# What you need to know about the PI System, DERS and Cybersecurity

Bryan Owen PE

OSIsoft – Security Architect

Alternate Title:

# DERS save the World!

Alternate Title 2:

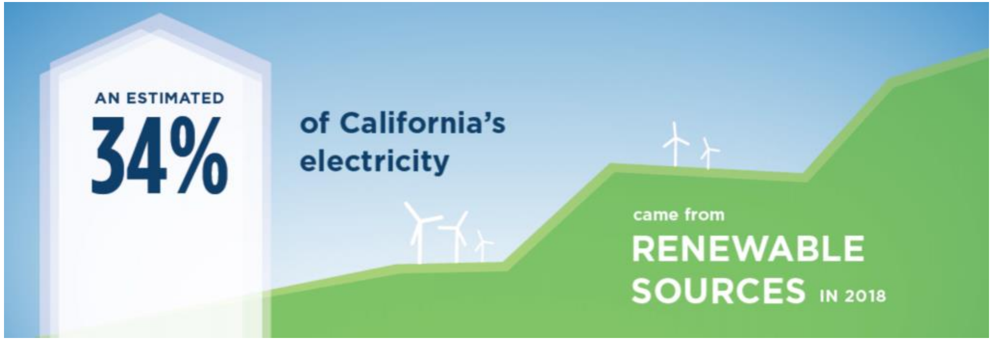
# How to prosper with DERS in the face of cyber threats.

# tl;dr

- DER POWER GENERATION MUST EXPAND RAPIDLY
- STATE OF CALIFORNIA IS STEPPING UP CYBERSECURITY
- CYBERSECURITY PROGRESS BY CONSORTIUM
- PRIORITIES BASED ON THREAT MODELS
- PI SYSTEMS HELP PROTECT UTILITY SCALE DERS
- FUTURE VISION AND APPROACH

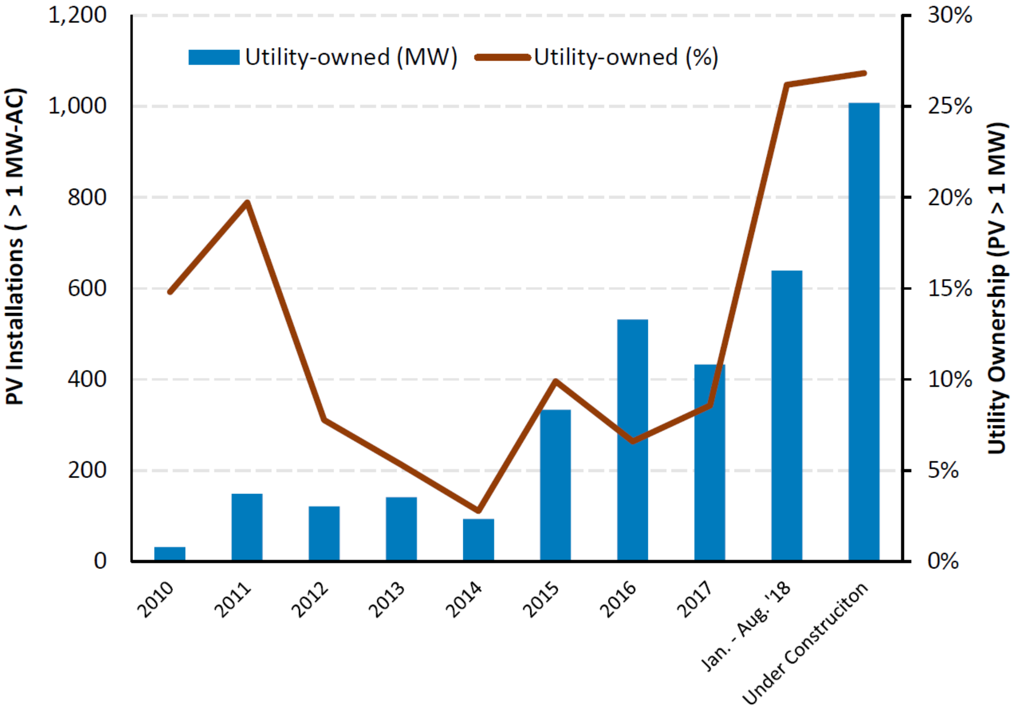
# California Senate Bill 100

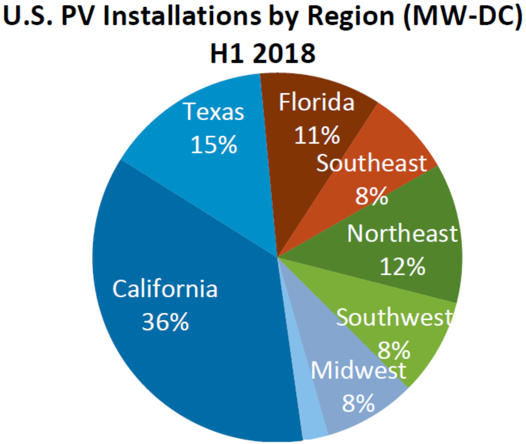
- 60% Renewable by 2030
- Zero-carbon by 2045
- Scope:
  - Retail customers
  - State agencies



