Kestrel Institute

Your DARPA-Ready Formal Methods Partner

Non-profit research institute – Palo Alto, CA – founded out of Stanford in 1981

Formal Methods Approaches at Kestrel

Correct-by-Construction Code Synthesis
- Refine specification to code (C, Java, etc.)
- Correctness proved by ACL2 theorem prover
- Can produce many diverse variants

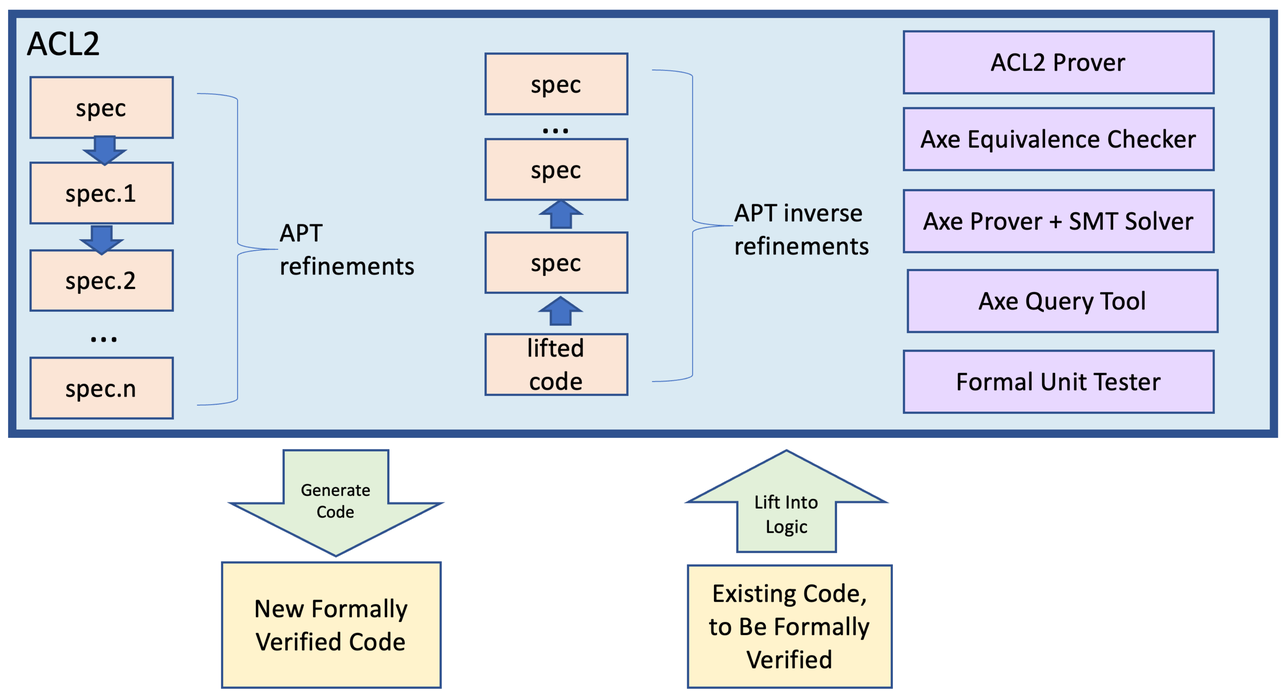
Formal Verification of Existing Code
- Lift code into logic and prove properties
- Equivalence check vs spec or golden model
- Answer yes/no questions about code

Formal Analysis of System Models
- Formalize architecture, requirements, etc.
- Prove properties of the models
- Later, prove that code implements the models

Verified Program Transformations
- Restructure code to increase security
- Compartmentalize, harden, change language
- Proofs ensure no errors introduced

