Arthur Amorim

Arthur.Amorim@ucf.edu · arthuramorim.net · Art-Amorim · Scholar
Orlando, FL · U.S. Citizen · **Eligible for DoD Secret Clearance**

Summary

Ph.D. candidate in formal methods (expected July 2026) with four years of applied research at Idaho National Laboratory building machine-checked security infrastructure for national-security-relevant embedded systems. Primary author of SPECTRE: a formally verified, runtime-enforced safety monitor framework for cyber-physical protocols, validated on deployed UAV (MAVLink/ArduPilot/PX4) and industrial control (Modbus) hardware. Work spans the full R&D lifecycle: protocol formalization, proof mechanization in F*, C synthesis for legacy retrofit, and physical testbed validation at sub-10% latency overhead.

Education

University of Central Florida — *Orlando, FL*
Ph.D., Computer Science — expected July 2026 · Advisor: Dr. Gary T. Leavens — 2023–present
M.S., Computer Science — GPA 3.93/4.00 — 2023–2025

Research Experience

Idaho National Laboratory, National & Homeland Security Directorate — *Idaho Falls, ID*
Ph.D. Intern, Formal Methods Researcher — May 2022–present

- Built **SPECTRE** (∼9,000 lines of F*): a formally verified, runtime-enforced safety monitor framework for cyber-physical protocols, with three certified deployment paths—static type checking (OCaml), distributed runtime monitoring, and C FSM synthesis for legacy embedded retrofit.
- Designed and mechanized **Facet**: the first fully mechanized RMPST metatheory in F*, proving subject reduction, deadlock freedom, progress, and projectability via computational reflection. Certified extraction ensures the proved object is the deployed object.
- Built **Platum**: a direct AST-to-C synthesis pipeline generating allocation-free, O(1)-memory FSM monitors deployable on ARM microcontrollers; achieved 4× latency reduction over prior work (∼13.3 μs/message).
- Composed monitors with **seL4 microkernel isolation** to defend against adversaries who have simultaneously compromised the OS-level network stack and ground control station.
- Validated on **MAVLink** (ArduPilot, PX4) and **Modbus**: formalized >8,000 lines of MAVLink in F*; demonstrated 100% detection of domain-specific behavioral attacks on a physical chemical mixing testbed at <10% latency overhead.

CyManII Cybersecurity Manufacturing Innovation Institute — *Joint Appointment*
Ph.D. Intern, Applied Formal Methods Researcher — Aug 2025–present

- Collaborated with industry partners on practical, provable security integration of SPECTRE in operational ICS environments.

Selected Publications

[1] Amorim et al. "Enforcing MAVLink Safety & Security Properties via Refined Multiparty Session Types." *NFM 2025.*

[2] Amorim et al. "UAV Resilience Against Stealthy Attacks." *ICUAS 2025.*

Technical Skills

Verification & Proof F* / Meta-F* , Z3 (SMT), nuXmv (model checking)
Systems & Protocols seL4 microkernel , MAVLink, Modbus, ARM embedded, ArduPilot/PX4
Languages F*, OCaml, C/C++, Python, Rust, LaTeX
Security Domains Threat modeling, embedded systems security, ICS/SCADA security, runtime enforcement, protocol verification