SHANE MCFLY

Curriculum Vitae
Golden, Colorado | shane@fluxconstant.com | fluxconstant.com
U.S. Citizen

PROFILE

Cybersecurity architect and Principal Investigator with over a decade securing mission-critical cyber-physical and control-system environments for national programs. Led multi-organization security engineering for Department of Energy full-scale exercises and architected the ARIES Cyber Range, a high-fidelity distributed emulation of multi-owner regional grid infrastructure. Nine publications spanning substation protocol security, distributed energy resource cybersecurity, and national Cyber-Informed Engineering doctrine. Sustained record of graduate instruction and professional training. FFRDC-experienced, working directly with federal sponsors, national laboratories, and interagency stakeholders.

EDUCATION

M.S., Computer Science University of Illinois at Urbana-Champaign.

B.S., Computer Science University of Illinois at Urbana-Champaign.

Doctoral coursework, Computer Science Colorado School of Mines (paused 2024).

TECHNICAL DOMAINS

Control & Cyber-Physical Systems SCADA and ICS architecture, DNP3, Modbus, IEC 61850/GOOSE, telemetry networks, NIST 800-82, Cyber-Informed Engineering, ICS incident response, distributed energy resources.

Systems Security Engineering Security architecture and requirements definition, threat and vulnerability analysis, mission-impact risk assessment, validation through full-scale operational exercise.

Embedded & Network Security Embedded and avionics systems security, intrusion detection, network forensics, graph-based traffic analysis, alert aggregation and causal reasoning, zero-trust segmentation, SDN.

Platform & Infrastructure Distributed and high-availability systems; virtualization (VMware vCenter, Proxmox, XenServer); containerization (Docker, Kubernetes); infrastructure-as-code (Terraform, Ansible); AWS and Google Cloud Platform; Linux systems administration; large-scale emulation and cyber range environments.

AI / ML Local LLM deployment, NPU hardware acceleration, distributed multi-agent architecture, MLOps pipelines.

PROFESSIONAL APPOINTMENTS

National Laboratory of the Rockies (formerly NREL) — Golden, CO 2019 – 2026
Senior Cybersecurity Researcher & Principal Investigator · DOE FFRDC

- **Principal Investigator, Liberty Eclipse:** Led the DOE CESER full-scale national exercise. Directed the Network/Communication Pillar, coordinating a cross-organizational engineering team to orchestrate and validate national grid recovery plans across highly distributed systems under live operational conditions. Interfaced directly with federal sponsors, utility operators, and interagency participants.
- **Security architecture, ARIES Cyber Range:** Architected the platform into a high-fidelity distributed environment emulating multi-owner power systems, regional grids, and large-scale data flows, enabling realistic evaluation of security posture, attack effects, and recovery procedures against representative infrastructure.
- **DER Cybersecurity Framework integration:** Led integration of NREL's Distributed Energy Resource Cybersecurity Framework with the ARIES Cyber Range, producing the Distributed Energy Resource Visual Emulator. First author on both resulting national laboratory publications.
- **Cyber-Informed Engineering:** Contributing author to the DOE/INL CIE Implementation Guide and co-author of the CIE Curriculum Guide, Version 2.0, and the nine-institution university adoption report.
- **Risk analysis & mission impact:** Evaluated threat and vulnerability likelihood against operational consequence to prioritize mitigations for critical infrastructure operators and federal sponsors.
- **Infrastructure delivery:** Led the team delivering Terraform and Ansible infrastructure-as-code for exercise and range environments across distributed sites. Delivered Liberty Eclipse infrastructure across three annual cycles on successive platforms — AWS in year one, VMware vCenter in year two, and Proxmox in year three. Portions of the ARIES Cyber Range ran on vCenter.
- **Research data strategy:** Identified the absence of labeled OT/ICS/SCADA data as the binding constraint on applying machine learning to control-system security. Directed a subcontract with the University of Illinois to capture and label Liberty Eclipse exercise data across successive annual cycles, establishing a labeled corpus in a domain with almost no public training data, with a path to bootstrap labels for the DARPA RADICS dataset through weak supervision.

