Cybersecurity Technical Controls for Utility OT and SCADA

September 22, 2021

Housekeeping – Zoom

Welcome to our webinar! Here are a few notes about using Zoom:

- You will be **automatically muted** upon joining and throughout the webinar.
- Please add comments or ask questions in the **chat box.**
- You can adjust your audio through the **audio settings.**
- If you have **technical issues**, please send a message directly to Britton Marchese.
- To **mute** or **unmute** yourself (during the Q&A portion), use the microphone icon.

Erick Conde

Project Management Specialist, SEED Office

USAID

USAID FROM THE AMERICAN PEOPLE NREL Transforming ENERGY CARILEC An Association Of Electric Energy Solution Providers

The USAID-NREL Partnership

USAID and NREL partner to deliver clean, reliable, and affordable power to the developing world. The USAID-NREL Partnership addresses critical aspects of deploying advanced energy systems in developing countries through:

- Policy, planning, and deployment support
- Global technical toolkits.

www.nrel.gov/usaid-partnership

The Caribbean Energy Initiative (CEI)

Focuses on bolstering the resilience and performance of energy systems across the region, recognizing the critical role that the stable and reliable supply of energy plays in the daily economy of the region as well as during the recovery phase from the impacts of disasters.

Improved Utility performance

Accelerated Private sector investment in modern power systems

Enhanced Energy sector resilience through regional cooperation

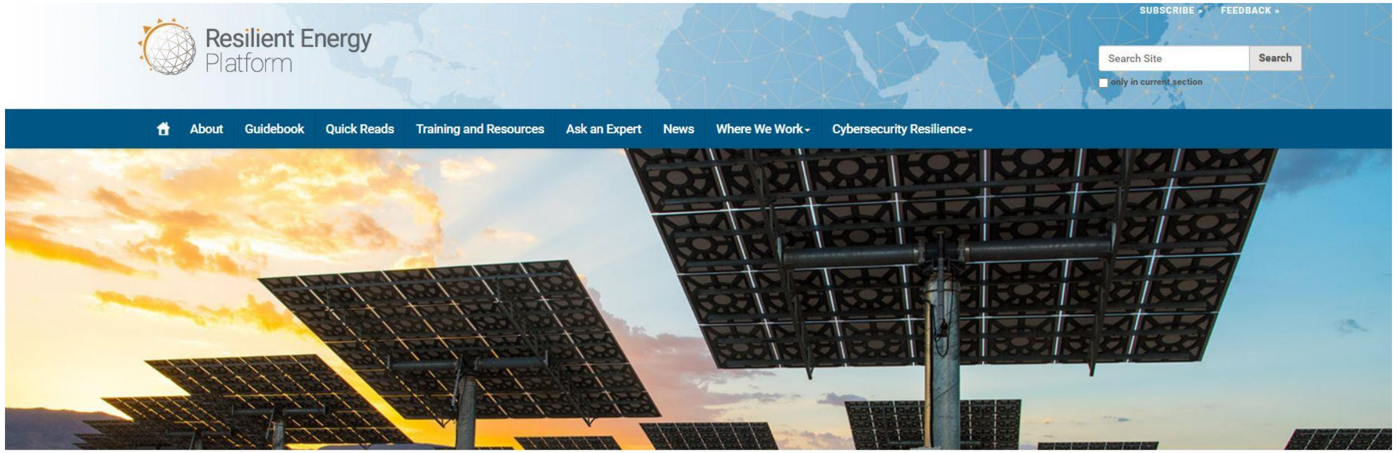
More information: https://www.usaid.gov/documents/1862/caribbean-energy-initiative

USAID FROM THE AMERICAN PEOPLE · NREL Transforming ENERGY · CARILEC An Association Of Electric Energy Solution Providers

Resilient Energy Platform

Developed through the USAID-NREL Partnership, the Resilient Energy Platform provides **expertly curated resources**, **training materials**, **tools**, and **technical assistance** to enhance power sector resilience.

The Resilient Energy Platform enables decision makers to **assess power sector vulnerabilities**, **identify resilience solutions**, and **make informed decisions** to enhance power sector resilience at all scales.



Developed through the USAID-NREL Partnership, the Resilient Energy Platform provides expertly curated resources, training materials, data, tools, and direct technical assistance in planning resilient, sustainable, and secure power systems.

https://resilient-energy.org/cyber

www.re-explorer.org

www.greeningthegrid.org

www.i-jedi.org

www.resilient-energy.org

Dr. Cletus Bertin
Executive Director
CARILEC

Regional Technical Controls Presenter

Edward Millington

- Cybersecurity Consultant and Enterprise Security Architect based in Barbados
- 20+ years' experience in Information Systems Security and ICT
- Experience in various industries – Internet Service Providers, ICT Service Providers, Telco, Banking, Government, Consulting
- Bachelor's Degree in Electronics
- Certified Information Security Manager Candidate (ISACA CISM) and Information Systems Security Professional (ISC2 CISSP)
- **Specialties:** Policy Development, IT & Security Governance, Cybersecurity Audits, Enterprise Defense & Security, Cybersecurity Incident Management, Malware & Attack Technologies, Security Operations

Member of Institute of Engineering and Technology (MIET)

