurity Engineer
Digital Foundations & Mathematics

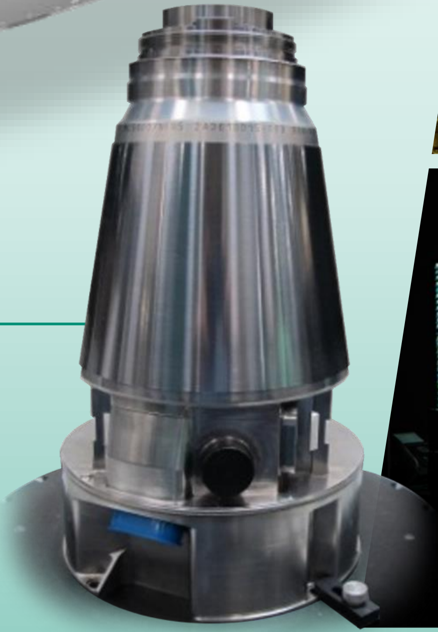
raheel.mahmood@sandia.gov

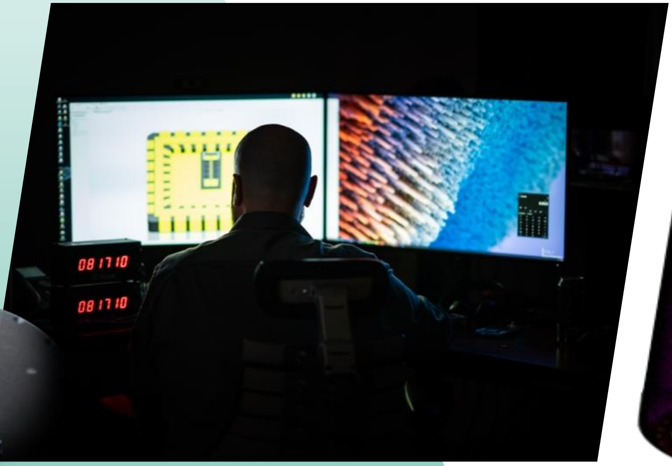
Presented at the MITRE DE and T&E Connect the Dots Workshop
27-29 June 2023 | Alexandria, VA

NUCLEAR DETERRENCE

A unique engineering challenge







Systems engineering & integration

Design agency for non-nuclear components

- Gas transfer systems
- Radar
- Safety systems
- Arming, fuzing and firing systems
- Neutron generators

Specialized component production

- Neutron generators
- Sandia external production
- Microelectronics
- Thermal batteries

Multidisciplinary R&D capabilities

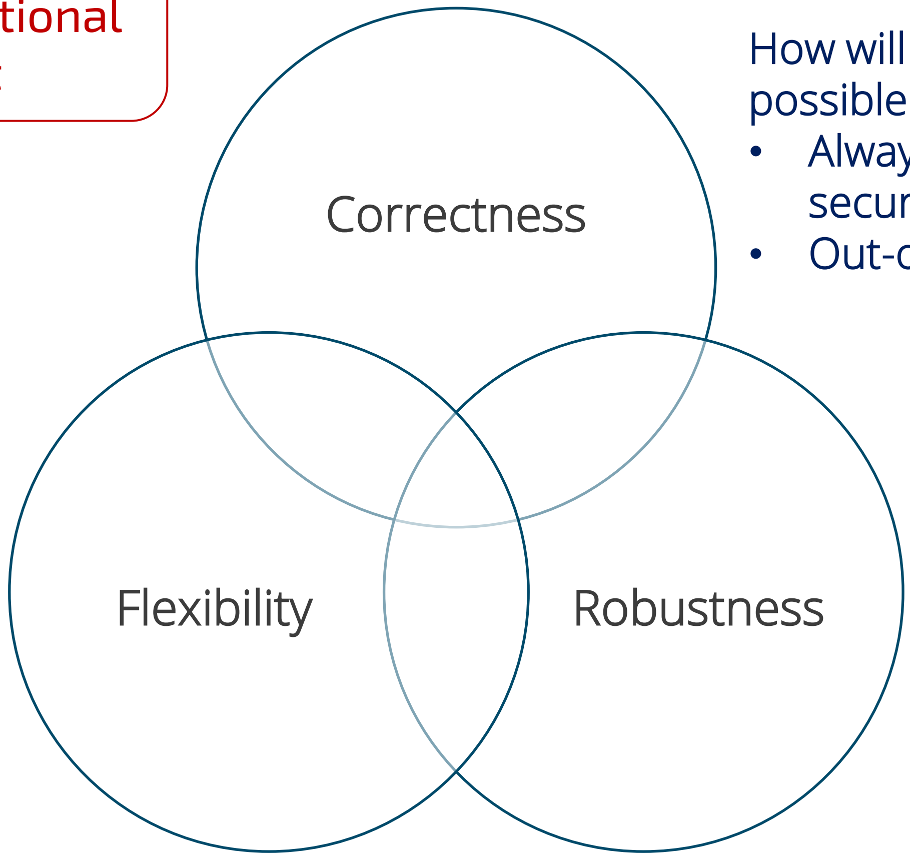
Required for design, qualification, production, surveillance, computation, experimentation

