U.S. DEPARTMENT OF ENERGY

OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Application of OT Ontologies to Protect and Control Access to Grid Assets Preventing Cyber Grid MIS-Operations

TDI Technologies, Inc

Samantha Pelletier

Cybersecurity for Energy Delivery Systems (CEDS) Peer Review

October 6-7, 2020

Project Overview

Objective

- Prevent Grid Mis-Operation by protecting and securing human access to operational assets, therefore preventing malicious and inadvertent operational commands leveraging MITRE ICS ATT&CK framework.

Schedule

- Project start (post Budget): 11/20/19
- Project end: 03/20/21
- Key Deliverables:
  - Define ATT&CK strategies that could cause high risk grid exposure and classified ones applicable to our use case.
  - Develop use cases to demonstrate mis-operation and protected mis-operation with the project.
  - Implement OT architecture to simulate Utility and Oil & Gas environments.

Total Value of Award:	**$ 1,865,615**
Funds Expended to Date:	**% 9**
Performer:	**TDI Technologies, Inc**
Partners:	**Red Trident** **MITRE** **PNNL** **Dominion Energy**

Advancing the State of the Art (SOA)

- **Describe current "state of the art"**
  - ATT&CK frameworks were defined for IT environments but not for ICS environments.
  - Project was going to study feasibility of creating a ICS version of the IT ATT&CK framework.
  - Unbeknownst to TDI, MITRE was creating ICS framework which has subsequently been released.
- **Describe the feasibility of your approach**
  - Is it feasible to intercept interactive human activity, compare it to TTP's (Tactics, Techniques, Procedures) from the ICS ATT&CK framework and stop mis-operation by preventing commands from making it an asset?
- **Describe how your approach is better than the SOA**
  - Extend and enhance ICS ATT&CK framework to include operational TTP's which can be validated, approved, and automated preventing mis-operation.
  - Improve Commercial industry technology that provides secure human access which can be captured, interrogated, and validated against operational and adversarial TTP's defined by MITRE and users of the technology.
    - Control and log human access to OT assets.
    - Collect and identify current and approved settings of OT Assets.
    - Identify, Alarm, and Compare human changes to operational technology to prevent human mis-operation.
    - Understand & Advise OT Settings as well as configuration changes which define safe operational characteristics and unsafe changes.

Advancing the State of the Art (SOA)

- **Describe how the end user of your approach will benefit**
  - An actor gains access to Critical Assets and issues commands as they interact with those assets, the solution will intercept and evaluate the risk of the command (or increased risk of the sequence of commands) based on the playbooks that represent the various TTP's. This will prevent the actor from executing an operational command that could change a configuration in a way that could cause disruptive or destructive events(s) to occur which may result in grid failure, production stoppage, or physical damage to humans and/or machines.

- **Describe how your approach will advance the cybersecurity of energy delivery systems**
  - Currently the ability to Identify, Protect, Detect, Respond, and Recover, from human actions beyond the HMI or Vendor Application are not available. This approach not only considers the NIST cybersecurity impact of an adversary, but enhances coverage to include operational considerations for insiders (vendors, privileged actor, and contractor). It minimizes the need for operations to become cyber security experts. By combining known adversarial TTPs with business operational TTPs and automation, our solution shortens the process of Observing, Evaluating, Deciding and Acting which can prevent mis-operation with minimal human interaction.

- **Describe the potential for sector adoption**
  - This solution captures business knowledge around a static world and institutionalizes it to solve cyber security issues and eliminates the challenge of an aging workforce resulting in loss of operational best practices.

Progress to Date

Major Accomplishments

- **Describe major accomplishments and milestones achieved**
  - Created the project team and brought a dedicated resource with industry knowledge.
  - Completed Project Planning and Management Task level.
  - Currently mid-way through Research and Development Task area.
    - Use Cases defined with Industry feedback.
    - Lab architecture was defined and documented.
    - Configuration of lab was constructed to simulate Utilities and Oil & Gas environments.

