Designing SCADA Systems for the Self-Verifiability of Their Security & Survivability

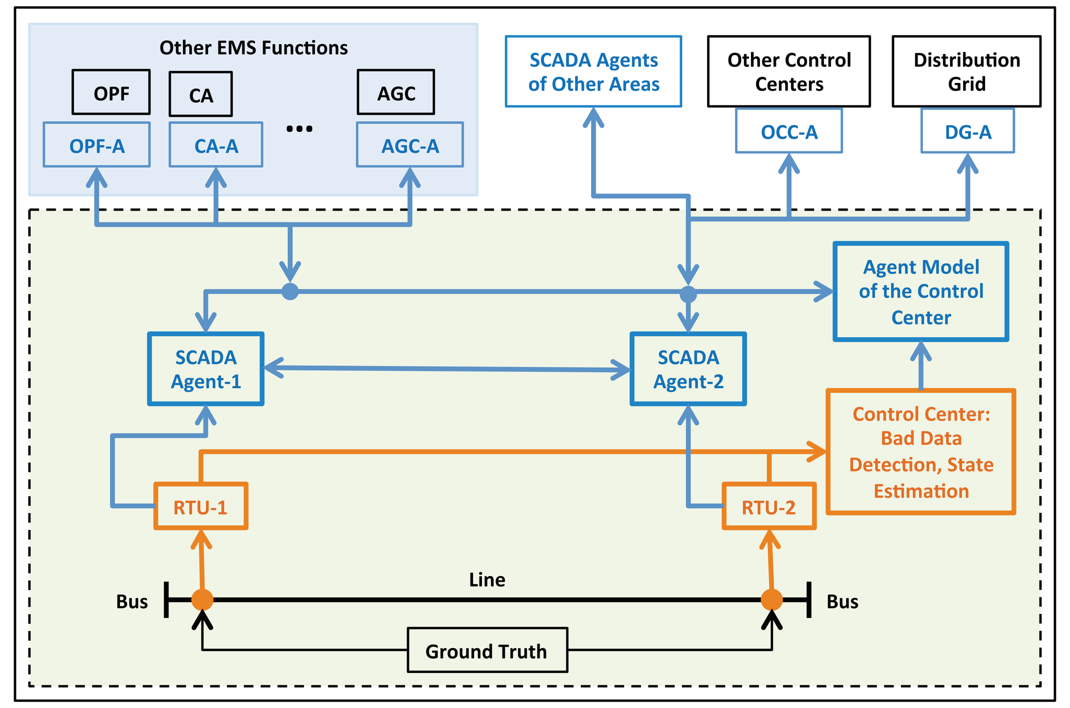
A Cyber-Physical and Agent-Based Approach to Detecting and Recovering from a False Data Injection Attack on a Power Grid SCADA System

