# Distributed Energy Resource (DER) Cybersecurity Standards

Jay Johnson, Sandia National Laboratories
Danish Saleem, National Renewable Energy Laboratory

NREL Cybersecurity & Resilience Workshop
Denver, Colorado, 9 October 2017

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.

# Agenda

- **DER Cyber Security Introduction**
- **DER Cyber Security Roadmap and Primer**
  - Roadmap plots course to improve DER cyber security in the next 5-10 years
  - Primer provides cyber security basics to DER vendors, aggregators, and utilities
- **DER Cyber Security Working Group**
  - Goals
  - Working groups
  - How to participate
- **DER Data and Communication Security Certification Procedures**
  - DER security controls and IEC 62351
  - Certification procedures and proposed revisions
  - Value of NREL Cyber-Physical Systems Security and Resilience R&D
  - Best practices and next steps

Sandia National Laboratories

# Why is DER cyber security important?

BBC NEWS

## Hackers 'could target electricity grid' via solar panel tech

By Chris Baraniuk
Technology reporter

08 August 2017 | Technology


The flaws were found in inverters, used to convert electricity produced by solar panels

**Hackers could target electricity grids through security flaws in solar panel equipment, a Dutch researcher has said.**

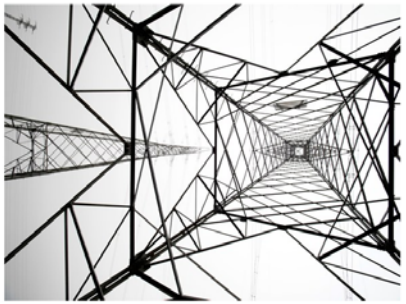
http://www.bbc.com/news/amp/technology-40861976

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

CULTURE | DESIGN | GEAR | SCIENCE

KIM ZETTER SECURITY 03.03.16 7:00 AM

## INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID



JOSE A. BERNAT BACETE/GETTY IMAGES

IT WAS 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their workday and head home through the cold winter streets. Inside the Prykarpattyaoblenergo control center, which distributes power to the region's residents, operators too were nearing the end of their shift. But just as one worker was organizing papers at his desk that day, the cursor on his computer suddenly skittered across the screen of its own accord.

https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

http://www.forbes.com/sites/thomasbrewster/2016/08/01/1000-solar-panels-tigo-vulnerable-hackers

Security / #CyberSecurity

AUG 1, 2016 @ 10:00 AM 35,875

The Little Black Book of Billionaire Secrets

## This Man Hacked His Own Solar Panels... And Claims 1,000 More Homes Vulnerable

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. FULL BIO

In this June 18, 2010, file photo, U.S. Senator Michael Bennet, D-Colo., center, helps as SolarCity employees Jarret Esposito, left, and Jake Torwatzky, install a solar panel on a home in south Denver. (AP Photo/Ed Andrieski)

Fred Bret-Mounet knows how best to secure his home: by hacking it.

When he equipped his house with a solar array - "like any good Californian" - his first thought was to test its security. After all, it was connected to the internet. Ergo, it almost certainly had some vulnerabilities. He wasn't to be disappointed. The problems he found, according to the security pro, could have allowed him spy on and hack the power supply of at least 1,000 homes.

His first concern was an open Wi-Fi access point being served from his solar array's Management Unit (MMU), a product from Tigo Energy, a device that allows panels to be controlled and monitored from the web. If anyone could login to that, they would have a good chance of spying on his home network, Bret-Mounet told FORBES. "Anyone within Wi-Fi range could connect to that device and potentially jump onto my home network, which is absolutely scary."

Sandia National Laboratories

# Why would PV groups lead cyber security efforts?

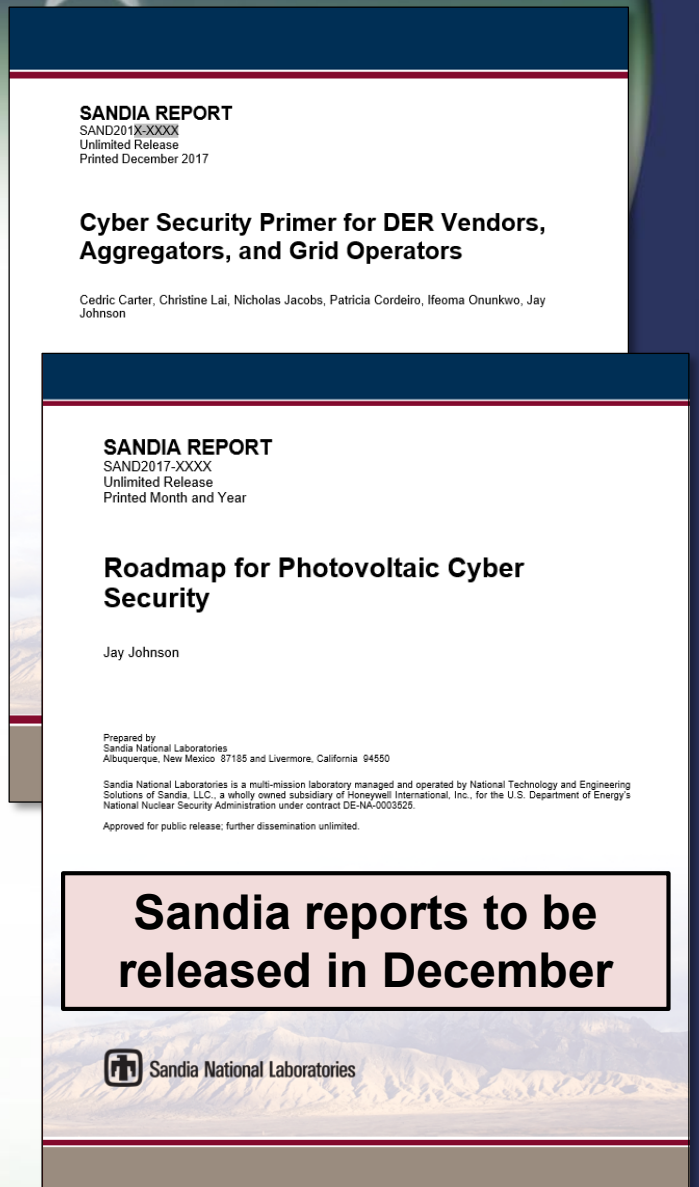
- **DER must provide critical reliability services going forward**
  - The current use case is PV-driven because of current penetration levels and deployment trends
- **Interconnection and interoperability standards in the US will soon require DER to provide communication-based grid services**
  - California Rule 21 requires autonomous functions, soon to require IEEE 2030.5 (SEP 2.0) communications to DER, and later communication-based grid support functions
  - IEEE 1547 full revision includes communication-enabled grid support functions for DER
- **DER must have robust cyber security. DER are inherently different than cyber 'business-as-usual' because:**
  - Unlike bulk generators, DER are connected to grid operators via public internet channels
  - Unlike most internet-of-things (IoT) devices, DER can more directly impact power system operations
  - DER typically have limited processing capabilities, so they typically do not support encryption or other security features.
- **Why should the government have a role here?**
  - Address long-term and short-term threats
  - Promote harmonization across the broader DER and utility sectors
  - Assist with orderly evolution of standards

