SOLAR ENERGY
TECHNOLOGIES OFFICE
U.S. Department Of Energy

Secure, Scalable Control and Communications for Distributed PV

US DOE SETO Portfolio Review
Washington DC
13 Feb 2018

Jay Johnson, Principal Member of Technical Staff,
Sandia National Laboratories

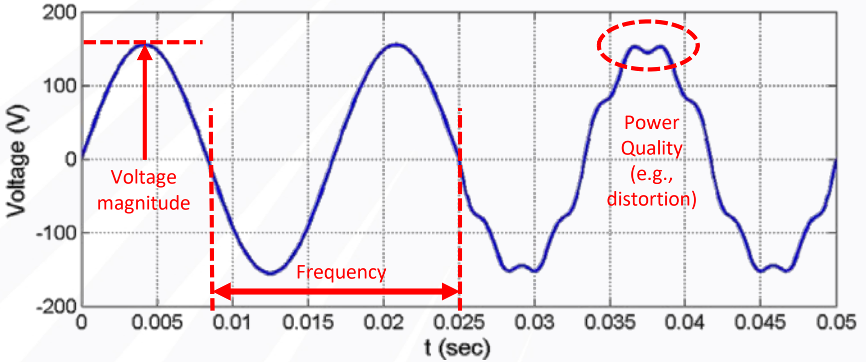
energy.gov/solar-office

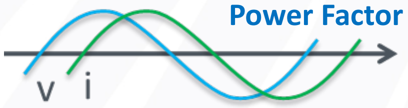
Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

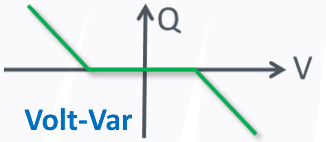
Increasing solar penetrations using communications

- 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



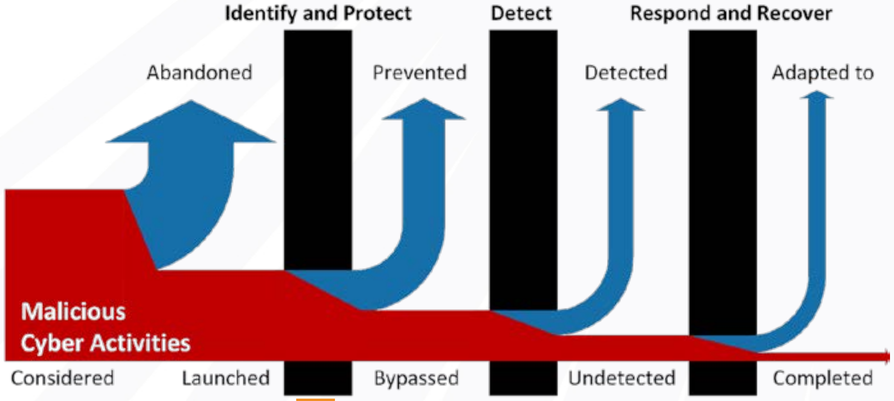




www.ucsusa.org

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.



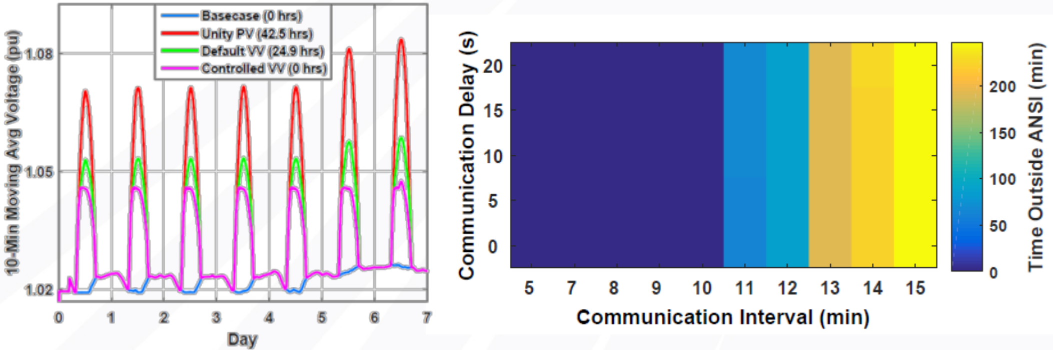
Network Protection R&D

- Network Segmentation
- Virtualized Testbed Environments
- Risk Quantification
- Threat Models
- Cyber Assessments
- Dynamic Networking and Moving Target Defense
- Trusted and Protected Computing
- Cryptography
- Engineering Controls for DER
- Physical Security
- Security for Cloud-Services
- Obfuscation and Deception
- Authentication

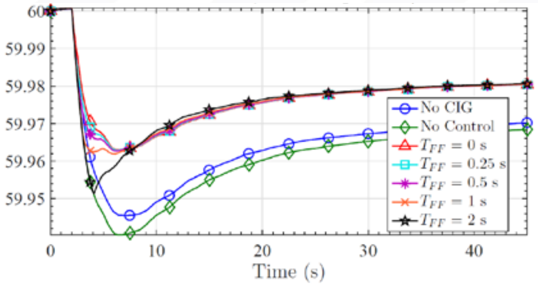
J. Johnson, “Roadmap for Photovoltaic Cyber Security,” Sandia Technical Report, SAND2017-13262, Dec 2017.

