Exceptional service in the national interest

Sandia National Laboratories

Secure, Scalable Control and Communications for Distributed PV



Jay Johnson
Sandia National Laboratories

SunShot National Laboratory Multiyear Partnership Workshop on
Numerical Analysis Algorithms for Distribution Networks
Argonne National Laboratory, Chicago, IL
21 July, 2017

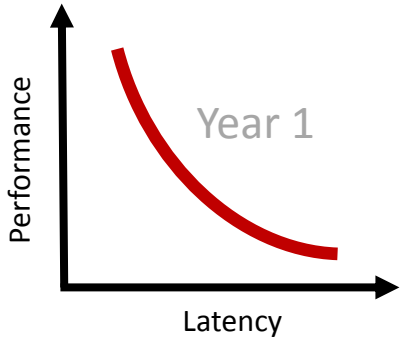
U.S. DEPARTMENT OF ENERGY

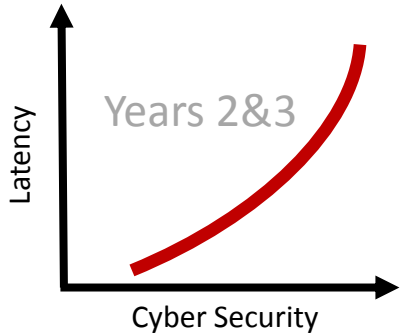
NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission 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-NA0003525.

System Performance vs Latency/Security

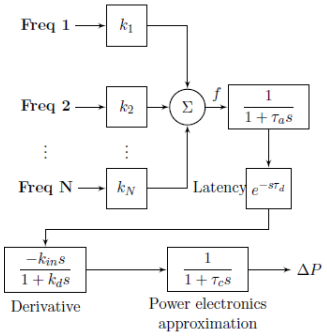
- We want two things:
  - **DER grid-support functionality** issued via communications from grid operators, utilities, and aggregators through the public internet
  - Highest degree of **cyber security** in DER control networks
- **Project Goal:** understand the tradeoffs between cybersecurity and control latency/power system performance
  - Changing network topology/security, changes communication speed and therefore grid performance
  - e.g., adding firewall rules, intrusion prevention systems, intrusion detection systems, enclaved networks, etc. adds more latency.
  - What ties cyber security to functionality is embedded in communications metrics: latency (response time), availability (dropped packets), scalability (number of DER), etc.

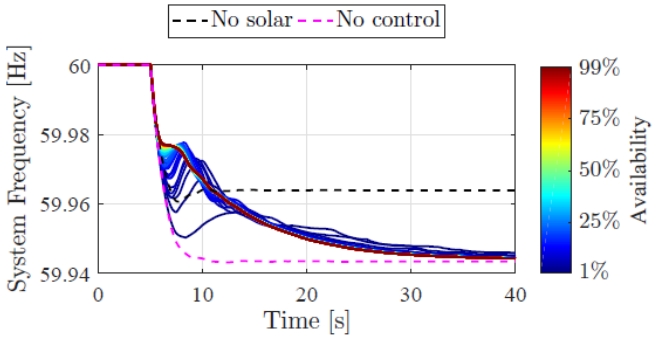




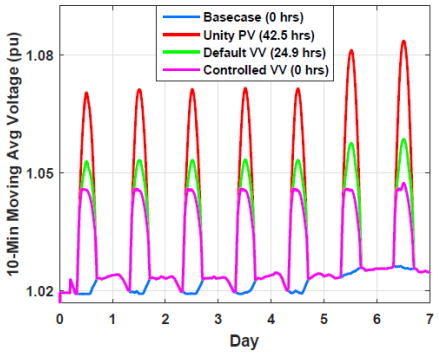
Power System Performance vs Latency

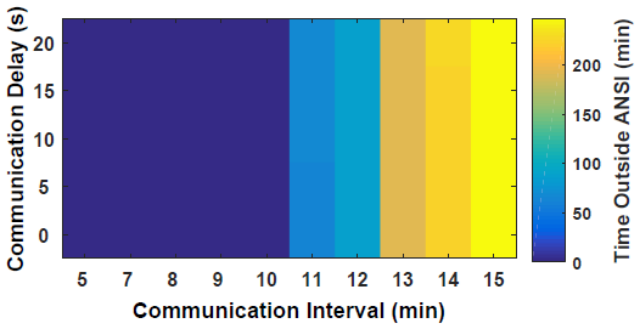
- Multiple control systems were analyzed to determine the performance vs communication metrics.
  - Synthetic inertia
  - Communication enabled fast acting imbalance reserve
  - Communication enabled frequency droop
  - Hierarchical control of Volt-VAr function
- Power system metrics determined for each control case varying availability and communication latency.