Sandia National Laboratories

# DER Cyber Security Primer and Roadmap

- **Primer:**
  - Cyber security principles
    - Confidentiality, integrity, availability, etc.
  - Types of cyber attacks and threats
  - DER communication protocols
  - Cyber security guidelines, standards, and best practices
  - DER cyber recommendations
- **Roadmap**
  - How PV cyber fits within the larger context of cyber security for critical infrastructure
  - Two-pronged approach:
    - Research and development
    - Stakeholder engagement
  - Intent is that this roadmap also acts as blueprint for other DER technologies

**There will be opportunities for broad stakeholder input**



SANDIA REPORT
SAND201X-XXXX
Unlimited Release
Printed December 2017

**Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators**

Cedric Carter, Christine Lai, Nicholas Jacobs, Patricia Cordeiro, Ifeoma Onunkwo, Jay Johnson

SANDIA REPORT
SAND2017-XXXX
Unlimited Release
Printed Month and Year

**Roadmap for Photovoltaic Cyber Security**

Jay Johnson

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

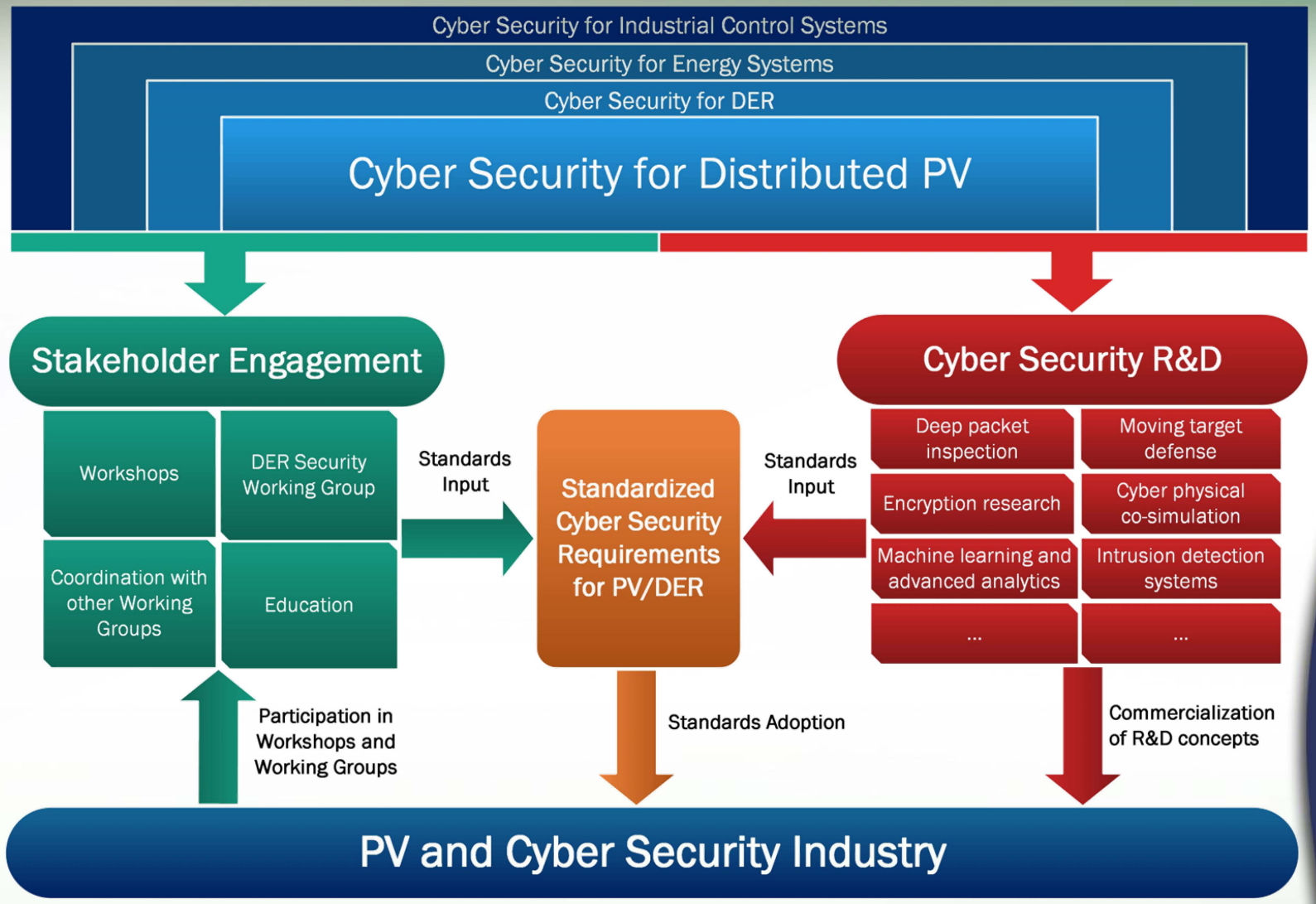
Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

Approved for public release; further dissemination unlimited.

