# SCEPTRE

## Industrial Control System Modeling and Simulation

Brian Wright

Sandia National Laboratories

# Why SCEPTRE?

Live control system testing is impractical
- Potential damage to the real system and dangers to human life

Traditional test beds are burdensome
- Expensive to build, maintain, configure, and operate

Lab-scale hardware testing setups are insufficient
- Effective at testing devices in isolation, but detrimental effects might only be seen in the context of a larger, networked system

Network simulation
- Mapping network events to physical process effects is difficult

SCEPTRE provides a cyber-physical interface to show how cyber-initiated events affect the physical world (and vice versa)

# SCEPTRE Overview

SCEPTRE is an application that uses an underlying network (e.g. Sandia's Emulytics™ Platform technologies) to run

ICS devices (simulated, emulated, real) communicate and interact via high fidelity SCADA protocols

Process simulation data is provided to all the ICS devices

All ICS devices are able to interact with the simulation, providing both updates and subscribing to the current state of the simulation

When the simulation state updates, all devices receive the current state so there is a common view of the simulation

Overall simulation is able to bridge multiple infrastructures into the same experiment to show interdependencies.

# SCEPTRE Components

## Control Systems devices

- Low fidelity simulated ICS devices
  - RTUs, PLCs, protection relays, FEPs
- Emulated PLCs, HMI services
- Hardware-in-the-loop (HITL) devices such as relays, PLCs, RTUs

## High fidelity SCADA protocols

- ModbusTCP, DNP3, IEC 61850 and 60870
- Written to specification
- Enabling technology that allows communication between HITL and simulated devices

## Process simulation

- Leverage industry standard software where possible (V&V)
  - PowerWorld, PyPower, PSS/E
- Develop our own simulated process when needed
  - Water treatment, refinery, natural gas pipeline, railroad signaling

# SCEPTRE Use Cases

Test and Evaluation
- Hardware, architectures, TTP, technology solutions
- Vary model fidelity depending on the questions being asked and scope

Mission rehearsal

Analysis
- Deploy network of interest to understand vulnerabilities and exploitable avenues
- Identify critical components on the control network and in the underlying infrastructure
- Ability to model infrastructure interdependencies within the same simulation

Training and Exercise Support
- Look-and-feel of real ICS networks by integrating industry HMI and service tools
- Faithful protocol traffic for deeper network inspection
- Ties to process models illustrate impacts of control system changes on physical systems
- Provided SCEPTRE environments to support various exercises

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Sandia National Laboratories

# Secure, Scalable Control and Communications for Distributed PV


Sandia National Laboratories

Principal Investigator: Jay Johnson

Contributors: Ray Byrne, Ricky Concepcion, Matt Reno, Jimmy Quiroz, Felipe Wilches-Bernal, Patricia Cordeiro, Cedric Carter, Ifeoma Onunkwo, Brian Wright, Ross Guttromson, Trevor Hutchins, Nicholas Jacobs, Christine Lai, Jordan Henry, Jason Stamp, Derek Hart



Sandia National Laboratories is a multi-mission 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-NA-0003525.

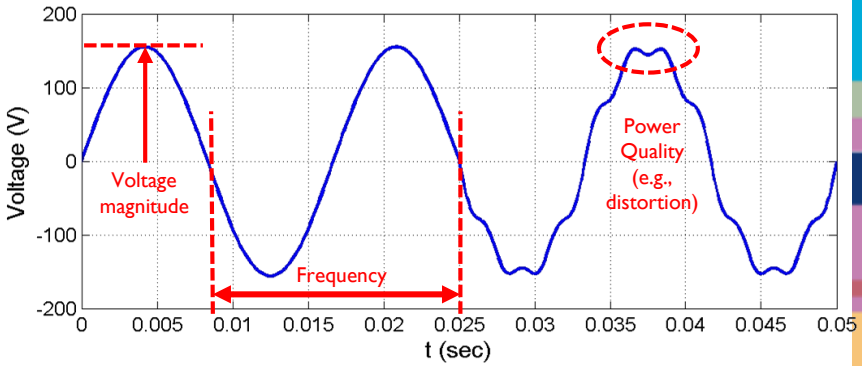
# Increasing solar penetrations using communications

Large-scale deployment of solar energy is limited by power system constraints:

- Voltage requirements (ANSI C84.1) and protection coordination on distribution systems
- Bulk system requirements (e.g., contingency reserves) as more generation becomes inertialess

These issues can be mitigated using inverter grid-support functions

- Grid operators need the ability to remotely adjust PV grid-support functions to unlock the full potential of distributed energy resources (DER)
- Interconnection standards (e.g., CA Rule 21, IEEE 1547) are being updated to require DER communications




