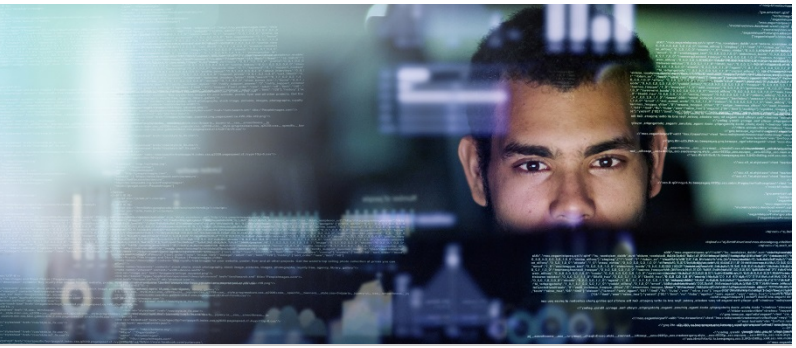
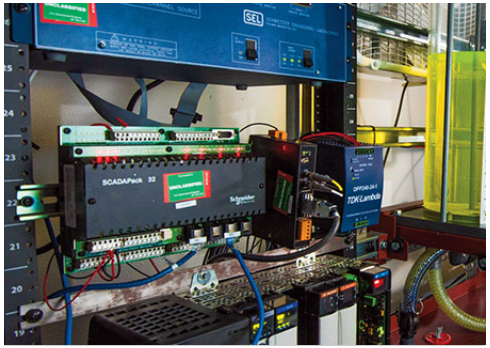
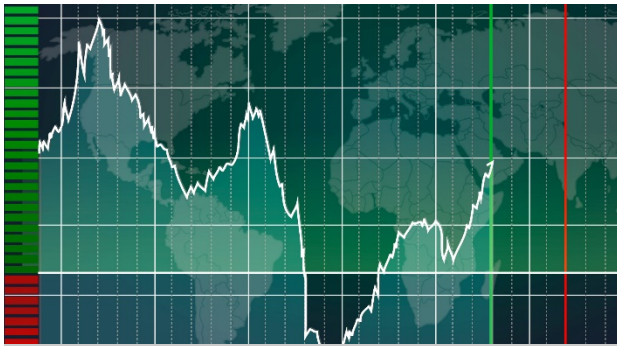
SAND2018-0280C

Exceptional service in the national interest

Sandia National Laboratories







Cyber Security Assessments of DER

June 2017

Sandia's DER Cyber Team

Cedric Carter
Ifeoma Onunkwo
Patricia Cordeiro
Jay Johnson

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

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

Outline

- Cyber Assessment Motivation
- Ideology, Methodology, and Sources
- Targeted Devices
- Cyber Assessment
  - Test Plan Overview
  - Test Cases
- Conclusions
- Q&A

Motivation for DER Cyber Assessments: DER Interoperability

- Distributed Energy Resource (DER) interconnection standards are being re-written to include communication requirements:
  - CA Rule 21 Phase 2 and 3 address communications and advanced grid functions requiring communications
  - IEEE 1547 full revision will require interoperability for DER equipment
- Many DER already include communications for monitoring and reporting
- New advanced grid function requirements require DER to adjust active and reactive power levels
- Control of an aggregation of DER is equivalent to controlling a large centralized power plant
- **It is critical to secure DER communications**