**Sandia reports to be released in December**

Sandia National Laboratories

# PV Cyber Security Approach (Draft)



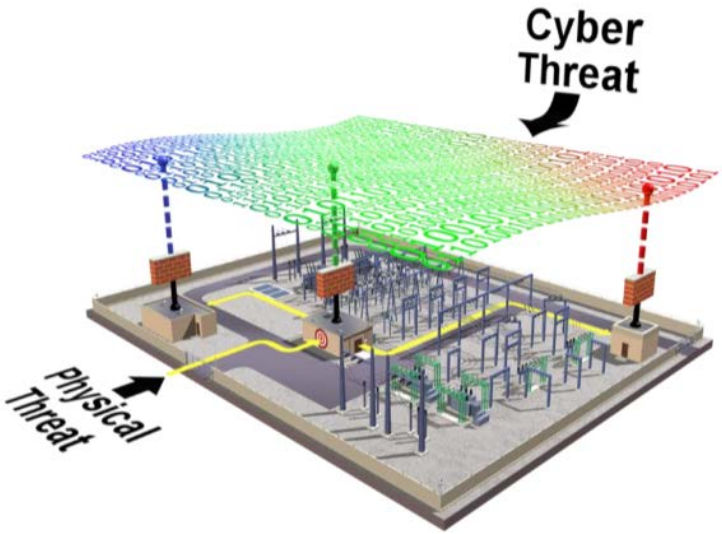

Sandia National Laboratories

# DER Cyber Security WG Goals

- The DER Cyber Security Working Group will bring together DER interoperability and cyber security experts to discuss security for DER devices, gateways, and other networking equipment, owned or operated by end users, aggregators, utilities, and grid operators.

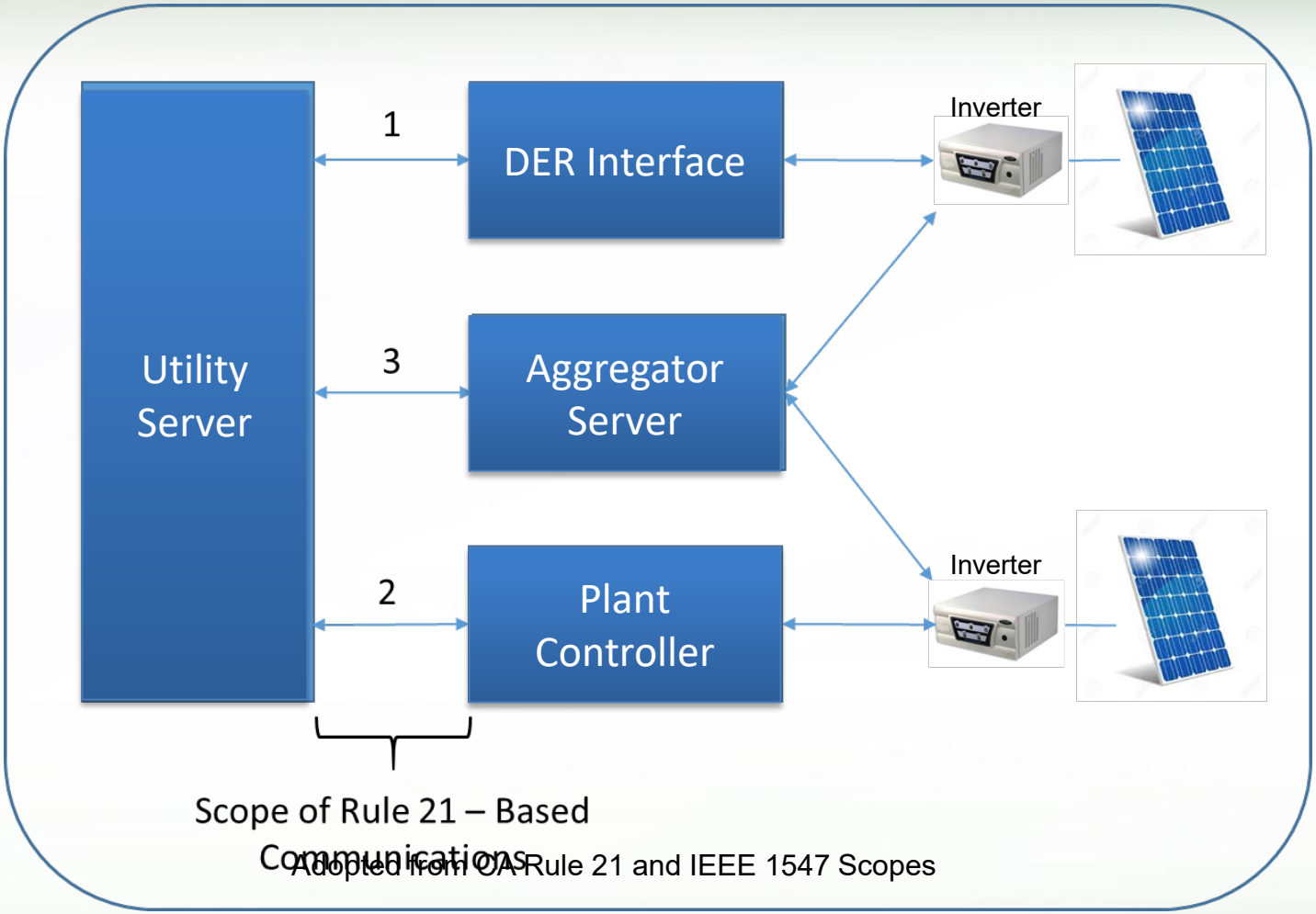
- **Primary Goal: generate a collection of best practices that act as basis for (or input to) national or international DER cyber security standards.**

- Secondary Goal: facilitate DER cyber security discussions among stakeholders to exchange perspectives and gain broad buy-in from the industry.




Sandia National Laboratories

# General scope of working groups




Adopted from CA Rule 21 and IEEE 1547 Scopes

Sandia National Laboratories

# Cyber security working group plan

- **Meeting rhythm**
  - Twice-per-month **working sessions** on key topics
    - In-depth explorations led by subject matter experts
    - Groups typically meet ten to twelve times per topic
    - Goal to create best practice or standards recommendations
  - Once-per-month **full group meeting**
    - Roadmap review with updated from working groups
    - Presentation of key cyber security concepts
      - Educate DER & power systems communities about cyber security topics
    - Work plan status & next steps
  - Periodic as-needed public webinars

Sandia National Laboratories

# Topics

**Intro to DER Cyber Presentations**

- Confidentiality, integrity, availability
- Authentication, authorization, accounting/non-repudiation
- “Light weight” DER cyber assessments with off-the-shelf cyber tools and applications
- Cyber resilience
- Encryption
- Presentations from partners and industry
- ….