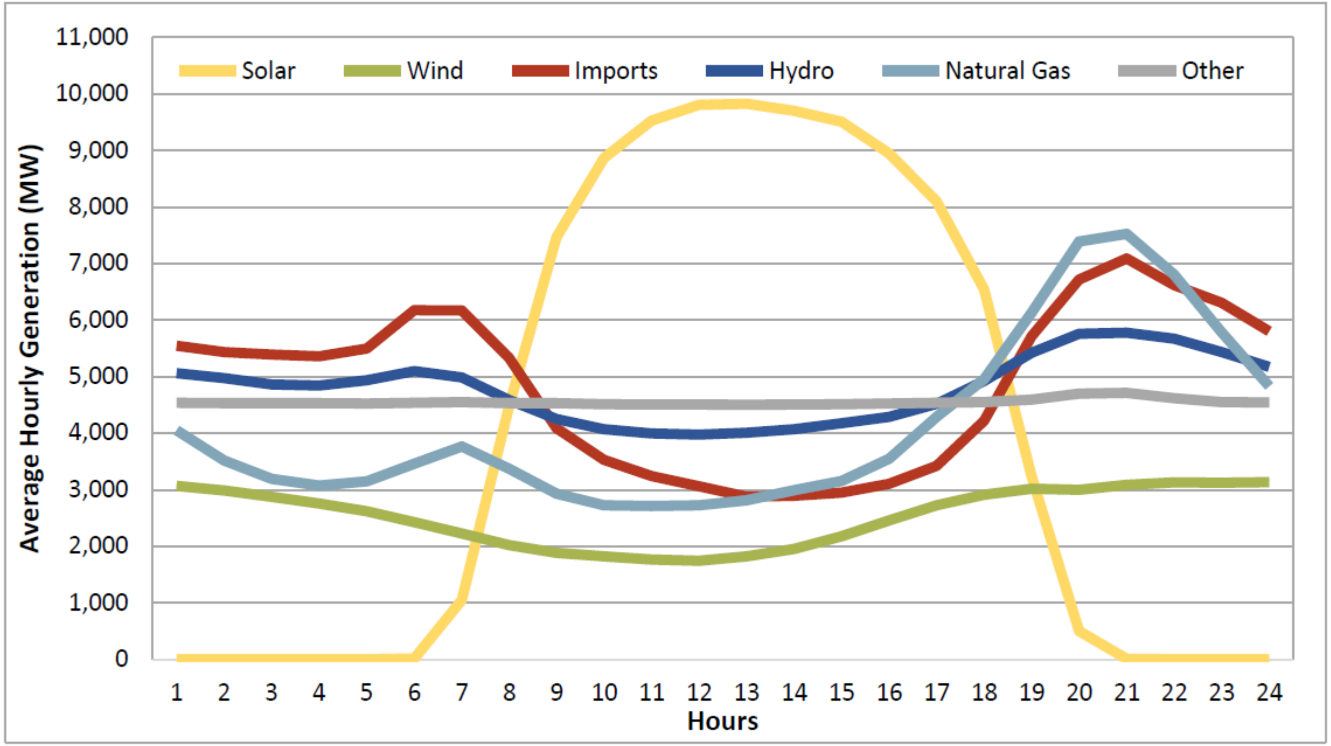
Source: California Public Utility Commission

# Solar Industry – PV Investment in US





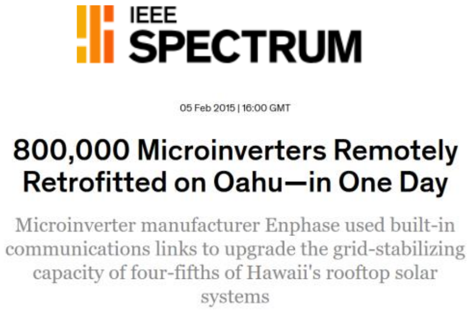
# 2019.Q2 Generation fuel type by hour



Source: Department of Market Monitoring – California ISO

# Grid support is needed to increase DER

| Smart Inverter – Grid Support 2.0 | |
|---|---|
| **Autonomous** | **Advanced** |
| • Anti-Islanding | • Connect/Disconnect |
| • Voltage Ride Through | • Max Active Power |
| • Frequency Ride Through | • Scheduling Power |
| • Ramp Rate | • Monitoring, Alarms, Status |
| • Dynamic Volt-Var | • Volt-Watt Control |
| • Fixed Power Factor | • Frequency-Watt Control |



IEEE SPECTRUM

05 Feb 2015 | 16:00 GMT

**800,000 Microinverters Remotely Retrofitted on Oahu—in One Day**

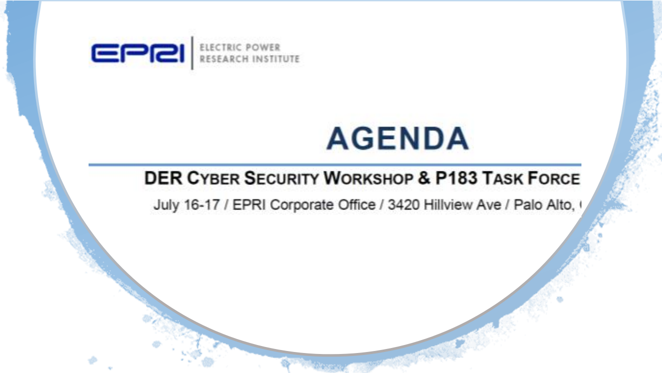
Microinverter manufacturer Enphase used built-in communications links to upgrade the grid-stabilizing capacity of four-fifths of Hawaii's rooftop solar systems

DER is already important to California energy supply.

Control functions make DER security an imperative!

# DER Task Force to advance cyber security

- Industry
- Utilities
- National Lab
- Regulators
- Standards Body



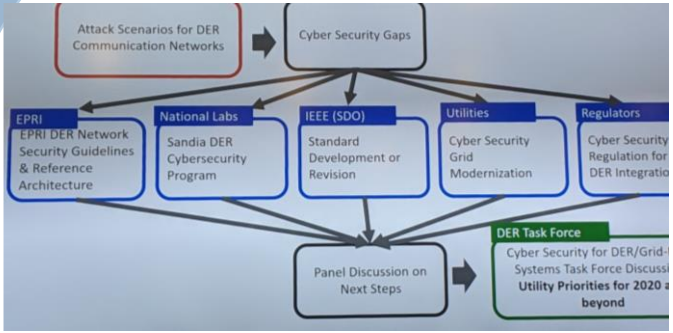
EPRI | ELECTRIC POWER RESEARCH INSTITUTE