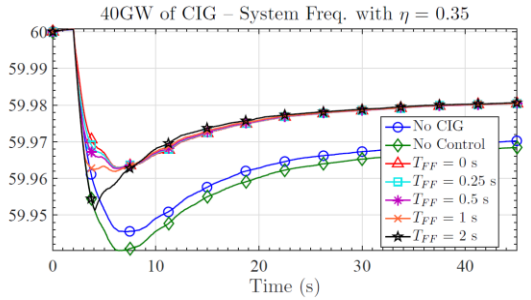


Communications Enabled Synthetic Inertia Controller and transient response with different availabilities.



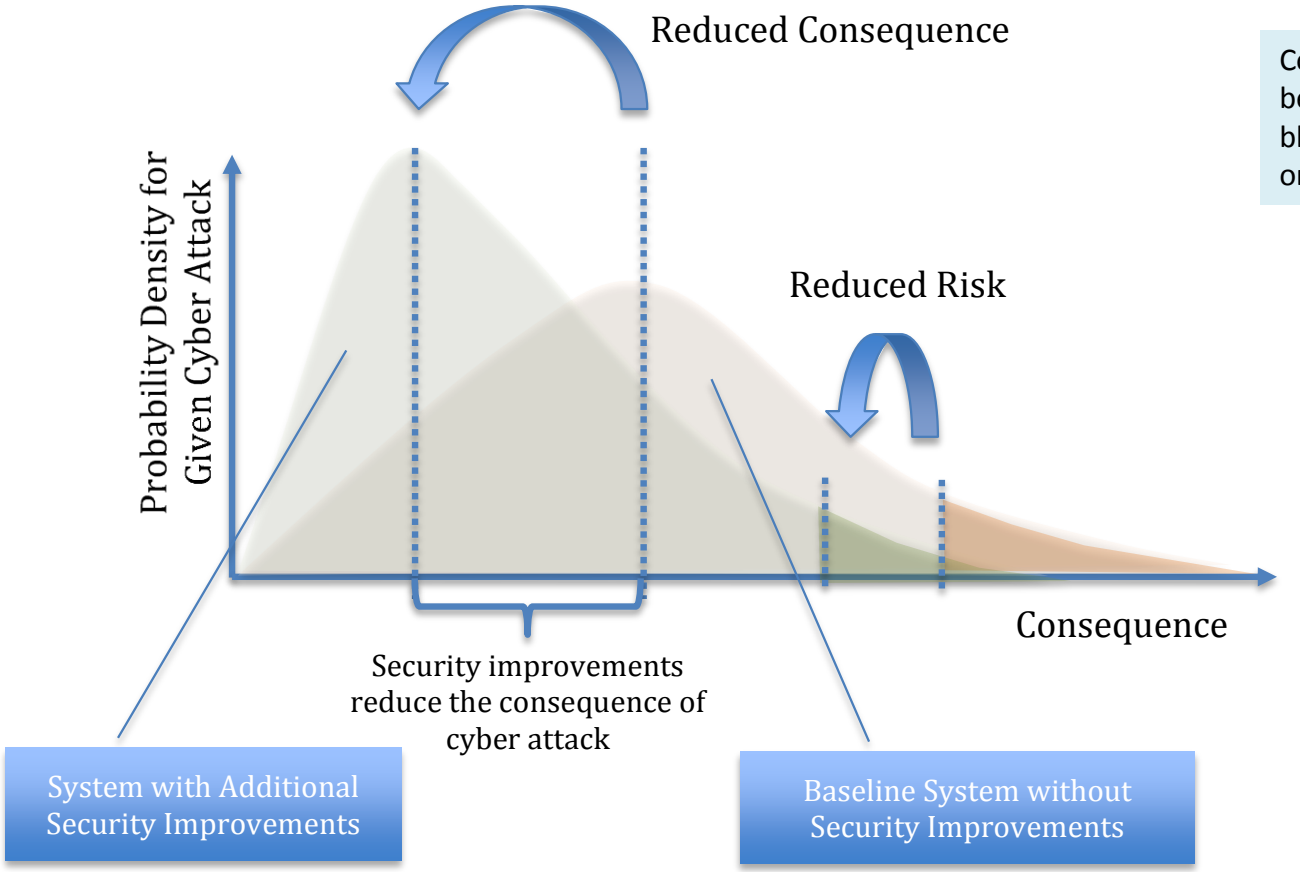


Voltage regulation requires regular communications, but it tolerant of communication delays up to 20 seconds.