- Major environmental test facilities & diagnostics
- Materials sciences
- Light-initiated high explosives
- Computational analytics

Sandia is responsible for design, development, and qualification of the non-nuclear components of U.S. nuclear weapons

SYSTEM REQUIREMENTS MUST SPECIFY BEHAVIOR ACROSS THE ENTIRE LIFECYCLE

Requirements that specify system behavior only in the expected operational environment are not sufficient



How will the specified system respond to any possible sequence or combination of inputs?

- Always/never requirements (safety, security, liveness)
- Out-of-nominal behavior

How will the specified system continue to meet its design requirements given changes to its environment?

- New and evolving threats
- Aging of materials
- Changes to storage, carriage, and delivery

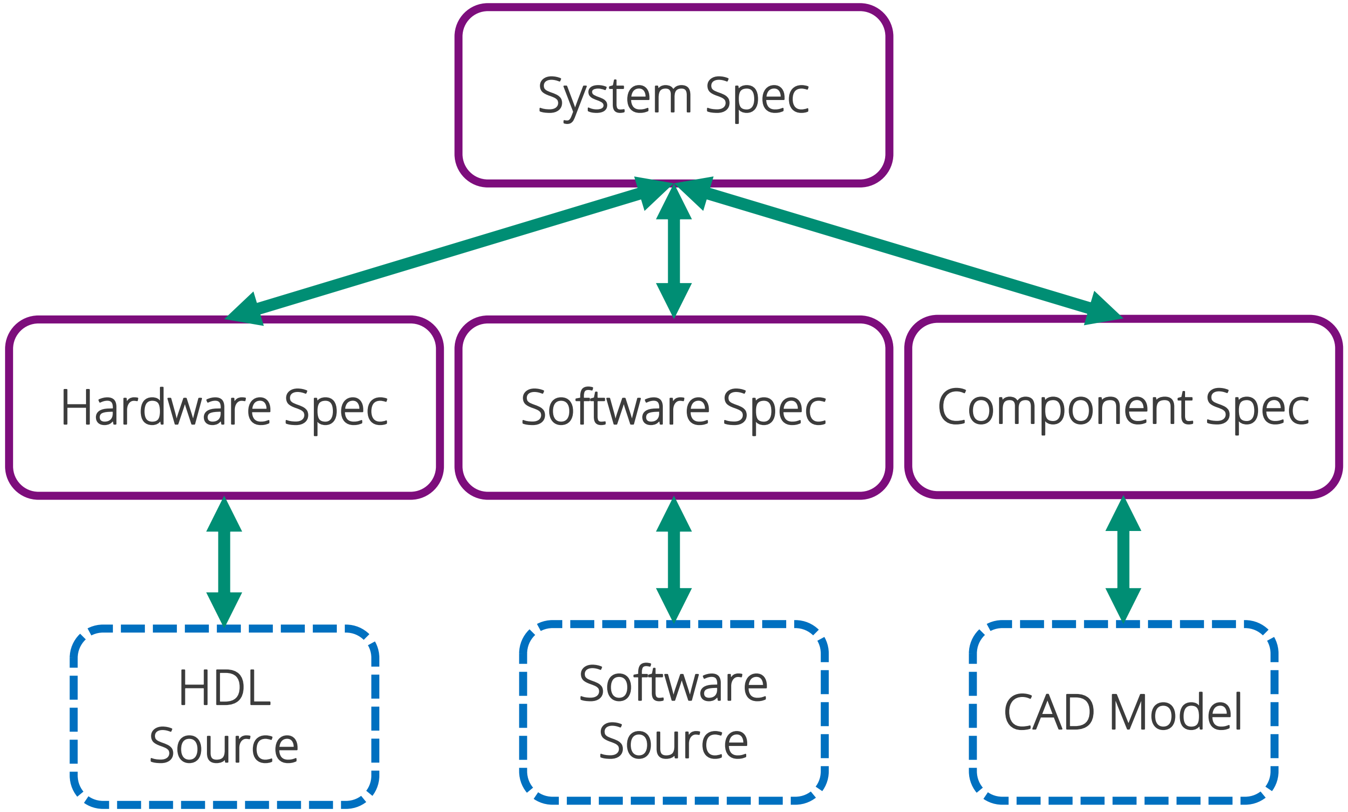
How will the specified system adapt to changes in its initial requirements?

