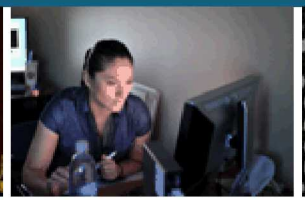
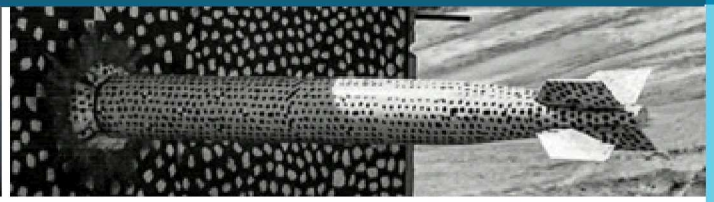
SAND2019-2216C

Analysis of System and Interoperability Impact from Securing Communications for Distributed Energy Resources





PRESENTED BY

Nicholas Jacobs

Nicholas Jacobs*, Shamina Hossain-McKenzie*, Deepu Jose*, Danish Saleem†, Christine Lai*, Patricia Cordeiro*, Adarsh Hasandka†, Maurice Martin†, Christopher Howerter*

*Sandia National Laboratories, †National Renewable Energy Laboratory

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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.

Outline

Integrating Distributed Energy Resources (DER) into Power Distribution Systems

DER Communications for Interoperability and Operations

Cybersecurity Considerations

Use Case: Hierarchical Volt-Var Control, 15-bus Distribution System Model

- With and Without Communication Assisted Grid-Support
- Impact of Communication Latency
- Impact of Loss of PV Generation

Conclusions

Challenges for DER Integration

Incorporation of high amounts of DER in the future grid

- Hawaii and California aim to be 100% renewable by 2045, several other states expected to follow
- CA Rule 21 recently updated to mandate new interconnection requirements, including for smart inverters
- As DER penetration increases, new control schemes and interoperability requirements are needed to adequately maintain grid reliability and performance

Integrating DER with Advanced Distribution Management Systems (ADMS) has potential for improving operation of the distribution grid, but also presents increased attack surfaces for cyber attack

- So how do we incorporate DER communications while maintaining grid security and reliability?
- To do this, we must understand the communications required and what security considerations are required
  - For instance, maintaining the security principles of **Confidentiality, Integrity, Availability, Authentication, and Non-Repudiation**

Sources

- https://www.scientificamerican.com/article/as-hawaii-aims-for-100-renewable-energy-other-states-watching-closely/
- https://www.npr.org/2018/09/10/646373423/california-sets-goal-of-100-percent-renewable-electric-power-by-2045
- http://www.ncsl.org/research/energy/renewable-portfolio-standards.aspx
- http://www.cpuc.ca.gov/Rule21/

DER Communications

"Smart" Inverters provide new opportunities for advanced control and management in distribution systems, such as in ADMS

The Common Smart Inverter Profile (CSIP) and related information models gives numerous types of information that smart inverters need to support for interoperability with grid operations

- For example, information pertaining to device registration, group management, power modes, control settings, measurements, status, and alarms

Sources:

- Common Smart Inverter Profile (CSIP), Version 2.1, available at https://sunspec.org/download/

DER Communications

Each type of communications and information may have different security requirements, so failing to protect this information may have different impacts to grid operations

This is demonstrated by examining requirements for security for each type of communication

Examples

- Device Registration
  - Required to create an identity for a device that can be verified. If not secured, an attacker could spoof an identity and send incorrect data, alarms, and more
  - Authentication and Integrity are critical
  - Out-of-band of grid-support functionality, so any processing delays from security protections should not impact operations
- Control Settings
  - Required for DER control for various grid-support functions, such as in an ADMS
  - Availability, Integrity, and Authentication are critical, and small delays from security protections should have minimal impact

Cybersecurity Protections

To provide guarantees on security in DER communications, various mechanisms can be employed

- With some cost for infrastructure and additional processing time, which adds latency to the DER communications

Examples:

- **Cryptographic protections:**
  - Encryption – protects confidentiality
  - Digital Signatures – protects authentication and integrity
  - Hash-based Message Authentication Codes – protects integrity
- **Logging:**
  - Events, traffic, etc. – protects non-repudiation
- Others…

A combination of such protections should be incorporated as needed, ideally with defense-in-depth to ensure security is preserved

- Such protections are commonly implemented in networks today, and additional delays can be expected to be on the order of milliseconds

Use Case: 15-Bus Distribution Feeder with PV

Why is this important?