**Development of DER Cyber Recommendations**

- Selecting the appropriate standard for these requirements: IEEE 1547.x, others?
- Where cyber security requirements will exist (inside/outside of DERs and plants, device vs. system level)
- Understand/refine IEEE 2030.5 and IEEE 1815 security features
- Addressing Modbus security challenges
- Cyber/interoperability certification process
- Auditing and interoperability (device and network)
- Assessments (Host based/Ad-Hoc)
- …

Sandia National Laboratories

# Working group structure (proposed)

SunSpec/Sandia DER Cybersecurity Workgroup

## Communication and Protocol Security

- **Define requirements and draft language for data-in-transit security rules.**
- Lead: ?
- Authentication
- Encryption requirements
- Acceptable transport protocols

## Secure Network Architecture

- **Create DER control network topology requirements and interface rules.**
- Lead: ?
- Segmentation
- Perimeter control
- Physical security

## Access Controls

- **Classify data types, associated ownership, and permissions. Define set of protection mechanisms.**
- Lead: ?
- Access control lists
- Password control
- Data privacy

## DER/Server Data and Communication Security

- **Define standardized procedure for DER and server vulnerabilities assessments.**
- Leads: Cedric Carter (Sandia) and Danish Saleem (NREL)
- Known equipment vulnerabilities
- Establish certification and auditing procedures (e.g., UL 2900, IEC 62351 Parts 3 and 4)
- Maintaining compliance, requirements for patching

# Next meetings

- **How to get started**
  - Sign up at http://sunspec.org/sunspec-cybersecurity-workgroup/
  - Review the background materials
  - Access workgroup page to track progress & get assignments
  - Download reading material or post comments
  - Contact membership@sunspec.org for enrollment questions.

- **Next monthly meeting in mid-October**
- **Working group leads are beginning to schedule events**

Sandia National Laboratories

# Cyber Security Workgroup portal

Join the SunSpec Alliance | Login | Register

SUNSPEC ALLIANCE

SEARCH THIS WEBSITE ...

HOME | ABOUT | MEMBERS | INITIATIVES | CERTIFICATION | SPECIFICATIONS | BEST PRACTICES | SOFTWARE | WORKGROUPS

## SunSpec DER Cybersecurity Workgroup

**How to Participate:**

The SunSpec Alliance is happy to announce the formation of our new Distributed Energy Resource (DER) Cybersecurity workgroup. This workgroup focuses on current issues in the U.S. supports SunSpec's involvement in projects with Sandia and the California Energy Commission. In order to kick this program off, SunSpec will be holding a public webinar to describe the nature of this work and enroll future participants. As this is a public webinar no IP Agreements are required but if you know you would like to participate in future calls you can formally enroll in the program and complete an IP Agreement here.

Enroll In Workgroup

**Initial Workgroup Webinar:**

This kickoff webinar includes an introduction by Tom Tansy of the SunSpec Alliance and features Jay Johnson of Sandia National Laboratories. Jay is an expert in Distributed Energy

SIGNUP FOR NEWSLETTER

Fields marked with a * are required.

**First Name** *

**Last Name** *

**Email** *

Submit

RECENT POSTS

# Danish Saleem Profile

***Education***

- MS Electrical Engineering (Florida International University)
- BE Electrical Engineering (NED university)

***Experience***

- Two years of experience in Power Systems
- One-and-a-half year of experience in learning networking and security

***Role in NREL***

- Serving as a Lab Manager in Cyber Physical Systems Security and Resiliency (CPSS&R) lab
- Working on DER security, standards and their testing & certification procedures.
- Leading subgroup 'DER/Server Data and Communication Security' within SunSpec Alliance DER security working group
- Member of SGCC committee

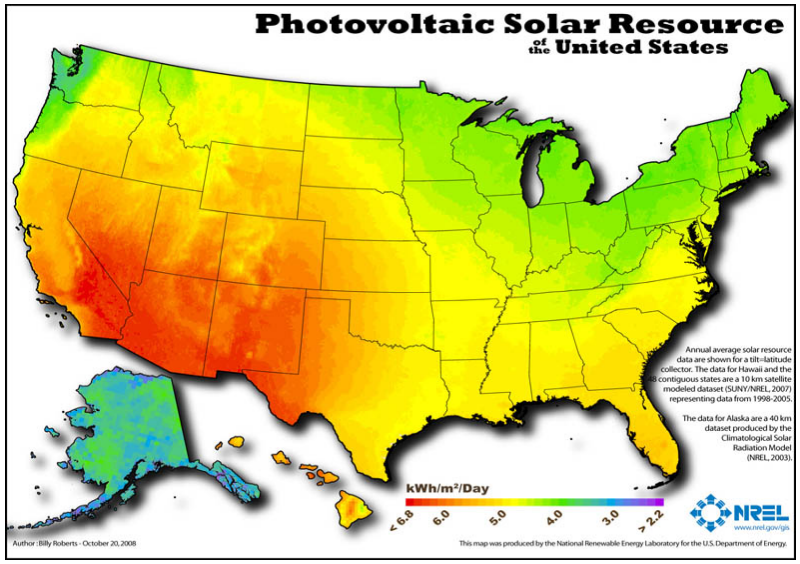
# AGENDA

- Overview
  - Background
  - Increased penetration of distributed generation (DG)
  - Goals and objectives
- Unique value proposition of NREL's cybersecurity team
  - Cyber Physical Systems Security & Resiliency (CPSS&R) testbed
- Security Controls for DERs
  - What most people think about security?
  - Basic and stringent security controls
  - Introduction to IEC 62351 standards and its parts
- Certification Procedures
  - Need of certification procedures
  - Purpose and intended audience
  - How we do it?
- Draft of Certification Procedure and Next Steps

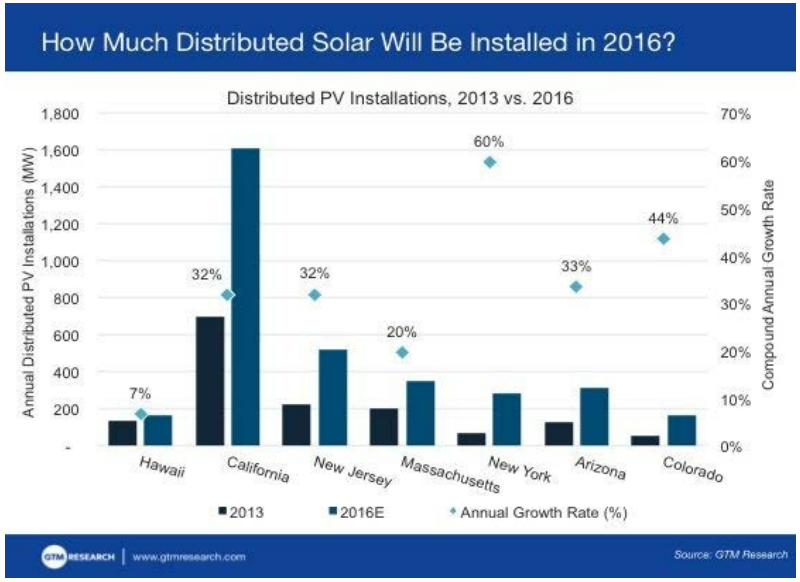
# OVERVIEW (1)