AGENDA

DER Cyber Security Workshop & P183 Task Force

July 16-17 / EPRI Corporate Office / 3420 Hillview Ave / Palo Alto,

## Gap Analysis



Attack Scenarios for DER Communication Networks → Cyber Security Gaps

EPRI: EPRI DER Network Security Guidelines & Reference Architecture

National Labs: Sandia DER Cybersecurity Program

IEEE (SDO): Standard Development or Revision

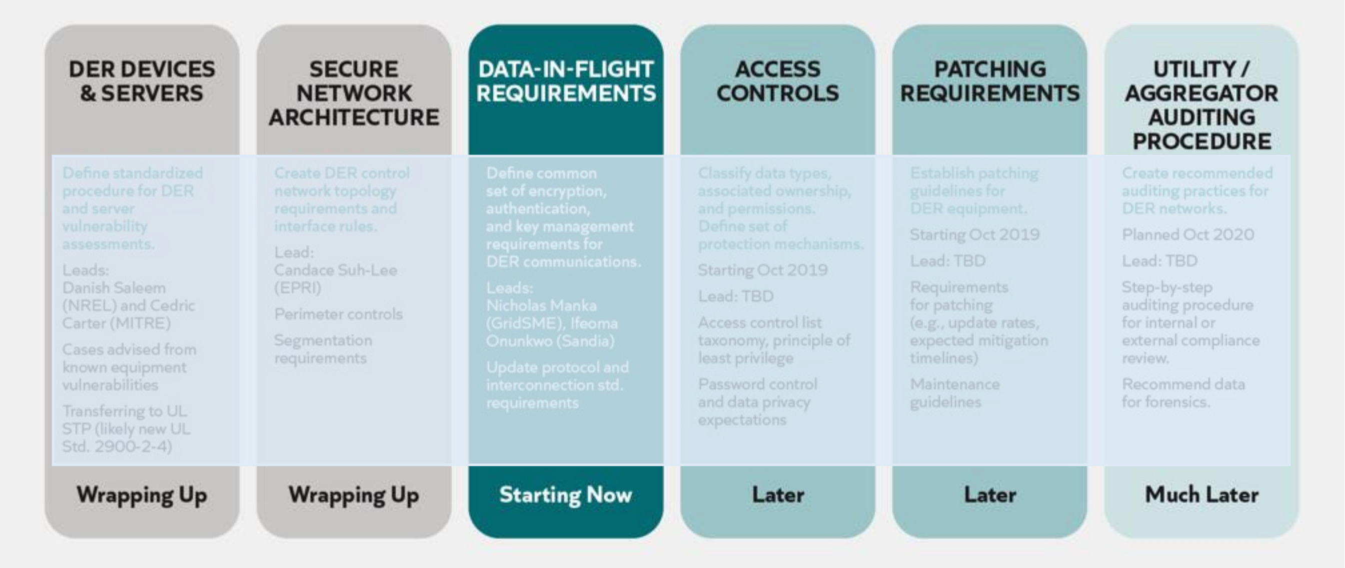
Utilities: Cyber Security Grid Modernization

Regulators: Cyber Security Regulation for DER Integratio

Panel Discussion on Next Steps →

DER Task Force: Cyber Security for DER/Grid-I Systems Task Force Discussi Utility Priorities for 2020 a beyond

# Cybersecurity status for DER in California

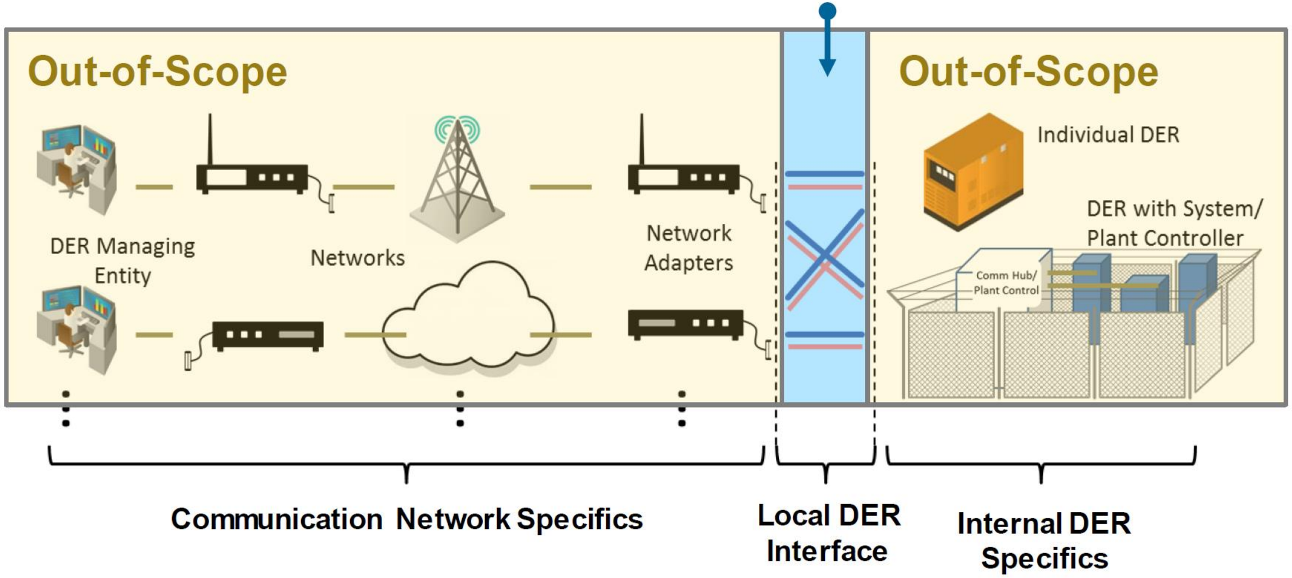


| DER DEVICES & SERVERS | SECURE NETWORK ARCHITECTURE | DATA-IN-FLIGHT REQUIREMENTS | ACCESS CONTROLS | PATCHING REQUIREMENTS | UTILITY / AGGREGATOR AUDITING PROCEDURE |
|---|---|---|---|---|---|
| Define standardized procedure for DER and server vulnerability assessments.<br>Leads: Danish Saleem (NREL) and Cedric Carter (MITRE)<br>Cases advised from known equipment vulnerabilities<br>Transferring to UL STP (likely new UL Std. 2900-2-4) | Create DER control network topology requirements and interface rules.<br>Lead: Candace Suh-Lee (EPRI)<br>Perimeter controls<br>Segmentation requirements | Define common set of encryption, authentication, and key management requirements for DER communications.<br>Leads: Nicholas Manka (GridSME), Ifeoma Onunkwo (Sandia)<br>Update protocol and interconnection std. requirements | Classify data types, associated ownership, and permissions. Define set of protection mechanisms.<br>Starting Oct 2019<br>Lead: TBD<br>Access control list taxonomy, principle of least privilege<br>Password control and data privacy expectations | Establish patching guidelines for DER equipment.<br>Starting Oct 2019<br>Lead: TBD<br>Requirements for patching (e.g., update rates, expected mitigation timelines)<br>Maintenance guidelines | Create recommended auditing practices for DER networks.<br>Planned Oct 2020<br>Lead: TBD<br>Step-by-step auditing procedure for internal or external compliance review.<br>Recommend data for forensics. |
| Wrapping Up | Wrapping Up | Starting Now | Later | Later | Much Later |

Source: SunSpec Alliance Distributed Energy Resource (DER) Cybersecurity workgroup

# IEEE 1547 and California Rule 21 is the standard for DER interconnection

Protocols: *IEEE 2030.5, IEEE 1815, Sunspec Modbus*



Source: IEEE Standards Association

# IEEE 1547 working group security topics

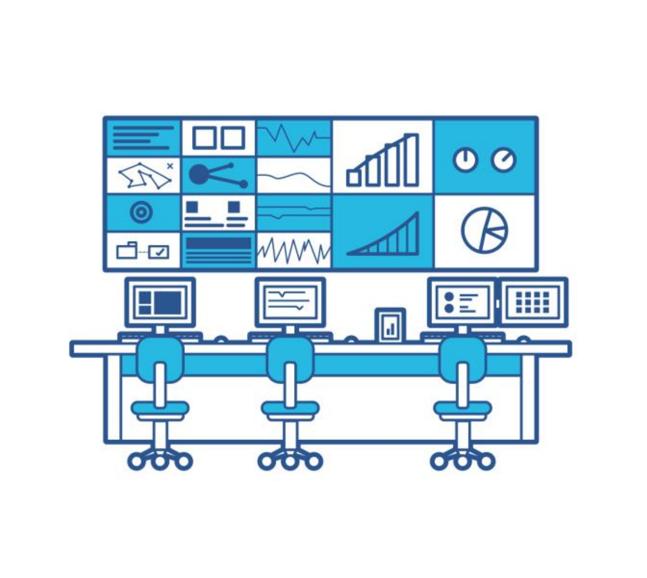
| | Discussion Examples |
|---|---|
| | Requirements if using HTTPS |
| | Interaction between cloud, mobile, utility, and on-site dashboards |
| • | DER configuration unlock codes |
| | Network gateway protocol conversions |
| • | Firmware update capability |