DER network parameters vs grid performance

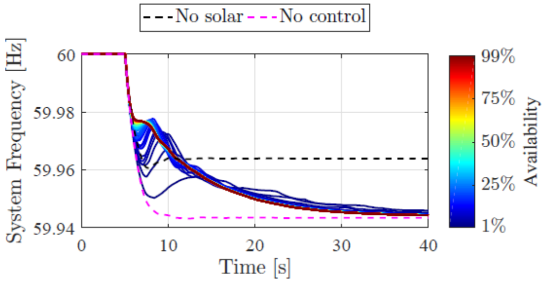
- Changing network topology/security features changes communication speed and power system behavior
- Multiple communications-enabled DER control approaches were simulated:
  - Synthetic inertia
  - Communication enabled fast acting imbalance reserve
  - Communication enabled frequency droop
  - Hierarchical control of volt-var (VV) function
- Power system metrics determined for each control case varying DER availability and communication latency.



Hierarchical VV control found to be tolerant of communication delays up to 20 s [1-2].



Communications Enabled – Fast Acting Imbalance Reserve (CE–FAIR) delays caused lower frequency nadirs [3].

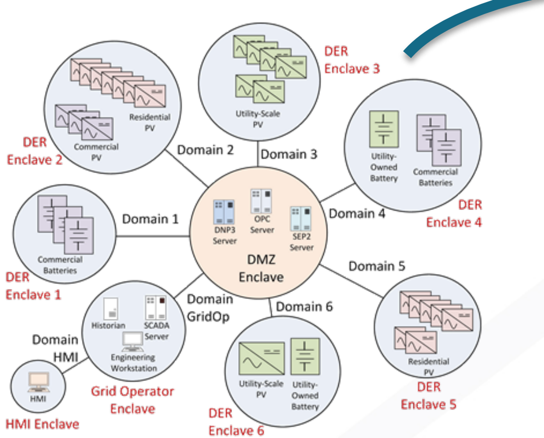


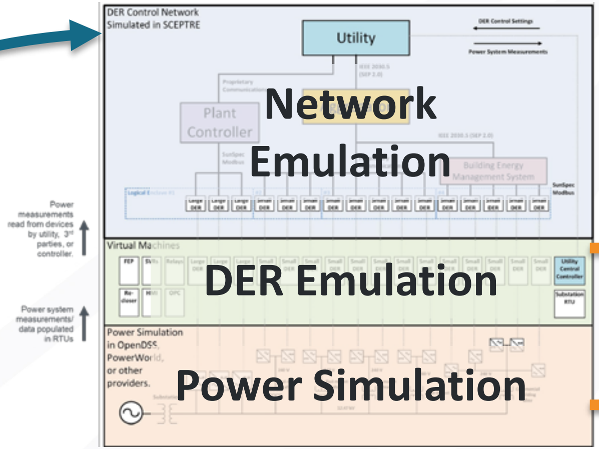
Communications Enabled Synthetic Inertia Controller transient response with different DER availabilities [4].

1. J. E. Quiroz, M. J. Reno, O. Lavrova, R. H. Byrne, "Communication requirements for hierarchical control of volt-VAr function for steady-state voltage," IEEE PESInnovative Smart Grid Technologies Conference (ISGT), Washington, DC, 2017.
2. M. Reno, J. Quiroz, O. Lavrova, and R. Byrne, ”Evaluation of Communication Requirements for Voltage Regulation Control with Advanced Inverters," IEEE North American Power Symposium, Denver, CO, September 2016.
3. R. Concepcion, F. Wilches-Bernal, R. Byrne, “Effects of Communication Latency and Availability on Synthetic Inertia," IEEE ISGT 2017, Arlington, VA, April 23-26, 2017.
4. F. Wilches-Bernal, R. Concepcion, J. Neely, R. Byrne, and A. Ellis, “Communication Enabled Fast Acting Imbalance Reserve (CE-FAIR),” IEEE Transactions on Power Systems.

Tying cyber security design to grid performance

DER control network architectures are emulated in the SCEPTRE environment.




DER Control Network Simulated in SCEPTRE
Utility
DER Control Settings
Power System Measurements
IEEE 2030.5 (SEP 2.0)
Proprietary Communications
Plant Controller
SunSpec Modbus
IEEE 2030.5 (SEP 2.0)
Building Energy Management System
SunSpec Modbus
Logical Enclave #1
Large DER
Small DER
Power measurements read from devices by utility, 3rd parties, or controller.
Virtual Machines
FEP
Relays
Re-closer
HMI
OPC
Utility Central Controller
Substation RTU
Power system measurements/ data populated in RTUs
Power Simulation in OpenDSS, PowerWorld, or other providers.
Substation

Network Emulation

DER Emulation

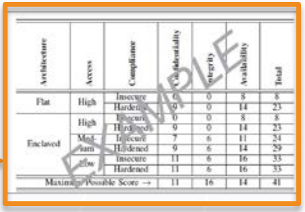
Power Simulation

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

SCEPTRE outputs:

- Cyber security metrics
- Communication parameters
- Power system performance

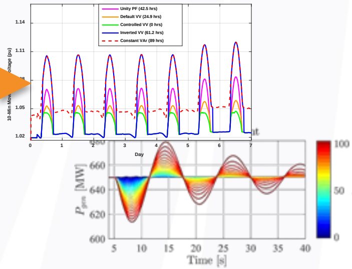
IDART Information Design Assurance Red Team



Architecture	Access	Compliance	Confidentiality	Integrity	Availability	Total
Flat	High	Insecure	0	0	8	8
		Hardened	9	0	14	23
Enclaved	High	Insecure	0	0	8	8
		Hardened	9	0	14	23
	Med-ium	Insecure	7	6	11	24
		Hardened	9	6	14	29
	Low	Insecure	11	6	16	33
		Hardened	11	6	16	33
Maximum Possible Score →			11	16	14	41

EXAMPLE

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.)