Objective

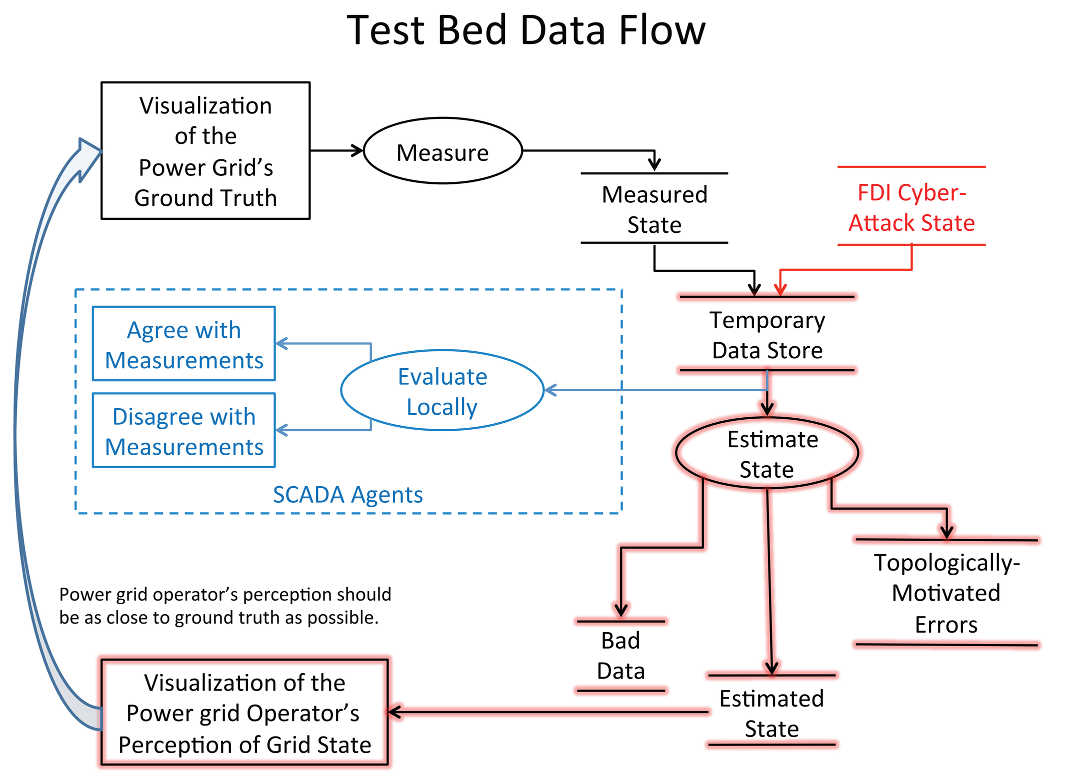
Provide algorithms that can enable SCADA / EMS systems to autonomously detect, isolate, and respond to false data injection (FDI) cyber-attacks

Technical Approach

- Focus on FDI attacks that create false sense of observable transmission grid state (address unobservability in future)
- Introduce autonomous software agents to model cyber-physical properties of the grid / EMS at their cyber-physical location
- Theoretically prove that for any and all vectors of FDI cyber-attack, the agents can autonomously detect it, 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.

Roadmap Milestones

3. Develop and Implement New Protective Measures to Reduce Risk

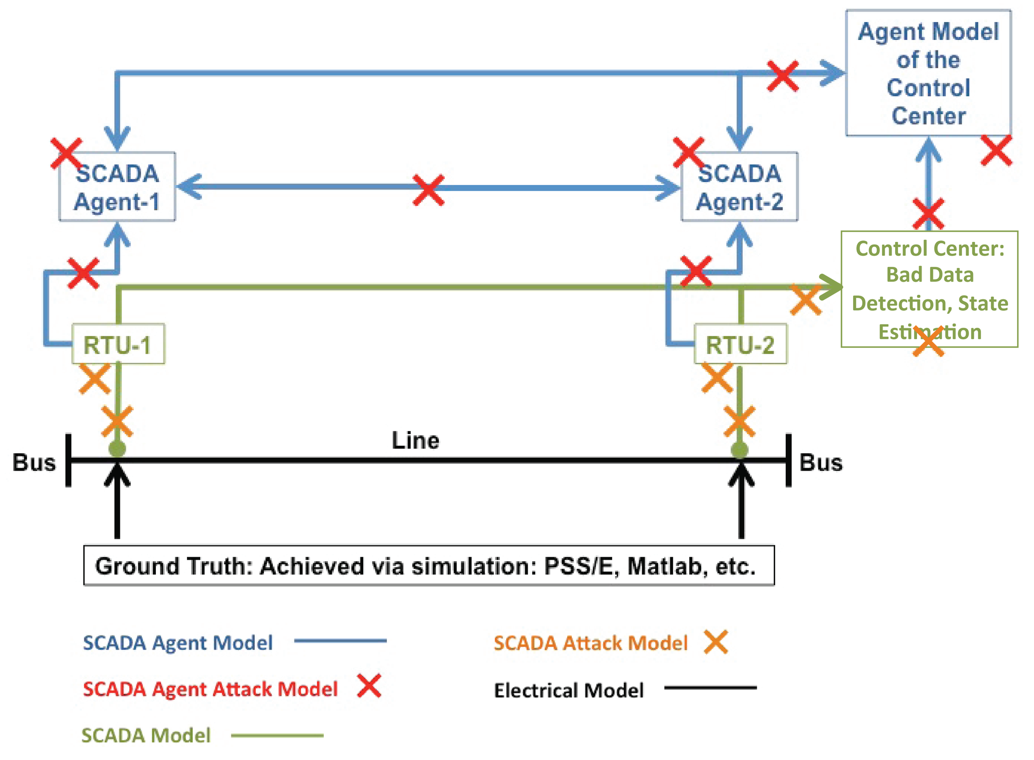
3.1 Capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes commercially available