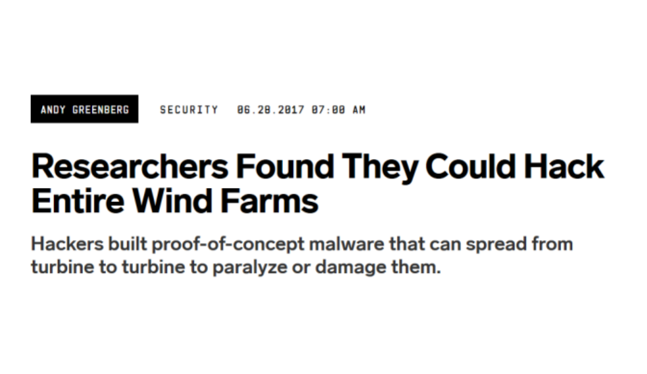
# DER Threat Models

# Threat Model #1

## Packet injection

- Wired
- Wireless
- Logical
- Physical
- Supply Chain

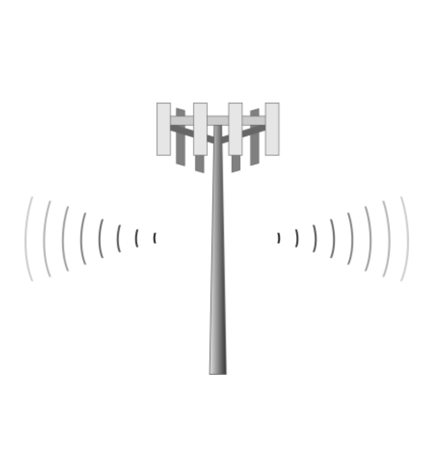




ANDY GREENBERG SECURITY 06.20.2017 07:00 AM

**Researchers Found They Could Hack Entire Wind Farms**

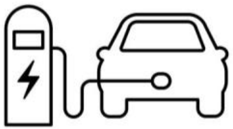
Hackers built proof-of-concept malware that can spread from turbine to turbine to paralyze or damage them.

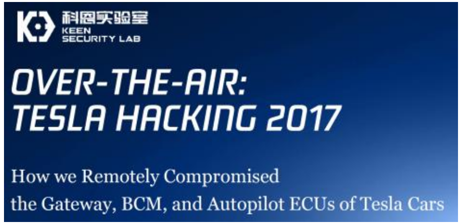


# Threat Model #2

## Firmware Update

- Wired
- Wireless
- Logical
- Physical
- Supply Chain

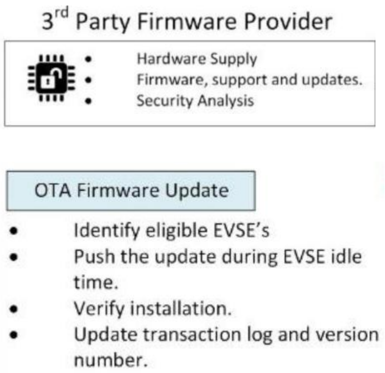




科恩实验室
KEEN SECURITY LAB

OVER-THE-AIR:
TESLA HACKING 2017

How we Remotely Compromised
the Gateway, BCM, and Autopilot ECUs of Tesla Cars



3rd Party Firmware Provider

- Hardware Supply
- Firmware, support and updates.
- Security Analysis

OTA Firmware Update

- Identify eligible EVSE’s
- Push the update during EVSE idle time.
- Verify installation.
- Update transaction log and version number.

*“I think one of the biggest concern for autonomous vehicles is somebody achieving a fleet-wide hack.” – Elon Musk*

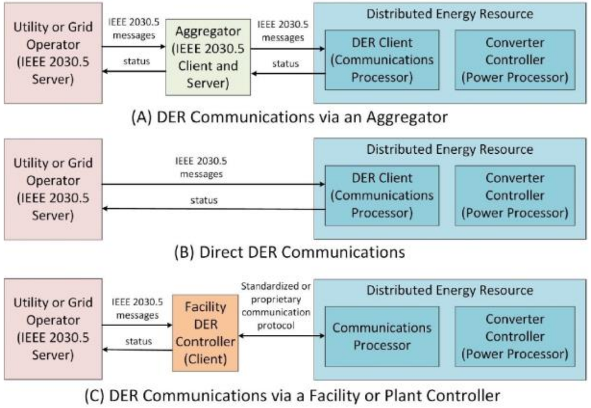
https://insideevs.com/news/334056/fleet-wide-autopilot-hack-is-teslas-biggest-security-concern/

# Threat Model #3

## Trust Anchors

- Wired
- Wireless
- Logical
- Physical
- Supply Chain

*Potential truck roll to replace root certificates*



Utility or Grid Operator (IEEE 2030.5 Server)
IEEE 2030.5 messages
status
Aggregator (IEEE 2030.5 Client and Server)
IEEE 2030.5 messages
status
Distributed Energy Resource
DER Client (Communications Processor)
Converter Controller (Power Processor)

(A) DER Communications via an Aggregator

Utility or Grid Operator (IEEE 2030.5 Server)
IEEE 2030.5 messages
status
Distributed Energy Resource
DER Client (Communications Processor)
Converter Controller (Power Processor)

(B) Direct DER Communications

Utility or Grid Operator (IEEE 2030.5 Server)
IEEE 2030.5 messages
status
Facility DER Controller (Client)
Standardized or proprietary communication protocol
Distributed Energy Resource
Communications Processor
Converter Controller (Power Processor)

(C) DER Communications via a Facility or Plant Controller

DER client id = X509 certificate

**IEEE 2030.5 PKI – Trust Chains**

1. Utility directly signs client certificate
2. Utility authorizes OEM to directly sign client certificate
3. Utility authorizes OEM issuing authority to sign client certificate

IEEE 2030.5 PKI certificates

- Allow and block lists
- No expiration
- No revocation

Source: SAND2019-1490 Recommendations for Trust and Encryption in DER Interoperability Standards