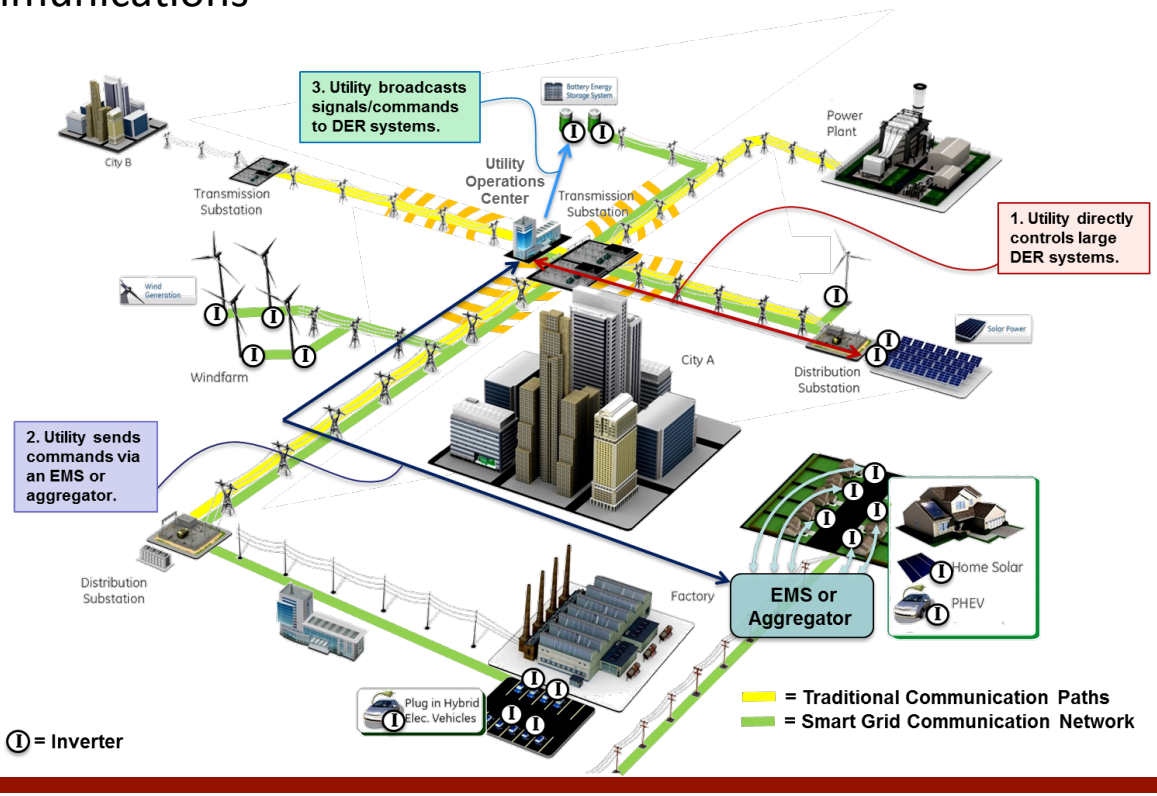
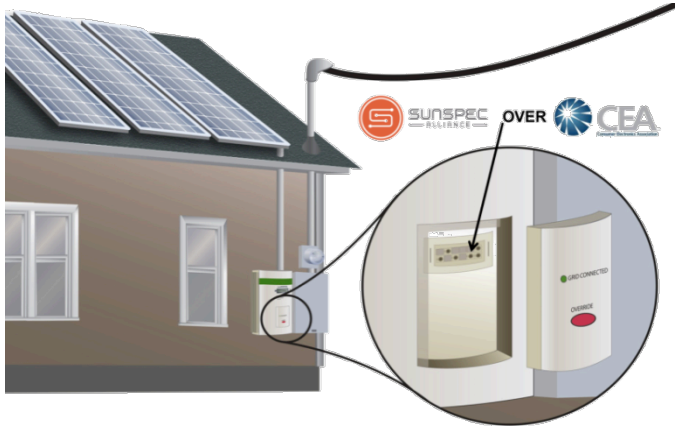


Image: Forbes India

Goals for DER Cyber Assessments

- Goal: **understand weaknesses** in the current state-of-the-art to assist solar industry with **good cyber-secure designs**
  - Partner with multiple vendors to address potential DER cyber security issues
    - Assessment to act as starting place for new SunSpec Alliance DER Cyber Security Working Group - ***starting soon***
- Scope: Target multiple Photovoltaic (PV) inverters and gateway devices to study and identify the **feasibility** and **ease** of cyber attacks on DER devices
- Outcome: Generalized recommendations for securing DER communications
  - Recommend communication protocols which provide the greatest security.

DOI: 10.1109/TDC.2016.7520035



Possible Translation Idea: SEP 2.0 to Modbus

Sandia National Laboratories

Who are we?

An ethical red team that identifies and defines security vulnerabilities in a system

source: WittySparks.com

Advantage

Performing methodical assessment of a network or system to reveal vulnerabilities and mitigate them, thereby resulting in stronger security