3.5 Capabilities that enable security solutions to continue operation during a cyber-attack that are available as upgrades and are built in to new security solutions

4. Manage Incidents

4.1 Tools to identify cyber events across all levels of energy delivery system networks commercially available

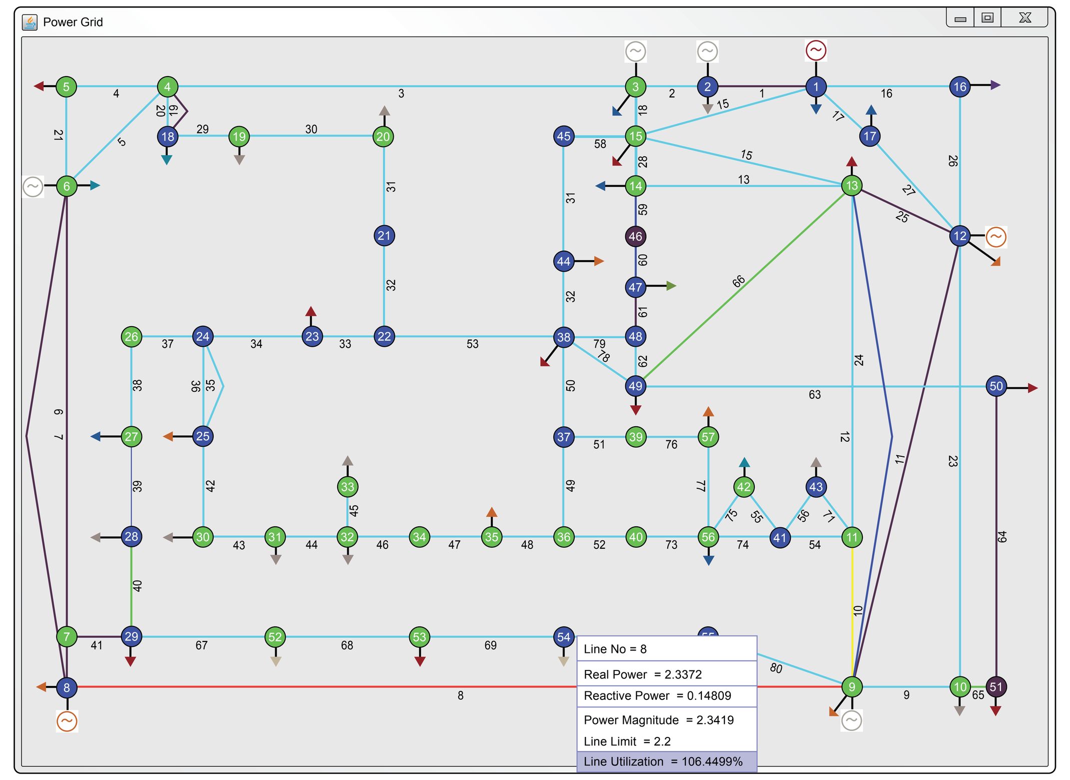
4.7 Capabilities for automated response to cyber incidents, including best practices for implementing these capabilities available



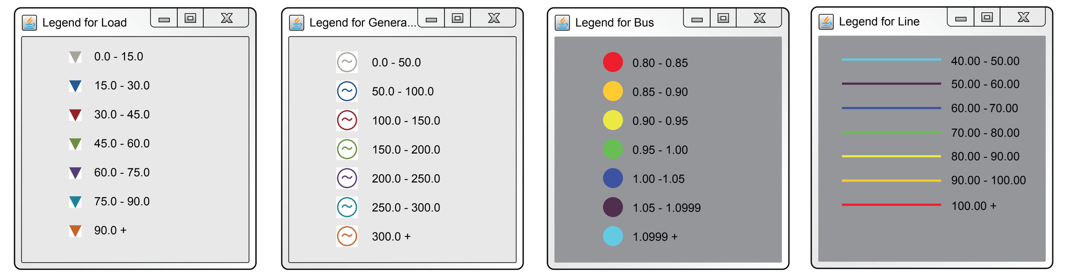
Five Simulation Models Required to Study the Proposed SCADA Agent Protection System