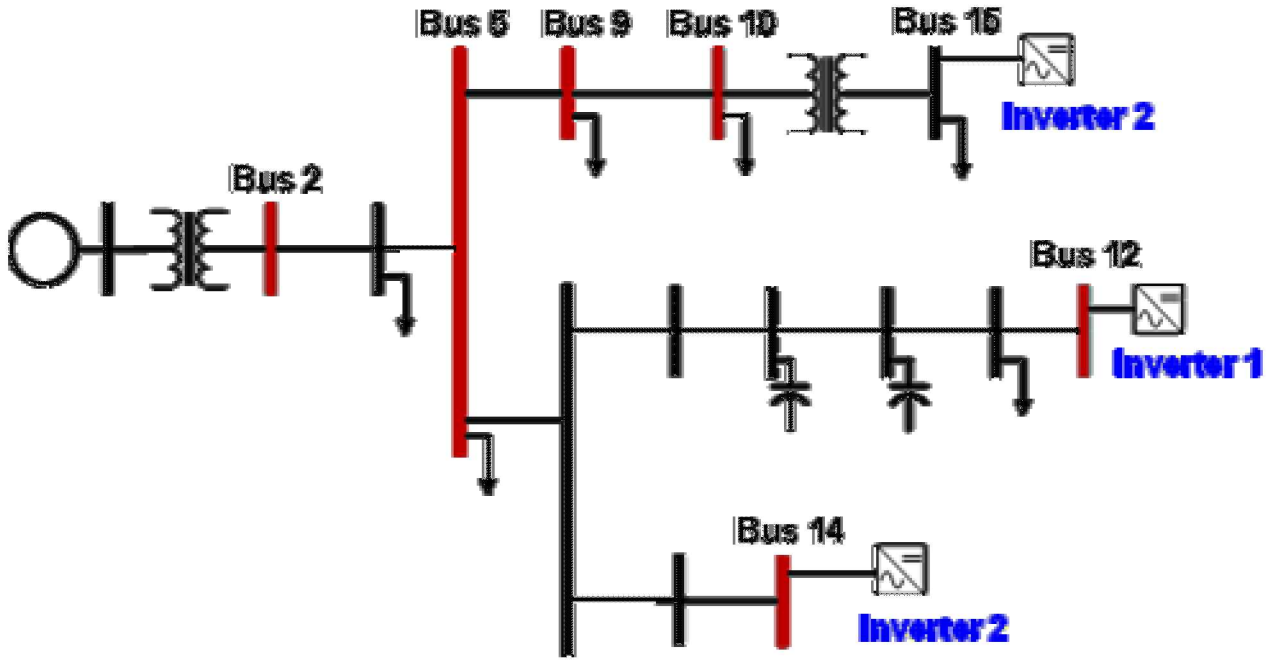
- Let us examine a small use case of a distribution feeder with an ADMS utilizing DER communications with and without security protections

This simulation, performed in Simulink for 5 minute scenarios, uses a 15-Bus reduced order model of a rural distribution feeder, with 11.2 MW PV generation and 4.4MW peak load

- 1.8MW of that load is switched on 2 minutes into the simulation

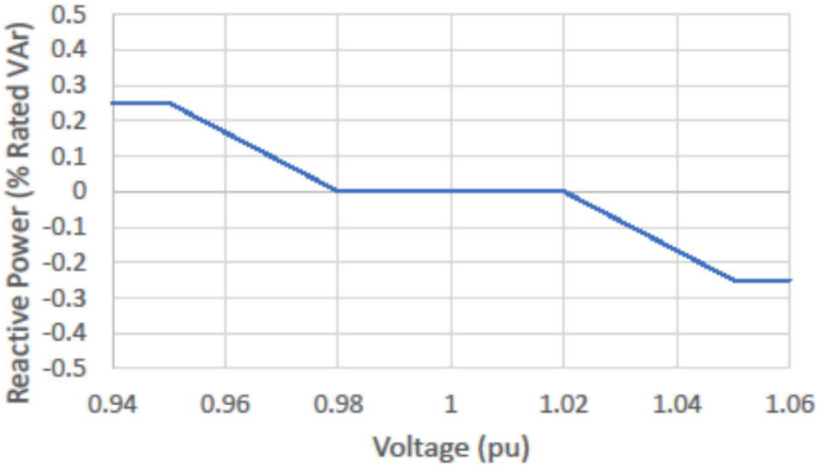
High amount of PV penetration

- **Inverter 1: 480 V, 258 KVA**
- **Inverter 2: 12,470 V, 10 MVA**
- **Inverter 3: 12,470 V, 1 MVA**