Full Member of the Chartered Institute of Information Security (MCIIS)

Member of the Information System Security Association (ISSA) - International Chapter

NREL Technical Controls Presenters

Anuj Sanghvi

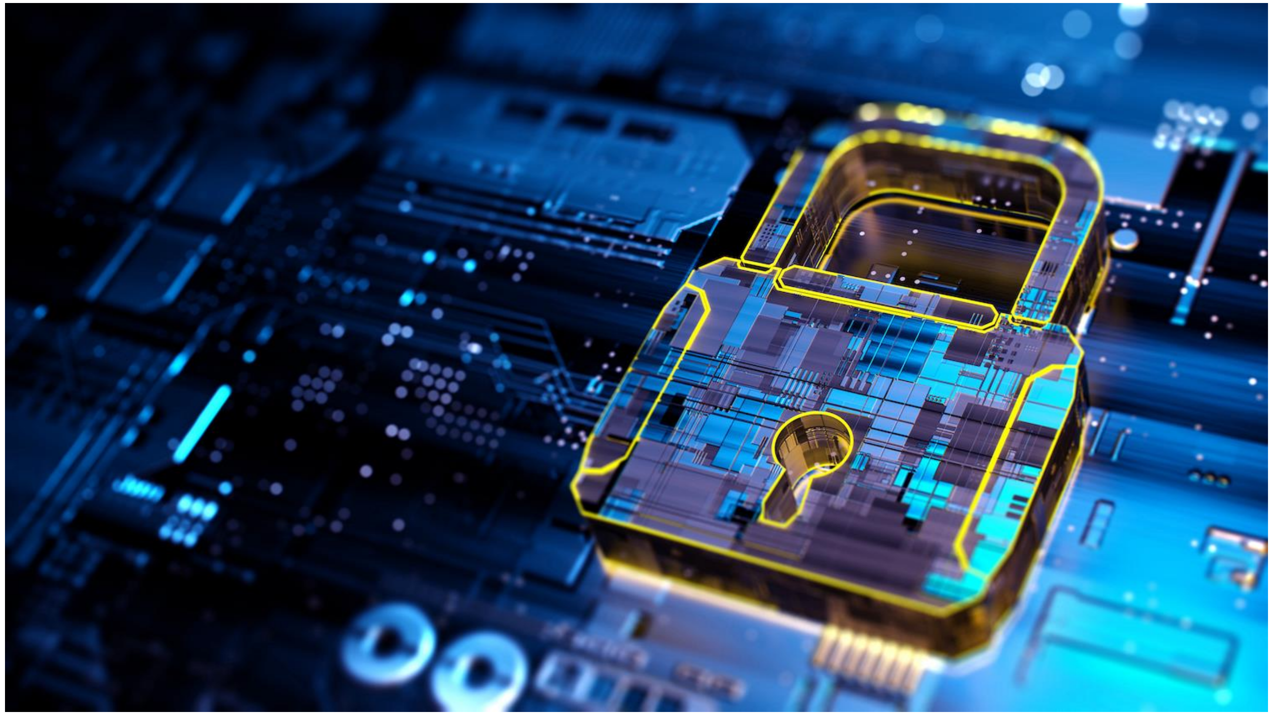
- National Renewable Energy Laboratory
- 3.5 years at NREL
- Masters in Electrical Engineering
- Technical lead — Distributed Energy Resource Cybersecurity Framework
- PI — Cybersecurity Value-at-Risk Framework
- Technical lead — Consequence Driven Cybersecurity Analysis for Extreme Fast Charging Infrastructure

Steve Granda

- National Renewable Energy Laboratory
- Computer Engineering
- 10+ years experience in systems, security, and software development
- Developer for Utility testbed for DARPA under the RADICS program
- Technical Lead — Grid Modernization Laboratory Consortium Firmware Command and Control

Agenda

- USAID-NREL Building Blocks Overview
- Risk Controls
- Cybersecurity Technical Controls
- Cybersecurity for OT and ICS
- SCADA Cybersecurity
- Resources and References
- Q&A