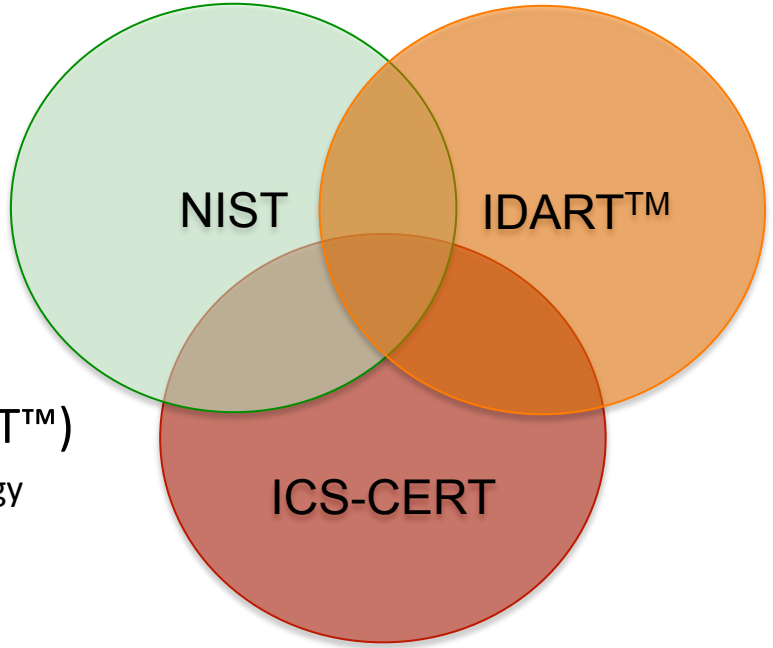
Disadvantage

Performing any fraudulent activity on someone else's network without approval is a crime

Ideology, Methodology and Sources – Part I

Sandia National Laboratories

- Our team combined practices from multiple sources in creating our cyber assessment test plan for DER devices at Sandia's Distributed Energy Technologies Lab (DETL)
- We identified gaps and correlations between multiple methodologies and best practices to form a practical test plan that would be utilized for a range of DER devices
- Sources include:
  - NIST
    - Guide to ICS Security
      - » (800-82, rev 1)
  - SNL/Information Design Assurance Red Team (IDART™)
    - Sandia's Red Teaming Methodology
  - DHS/ICS-CERT
    - Cyber Security Assessments of ICS
      - » Practice Guide

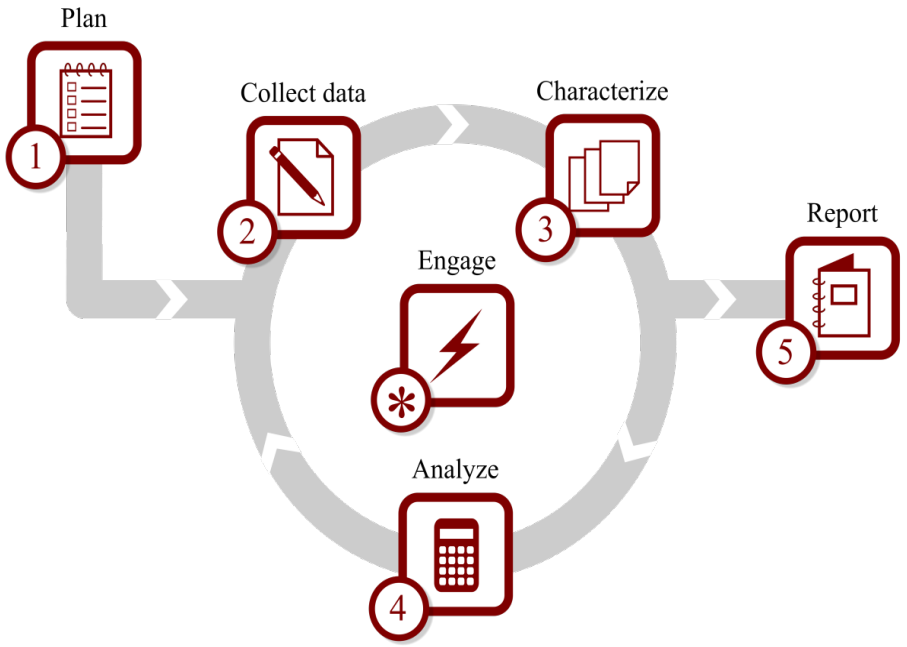


Ideology, Methodology and Sources - Part II

Sandia National Laboratories

Information Design Assurance Red Team (IDART™)

- Authorized, adversary-based assessment for defensive purposes
- Understand adversaries and operational environments, assess threats



