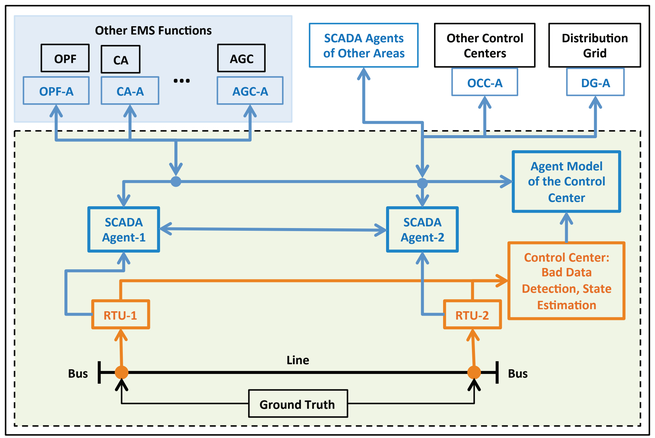
even if some agents may be compromised

- Validate proof by modeling and simulation
- Implement proof-of-concept on SCADA devices



SCADA Agent Architecture

Test Bed Data Flow

Table 1: SCADA Attack Matrix

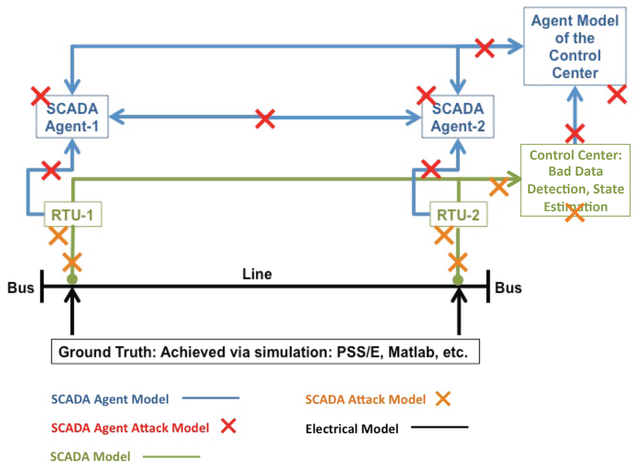
Adapted from [2], which appears in [1].

Description of Attack	Type of Attack	Attack Motive	Impact to Victim	Impact Rating (1 = largest immediate impact 5 = least immediate impact)	Items Needed for Attack	Estimated Time to Implement Once System is Compromised
Denial of Service	System Shutdown	Wish to take down server and cause immediate shutdown situation	SCADA Server locks up and must be rebooted. When SCADA Server comes back on-line, it locks up again. Operations can no longer monitor or control process conditions, and the system will ultimately need to be shut down	2	Ability to flood the server with TCP/IP calls, the IP Address of SCADA Server, and the path to the server	5 min.
Take Control of SCADA System	Gain Control	Gain control of SCADA System to impact damage on industrial systems, possibly causing environmental impact, and damage corporate identity through public exposure	Highest impact, since attacker can then manually override safety systems, shut down the system, or takes control of the plant operational conditions.	1	IP Address of SCADA Server, path to server, and either Trojan or back door installed. (Can also use PCAnywhere, Terminal Services, SMS, or other system admin services.)	1 hr.
Change Data Points or Change Setpoint(s) in SCADA System	Information Tampering	Desire to modify corporate data or process setpoints for malicious purposes	Higher impact since modified setpoint or control points can have adverse effects on controlled process, and potentially cause a shutdown condition	2	IP Address of SCADA Server, access to these servers, and some knowledge of SCADA software system inner workings	45 min.
Modify Data points on SCADA graphics to deceive Operators that system is out of control and must ESD (Emergency Shut Down)	System Shutdown	Cause danger to the facility or company by staging a false alarm shutdown of the plant or facility	Operations can no longer trust the SCADA System, and the attacker has deceived the Operator into thinking that there was an emergency condition in the plant	2	IP Addresses of SCADA servers, and access to them through the company network	45 min.
Capture, Modify, or Delete Data Logged in Operational Database SQL Server, PI Historian, Oracle, Sybase, etc.)	Information Tampering	Desire to modify corporate data or process setpoints for malicious purposes	Higher impact since modified setpoint or control points can have adverse effects on controlled process, and potentially cause a shutdown condition	3	IP Address of SCADA Server, path to database server, and knowledge of SCADA software structure	45 min.

Red box highlights: This research directly responds to this threat.

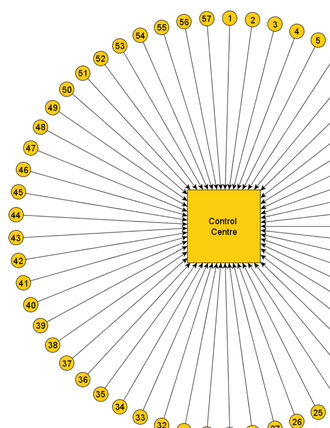
Orange / yellow box highlights: This research has the potential of responding to this threat. The potential response is not yet under investigation.

4.7 Capabilities for automated response to cyber incidents, including best practices for implementing these capabilities available



Five Simulation Models Required to Study the Proposed SCADA Agent Protection System

Power Flow on the power line, expresse of line capacity.



For now, we assume that all RTUs comm with the control center.

Team Members

Joseph Andrew Giampapa
Software Engineering Institute
PI, Project Point of Contact

Gabriela Hug-Glanzmann
Electrical and Computer Engineering,
Carnegie Mellon University
Co-PI, Assistant Professor

Soummya Kar
Electrical and Computer Engineering,
Carnegie Mellon University
Researcher, Assistant Research Professor

Kawa Cheung
MS Student,
Electrical and Computer Engineering,
Carnegie Mellon University
Research Assistant

Mayank Kamalchand Malu
MS Student,
Institute for Software Research,
Carnegie Mellon University
Research Programmer

Contact Information

Joseph Andrew Giampapa
Senior Member of the Research Technical Staff
Research, Technology, and System Solutions (RTSS) Program
Software Engineering Institute
Telephone: +1 412-268-6379
Email: garof@sei.cmu.edu

RTSS Concept Lab

Software Engineering Institute | Carnegie Mellon

ie Roadmap interactive energy Roadmap to Achieve Energy Delivery Systems Cybersecurity