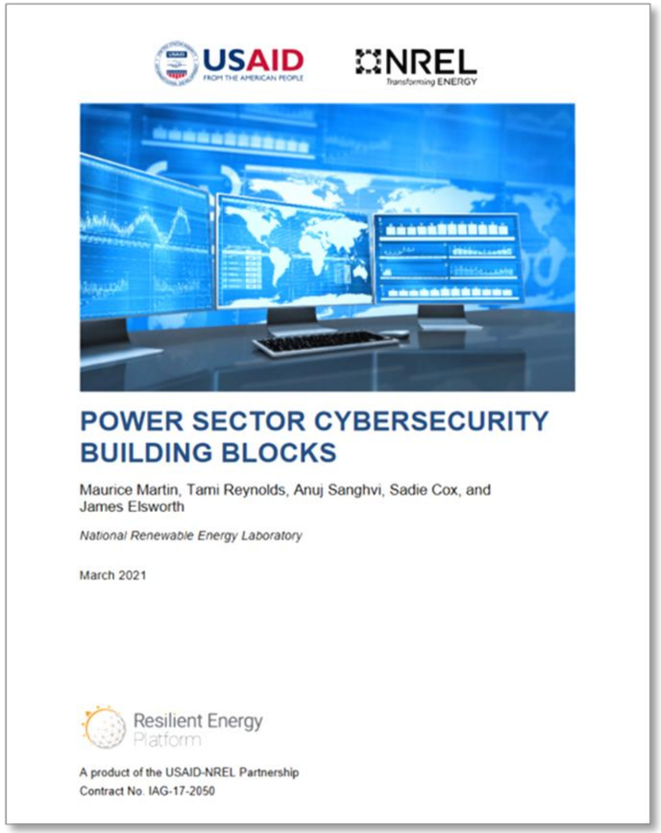
FROM ISTOCK 468171529

USAID FROM THE AMERICAN PEOPLE NREL Transforming ENERGY CARILEC An Association Of Electric Energy Solution Providers

Power Sector Cybersecurity Building Blocks

Building Blocks: Description

- Clusters of related activities that support a well-rounded cyber program
- Encourage utilities to think about different areas of cybersecurity
- Draw from established best practices
- Span multiple stakeholders
- Interconnected and mutually supporting
- Not the last word!