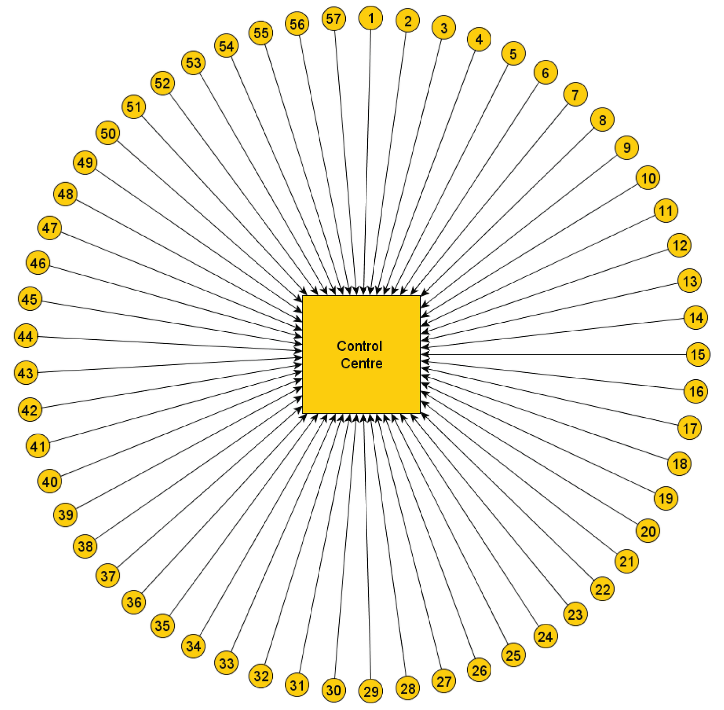
The Simulation Test Bed

Power grid, showing an overload condition on Line 8. Clicking the mouse on the line shows its properties.



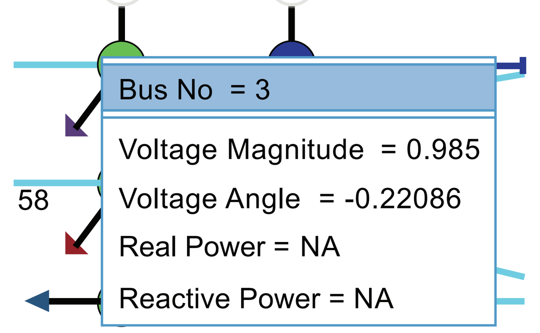
Power Flow on the power line, expressed as a percentage of line capacity.



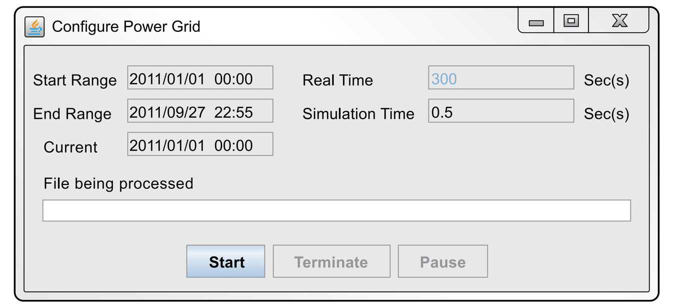


For now, we assume that all RTUs communicate directly with the control center.

Clicking the mouse over a bus icon shows its properties.



The main control window for the power grid simulator. By default, a half-second of simulation time corresponds to 5 minutes of real time. We use historical data published by the Bonneville Power Administration on their website. Our current data set is for the period 1 January–27 September 2011.



Total load, expressed in per unit (p.u). Load measurements are represented in 5-minute intervals.