## *Background*

- There is more and more penetration of DERs into the grid and their security is very important.
- There is a big gap and lack of consistency in the adoption of stringent security controls for the data and communication infrastructure of DERs
- Increasing cybersecurity threats become particularly evident in the recent wannacry ransomware attack, Equifax cyberattack and Stuxnet
- Vendors are using their proprietary protocols which are not interoperable with the security controls of utility




Source: National Renewable Energy Laboratory



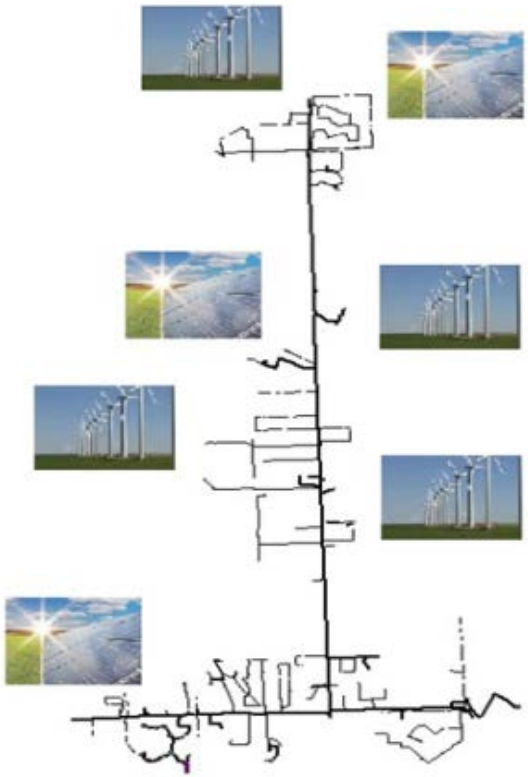

Source: GTM Research/SEIA

# OVERVIEW (2)

## *Increased penetration of Distributed Generation (DG)*

- Significant increase in DG deployment is experienced in many utilities in the U.S., primarily due to:
  - Decreasing cost of DG technologies
  - Customer desire for increased control of the energy consumption and reducing electricity payments
  - Federal and state incentives supporting renewable generation

- The potentially significant DG penetration will result in a number of challenges, one of the most significant being the impact on the security of the grid and the connecting DERs



## *Goals and Objectives*

- Accelerate the adoption of stringent security controls for DERs

- Standardize certification procedures for DER security

- Address the potential of DER cybersecurity issues by establishing partnership with multiple vendors

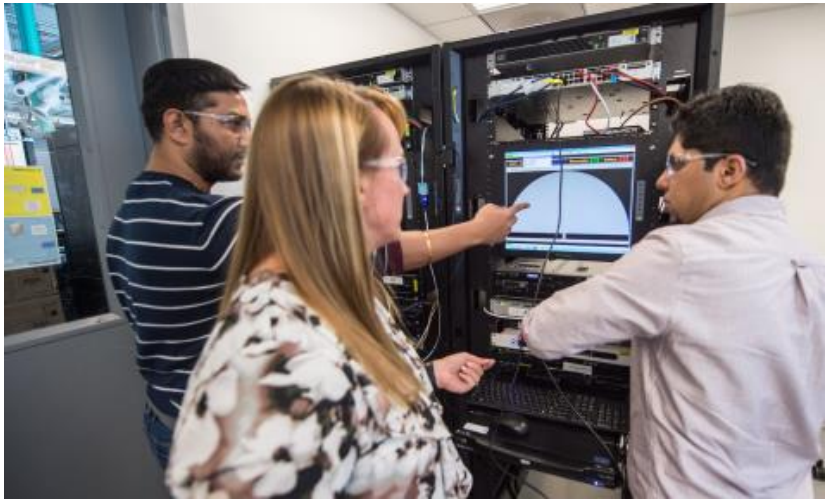
# Unique Value Proposition NREL's Cybersecurity Team

- Deep expertise in:
  - Power Systems SCADA
  - Cybersecurity
  - Networking
  - Distributed Energy Resources

- Advanced research/user facility at NREL's Systems Performance Laboratory at the Energy Systems Integration Facility
  - Complete testbed with modular power systems, communications and cybersecurity capabilities
  - Vendor and technology agnostic perspective
  - Ability to pen test at interface, component or systems level

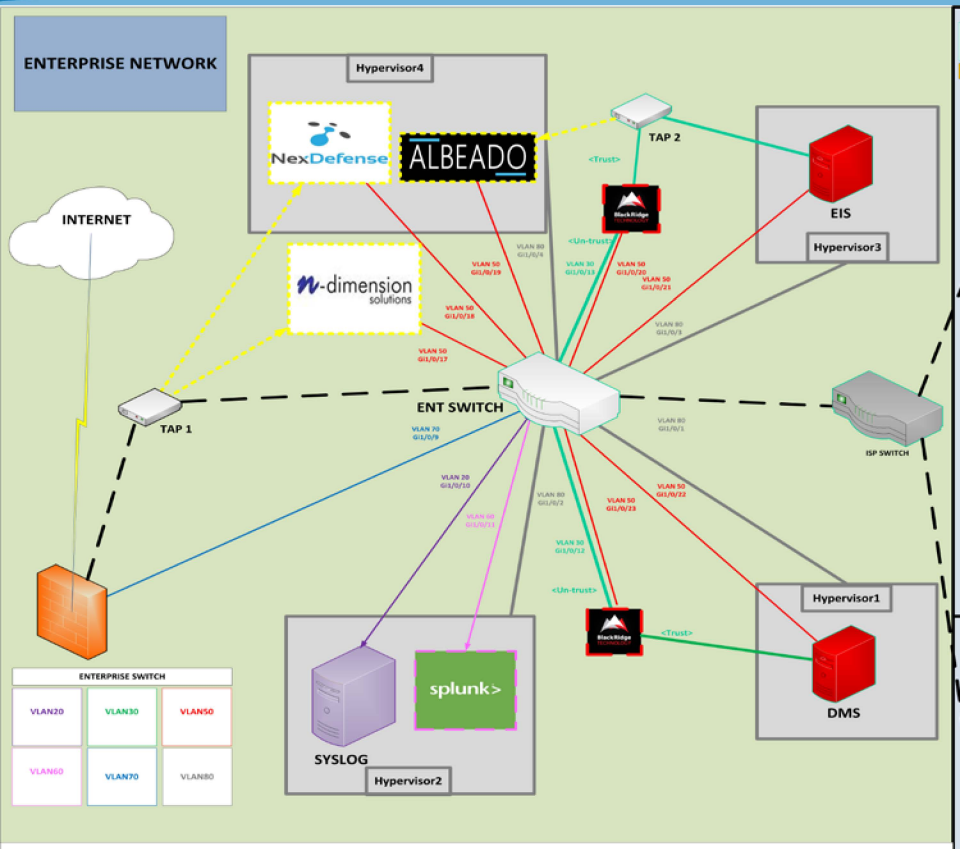
- Flexibility to expand to water, oil and gas, and thermal systems testing for cybersecurity and resilience