POWER SECTOR CYBERSECURITY BUILDING BLOCKS

Maurice Martin, Tami Reynolds, Anuj Sanghvi, Sadie Cox, and James Elsworth

National Renewable Energy Laboratory

March 2021

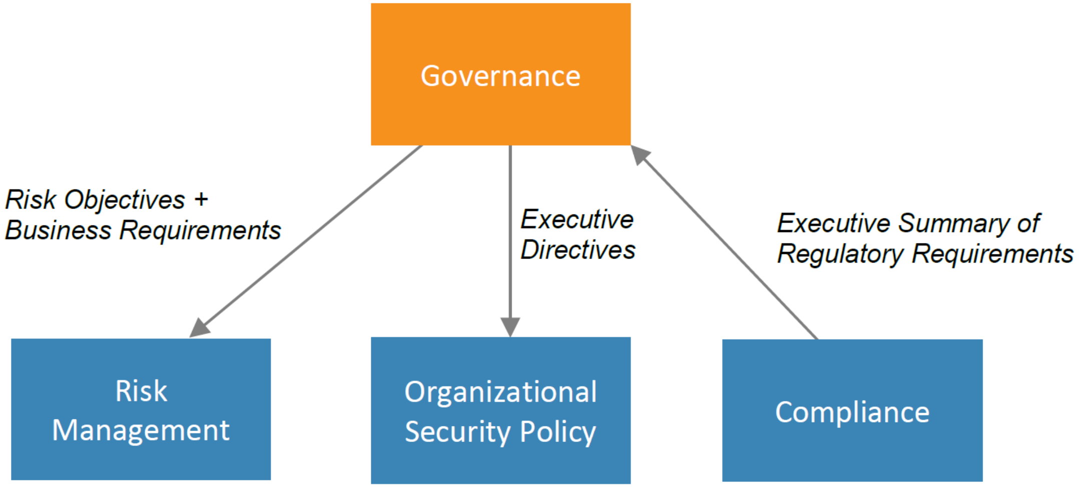
Resilient Energy Platform

A product of the USAID-NREL Partnership
Contract No. IAG-17-2050

Read the full report at:
https://resilient-energy.org/cyber

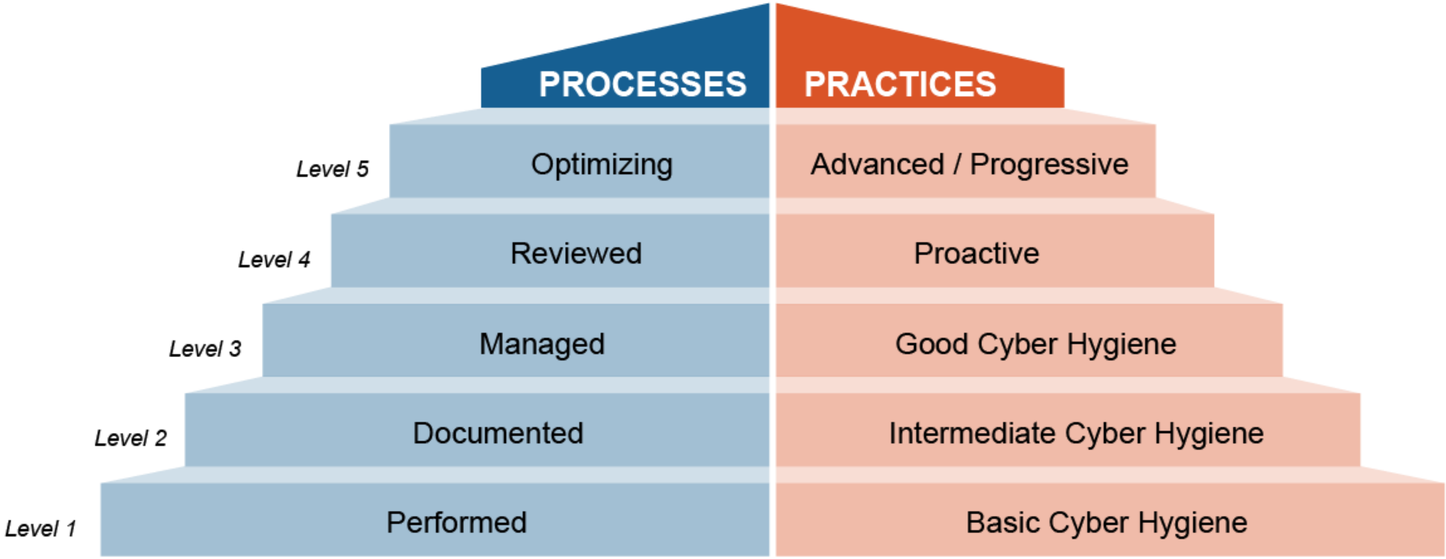
Information Security Governance Program

- Program should be risk-based.
- Drives the creation of policies which can increase Operational Maturity.
- Creates a Culture of Security.
- A matured program will provide the ability to effectively and efficiently mitigate threats.
- A well-established program will give insight to incident response.


Governance
Risk Objectives + Business Requirements
Executive Directives
Executive Summary of Regulatory Requirements
Risk Management
Organizational Security Policy
Compliance

Business Maturity and Good Governance

- Using the Cybersecurity Maturity Model Certification (CMMC) Framework will allow greater levels of Business Maturity Operations.
- CMMC Level 2+ demonstrates and defined an Information Security Governance Program in operation.
- Processes and Practices operating at CMMC Level 3 and above demonstrate risk-based operations in defending and securing critical IT/OT systems.



	PROCESSES	PRACTICES
Level 5	Optimizing	Advanced / Progressive
Level 4	Reviewed	Proactive
Level 3	Managed	Good Cyber Hygiene
Level 2	Documented	Intermediate Cyber Hygiene
Level 1	Performed	Basic Cyber Hygiene

CMMC Levels, Processes and Practices

SOURCE: https://aws.amazon.com/blogs/publicsector/how-plan-cybersecurity-maturity-model-certification-cmmc/

Risk Controls

Introduction to Controls

	Preventive	Detective	Corrective	Recovery
Physical Control	Physical Barriers	Cameras	Access Card Termination	Offsite Facility
Technical Control	Firewall, Endpoint Security, IPS, Encryption	IDS, Honeypots, Traffic Monitoring	Patching, Updates, User/Connection Termination	Backups, Recovery Systems
Administrative Control	Data/Role Classification	Access Controls & Logs	Process Termination	Disaster Recovery Planning

Cybersecurity Technical Controls

echnical Controls

ardware and software components that protect a system ainst cyberattacks”

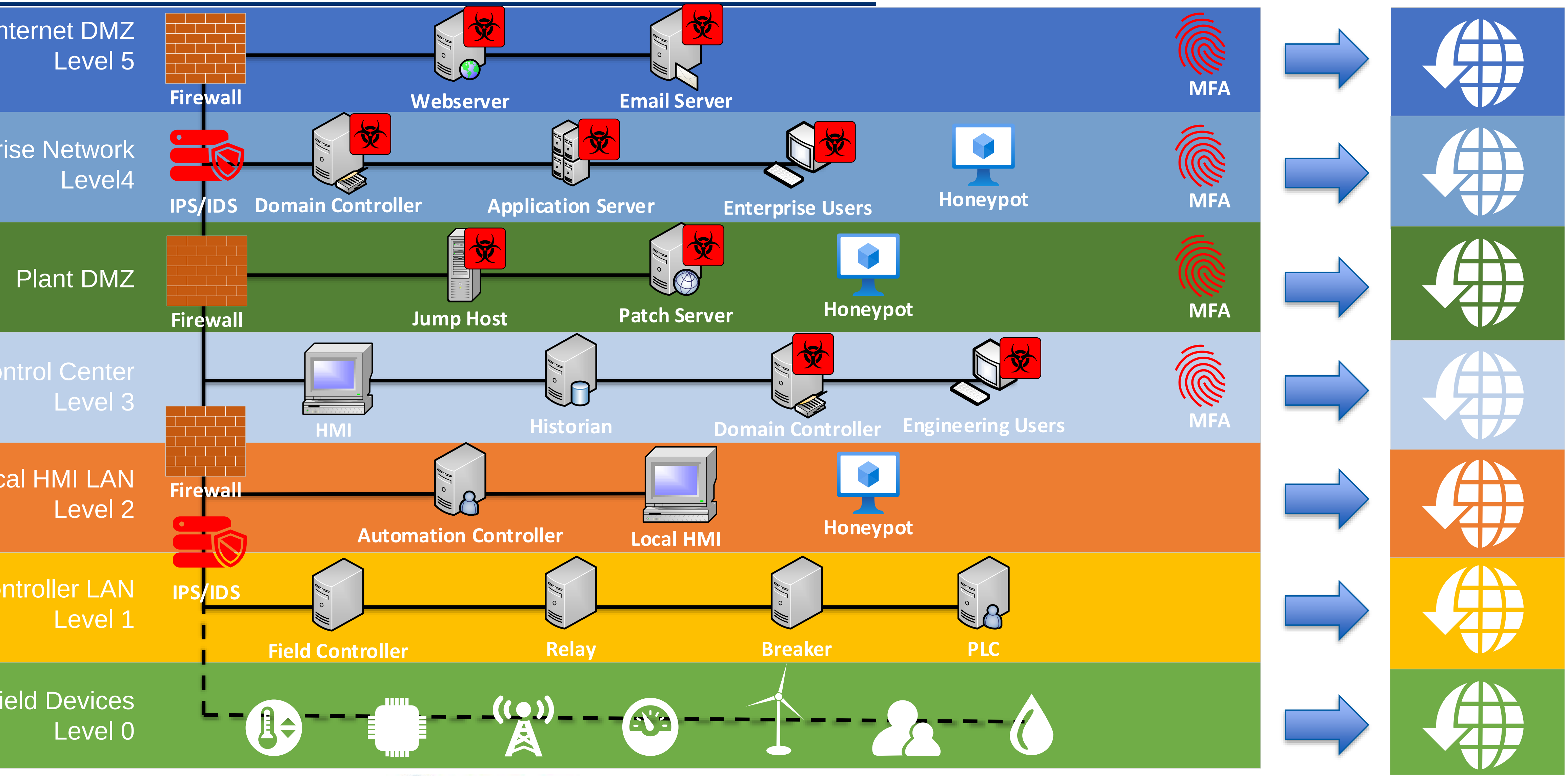
	Preventative	Detective	Corrective	Recovery
Technical Control Examples	Firewall, Endpoint Security, IPS Encryption	IDS, Honeypots, Traffic Monitoring	Patching, Updates, User/Connection Termination	Backups, Recovery Systems