Influence of converter interfaced generators (CIGs) Communications Enabled – Fast Acting Imbalance Reserve (CE–FAIR) delay on N-1 nadir in western North American Power System.

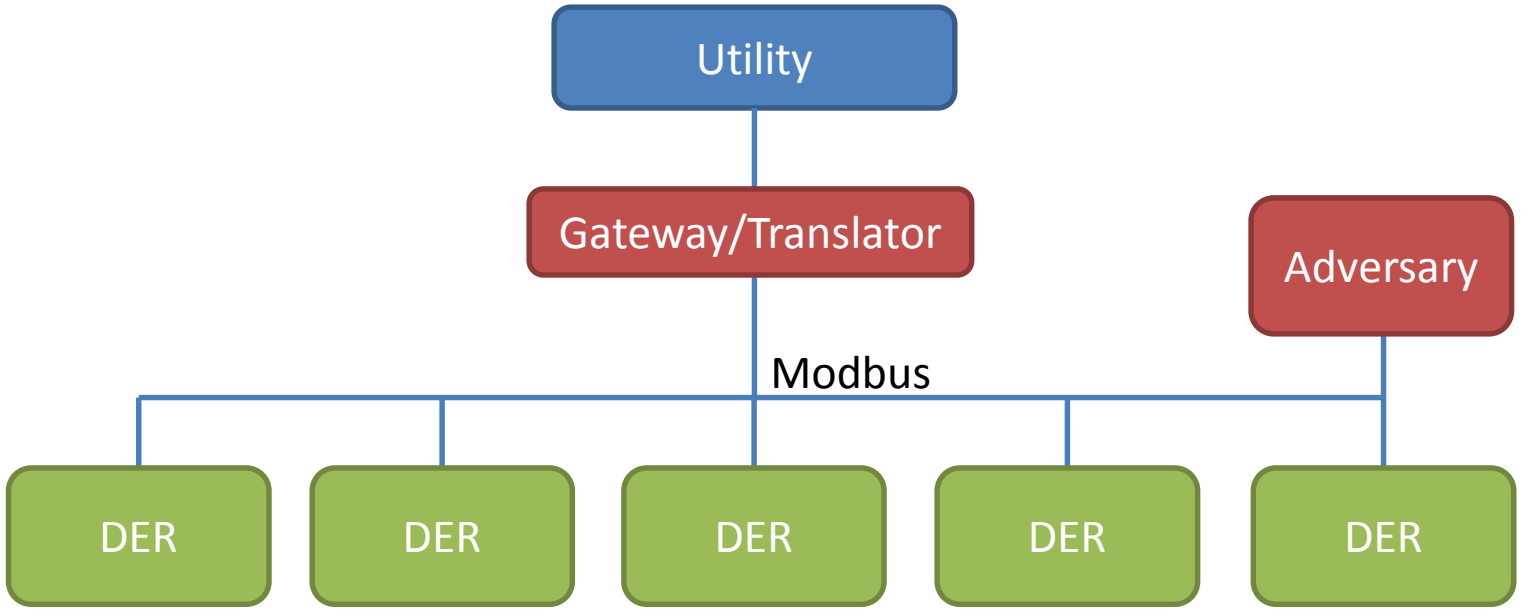
Evaluating Cyber Security Options



Consequence could be in $, lost load, blackout duration, or other units.