Formal Unit Testing
- Evolve unit tests into powerful, automatic proofs

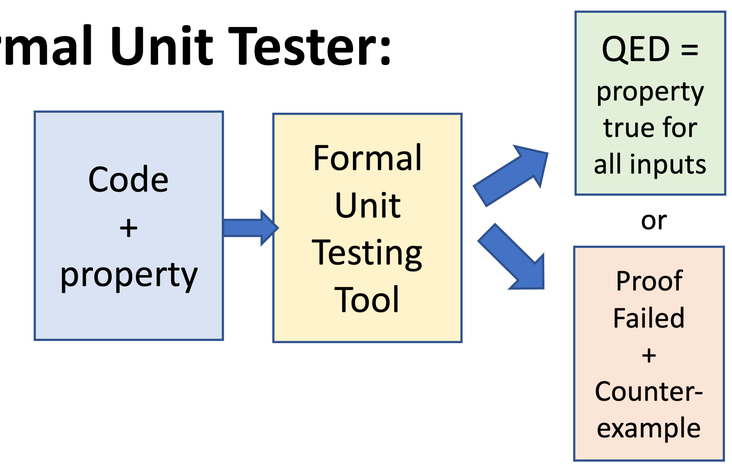
Pathways to Formally Verified Code



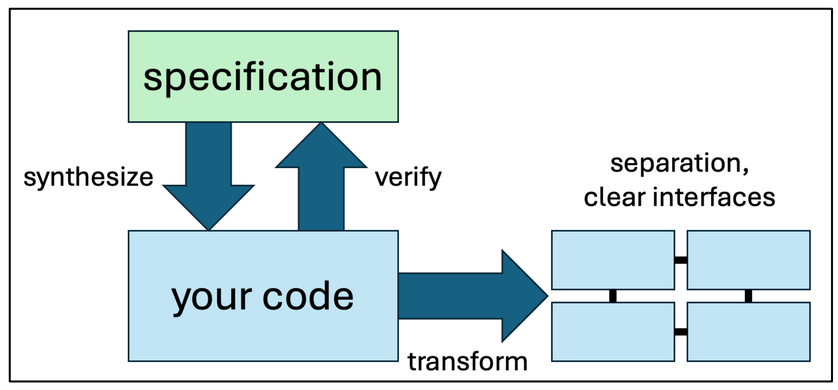
Benefits:

- High-assurance code: Correctness, Safety, Cybersecurity
- Clarity of requirements and architecture
- Deeper understanding of code
- Robust code maintenance and evolution
- Certification help (synthesize evidence along with code):
  - Common Criteria, DO-178B/C, FIPS-140-3, etc.

Formal Unit Tester:



Formal Methods Workflows:



Example Application Areas:

- Protocols
  - Command parsing
  - TCP/IP, HTTP
  - XML, JSON, ASN.1
  - LangSec
- Cryptography
  - Ciphers, Hashes, Blockchain
  - Zero-knowledge proofs
- Cyberphysical systems
  - Satellites
  - Aviation / MAVLink
- Mobile phone apps (Android)
- Safe and trustworthy AI
- Multi-Level Security
- Separation Kernels (seL4)
- Verifying compilers
- Binary Analysis (x86, RISC-V)
- Many more

Kestrel's Sponsors:

- DARPA, AFRL, ONR, DoD, IARPA, AFOSR, NASA, NSF, Ethereum Foundation, Sandia National Laboratories, and more

Kestrel's DARPA Experience:

- CPM, Assured Autonomy, MUSE, HACMS, CRASH, F6, PEARLS, APAC, IDAS, Space-BACN, PlanX, CASE, RSPACE, SoSITE, and others

Kestrel's Collaborators:

- MIT, Stanford, Vanderbilt, UT-Austin, UVA, Michigan, CMU, Northwestern, GWU, SUNY
- Raytheon BBN, Collins Aerospace, Boeing, SRI, DOLL Labs, BAE, GE, CACI, Charles River Analytics, Aarno Labs, Leidos, SIFT, Draper, Two Six Labs, GITI, Sandia

AI for Formal Methods:

- Proof creation, repair
- Spec and test creation

Formal Methods for AI:

- Formal verification of LLM-created code (Vibe Coding)
- Verified monitors / wrappers for AI systems

ACL2 Theorem Prover

- Industrial-strength
- High-performance
- Award-winning
- Active community
- Many Kestrel extensions

Contact Us to Collaborate:

www.kestrel.edu
info@kestrel.edu