Challenges to Success

Award budget not finalized until 8/01/2019, award granted on 09/25/2018

- Project definition refinement after award and re-approval (6 months).
- Performed 6 months of initial research and plan development “at-risk”.
- Worked through notional solution to be prepared for budget release.
- Consulted with partners “at-risk” to determine use-cases for research.

COVID-19 pandemic

- Using ConsoleWorks, our team was able to securely get access into our internal infrastructure to begin working on configuration of assets.

Working with the unknown

- Validate the feasibility of operational TTPs within the MITRE framework.
- OT Protocols.

Collaboration/Sector Adoption

Plans to transfer technology/knowledge to end user

What category is the targeted end user for the technology or knowledge?

- Asset Owners, Vendors, and OEMs are all targets.

What are your plans to gain industry acceptance?

- Industry advisement team.
- White papers and other collateral such as user guides.

Describe testing and demonstrations planned

- Demos to advisory team.
- Demos at industry events.
- Video demo POC.

What is the timeline for demonstration and sector adoption?

- First demo is a short POC video.
- By the first of the year doing more advanced POC demonstration to the advisory board to get a deeper understanding of requirements.
- Enter into development phase based on feedback from advisories and DOE.

Next Steps for this Project

Approach for the next year or to the end of project

- Complete implementation of simulated Utilities and Oil & Gas environments in our lab.
- Implement ConsoleWorks and our integration of the MITRE ATT&CK techniques that have been targeted.
- Implement automated responses to prevent mis-operations by human interaction.
- Perform in-house demonstrations.
- Present and demonstrate with Industry.
- Commercialization planning.

Upcoming significant events

- Demonstrations of POC.
- Anticipated discoveries based on doing demonstrations with industry advisors.

MITRE ATT&CK TTP's Selected

Modify Control Logic (T833)

- Adversaries may place a malicious code in a system, which can cause the system to malfunction by modifying its control logic. Control system devices use programming languages (e.g. relay ladder logic) to control physical processes by affecting actuators, which cause machines to operate, based on environment sensor readings. These devices often include the ability to perform remote control logic updates.
  - **Example:** Remotely be able to change the safety logic in a PLC so that the system does not respond to a critical event and allows the process to operate outside the intended boundaries of control.
  - **Example:** a motor automatically stops at 3 feet above 0 feet to prevent cavitation and damage to motor. Logic is remotely changed to allow the pump to run to zero feet, overheat, and explode.

Unauthorized Command Message (T855)

- Adversaries may send unauthorized command messages to instruct control systems devices to perform actions outside their expected functionality for process control. Command messages are used in ICS networks to give direct instructions to control systems devices. If an adversary can send an unauthorized command message to a control system, it can then instruct the control systems device to perform an action outside the normal bounds of the device's actions. An adversary could potentially instruct a control systems device to perform an action that will cause an Impact
  - **Example:** Remotely being able to send a packet to a control system that will change its state from running to stop. Based on system and protocol vulnerabilities, an operator may not see the change in PLC status and run a plant into being offline

MITRE ATT&CK TTP's Selected

Detect Operating Mode (T868)

