|galois|

Halden Perspectives

Joe Kiniry

Principal Scientist

Galois

April 2022

galois

Correctness

Cryptography

Security

AI and ML

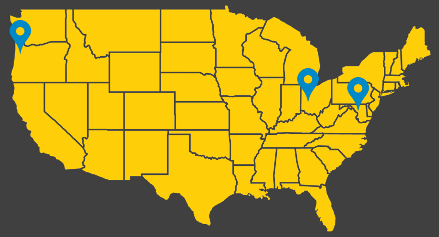
Advancing computer science R&D
Creating trustworthiness in critical systems

Clients

DOE	DARPA	NASA
DHS	AMAZON	NIST

Offices

Portland, OR
Dayton, OH
Arlington, VA



History

Founded in 1999
100+ employees

A different kind of company

No managers

We have no fixed hierarchy of rigid positions and titles, and no traditional managers.

Radical transparency

Everything is transparent by default: company financials, decision making, open meetings, and even salaries.

Choose your work

Research engineers choose the projects they work on, and move freely between projects depending on personal interests and career goals.

Ownership

Employees own the majority of the company together, making important decisions as a group and partaking in the financial success of the company.

More info at lifeatgalois.com

A Galois Frame of Reference

- R&D focused on national security and nationally critical infrastructure
- >90% clients are the U.S. federal government; the rest are industry
- our oldest and biggest clients are all DoD/IC (DARPA, NSA, etc.)
- clients primarily ask us to solve unsolved problems, or transition recently published papers in top venues into tools ready for transition
- often we develop new formal methods and build tools that embody those formal foundations that can be used by everyday engineers
- our core strengths are formal methods, programming languages, classic systems research (operating systems, hypervisors, networking, cyber-physical, etc.), formal modeling, formal verification, model-based engineering, and rigorous digital engineering
- our customers care about evidence, not process, and want formal and practical evidence of systems' correctness and security, and do not often trust proprietary tools, technologies, or opaque and informal arguments

Project Areas pre-NRC

- designing and creating assurance tools used by the NSA to create, evaluate, and assure assets
- creating new programming and specification languages to reason about properties that COTS tools cannot, esp. around security, compositional correctness, and real-world software and hardware
- clients care deeply about correctness and security, and sometimes demand a safety case, and thus model-based engineering with formal foundations is prolific, and few proprietary tools are used
- working for the NRC on a DI&C system is a new domain, but it tastes/feels like many others

HARDENS

- **HARDENS** (*High Assurance Rigorous Digital Engineering for Nuclear Safety*) is a R&D project run by Galois for the *Nuclear Regulatory Commission* (NRC)
- the purpose of HARDENS is to demonstrate and educate about cutting-edge, high-assurance model-driven engineering
  - our focus is on nationally critical infrastructure, and thus safety-critical embedded systems
- within HARDENS, Galois has designed and built a demonstration Reactor Trip System (RTS) that is representative of a Digital Instrumentation & Control (DI&C) system for a Nuclear Power Plant (NPP)
  - the RTS is fault-tolerant and high-assurance
  - the RTS has a physical manifestation (an FPGA board plus sensors/actuators) and a set of digital twins

The RDE Research Program

- **Rigorous Digital Engineering (RDE)**
  - **Rigorous** = use *applied formal methods* to reason about *models, implementations, and evidence*
  - **Digital** = use digital, mechanized, computational, denotational and executable models of components and systems to create *digital twins* (executable digital representations of components and systems) and *digital threads* (relations between digital and physical artifacts with known, evidence-based fidelity)
  - **Engineering** = process, methodologies, tools, and technologies supporting *all* forms of engineering (particularly domain, requirements, software, firmware, hardware, safety, systems, and security engineering)

Models and Reasoning at Galois

- models are primarily those that support RDE
  - digital, mechanized, computational, denotational and executable models of components & systems
- generally, models must have well-understood and maintainable relationships to other models and implementations
- models are either written by hand, generated from other artifacts (semi-formal or formal), or lifted/extracted from implementations (software, binaries, & hardware designs)
- reasoning about models and implementations is accomplished using one of dozens of formal reasoning techniques
  - interactive specification and proofs in a Logical Framework
  - automated reasoning with SAT/SMT
  - type systems, symbolic evaluation, and logic-based reasoning with various Hoare, separation, and domain-specific logics are popular
  - model checking and abstract interpretation, less so

Sufficient Evidence

- common widely acknowledged characteristics: unambiguous, consistent, complete, validated, verifiable, demonstrable, modifiable, traceable
- uncommon characteristics that we insist upon:
  - refinement-centric reasoning that leads to realizability,
  - machine interpretability, grounded in mechanized logic,
  - objective validity (independent of observer),
  - universality (all properties must be demonstrated for all models, all twins, and all implementations),
  - compositionality (properties and their evidence must compose with no unknown emergent behavior or properties),
  - multiplicity (demonstrate and prove each property about each model/component at least two ways)

Structured Argumentation

- structured safety argumentation is only one piece
  - structured correctness argument
  - structured security argument
  - all grounded in domain engineering model
  - traceability from natural language to formal proof about deployed implementations
- how to incorporate hazard analysis with RDE
  - drives decisions about assurance goals
  - informs architectural design decisions to optimize the non-behavioral dimensions of our product line (power, performance, resources, security, size, weight, cost [incl. NRE, certification, and maintenance])

Additional Slides Reflecting Upon Questions Posed in Earlier Meetings

I intend to fill these in after participating into the April workshop, and upload those reflections to share will everyone. -Joe

Evidence Necessary to Eliminate Design Diversity

- To be completed later in April if there is interest from the community.

No Worse Than

- To be completed later in April if there is interest from the community.

Independently Verifiable Evidence

- To be completed later in April if there is interest from the community.

Uncertainties Degrade

- To be completed later in April if there is interest from the community.

Practitioner Competence in Hazard Identification

- To be completed later in April if there is interest from the community.

Compliance with Standards

- To be completed later in April if there is interest from the community.

Evaluating Adequacy without Design Diversity

- To be completed later in April if there is interest from the community.

Requirements vs. Design Diversity

- To be completed later in April if there is interest from the community.

Sufficient Evidence

- common widely acknowledged characteristics: unambiguous, consistent, complete, validated, verifiable, demonstrable, modifiable, traceable
- uncommon characteristics that we insist upon:
  - realizability,
  - machine interpretability,
  - objective validity (independent of observer),
  - universality (all properties must be demonstrated for all models, all twins, and all implementations),
  - compositionality (properties and their evidence must compose with no unknown emergent behavior or properties),
  - multiplicity (demonstrate and prove each property about each model/component at least two ways)

Integrating Disparate Evidence

- To be completed later in April if there is interest from the community.

Question Set 1

- To be completed later in April if there is interest from the community.

Question Set 2

- To be completed later in April if there is interest from the community.