- Life extension
- Changes to mission or target

DESIGN SPECIFICATIONS CONSTRAIN ALLOWED BEHAVIORS

Component design must not violate constraints specified at system level

Prove correctness of design with respect to requirements at the highest possible level of abstraction (lowest complexity)



~~Document~~
~~Descriptive Model~~
Executable Specification

~~Traceability~~
Mathematical Refinement

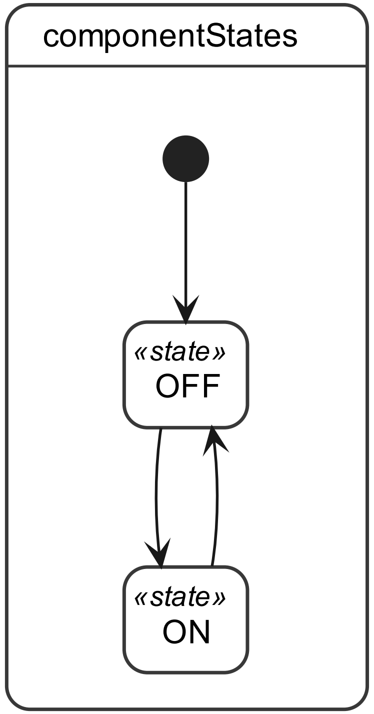
Engineering Implementation

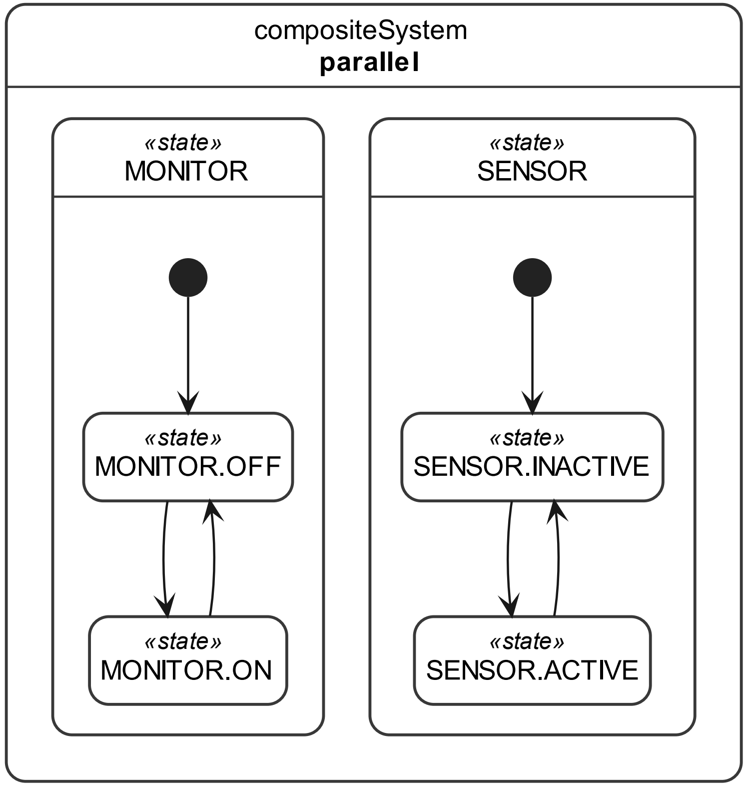
DESIGN SPECIFICATIONS AS STATE TRANSITION SYSTEMS

The **state** of the system depends on past inputs and determines how the system will respond to future inputs.
The **state machine** specifies all the possible evolutions of the system state over time.