- **Test systems:** Built the hardware-in-the-loop test system underpinning NREL's Advanced Grid OT Edge-Level Threat Detection research.
- **Workforce programs:** Led the laboratory initiative supporting the national DOE CyberForce Competition.

Colorado School of Mines — Golden, CO 2020 – Present
Adjunct Faculty, Department of Computer Science

- Graduate coursework in system security, SCADA architectures, and network forensics.
- Designed a hands-on laboratory series in which students construct, instrument, and secure cyber-physical system simulations end to end.

University of Illinois — Information Trust Institute — Urbana, IL 2017 – 2019
Research System Administrator

- Developed complex smart grid simulations for the DARPA RADICS program, focused on resilient black-start recovery of the U.S. power grid following a cyber attack. Built and operated the simulation environment on VMware vCenter.

Boeing Research & Technology — St. Louis, MO 2015 – 2016
Systems & Networks Research Engineer

- Vulnerability assessments on proprietary embedded aircraft networks; containerized threat log analysis and intrusion detection software for commercial avionics systems. Built and managed the research testbed on XenServer.

Parkland College — Champaign, IL 2017 – 2019
Faculty, Business / Computer Science & Technologies

- Coursework in Linux systems administration, cybersecurity, and networking fundamentals.

PUBLICATIONS

ORCID: orcid.org/0009-0005-2605-7878

Peer-Reviewed

- Battista, J., Nahrstedt, K., Valdes, A., McFly, S. "Alerga: Alert Aggregation and Reasoning in GOOSE Simulation Pipeline." 2023 IEEE SmartGridComm. doi:10.1109/SmartGridComm57358.2023.10333915
- Battista, J., Nahrstedt, K., Valdes, A., McFly, S. "Flock: A Framework for Alert Aggregation and Reasoning in GOOSE Messages." University of Illinois at Urbana-Champaign, 2022.
- Palmer, I., Rogers, E., McFly, S. "A Graph-Based Analysis of Industrial Control Systems Network Traffic." International Journal of Industrial Control Systems Security, 2020. Presented at HotSoS, 2019.

National Laboratory Reports & Federal Guidance

- McFly, S., Peterson, J., Cryar, R., Reynolds, T. "Distributed Energy Resource Visual Emulator: Phase 1." NREL, 2023. First author. doi:10.2172/1922814
- McFly, S., Peterson, J., Reynolds, T. "Distributed Energy Resource Cybersecurity Framework and Cyber Range Integration." NREL, 2022. First author. doi:10.2172/1868050
- Wright, V. L., Meng, J. P., Anderson, R. S., … McFly, S., et al. "Cyber-Informed Engineering Implementation Guide." Idaho National Laboratory / U.S. DOE, 2023. INL/RPT-23-74072. OSTI 1995796.
- Lampe, B. R., Cole, D., McFly, S., Casey, O. B., et al. "Cyber-Informed Engineering (CIE) Curriculum Guide." Idaho National Laboratory, 2024.
- Lampe, B. R., Lyons, W., Zonouz, S., … McFly, S., et al. "CIE Curriculum Guide, Version 2.0." Idaho National Laboratory. doi:10.2172/3006953
- Lampe, B., Huang, E., Cole, D., McFly, S., et al. "Cyber-Informed Engineering Adoption in University Engineering Programs." Idaho National Laboratory, 2024. doi:10.2172/2478666

Acknowledged Contribution

- Hupp, W., Hasandka, A., Singh, V. K., Baniahmed, S. A. "Advanced Grid Operational Technology Edge-Level Threat Detection." NREL, 2023. Built the hardware-in-the-loop test system used for this research. doi:10.2172/1960418

In Progress

- "Context Persistence and State Integrity Challenges in Heterogeneous Distributed Multi-Agent LLM Architectures." Working paper.