# DER communications are a cyber security risk

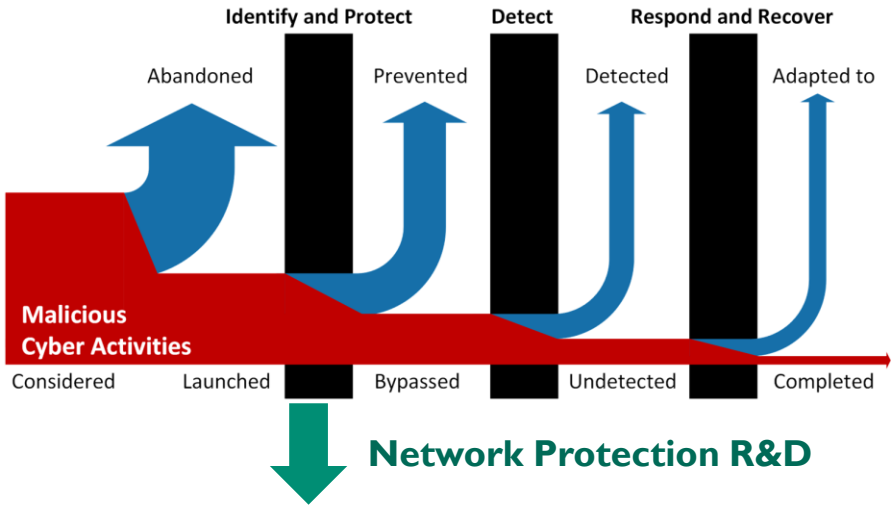
Adding DER communication requirements introduces new cyber security risks

These risks can be mitigated using a multi-pronged approach:

- Stakeholder/industry outreach and education
- Cyber security standards and guidelines
- Research and development

Project goal: Find optimal network architecture by quantifying tradeoffs between cyber security and communication latency/power system performance

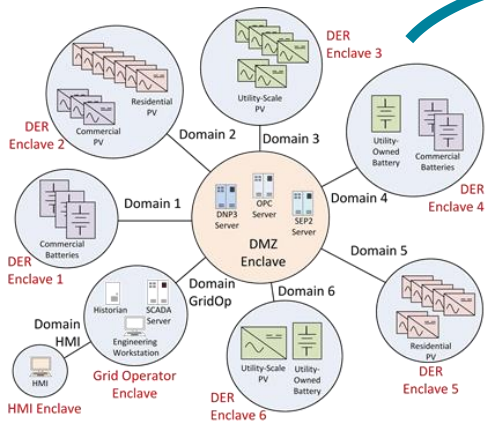
- Phase 1: compare power system performance by varying communication latency, dropout, and availability metrics.
- Phase 2: compare cyber security architectures by studying their effect on communication and cyber security metrics.

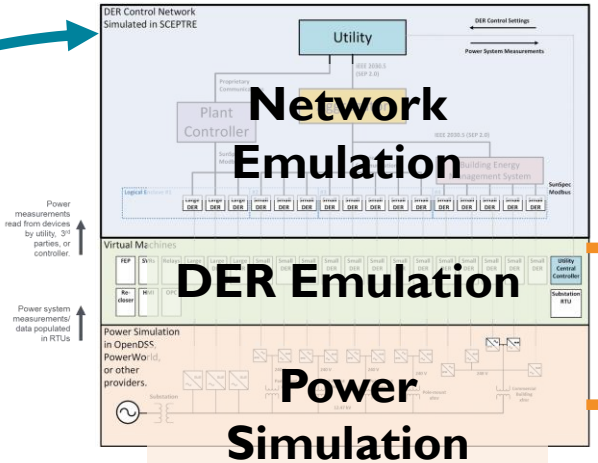



J. Johnson, "Roadmap for Photovoltaic Cyber Security," Sandia Technical Report, SAND2017-13262, Dec 2017.

# Tying cyber security design to grid performance

DER control network architectures are emulated in the SCEPTRE environment.



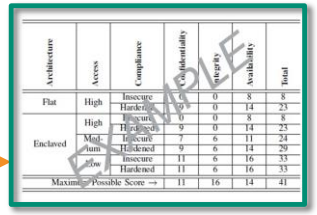



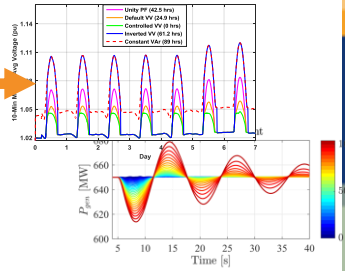

SCEPTRE: a live, virtualized power system and control network co-simulation platform

SCEPTRE outputs:
- Cyber security metrics
- Communication parameters
- Power system performance