# DER Weakest Links

## Physical Access

Keypads

Comm ports

Trip inputs

Control outputs

## Supply Chain

HW/FW/SW provenance

Lifecycle support

Trust anchors

## Remote

Applications

Comm Protocols

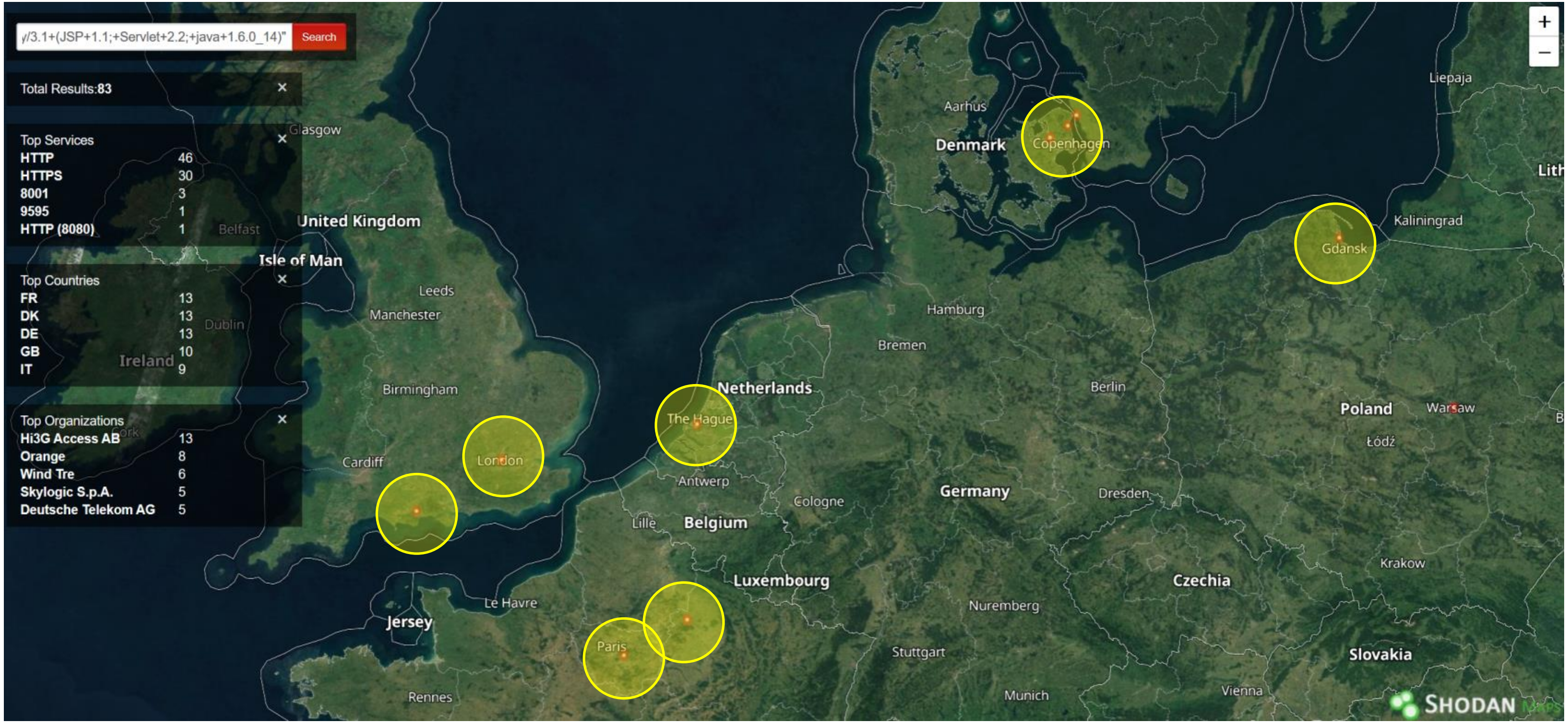
Configuration

Logging

# DER Solution Approaches

- System architecture
- Cyber-physical intrusion detection
- Configuration monitoring

# Wind farms aren’t ready for the wild, wild web



y/3.1+(JSP+1.1;+Servlet+2.2;+java+1.6.0_14)" Search

Total Results:83 ×

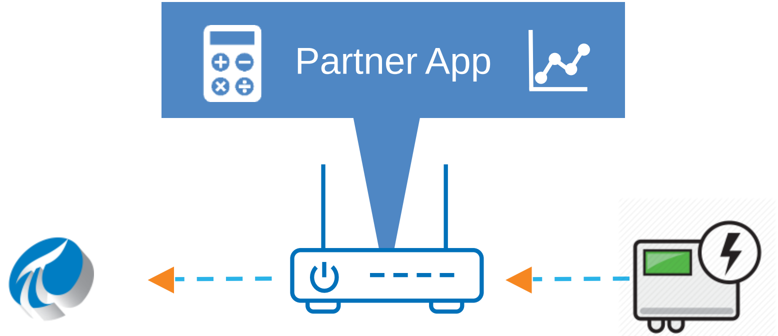
| Top Services × | |
|---|---|
| HTTP | 46 |
| HTTPS | 30 |
| 8001 | 3 |
| 9595 | 1 |
| HTTP (8080) | 1 |

| Top Countries × | |
|---|---|
| FR | 13 |
| DK | 13 |
| DE | 13 |
| GB | 10 |
| IT | 9 |

| Top Organizations × | |
|---|---|
| Hi3G Access AB | 13 |
| Orange | 8 |
| Wind Tre | 6 |
| Skylogic S.p.A. | 5 |
| Deutsche Telekom AG | 5 |

Shodan dork: http.title:"Nordex Control" "Windows 2000 5.0 x86" "Jetty/3.1 (JSP 1.1; Servlet 2.2; java 1.6.0_14)“ – Accessed Sep 2019