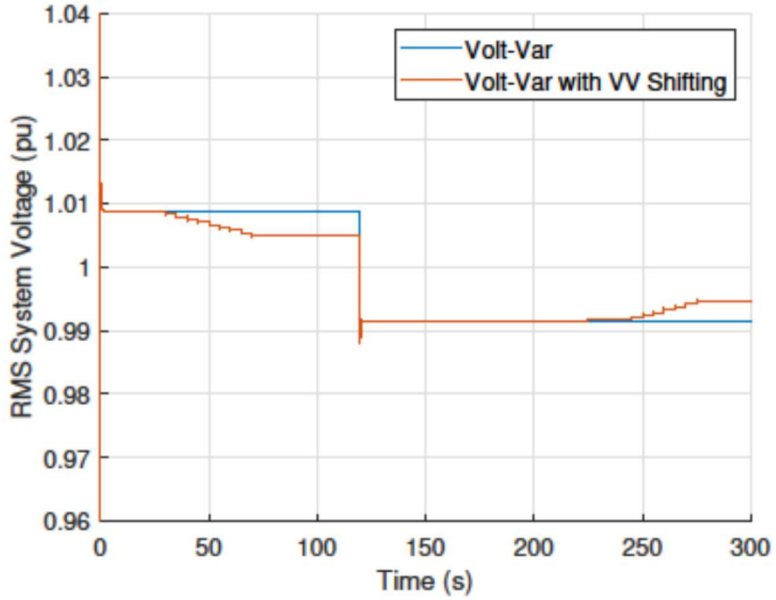
Use Case: Hierarchical Volt-Var Control

Each inverter is set to use Volt-Var Control, with the initial Volt-Var curve seen here



Additionally, a central controller shifts the Volt-Var curve to the right or left based on voltage across the feeder

- Increasing reactive power injection if voltage is low, and vice versa
- This requires additional communication for awareness of conditions across the feeder
- Improves overall voltage performance and minimizes deviation from nominal



This control algorithm was developed in [Quiroz, et al, 2017]

Reference:

J. E. Quiroz, M. J. Reno, O. Lavrova, and R. H. Byrne, "Communication Requirements for Hierarchical Control of Volt-VAr Function for Steady-State Voltage," in 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Apr. 2017.