Key concepts:

- Data (inputs, outputs, registers)
- Transitions (guards, actions)
- Parallel vs. sequential construction
- Hierarchy
- Atomic behaviors
- Non-determinism





REQUIREMENTS AS TEMPORAL LOGIC PROPERTIES

Safety and liveness properties in Linear Temporal Logic (LTL):

(For all time > 0, …)

The system shall always (or never) […]

The system shall eventually […]

LTLSPEC

G (X -> Y)

Reachability as Computation Tree Logic (CTL):

(For all initial states, …)

The system shall be capable of […]

CTLSPEC

AG !(X)

Invariants must always hold (special case of CTL)

Requirements that specify system behavior only in the expected operational environment are not sufficient

FORMALIZATION OF REQUIREMENTS REMOVES AMBIGUITY

☺ While on and sensing, the system shall indicate an alarm when two consecutive data measurements exceed the maximum value

LTLSPEC G((InState_SENSE & datIn__power & (datIn__data >= datIn__max_data) & X(datIn__power) & X(datIn__data >= datIn__max_data)) -> (QQ_SKIP | X(QQ_SKIP) | X(X(datOut__alarm))));

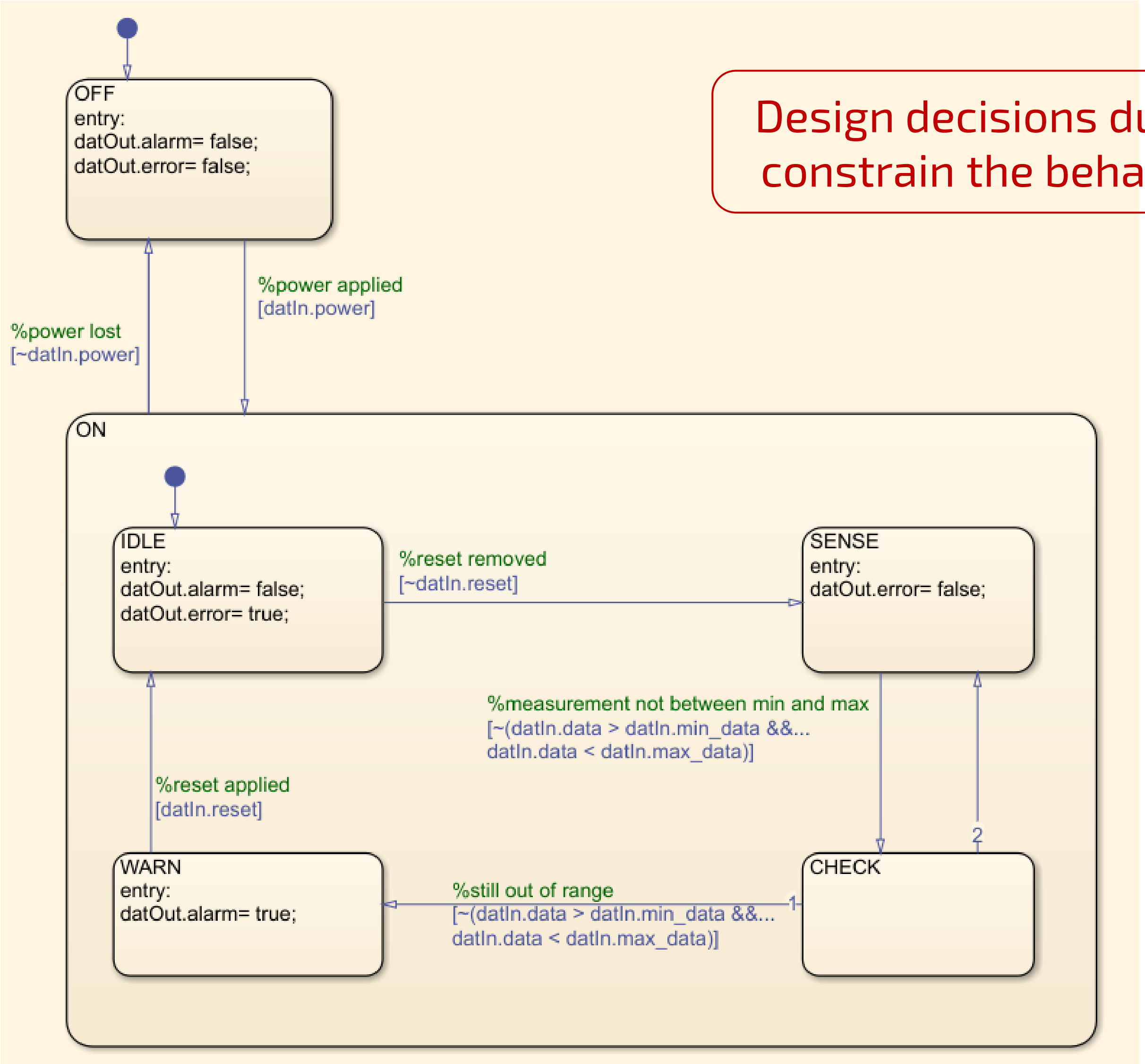
☺ Error and alarm shall not be indicated when power is removed