# Do not directly expose DERS to the internet [S-O-S] Stuff off Shodan



Utility / DER Aggregator

Edge Data Store, PI System, OSIsoft Cloud Services

Utility Scale DER

**2018 - PI World - Barcelona - Transmission & Distribution**

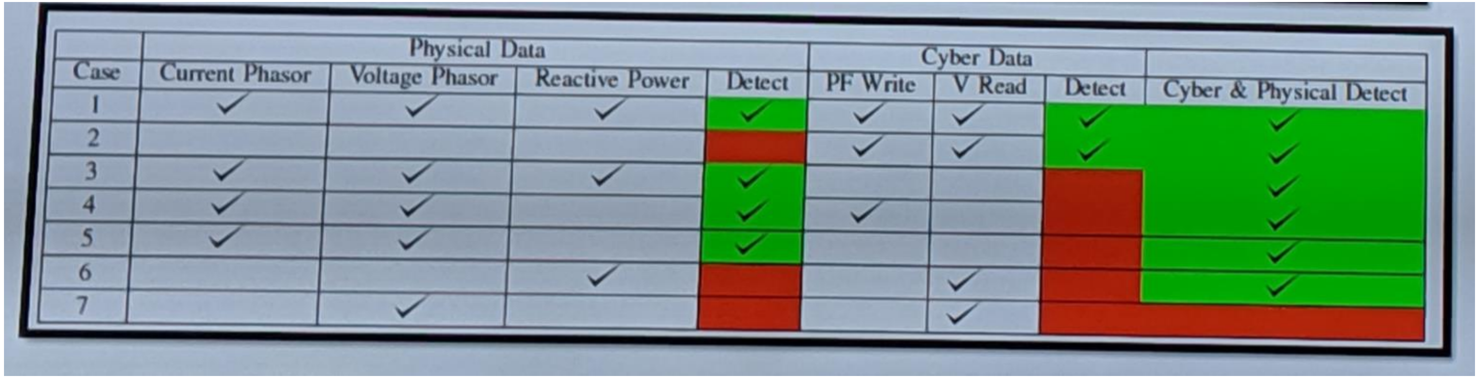
***Real-time Microgrid and DERMS Power Control using the PI System and PXiSE Advanced Control Solution***

PXiSE brings new intelligence and autonomy to grid control

Insightful high-speed phasor data
Multi-level system feedback control
System model, optimization, & artificial intelligence
OSIsoft PI data technology
Intelligent software

# Cyber-physical intrusion detection strategy

- aka ‘Digital Twin’ asset models vs field instrumentation
- Increased coverage and lower false positive confirmed in Sandia lab simulation
- Secondary IoT sensors could further enhance detection of injected packets

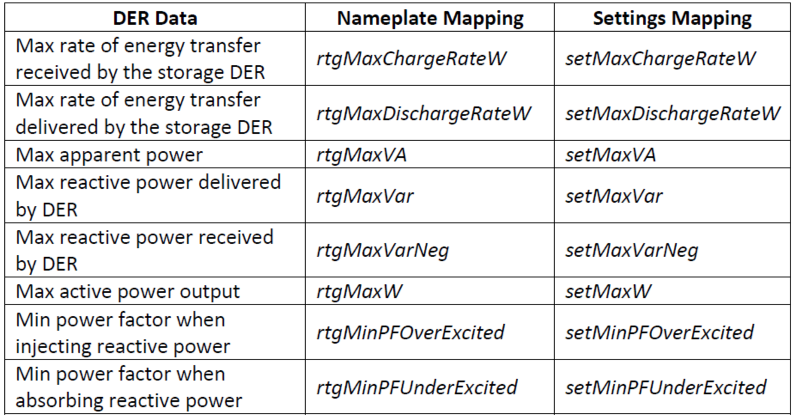


|  | Physical Data |  |  |  | Cyber Data |  |  |  |
|---|---|---|---|---|---|---|---|---|
| Case | Current Phasor | Voltage Phasor | Reactive Power | Detect | PF Write | V Read | Detect | Cyber & Physical Detect |
| 1 | ✓ | ✓ | ✓ | 🟩 ✓ | ✓ | ✓ | 🟩 ✓ | 🟩 ✓ |
| 2 |  |  |  | 🟥 | ✓ | ✓ | 🟩 ✓ | 🟩 ✓ |
| 3 | ✓ | ✓ | ✓ | 🟩 ✓ |  |  | 🟥 | 🟩 ✓ |
| 4 | ✓ | ✓ |  | 🟩 ✓ | ✓ |  | 🟥 | 🟩 ✓ |
| 5 | ✓ | ✓ |  | 🟩 ✓ |  |  | 🟥 | 🟩 ✓ |
| 6 |  |  | ✓ | 🟥 |  | ✓ | 🟥 | 🟩 ✓ |
| 7 |  | ✓ |  | 🟥 |  | ✓ | 🟥 | 🟥 |

# Plan for increases in DER monitoring… don’t trust that a DER is configured as expected.

## DER security related monitoring

- Network perimeter indicators
- Authentication and cipher use
- Device provisioning stats
- PKI trust indicators
- SNMP device telemetry
- **Power system data**
- Security event logging



| DER Data | Nameplate Mapping | Settings Mapping |
|---|---|---|
| Max rate of energy transfer received by the storage DER | *rtgMaxChargeRateW* | *setMaxChargeRateW* |
| Max rate of energy transfer delivered by the storage DER | *rtgMaxDischargeRateW* | *setMaxDischargeRateW* |
| Max apparent power | *rtgMaxVA* | *setMaxVA* |
| Max reactive power delivered by DER | *rtgMaxVar* | *setMaxVar* |
| Max reactive power received by DER | *rtgMaxVarNeg* | *setMaxVarNeg* |
| Max active power output | *rtgMaxW* | *setMaxW* |
| Min power factor when injecting reactive power | *rtgMinPFOverExcited* | *setMinPFOverExcited* |
| Min power factor when absorbing reactive power | *rtgMinPFUnderExcited* | *setMinPFUnderExcited* |

*Table 12 - Nameplate Ratings and Adjusted Settings Mapping*

# What should success for PI System, DER and Cybersecurity look like?

# Capability vision of future distribution grid

### Pervasive communications

- Visibility to grid-edge devices and customer-owned loads
- Applications can talk to each other on-demand
- Real-time and right-time transfer of data

### Autonomous devices

- Capability to make the right decision resides on devices
- Localized intelligence supported by central data management

### Data management at scale

- Support exponential growth in data
- Effective management that turns data into right information
- Data from devices, customers and their suppliers

### Workforce innovations

- Retain operational expertise
- Effective use of technology
- Learning through AR/VR

### Agile corporate decisions

- Support for disruptive change
- Accountability to execute strategy
- Methodology to measure value-driven goals (e.g. carbon reductions, security, customer trust)

Source: based on a large US investor owned utility grid modernization workshop

# Realistic vision of secure future capability

### Secure Pervasive communications

- Risk-based security for communication protection
- Strategic network segmentation
- Self-healing communication network

### Secure Autonomous devices

- Devices are secure out-of-the-box
- ***Secure managed continuous automatic updates to software/firmware with in-time security validation***
- Autonomous reporting and recovery

### Secure Data management at scale

- Uniform privacy regulation
- Secure data storage and processing
- Effective anonymization / tokenization of data

### Secure Workforce innovations

- Security built into operation and maintenance manuals
- AR/VR aided security learning, incident response, and digital restoration
- OT learning for IT security personnel

