Consortium Enabling Cybersecurity Opportunities & Research

SAND2019-7977D

Field Device Assessment Methodology

Maria C. Gaitan-Cardenas, North Carolina A&T
Zoe Dormuth, University of Minnesota

Project Mentor: Mark Woodard, 5883

CECOR

Problem Statement

Industrial Control System (ICS) field devices play a critical role in the safe and reliable operation of critical systems.

- Devices are often full of cyber security vulnerabilities that can lead to significant risks for mission performance, or even unsafe conditions during routine Operational Test and Evaluation.
- Cyber security issues faced by ICS differ from typical information technology, and this requires a different and more specific approach to assess, test, and mitigate ICS vulnerabilities.
- Finding vulnerabilities in ICS field devices becomes increasingly necessary as technology continues to grow and develop.

Using the FDAM approach allows for the finding and mitigation of device vulnerabilities.

Objectives

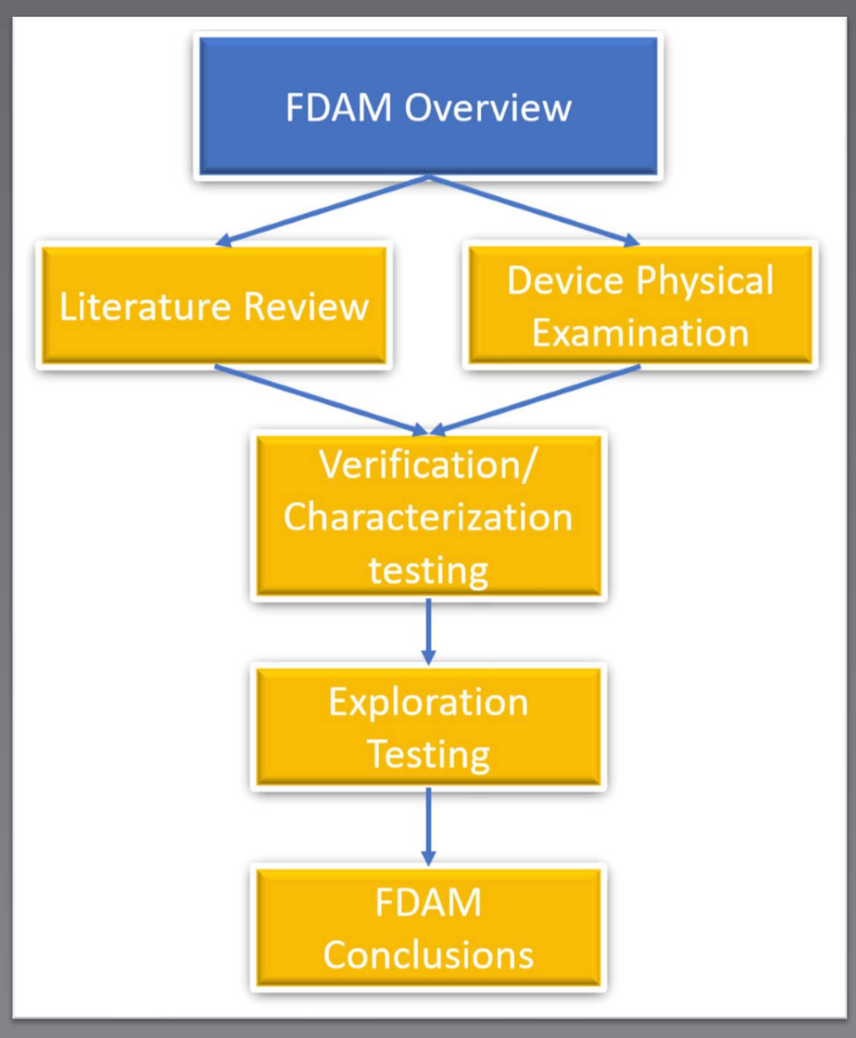
Assess **physical** and **software** vulnerabilities of an SEL 2414 Transformer Monitor Relay using the FDAM approach.

Technical Challenges

- Getting familiarity ICS protocols, device types and vendor software.
- Effectively communicating with the SEL-2414 through Serial connection.
- Implementing a brute force search to find undocumented commands through the serial connection.
- Distinguishing the difference between ICS and IT security.

Approach

The Field Device Assessment Methodology (FDAM) approach focuses on mitigating risks specifically for ICS field devices.



- **Literature Review:** Gather background information about the device and research both known and potential vulnerabilities and mitigations.
- **Device Physical Examination:** Examine hardware subcomponents that might have potential vulnerabilities.
- **V/C Testing:** Determine the effects of the vulnerabilities and mitigations that were selected for testing.
- **Exploration Testing:** Further exploration of newly discovered potential device or application-specific vulnerabilities.
- FDAM Conclusion: Present and compile the information found through the FDAM approach. Assign risk scores to vulnerabilities and propose mitigations.

U.S. DEPARTMENT OF ENERGY
National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2019-???????

Sandia National Laboratories