LTLSPEC G((!datIn__power) -> (QQ_SKIP | X(!(datOut__error & datOut__alarm))));

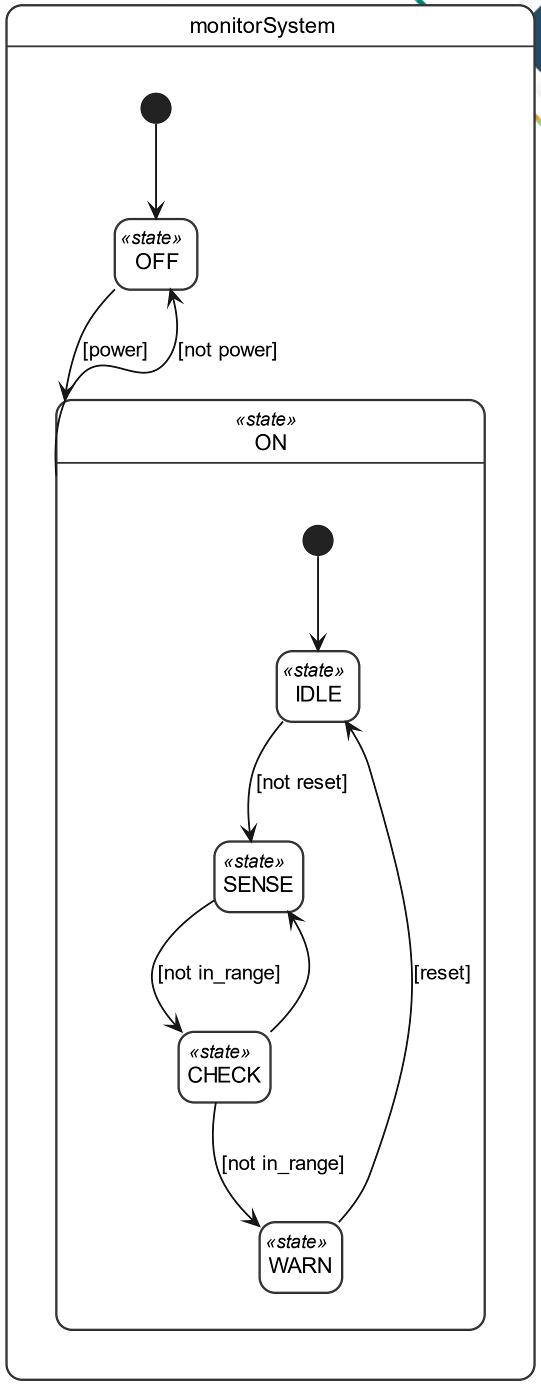
☹ The system shall not indicate an alarm when a reset is applied while powered