### Secure Agile corporate decisions

- Accurate and rapid risk assessment methodology and tools

Source: based on a large US investor owned utility grid modernization workshop

# Approaches to achieve the future vision

### Technical

- Adoption of security standards for new technology
- Enable security monitoring out-of-the-box
- Electric sector M2M automated cybersecurity information sharing
- Effective data protection for large-scale data sets

### Financial

- Standard cybersecurity benchmarks and KPIs to promote investment
- Investment to innovate cybersecurity technology for SCADA/DER devices
- Effective risk transfer through cyber-insurance

### Regulatory

- Engage with regulators and industry groups to influence emerging cybersecurity standards
- Build cybersecurity into device certification process
- Incident response processes incorporating 3rd parties and customers

Source: based on a large US investor owned utility grid modernization workshop

# PI System, DERS and Cybersecurity

- Bryan Owen PE
- Security Architect
- bryan@osisoft.com
- @bryansowen

# Questions?

Please wait for the **microphone**

State your **name & company**

# Please remember to…

## Complete Survey!

Navigate to this session in mobile agenda for survey

TO DOWNLOAD APP, SEARCH OSISOFT

謝謝 KEA LEBOHA

DZIĘKUJĘ CI TAPADH LEIBH 고맙습니다

NGIYABONGA БАЯРЛАЛАА MISAOTRA ANAO

TEŞEKKÜR EDERIM OBRIGADO شكرا

DANKIE TERIMA KASIH GRÀCIES DANKON TANK TAPADH LEAT SALAMAT

KÖSZÖNÖM СПАСИБО MULȚUMESC

OSIsoft PI World

РАКМЕТ СІЗГЕ FAAFETAI

GO RAIBH MAITH AGAT HVALA ESKERRIK ASKO

БЛАГОДАРЯ GRACIAS

## THANK YOU

HVALA ХВАЛА ВАМ

ТИ БЛАГОДАРАМ MAHADSANID TEŞEKKÜR EDERIM

DANK JE ΕΥΧΑΡΙΣΤΩ GRATIAS TIBI ДЗЯКУЙ GRAZIE

TAK DANKE

AČIŪ SALAMAT MAHALO IĀ ʻOE TAKK SKAL DU HA DI OU MÈSI

RAHMAT MERCI GRAZZI ÞAKKA ÞÉR FALEMINDERIT ありがとうございました ĎAKUJEM

HATUR NUHUN РАХМАТ САГА SIPAS JI WERE TERIMA KASIH MATUR NUWUN

CẢM ƠN BẠN UA TSAUG RAU KOJ

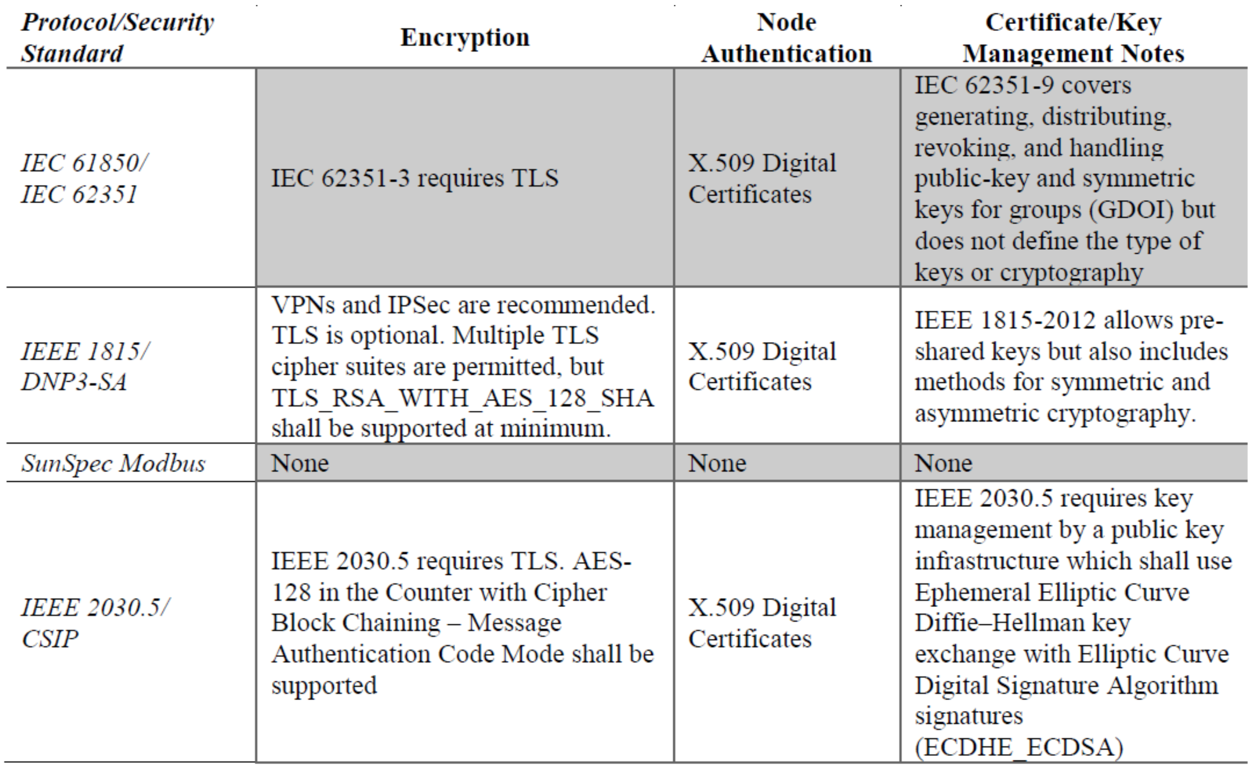
WAZVIITA ТИ БЛАГОДАРАМ СИПОС

# Bonus Slides

# Safer software: Security Development Lifecycle

- Dynamic Scanning
  - Qualys
  - SSL Labs
  - BitSight
- Fuzzing
  - Microsoft Security Risk Detection
- Static Analysis Security Tool
  - Synopsys Coverity
- Software Component Analysis
  - Synopsys Black Duck
- Penetration testing
- OSIsoft development best practices