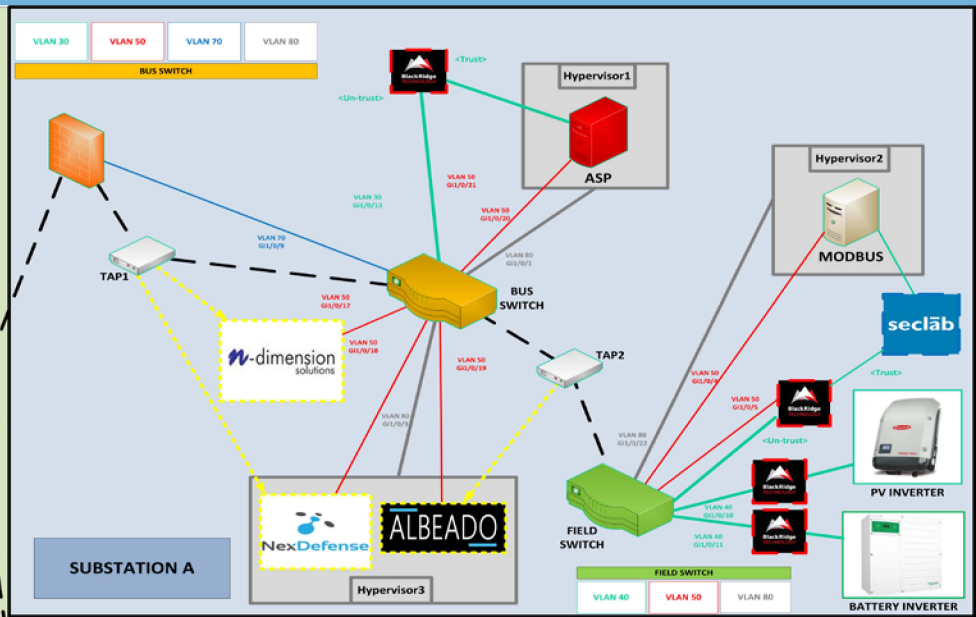
*NREL, 43409*

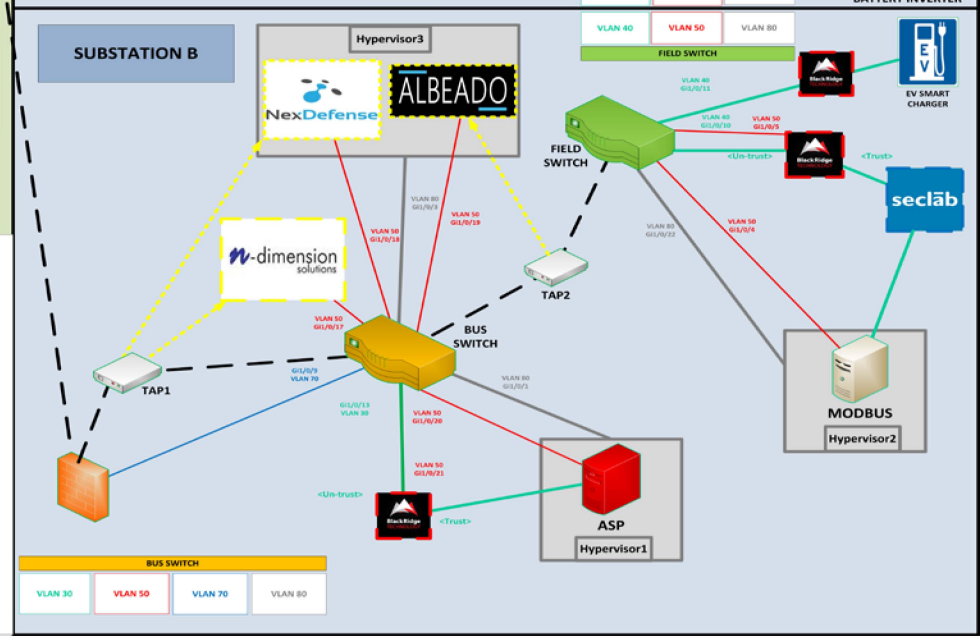


*NREL, 43396*

# Cybersecurity Testbed Network View




CYBER PHYSICAL SYSTEMS SECURITY & RESILIENCY NETWORK

NREL
NATIONAL RENEWABLE ENERGY LABORATORY

# Security Controls for DERs (1)

Most people think security as to lock down everything using encryption and authentication at device level but there are limitations to this approach.