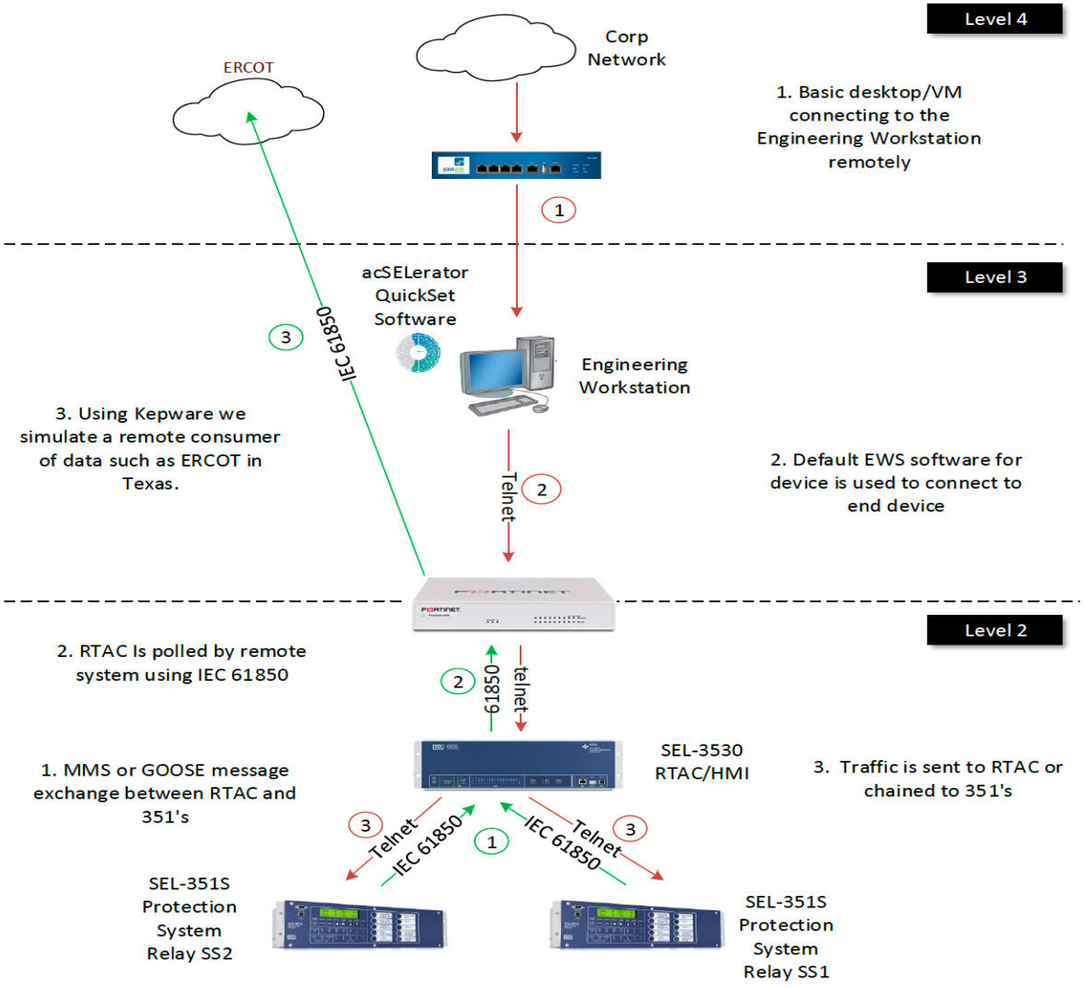
- Adversaries may gather information about the current operating state of a PLC. CPU operating modes are often controlled by a key switch on the PLC. Example states may be run, prog, stop, remote, and invalidate. Knowledge of these states may be valuable to an adversary to determine if they are able to reprogram the PLC.
    - **Example:** Remotely access any interface that would allow an adversary to see the status of a controller. Run a show status command, allow remote engineering software to run the command, or allow a tag browser to see valid tag data representing controller status.

Detect Program State (T870)

- Adversaries may seek to gather information about the current state of a program on a PLC. State information reveals information about the program, including whether it's running, halted, stopped, or has generated an exception. This information may be leveraged as a verification of malicious program execution or to determine if a PLC is ready to download a new program.
    - **Example:** Program States in a PLC are typically based on variables or static settings forcing the system to run continuously, time based, or event driven. Many processes have separate programs that run at different stages of a process such as start-up, normal, upset, shutdown. In addition to having programs for the various functions of a system. Knowing the state can determine what stage the process is in or if you have made an impact to the system.