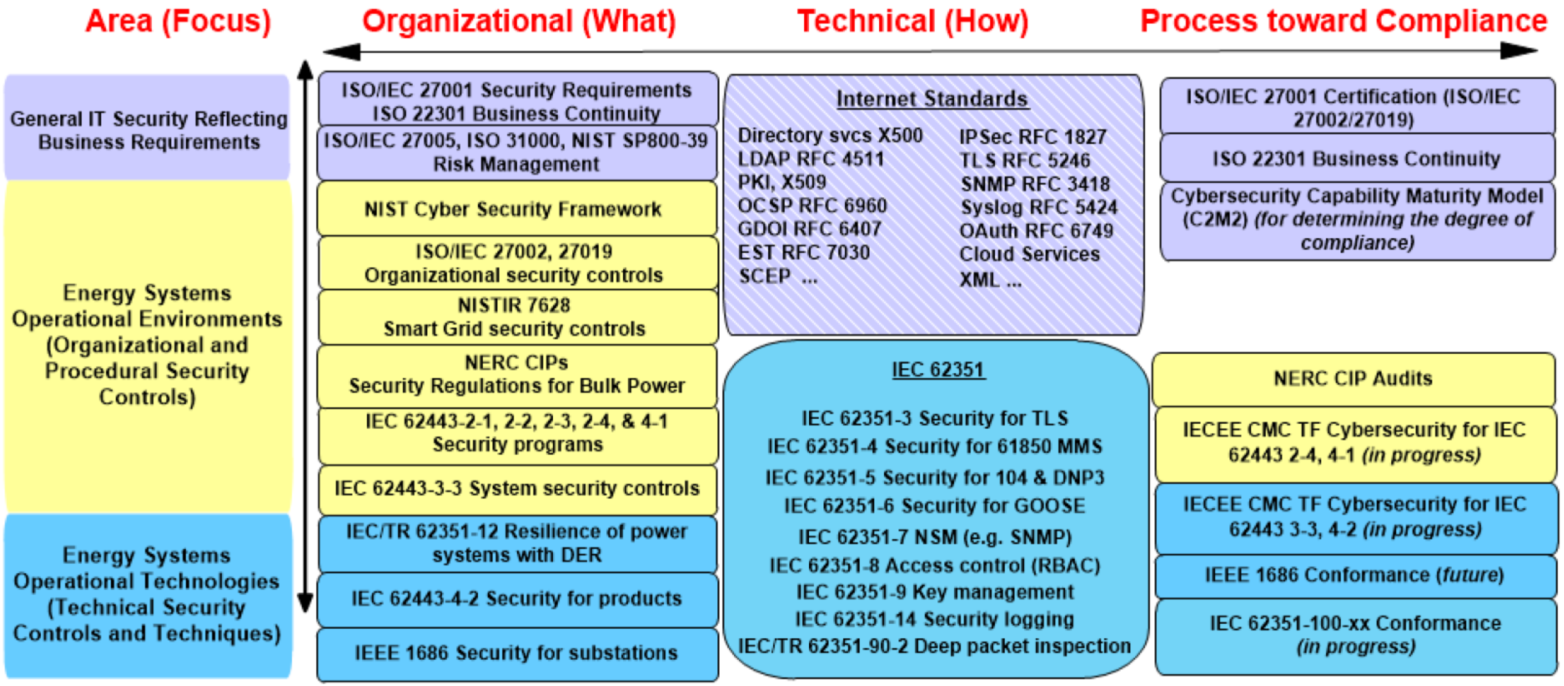
# Trust and cryptography in common DER protocols



| *Protocol/Security Standard* | **Encryption** | **Node Authentication** | **Certificate/Key Management Notes** |
|---|---|---|---|
| *IEC 61850/ IEC 62351* | IEC 62351-3 requires TLS | X.509 Digital Certificates | IEC 62351-9 covers generating, distributing, revoking, and handling public-key and symmetric keys for groups (GDOI) but does not define the type of keys or cryptography |
| *IEEE 1815/ DNP3-SA* | VPNs and IPSec are recommended. TLS is optional. Multiple TLS cipher suites are permitted, but TLS_RSA_WITH_AES_128_SHA shall be supported at minimum. | X.509 Digital Certificates | IEEE 1815-2012 allows pre-shared keys but also includes methods for symmetric and asymmetric cryptography. |
| *SunSpec Modbus* | None | None | None |
| *IEEE 2030.5/ CSIP* | IEEE 2030.5 requires TLS. AES-128 in the Counter with Cipher Block Chaining – Message Authentication Code Mode shall be supported | X.509 Digital Certificates | IEEE 2030.5 requires key management by a public key infrastructure which shall use Ephemeral Elliptic Curve Diffie–Hellman key exchange with Elliptic Curve Digital Signature Algorithm signatures (ECDHE_ECDSA) |

Source: SAND2019-1490 Recommendations for Trust and Encryption in DER Interoperability Standards

# View of key cybersecurity standards



**Area (Focus)**

- General IT Security Reflecting Business Requirements
- Energy Systems Operational Environments (Organizational and Procedural Security Controls)
- Energy Systems Operational Technologies (Technical Security Controls and Techniques)

**Organizational (What)**

- ISO/IEC 27001 Security Requirements<br>ISO 22301 Business Continuity
- ISO/IEC 27005, ISO 31000, NIST SP800-39 Risk Management
- NIST Cyber Security Framework
- ISO/IEC 27002, 27019 Organizational security controls
- NISTIR 7628 Smart Grid security controls
- NERC CIPs Security Regulations for Bulk Power
- IEC 62443-2-1, 2-2, 2-3, 2-4, & 4-1 Security programs
- IEC 62443-3-3 System security controls
- IEC/TR 62351-12 Resilience of power systems with DER
- IEC 62443-4-2 Security for products
- IEEE 1686 Security for substations

**Technical (How)**

Internet Standards

- Directory svcs X500
- LDAP RFC 4511
- PKI, X509
- OCSP RFC 6960
- GDOI RFC 6407
- EST RFC 7030
- SCEP ...
- IPSec RFC 1827
- TLS RFC 5246
- SNMP RFC 3418
- Syslog RFC 5424
- OAuth RFC 6749
- Cloud Services
- XML ...

IEC 62351

- IEC 62351-3 Security for TLS
- IEC 62351-4 Security for 61850 MMS
- IEC 62351-5 Security for 104 & DNP3
- IEC 62351-6 Security for GOOSE
- IEC 62351-7 NSM (e.g. SNMP)
- IEC 62351-8 Access control (RBAC)
- IEC 62351-9 Key management
- IEC 62351-14 Security logging
- IEC/TR 62351-90-2 Deep packet inspection

**Process toward Compliance**

- ISO/IEC 27001 Certification (ISO/IEC 27002/27019)
- ISO 22301 Business Continuity
- Cybersecurity Capability Maturity Model (C2M2) *(for determining the degree of compliance)*
- NERC CIP Audits
- IECEE CMC TF Cybersecurity for IEC 62443 2-4, 4-1 *(in progress)*
- IECEE CMC TF Cybersecurity for IEC 62443 3-3, 4-2 *(in progress)*
- IEEE 1686 Conformance (*future*)
- IEC 62351-100-xx Conformance *(in progress)*

Source: Xanthus Consulting International