dversary Examples:

- Malicious USB drop in parking lot
- Unauthorized Network/Server/Device access
- Coffee Shop Attacks
- External Vendor connecting internal network
- Email Spear/Phishing, Crypto Lockers, etc.

echnical Controls

Resilient Energy
Platform



nternet DMZ
Level 5
Firewall
Webserver
Email Server
MFA

rise Network
Level4
IPS/IDS
Domain Controller
Application Server
Enterprise Users
Honeypot
MFA

Plant DMZ
Firewall
Jump Host
Patch Server
Honeypot
MFA

ntrol Center
Level 3
HMI
Historian
Domain Controller
Engineering Users
MFA

cal HMI LAN
Level 2
Firewall
Automation Controller
Local HMI
Honeypot

ntroller LAN
Level 1
IPS/IDS
Field Controller
Relay
Breaker
PLC

ield Devices
Level 0

dditional Technical Controls

rrent Industry Defense-in-Depth implemented curity strategy:

- Firewalls
- Network Segmentation
- Auditing and Accounting
- Access Control
- Configurations and Change Management

xtGen Security Strategy: **Zero-Trust Model**

- Enhances existing security strategy through the addition of:
  - NextGen Firewalls
  - Security Zones
  - Identity and Access Management
  - Encryption of Data and Communications
  - Threat Hunting & Detection Tools
  - Threat Intelligence

SOURCE: https://colortokens.com/blog/business-drivers-for-zero-trust-security/

Cybersecurity for Operational Technology (OT) and Industrial Control Systems (ICS)

hat is Operational Technology?

erational Technology: focuses on hardware software that is used to monitor, change, or ntrol physical devices, events, and processes hin a system.

ormation Technology: focuses on hardware software related to enterprise or business end an organization and occasionally industrial.

ese systems operate together but can fer with regards to policy, operation, d protection.