IDART
Information Design Assurance Red Team

Power system studies

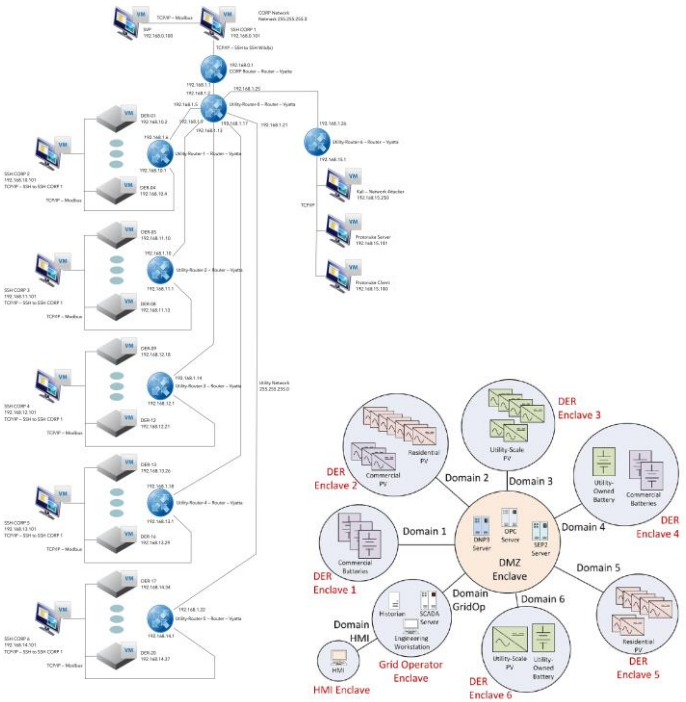


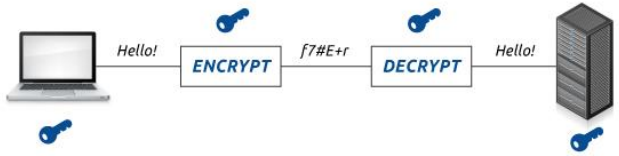

Multiple DER network architectures will be simulated to determine:
1. Cyber security resilience
2. Communication latency, dropout, and availability
3. Power system performance metrics (voltage, nadir, etc.)

# Cybersecurity Features Implemented in SCEPTRE

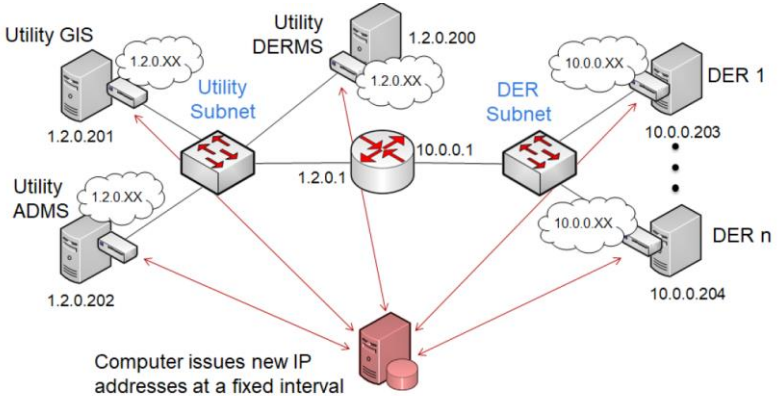
1. Segmentation




## 2. Encryption




## 3. Moving Target Defense



# Red Team Assessments

The red team modeled a threat from an attacker equipped with specialized knowledge of DER system protocols with considerations for potential insider access, not nation state adversary

The red team had two forms of access to the system, representing:

- **Network Attacker -** An intruder who has access to a subnet where the inverters are deployed. This adversary has no access to the DER device but does have access to one of the network switches (through public networks or as ISP operator).
- **Homeowner Attacker -** The intruder is on the DER home area network (HAN) with physical access to the DER.

Red Team conducted the following:

- Reconnaissance: inspecting the system to determine IP address, IP ports, slave ID, protocols, etc.
- Code Injection: malicious code injection, such as a reply attack.
- Interception: man-in-the-middle (MITM) or eavesdropping of authenticated communications.
- Denial of Service: rendering the system unusable to authorized users, such as overloading the RTU processors.

# Methodology

Assessment incorporated elements from:

- Sandia National Laboratories' Information Design Assurance Red Team (IDART)
- NIST's Guide to Industrial Control Systems (ICS) Security Guidelines
- Department of Homeland Security's ICS-CERT Recommended Best Practices
- Collective expertise of PV inverter communications

The general process:

- A Kali Linux machine probed available subnetworks. Nmap and OpenVAS provided IP identification, host fingerprinting and vulnerability assessments of the devices on the network.
- TCPdump and Wireshark captured packets on the flat networks for use in a replay attacks, and ID'ed comm protocols and encrypted links
- SunSpec Dashboard and ModbusPal were used to craft specific protocol traffic to the target devices.