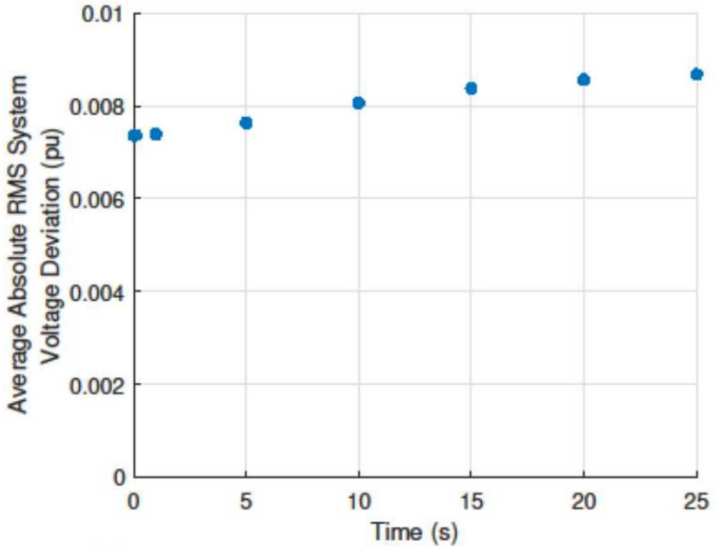
Impact from Communications Latency

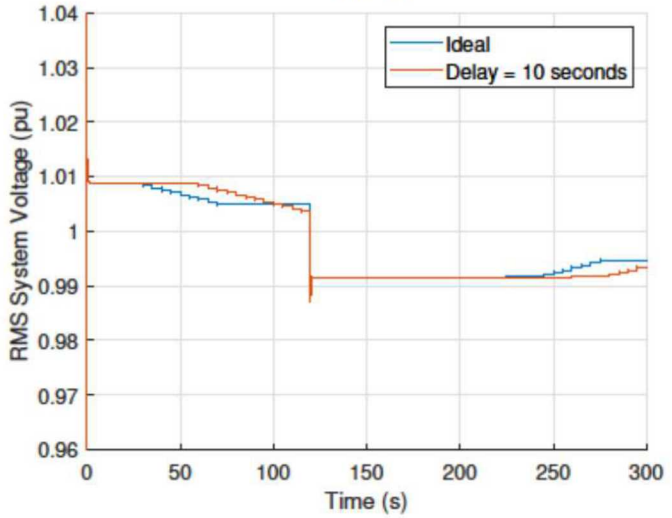
Adding additional security protections in the communications path can be expected to slow communications

- Due to extra processing and “hops” in the communications path

When implementing these delays, it is found that such delays will impact performance but not significantly even at high amounts of latency

- In other words, the central controller updates at a slow enough rate that even large time delays have little impact
- Moreover, additional latency does not affect the local control of the inverters themselves





Impact from Loss of PV Generation

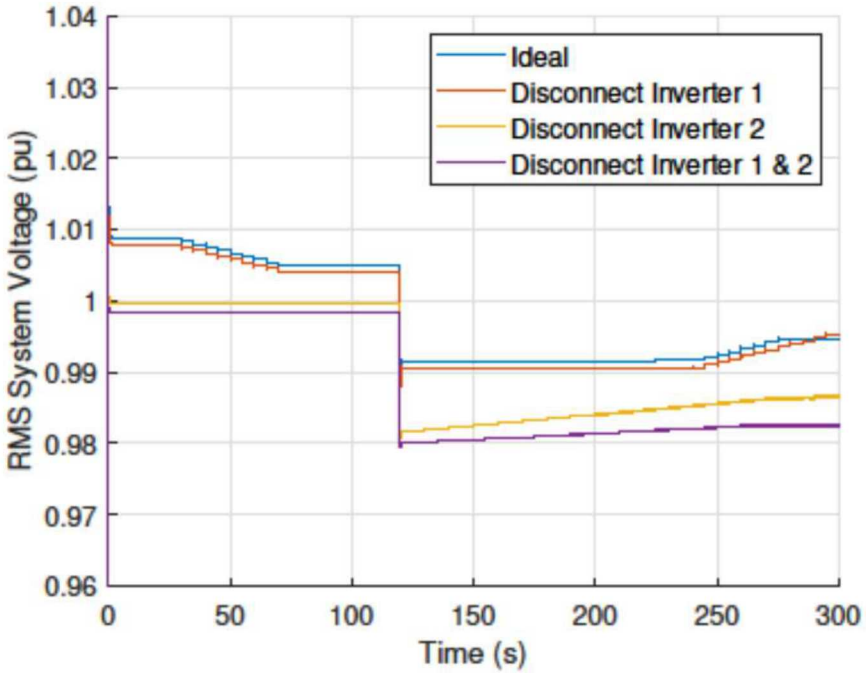
Conversely, what if some of the PV generation is disabled by a malicious or inadvertent command to disconnect?

- This represents a loss in Availability

Overall impact to system voltage depends on the amount of generation capacity that has been lost

- For instance, comparing Inverter 1 (258KVA) to Inverter 2 (10MVA)

The impact to system voltage is most severe on the buses local to the inverter(s) that have been disabled



Conclusions

The future grid is expected to contain high amounts of distributed generation sources, and communications for these DER will be needed to adequately support grid services

These communications can be protected, with the cost of adding security infrastructure and additional processing delays

The impact of security protections to distribution operations is expected to be minimal, as shown here in a single use case of communication assisted hierarchical Volt-Var control

Future work can extend this to study aspects such as:

- Further study on the impact to DER from various attack classes, such as false data injection, man-in-the-middle, hardware trojans, and others
- Extension to other control modes, such as frequency support functions

Thank You!

Contact Info:

Nicholas Jacobs

njacobs@sandia.gov