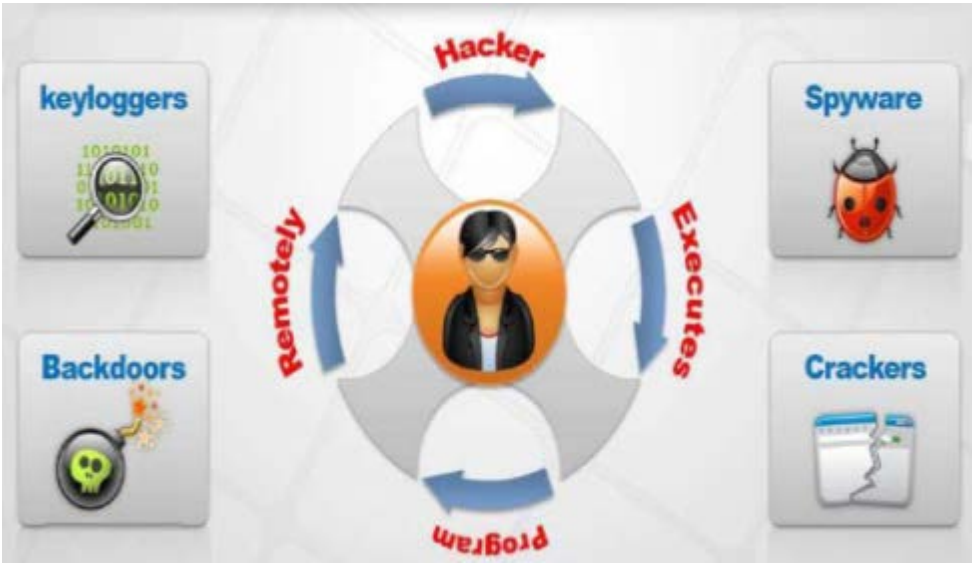
Source: EC-council (CEH training)

***Approach*: Lock down everything**

- Encryption in all communications
- Protocol level security enforced
- Advanced end-device level authentication and monitoring

***Limitations***

- Reactive – hackers are always ahead of the organization's cybersecurity capabilities (security standards process too slow)
- Too much overhead (e.g. memory, processing, networking)
- Fork lift upgrades of legacy equipment required (very costly)



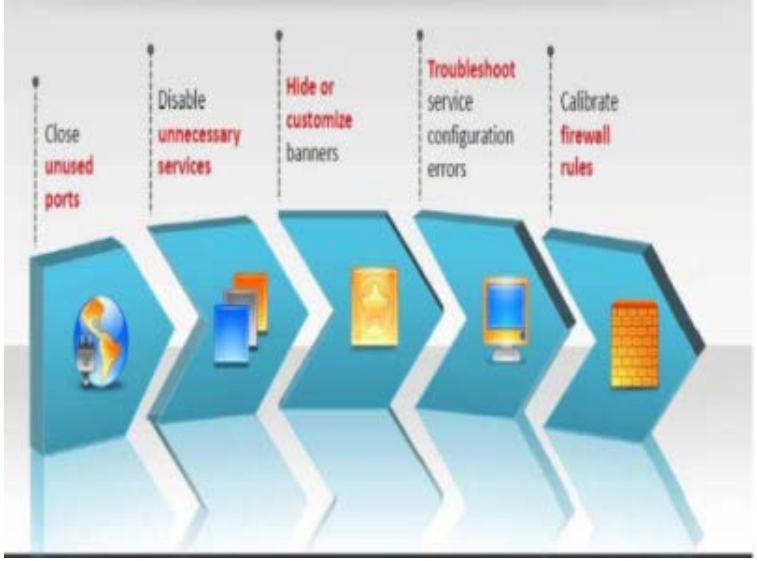

Source: EC-council (CEH training)

# Security Controls for DERs (2)

## *What are the basic and stringent security controls ?*

- Basic security controls
  - Strictly enforce role-based access controls.
  - Network segmentation with different VLANs to create air gap between OT, IT and Management networks
  - Locking down each DER on a .252 mask
  - Periodically updating of software security patches
  - Encrypt selectively to minimize processing overhead and application latency
  - Systemically Secure the network by implementing 9 layer architecture with intrusion detection (context based and signature based) and in-line blocking tools
  - Disabling all unused ports to eliminate unauthorized access


Source: EC-council (CEH training)




Source: EC-council (CEH training)

# Security Controls for DERs (3)

## *What are the basic and stringent security controls?*

- Stringent security controls
  - Transport layer security (TLS) should be activated in the DERs like inverters, microgrid controllers etc
  - Session resumption should happen if the session is severed for the time less than TLS session resumption time using the secret session key.
  - Session negotiation should happen if the session is severed for the time greater than the TLS session renegotiation time.
  - Use of Message Authentication Code (MAC)
  - Support for multiple Certification Authorities (CA)
  - Capability of terminating the session if a revoked certificate is used to establish the connection. This is done by using Certification Revocation list (CRL)
  - Capability of identifying and terminating the session if a expired certificate is used to establish the connection.

## *How do we do it?*

- Making a detail test plan and codifying them into certification standard
- Update IEC 62351 DER standards with new High level test cases

# Security Controls for DERs (4)

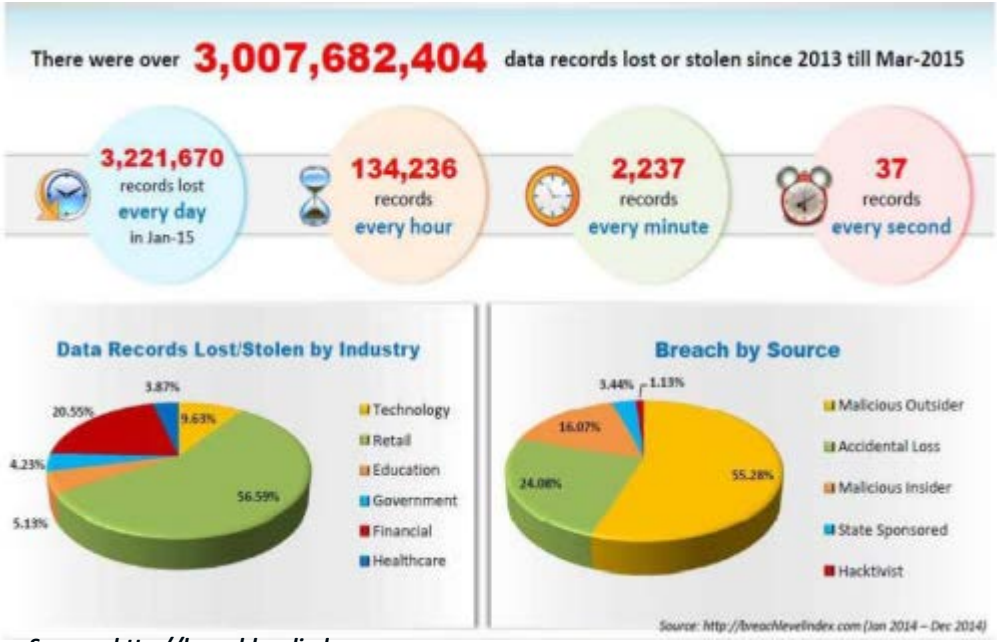
## *Introduction to IEC 62351 standards*

- IEC TC57 WG15 was formed in 1999 to undertake the development of cybersecurity standards for power systems communication.
- They came up with IEC 62351 which are the standards for securing the power systems management and associated information exchange
- Parts 1 and 2 are introduction and Glossary. Parts 3-6 are for "Data and Communication Security Requirements" and Parts 7-11 are for "End-to-End Security Requirements"
- In the Certification Procedures document, as of now, we have developed the detail test plan which covers the test cases, methodology, purpose and the action items for securing the DERs over TCP/IP.