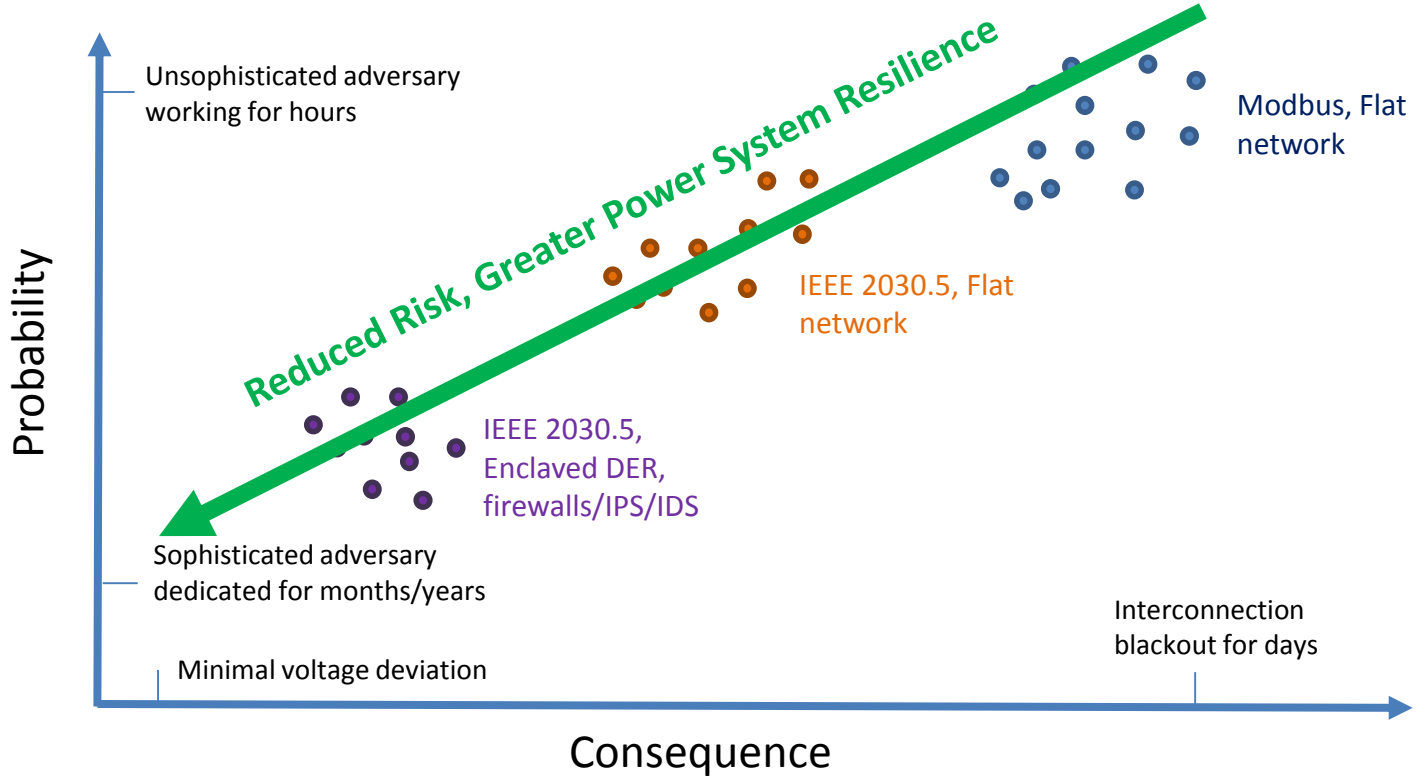
Towards Cyber Resilience

- Imagine a world where…
  - Millions of DER are deployed on distribution systems and communicate with the utility on a flat network via TCP Modbus… and there's a bad guy on the internet.



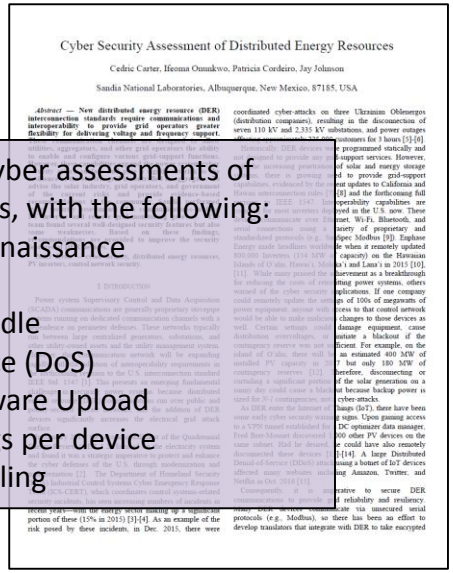
Grid Resilience (conceptualized)

- Risk = (probability) x (consequence)
  - Populate a single point for a given attack vector (method of cyber attack and target).



Challenge is Quantification

- How do we quantify the probability of a successful cyber security attack?
  - Red team assessments of DER devices and DER networks
- How do we quantify consequence
  - 'Nightmare' scenarios for different DER control functions

