SCC · NRC · ROCKVILLE

The AI wrote it. The theorem prover signed it.

Joseph Kiniry at the 24th Software Certification Consortium, hosted at the Nuclear Regulatory Commission.

SWIPE →

THE TRUST ARGUMENT

AI in the generation path doesn't enlarge the trusted computing base.

The proof kernel is still the trust anchor.
Same as it ever was.

"SIGNED" IS LITERAL

The theorem prover emits a machine-checkable certificate.

Remove the AI from the pipeline. **The certificate still replays.**

CHAIN OF CUSTODY

Every HOARDE artifact carries six pieces of evidence.

01 Identity

02 Provenance

03 Model and seed

04 Signed human review gate

05 Machine-checkable certificate

06 Dependency graph that propagates invalidation

POLICY ENFORCEMENT

Three controls. Evidence that maps to the standards.

01 Capability isolation

02 Append-only audit logs

03 Non-repudiable review attestations

MAPS DIRECTLY ONTO

CbyC | DO-178C | IEC 61508 | ISO 26262

THE HARD QUESTIONS

Q · NON-DETERMINISM

What's certified is **verification**, not generation.

Q · MODEL DRIFT

Treat it like **tool versioning**.

Q · SPEC FIDELITY

Still the engineer's responsibility. **Now with a lot of help.**

LET'S TALK

If you work on certified software, the conversation is just getting interesting.

We'd love to talk.

Sigil Logic

AI-augmented rigorous engineering with formal methods.