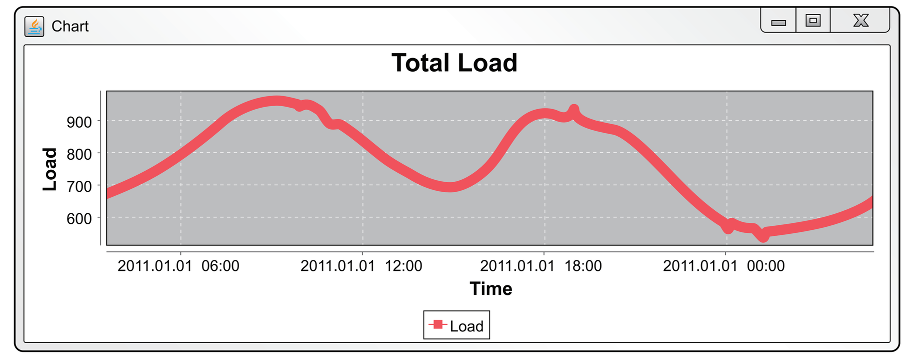


Table 2: Summary of Results from [4]

	Method	Pros	Cons
1	TAA-AAVD	1. Will find all AC measurements for the AMS, including for buses with no power injections 2. AMS includes AC measurements.	1. Requires comprehensive knowledge of the power grid topography and of the SCADA system
2	AAMA-AAVD	1. AMS includes AC measurements. 2. Does not require knowledge of grid topography	1. Will not consider measurements for buses with no power injections 2. Non-linear Jacobian matrix computations
3	TAA-DAVD	1. Will find all DC measurements for the AMS, including buses with no power injections 2. Linear matrix, easier to calculate	1. Prone to introducing error that is detectable by bad data detection 2. Requires comprehensive knowledge of the power grid topography and of the SCADA system
4	DAMA-DAVD	1. Will find DC measurements for AMS 2. Does not require knowledge of grid topography 3. Linear matrix, easier to calculate	1. Prone to introducing error that is detectable by bad data detection 2. Will not consider measurements for buses with no power injections

Results to Date: Techniques to Assess AC Grid Vulnerabilities

- Self-assessment techniques appear in [4].
- *Table 2* summarizes the techniques.
- Please see summary white paper.

Take-Away Message

Comprehensive power grid SCADA security requires a cyber-physical systems approach.

- ***Evaluate the threat with respect to its impact on properties of the power grid, not just the cybernetic infrastructure.***
- ***Remedies should also focus on mitigating the impact of the threat, especially for cost-effective solutions to cyber-security.***

Knowledge to avert threat can be leveraged from multiple perspectives and subsystems:

- ***Electrical properties, control theory, cybernetic properties***
- ***Knowledge from other EMS functions***

References

1. National Communications System (NCS), Technical Information Bulletin 04-1, "Supervisory Control and Data Acquisition (SCADA) Systems," NCS TIB 04-1, October 2004, pp. 76. http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf
2. J. Pollet, "SCADA Security Strategy," Plant Data Technologies. 8 August 2002. Appears as "Table 6.1 SCADA Attack Matrix," in [1].
3. Energy Sector Control Systems Working Group (ESCSWG), "Roadmap to Achieve Energy Delivery Systems Cybersecurity," September 2011, p. 81. https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/roadmap.pdf
4. G. Hug-Glanzmann and J.A. Giampapa, "Vulnerability Assessment of AC State Estimation with Respect to False Data Injection Cyber-Attacks," in *IEEE Transactions on Smart Grid*, Vol. 3, No. 3, pp. 1362–1370, September 2012, DOI: 10.1109/TSG. 2012.2195338. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6275516&isnumber=6275510
5. A. Tajer, S. Kar, H.V. Poor, and S. Cui, "Distributed Joint Cyber Attack Detection and State Recovery in Smart Grids," in *Proceedings of Cyber and Physical Security and Privacy* (IEEE SmartGridComm), © 2011 IEEE, pp. 202–207. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06102319

Disclaimer

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

ieRoadmap interactive energy Roadmap to Achieve Energy Delivery Systems Cybersecurity