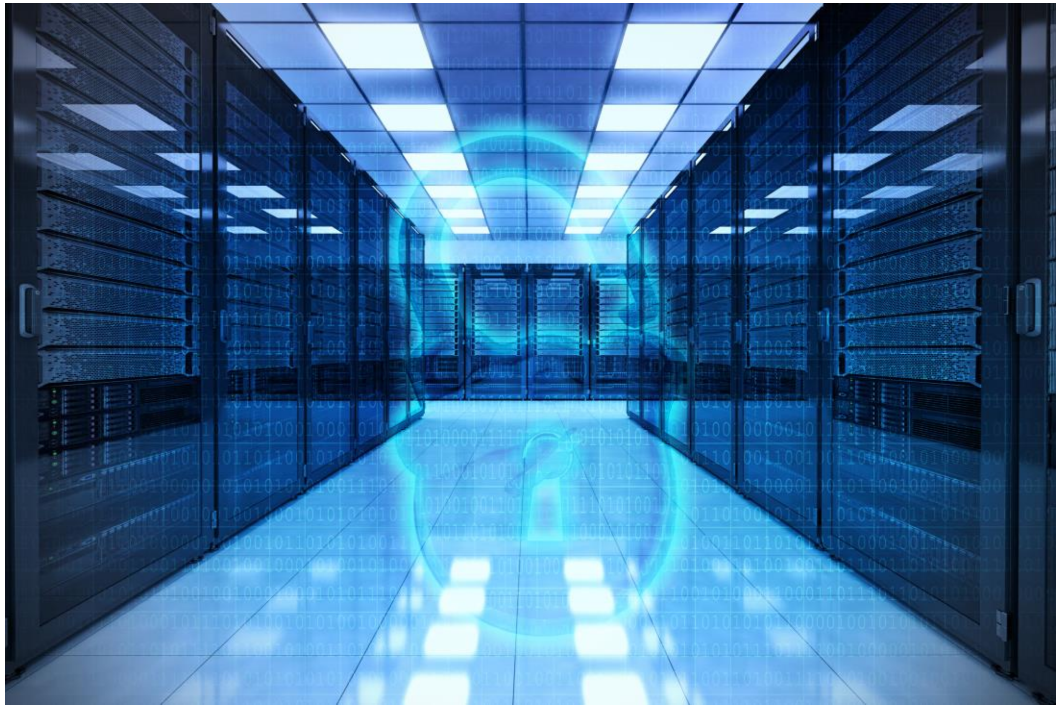


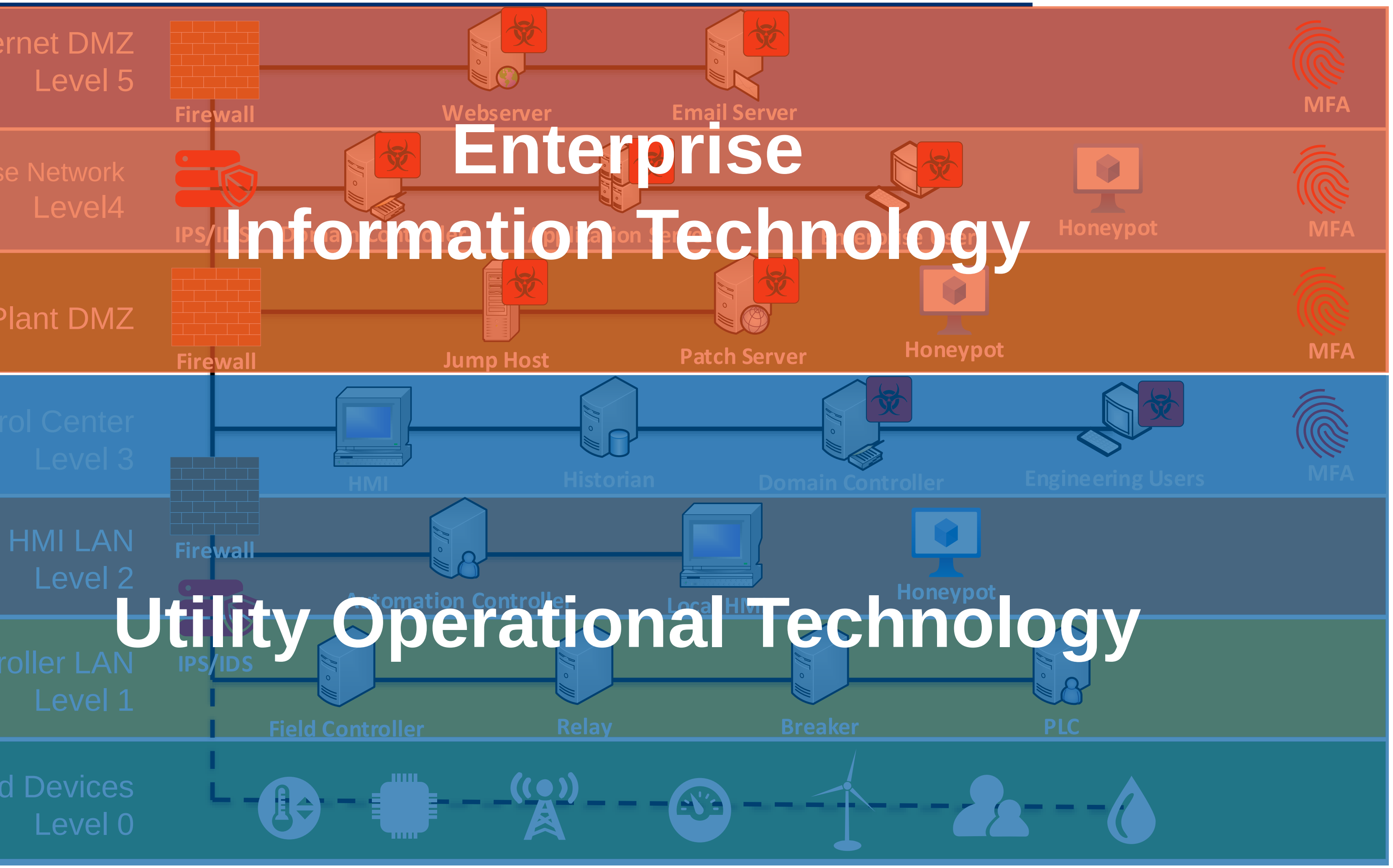
PHOTO FROM ISTOCK | 1312283188

What is the difference between an ICS device running Linux versus an Application Server running Linux?

ecurity Tradeoffs with IT and OT

ormation Technology	Operational Technology
adily Swapped/Replaced/Virtualized	Long Equipment Life Cycles
dated Frequently	Patching relies on overall System Stability (Grid)
neduled Downtime/Service Windows	Cannot bring down critical paths for Critical Infrastructure (i.e., hospitals)
k with Legacy Software, Protocols, Connections n be mitigated easily with smaller life cycles	Legacy Protocols, Connections, Software oftentimes cannot be changed due to infrastructure costs
oduction and Dev environments	Upgrades cannot easily be performed or tested
set Management, Monitoring, and Enumeration tomated	Asset Management, Monitoring, Enumeration is oftentimes Manual
ange Management Support	Configuration Management often proprietary format