LTLSPEC G((datIn__reset & datIn__power & X(datIn__power)) -> (QQ_SKIP | X(!datOut__alarm)));

REFINEMENT PROVIDES EVIDENCE OF TRACEABILITY



Design decisions during development constrain the behavior of the system



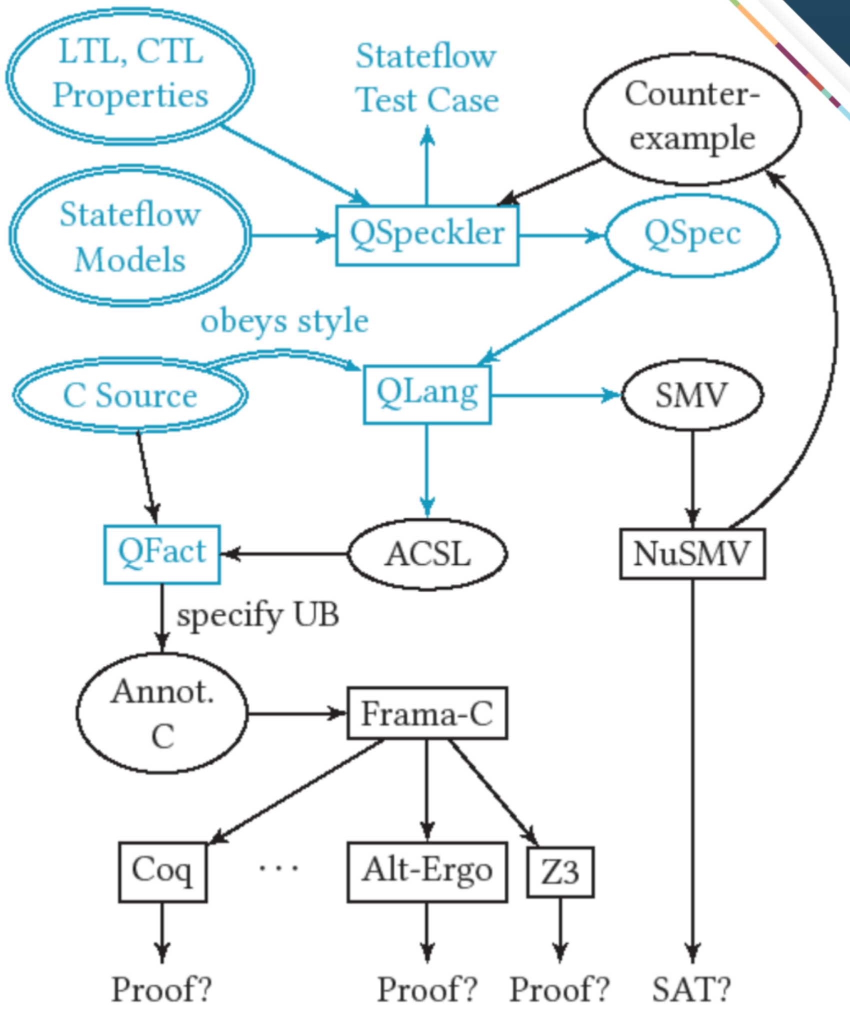
ONE Q.E.D. TO RULE THEM ALL

Empower engineers to provide justification for design decisions made during development

Reduce risk of system failures and vulnerabilities due to incorrect specification

Systems engineering approach that emphasizes design correctness and mathematical rigor

Assurance case built early in program is updated as system design and requirements evolve



Samuel D. Pollard, Robert C. Armstrong, John Bender, Geoffrey C. Hulette, Raheel S. Mahmood, Karla Morris, Blake C. Rawlings, and Jon M. Aytac. 2022. Q: A Sound Verification Framework for Statecharts and Their Implementations. In Proceedings of the 8th ACM SIGPLAN International Workshop on Formal Techniques for Safety-Critical Systems (FTSCS '22), December 07, 2022, Auckland, New Zealand. ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3563822.3568014

THANK YOU!