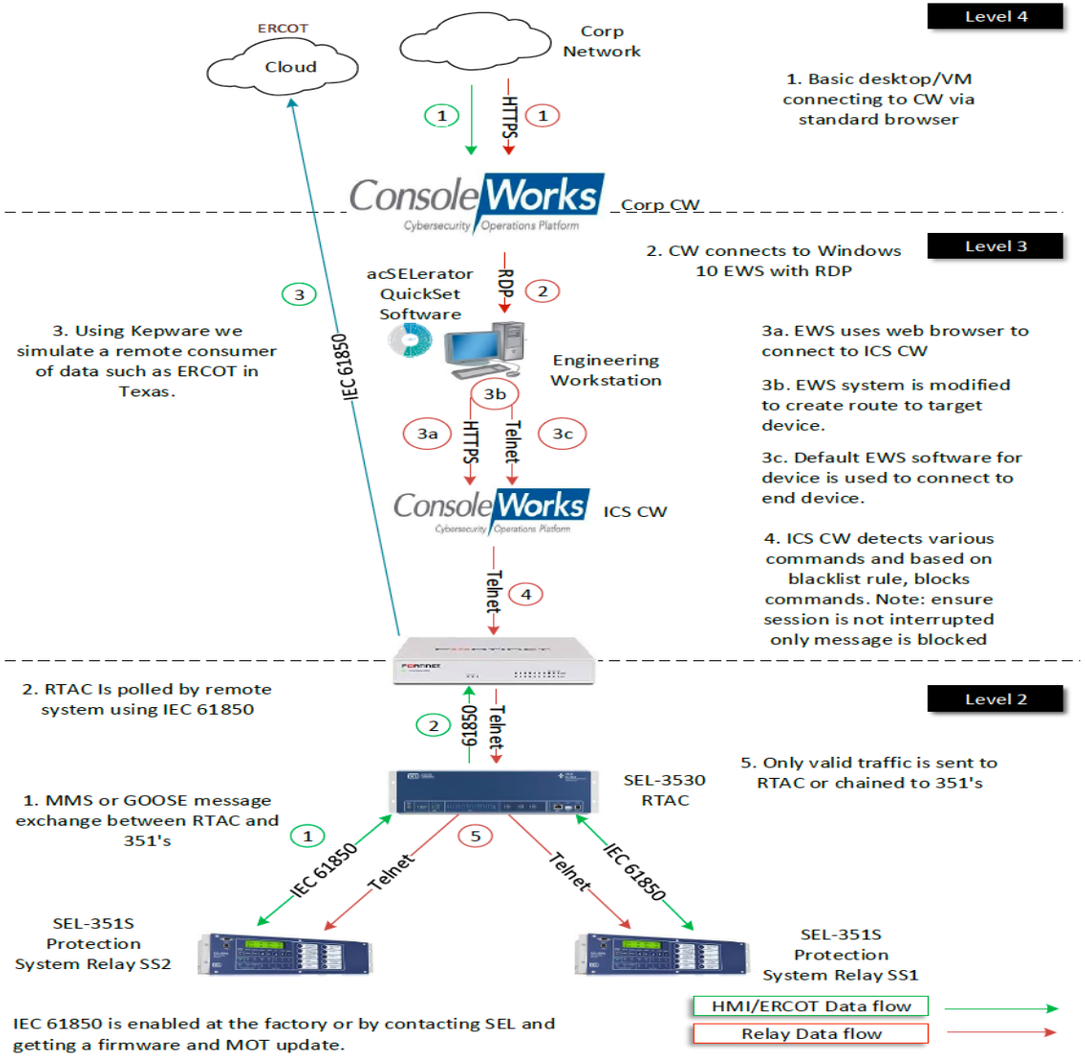
Scenario without Solution

In this scenario, we are showing how a real-world industry operates when trying to connect to the RTAC or relays at level 2 of the Purdue model.
This shows how vulnerable and unsecure the connections are without monitoring or controlling who is accessing what.



Scenario with Solution

In this scenario, we are showing how a real-world industry operates when trying to connect to the RTAC or relays at level 2 of the Purdue model. This shows a control and monitoring solution at different levels of the Purdue model which will manage who is accessing what.



POC Demo Video

This proof of concept was created as an example of how the ConsoleWorks technology can be used to intercept commands to prevent possible grid mis-operation.

The research project will leverage the MITRE ATT&CK framework for Industrial Control Systems as a method of evaluating the sequence of actions from a possible bad actor.

https://www.tditechnologies.com/de-foa-0001755-poc/