-OT Convergence



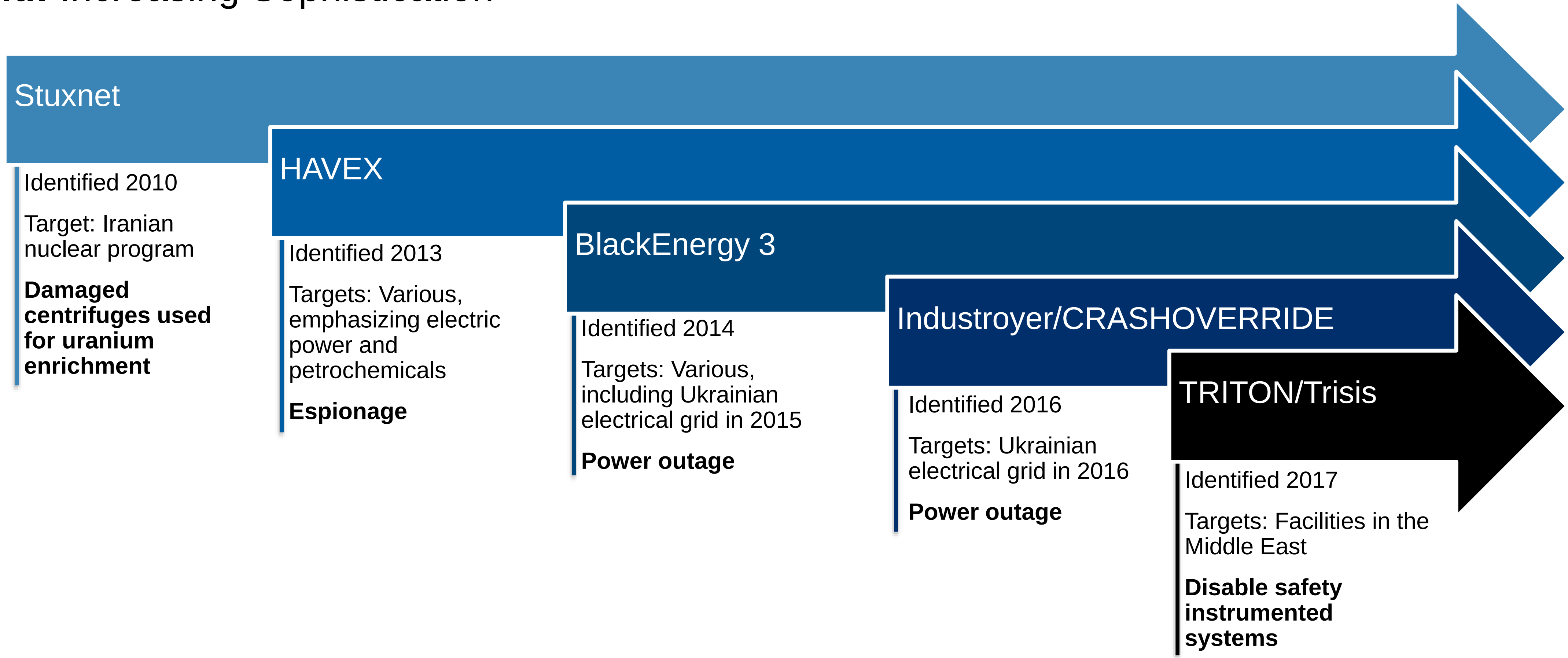
IT/OT can share:

- Processes
- Boundaries
- Assets
- Users
- Networks
- Data

…Especially Attacks!

perational Technology Cyber Attacks

end: Increasing Sophistication



Stuxnet

Identified 2010

Target: Iranian nuclear program

Damaged centrifuges used for uranium enrichment

HAVEX

Identified 2013

Targets: Various, emphasizing electric power and petrochemicals

Espionage

BlackEnergy 3

Identified 2014

Targets: Various, including Ukrainian electrical grid in 2015

Power outage

Industroyer/CRASHOVERRIDE

Identified 2016

Targets: Ukrainian electrical grid in 2016

Power outage

TRITON/Trisis

Identified 2017

Targets: Facilities in the Middle East

Disable safety instrumented systems

d R. E. Fisher, “History of Industrial Control System Cyber Incidents,” INL/CON--18-44411-Rev002, 1505628, Dec. 2018. doi: 10.2172/1505628.
of Cyber Attacks on Electric Operations,” Jul. 30, 2019. https://www.dragos.com/blog/industry-news/the-evolution-of-cyber-attacks-on-electric-operations/ (accessed Aug. 24, 2021).
: Analysis of Safety System Targeted Malware,” Dragos Inc., 2017. Accessed: Aug. 24, 2021. [Online]. Available: https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf

T Cybersecurity Objectives

- IIST SP-800-82:
  - Restricting logical access to ICS network
  - Restricting physical access to ICS network and devices
  - Protecting individual ICS components from exploitation
  - Restricting unauthorized modification of data
  - Detecting cybersecurity events and incidents
  - Maintaining functionality during adverse conditions
  - Restoring the system after an incident
- le of security-by-design
  - Avoid problems by addressing concerns earlier in the design process.