# Certification Procedures (1)

## *What is the need of Certification Procedures?*

- There were 3,007,682,404 data records lost or stolen since 2013 till March 2015
- The WannaCry ransomware attack, that happened in May 2017, effected 200,000 people and 300,000 computers from 150 countries
- Recent data breach of Equifax cost almost 120 million customers lose their Personal Identifiable Information (PII)
- eBay data breach cost 145 million customers lose their PII
- The Home Depot data breach cost 56 million customers lose their Debit and credit card numbers




*Source: http://breachlevelindex.com*


*Source: http://bankinfosecurity.in*

# Certification Procedures (2)

## *Purpose*

- Protects against:
  - Eavesdropping and replay (through TLS encryption)
  - Man-in-the- middle security risk
  - Spoofing through security certificates (node authentication)
- Cover previously used profiles by:
  - IEEE 1815 (DNP3) over TCP/IP
  - IEEE 2030.5 (SEP2)
  - IEC 60870-6 (ICCP)
  - IEC 60870-5 (part 104)
  - IEC 61850 over TCP/IP

## *Who would be intended audience?*

- Initial audience would be experts who are developing or making use of security protocols in the field of power systems management and associated information exchange.
- Subsequent audience would be developers of products that will implement these procedures
- Some procedures can also be used by managers and executives in order to understand the purpose

# Draft of Certification Procedures and Next Steps

Certification Procedures (workshop).docx

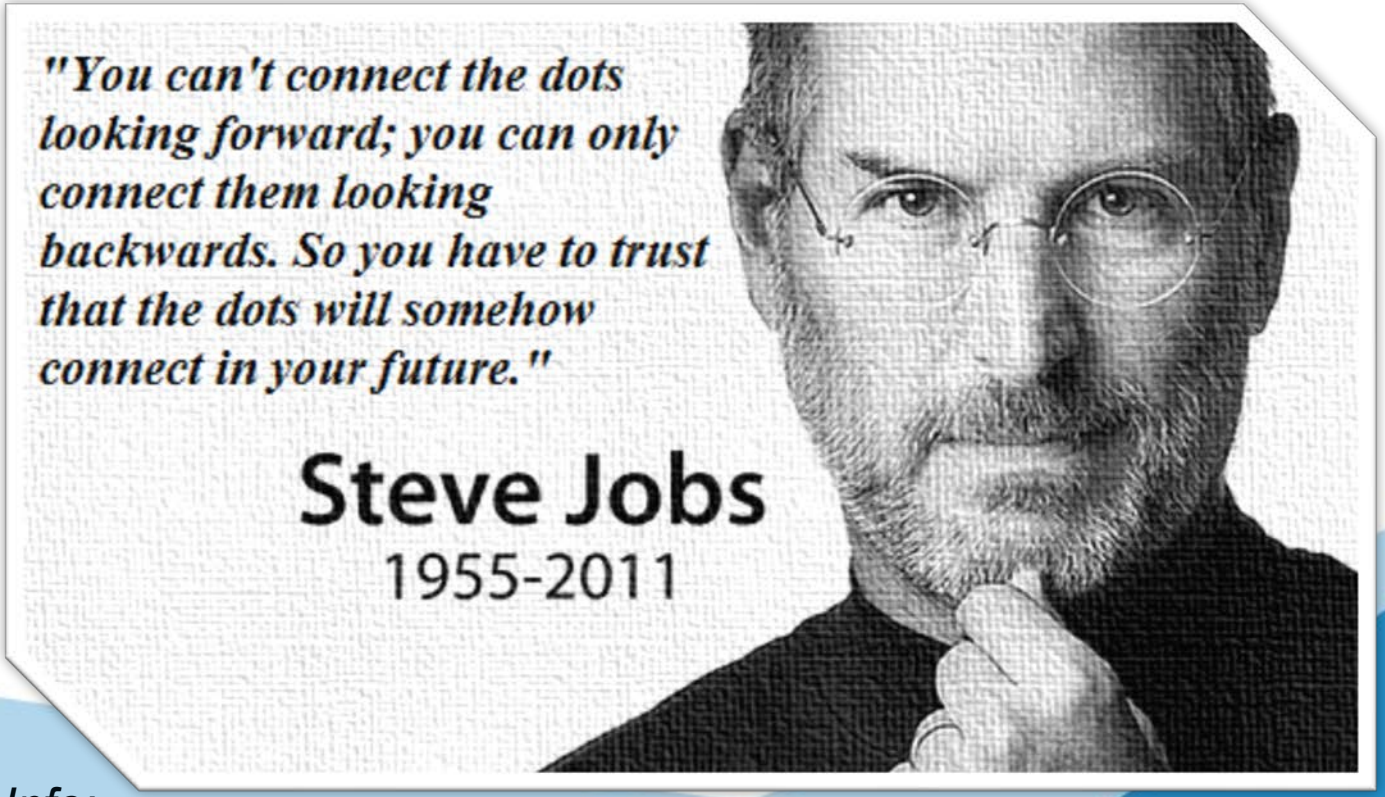
## *Next Steps*

- To foster interoperability, information models, communication protocols, and cybersecurity controls used for information exchanges should be international standard

- Create a certification procedure document that takes the high level test cases from of cybersecurity, converting them into detail test plans and then develop a document that certification labs can use.

- The security controls doesn't adhere to Modbus protocol, therefore we will continue working on these security controls to extend them to Modbus as well because lot of DERs still use Modbus for communication.

- To ensure minimum cybersecurity policies, controls, procedure that ensure authentication, authorization, accountability and integrity of the data and communication  information exchange.




*Contact Info:*

**Jay Johnson**
jjohns2@sandia.gov
505-284-9586

**Danish Saleem**
danish.saleem@nrel.gov
720-404-5912

www.nrel.gov

NREL
NATIONAL RENEWABLE ENERGY LABORATORY

NREL/PR-5C00-70454