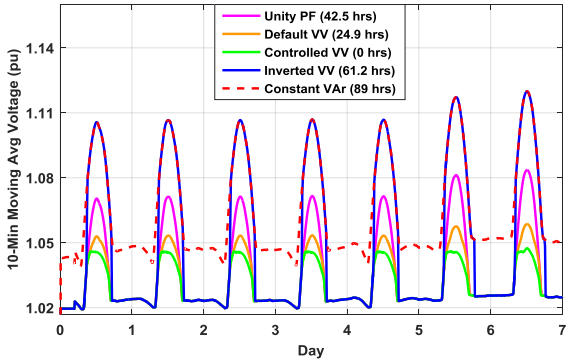

Cyber Security Assessment of Distributed Energy Resources

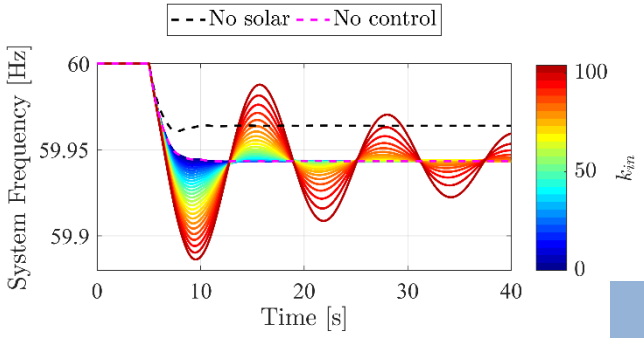
Cedric Carter, Ifeoma Onunkwo, Patricia Cordeiro, Jay Johnson

Sandia National Laboratories, Albuquerque, New Mexico, 87185, USA

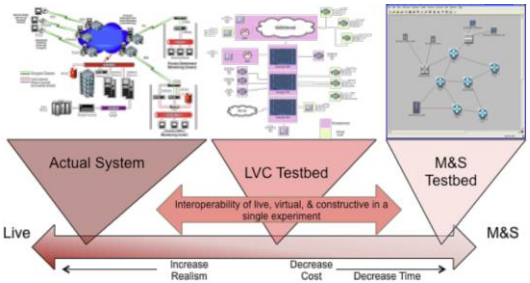
Sandia conducted cyber assessments of multiple DER devices, with the following:

- Network Reconnaissance
- Packet Replay
- Man in the Middle
- Denial of Service (DoS)
- Modified Firmware Upload
- Maintained Logs per device
- Password Handling





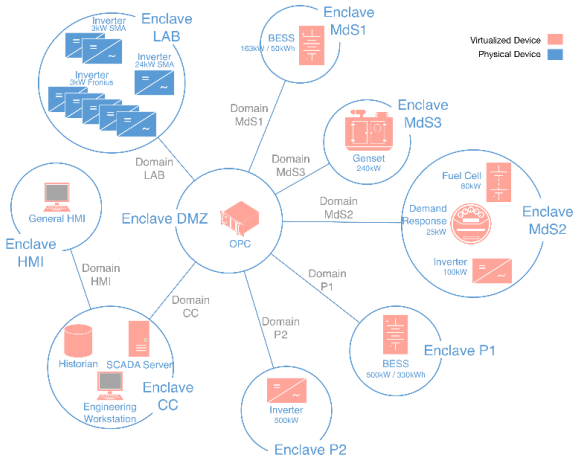
Sandia determining results of different DER attacks using grid-support functions.



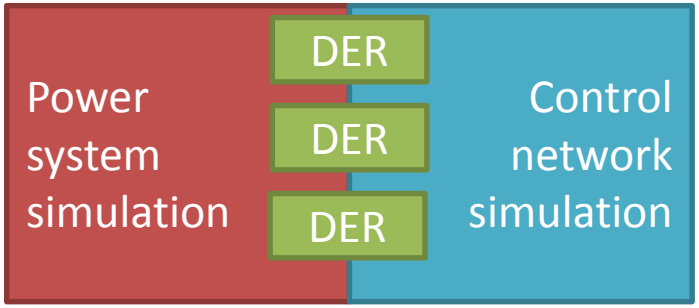
SCEPTRE emulates the power system and the control network at the same time so that changes in either one are represented in the other.

System Performance vs Cyber Security

- Sandia is looking at different cyber security architectures, DER communication protocols, and network security measures to determine the probability and consequence of cyber attacks.
  - Assessed in SCEPTRE environment which simulates the power system, DER devices, and networking devices.
- Work in progress:
  - Creating OpenDSS driver for SCEPTRE to run distribution cases.
  - Deploy SunSpec System Validation Platform Scripts in a Windows VM for the centralized controller for distribution (voltage regulation) and transmission (synthetic inertia) test cases.
  - Creating SunSpec RTUs to control devices and get power system data to the controllers.
  - Cyber architectures for distribution and transmission cases.
  - Emulated latencies for geographical distances. Networking latencies will be simulated realistically since they are captured by the virtualized machines.
  - Red team assessments of the cyber architectures + determination of resilience metrics (e.g., time to reach certain areas in the network).



Cyber Reference Architecture which enclaves DER devices to minimize common-mode vulnerabilities.



DER devices exist in both the control system simulations as power elements and in the control network as RTU devices.

Questions

Jay Johnson

jjohns2@sandia.gov

Photovoltaic and Distributed Systems Integration

Sandia National Laboratories

P.O. Box 5800 MS1033

Albuquerque, NM 87185-1033

Phone: 505-284-9586