INVITED TALKS, PANELS & PRESENTATIONS

- *"Ensuring Continuity & Aggregator Roles (led Focus Sessions 3 & 4)"* — Aggregation and Grid Security Workshop 2025
- *"Cybersecurity for Operational Technology (panel)"* — 2nd Annual ICS/SCADA Cybersecurity Symposium2025
- *"Where's Waldo? Find the Raspberry Pi in the Cyber Defense Exercise"* — ICS Village, DEF CON 2024

- *"Scaling to Secure the Clean Energy Transition through Cyber Defense Exercises"* — DOE Energy Transition Summit, Arlington, VA 2024
- *"A Day in the Life of a [National Lab Researcher] (invited lecture)"* — Information Trust Institute / CSL, University of Illinois 2024
- *"Engineering-In Cyber (co-presented with Virginia Wright, INL)"* — Hack the Capitol 7.0, May 30–31 2024
- *"Renewable Energy Expertise as Context for Satellite Intelligence (lightning talk)"* — GEOINT Symposium, St. Louis, MO 2023
- *"Cyber Across the Federal Government (panel, with Chris Inglis)"* — University of Colorado Colorado Springs2023
- *"Fear and Loathing on Plum Island (panel)"* — ICS Village, DEF CON 2023
- *"Reskilling to Close the Cyber Workforce Gap"* — DOE Cybersecurity and Technology Innovation Conference, Portland 2022
- *"Operational Technology Security Track (panel)"* — DOE Cybersecurity and Technology Innovation Conference, Portland 2022
- *"OT Network Monitoring Fundamentals (lead presenter)"* — CREDC Summer School 2017
- *"Containing Vulnerabilities in Containers"* — Cyber Defense & Disaster Recovery Conference 2016
- *"Maintaining Privacy on Social Media"* — Crypto & Privacy Village, DEF CON 2015

TEACHING & CURRICULUM DEVELOPMENT

Cyber Fire Foundry — DOE OCIO-Funded Cyber Training Program 2023 – Present
Instructor, Curriculum Developer & Challenge Systems Architect

- **Curriculum:** Developed the curriculum and training systems for the program's OT Security course.
- **Challenge platform:** Architected the containerized interactive challenge platform used to deliver hands-on scenarios to professional cyber operators.
- **Scenario development:** Integrated Grid Incident Recovery Challenge — DEF CON ICS Village 2025, BSides Denver 2025, Cyber Fire Foundry 2025-2, Cyber Fire Foundry London 2026. Grokwell, an Agentic ICS Incident Recovery Challenge — DEF CON ICS Village 2026 (writeup: https://github.com/irish-bug/grokwell-writeup/tree/master). Hack the Wind Turbines — DEF CON ICS Village 2023, 2024.
- **Continuity:** Program work performed under NREL/NLR through 2026; scheduled to continue independently under subcontract beginning November 2026.

Other Professional Training

- **Security Plus Data Science:** Two-day training, NOLACON. Co-developed and co-taught with Imani Palmer (2022); delivered solo (2023).
- **DEF CON ICS Village (2017):** Co-presented a control-system training exercise with Matt Luallen of CybatiWorks.

VILLAGE LEADERSHIP

- **DEF CON ICS Village (2023–2026):** Content sponsor and challenge designer.
- **DEF CON Ethics Village (2018, 2019, 2021):** Founder and Chairperson. Established the village and hosted international workshops on ethical challenges in information security and privacy.

ADVISORY & SERVICE

- **Colorado School of Mines — CCSP Industry Advisory Board:** Industry board member shaping curriculum; guest lecturer on cybersecurity for physical systems.
- **DER Cybersecurity Framework (DER-CF) core team:** National Renewable Energy Laboratory.

INDEPENDENT RESEARCH & DEVELOPMENT

- **Multi-Agent AI Infrastructure:** Low-latency edge inference node (Raspberry Pi 5 / Hailo-10H NPU) achieving 10–25x throughput over CPU execution; hybrid local-cloud routing plane; zero-trust proxy enforcing inline PII redaction via named entity recognition before cloud transit.
- **Chord-Forge:** Vector-based calculation engine mapping finger placement and chord voicings across stringed instrument configurations; containerized cross-platform deployment.

AWARDS & HONORS

NREL President's Award (2022) · NREL Key Contributor Award (2022, 2023) · Illinois Cyber Security Scholars Program (CyberCorps SFS) · Hites Endowment