For each scenario, the DER communication network was evaluated for vulnerabilities to DoS, Replay, and MITM attacks. Risk scores were then calculated for:

- Confidentiality based on the replay and MITM attacks
- Integrity based on the replay and MITM attacks
- Availability based on the DoS attack
- A total risk score (3-15) for the given security features

# Theoretical vs Actual Security Scores for Different Security Defenses

If properly implemented, the following results were expected:

| Topology | Encryption | Access | Attacks | | | Risk Level | | | Total Score |
|---|---|---|---|---|---|---|---|---|---|
| | | | DoS | Replay | MITM | C | I | A | |
| Flat | None | Insider | ✓ | ✓ | ✓ | 5 | 5 | 5 | 15 |
| Flat | None | Outsider | ✓ | ✓ | ✓ | 5 | 5 | 5 | 15 |
| Flat | RFC 7539 | Insider | ✓ | | | 1 | 1 | 5 | 7 |
| Flat | RFC 7539 | Outsider | ✓ | | | 1 | 1 | 5 | 7 |
| Segmented | None | Insider | ✓ | o | o | 3 | 3 | 4 | 10 |
| Segmented | None | Outsider | ✓ | | | 2 | 2 | 3 | 7 |
| Segmented | RFC 7539 | Insider | ✓ | | | 1 | 1 | 4 | 6 |
| Segmented | RFC 7539 | Outsider | ✓ | | | 1 | 1 | 3 | 5 |
| Flat MTD | None | Insider | ✓ | | | 1 | 1 | 5 | 7 |
| Seg MTD + WL | RFC 7539 | Outsider | | | | 1 | 1 | 2 | 4 |

- ✓ indicates the attack is possible for all DER devices
- o indicates the attack could succeed for a portion of the DER devices
- WL indicates whitelisting of the MTD network
- RFC 7539 is the IETF Protocol for the ChaCha20 stream cipher and Poly1305 authenticator

The red team was able to subvert the environments and found the following:

| Topology | Encryption | Access | Attacks | | | Risk Level | | | Total Score |
|---|---|---|---|---|---|---|---|---|---|
| | | | DoS | Replay | MITM | C | I | A | |
| Flat | None | Insider | ✓ | ✓ | ✓ | 5 | 5 | 5 | 15 |
| Flat | None | Outsider | ✓ | ✓ | ✓ | 5 | 5 | 5 | 15 |
| Flat | RFC 7539 | Insider | ✓ | ✓ | ✓ | 5 | 5 | 5 | 15 |
| Flat | RFC 7539 | Outsider | ✓ | ✓ | ✓ | 5 | 5 | 5 | 15 |
| Segmented | None | Insider | ✓ | ✓ | ✓ | 5 | 5 | 5 | 15 |
| Segmented | None | Outsider | ✓ | ✓ | | 5 | 5 | 5 | 15 |
| Segmented | RFC 7539 | Insider | ✓ | ✓ | ✓ | 5 | 5 | 5 | 15 |
| Segmented | RFC 7539 | Outsider | ✓ | ✓ | o | 5 | 5 | 5 | 15 |
| Flat MTD | None | Insider | ✓ | | | 1 | 1 | 5 | 7 |

- ✓ indicates the attack is possible for all DER devices
- o indicates the attack could succeed for a portion of the DER devices
- WL indicates whitelisting of the MTD network
- RFC 7539 is the IETF Protocol for the ChaCha20 stream cipher and Poly1305 authenticator

- Results show the importance of properly deploying the environments.
  - The bump-in-the-wire device creating the RFC 7539 SSH tunnel was left unsecured (no password), which enabled the red team to pivot into the rest of the network and attack all the DER devices using replay and MITM attacks.

# Findings

Denial of service is very difficult to prevent. Aggregators/utilities should implement firewall whitelists to prevent these types of attacks.

Segmentation makes it difficult for the adversary to move between subnets. Only through flaws in the networking implementation could the red team manipulate all DER devices.

Encryption between the DERMS and DER drastically reduces the risk of Replay and MITM attacks.

MTD has the potential to drastically improve security for DER networks, but this is still an area of research.

# Future Work Recommendations

Power system co-simulation environments (in SCEPTRE) are powerful and should be used to study a range of cybersecurity features or approaches:

- DER communication architectures, IDSs, IPSs, firewall rules, access controls, encryption requirements, etc.
- Positive findings should be widely spread to the industry and codified where applicable

Simulating power system control algorithms to determine sensitivities to latency, dropouts, and availability should be expanded to other control methods.

- Additional work is needed to better quantify round-trip communication times because these latencies directly impact power system operations.

New approaches for low or no communication power system fallback operating modes should be developed and demonstrated.