IDART™ Methodology Overview Framework, 2014

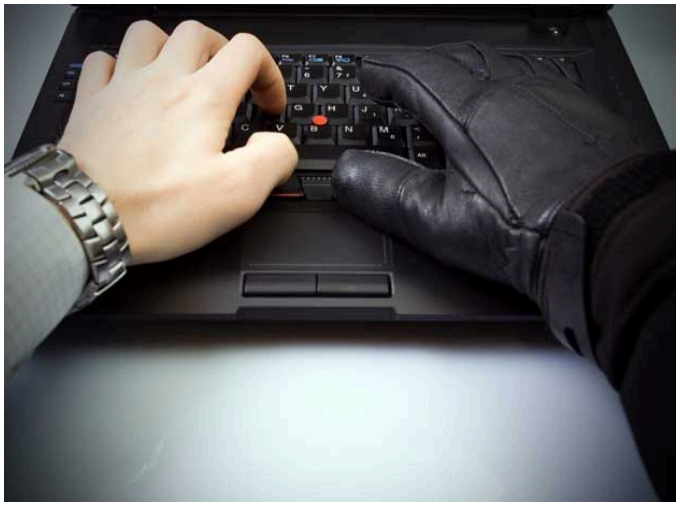
Targeted Devices

- *Completed DER Assessments*
  - **Inverter**
    - NRTL-listed inverter with a user-friendly graphic display
    - Equipped with serial and Internet Protocol (IP) interfaces for communication
  - **Two PV Gateways**
    - Provides data exchange with the vendor's inverter
    - A Graphical User Interface (GUI) for easy PV data monitoring
- *Current Work*
  - **Additional Inverters**
    - Residential solar inverter that has wireless and serial capabilities for communication
    - Microinverter-based system communicating with gateway

Cyber Assessment

Sandia National Laboratories

- Test Plan Overview
  - The overall goal of our vulnerability assessment and ethical penetration test were not to seek a "100-percent" secure system, but rather to take a snapshot of the security profile of the system
    - *This enables the team understand potential security risks and provide mitigations*
    - *Recommendations fed back to manufacturers*
    - *Generalized recommendations will be shared with solar industry*
  - For our vulnerability and penetration tests, we used Kali Linux OS and a range of 3rd party tools that are equipped with network scanning and network exploit tools
  - The test cases were modeled based on an adversarial attack pattern that could be carried out on a DER device or network



Source: http://www.security-faqs.com/wp-content/uploads/2011/06/what-is-an-ethical-hacker.jpg

Cyber Assessment

- Test Cases
  - In our assessment, we performed and/or evaluated the following:
    - *Network Reconnaissance*
    - *Packet Replay and Authentication of Data*
    - *Man in the Middle Attack*
    - *Denial of Service Attack*
    - *Vulnerability Scans*
    - *Modification Firmware Upload*
    - *DER Log Management*
    - *Password Handling*
  - Details are presented in the final manuscript paper
  - Two examples are shown in the next slide

Cyber Assessment

- *Packet Replay*
  - Validates the protection and authentication of data transfer from source transmitter (TX) to the destination receiver (RX)
    - Some DER clients' traffic can be replayed impersonating a legitimate user
    - Traffic replay could change inverter functions, settings, DER name, IP address, etc.
- *Man-in-the-Middle Attack*
  - Verifies communication is secure and confidential over authenticated channels
  - Targeted TCP/UDP connection between the client and the DER
  - A successful Man in the Middle intercepts, alters, or blocks communication
    - Address Resolution Protocol (ARP) poisoning forces malicious entries in a victim's ARP table and links the attackers MAC address with the IP address of the victim

Packet Replay

Eavesdrop → **Custom script** → **Digital & Physical effects**
Voltage settings were updated

MiTM

Network Access → **ARP Poison** → **Digital effects**
HMIs report false state

Conclusions

Sandia National Laboratories

- New DER interconnection/interoperability standards are **requiring DER to communicate** over open Internet channels to aggregators and utilities
- This **expands the cyber attack surface** of the DER
  - Unauthorized aggregation control of DER devices could cause large-scale power disruptions
- Sandia **investigated DER devices** to understand current security practices and system weaknesses in order to advise the DER industry
- **Extensive recommendations** provided in paper, e.g.:
  - Encrypt and authenticate data exchange ***{Client<->[DER|SERVER]}***
  - Application services should be running on secure ports
  - Update devices to the latest patches and firmware regularly
  - Secure password strategies and polices should be implemented
  - Vulnerable applications like FTP or HTTP should be replaced with better secure versions like FTPS or HTTPS ***{FTP-SSL, HTTP-SSL/TLS}***
  - Implement proper firewall/network gateway rules to mitigate the effects of denial of service or unauthorized access
  - DER devices should be enclosed in a physical barrier to prevent unauthorized access ***{Physical Security}***
  - Manufacturers should practice the *Principal of Least Privilege* on all applications operating on DER devices and systems.

Sandia National Laboratories

Q&A

If interested in joining the SunSpec **DER Cyber Security Working Group** please contact Jay Johnson at jjohns2@sandia.gov