s://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

PHOTO FROM ISTOCK | 1199783806

Supervisory Control and Data Acquisition (SCADA) Cybersecurity

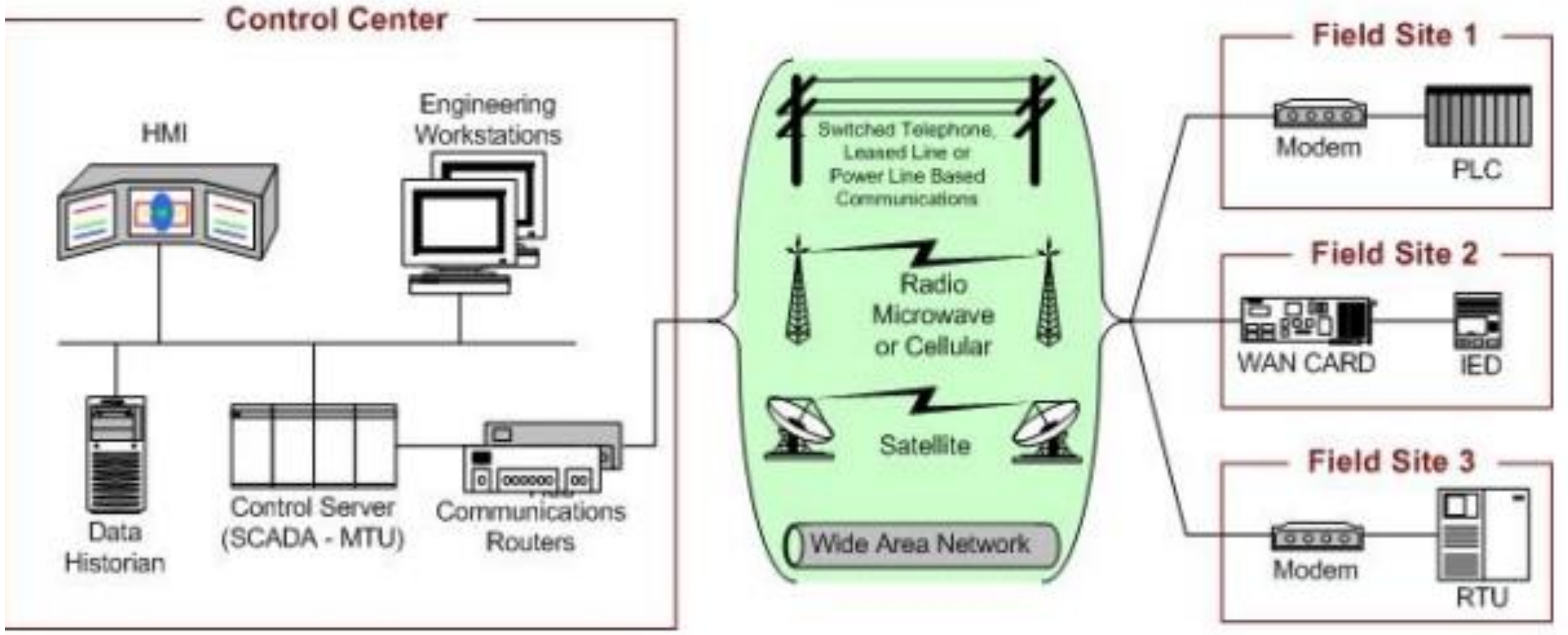


Illustration from NIST SP 800-82

CADA System General Layout

CADA Properties

Resilient Energy Platform

- Access control for monitoring/control end points for both new and legacy equipment
- Tailored implementation of communication and network security
- SCADA networks pushing outward and closer to grid edge
- SCADA systems control physical devices and processes — this leads to special requirements
- Cyber incident response can lead to unintended consequences in the physical systems being controlled
  - Ex. Disconnecting a malware-affected generation station leads to cascading outage
- Independent Patch Management Strategy

PHOTO FROM ISTOCK | 1289956604

ADA Security st Practices

nproving ICS Cybersecurity fense-in-Depth es (Department of nd Security, Sep 2016)

- Isolate the SCADA network as much as possible
- Remove unnecessary devices and services from the SCADA network
- Access and Authentication Controls
- Deploy IDS
- Have “red teams” identify possible SCADA attack scenarios
- Review the physical security of remote sites connected to the SCADA network
- Conduct periodic cybersecurity assessments

commendations

se-in-Depth
oach

Strategy

- Firewalls
- Demilitarized Zones
- Security Policies
- Training Programs
- Incident Response Mechanisms
- Physical Security

Possible Attack Vectors

- Backdoors and hole in network perimeter
- Vulnerabilities in common protocols
- Attacks on field devices
- Database attacks
- Communication hijacking and ’man-in-middle’ attacks
- Spoofing attacks
- Attacks on privileged and/or shared accounts

esources

The USAID-NREL Partnership can help as your organization implements technical controls for OT and SCADA:

- Visit our website at: https://resilient-energy.org/cybersecurity-resilience.
- Read the guidance document: Power Sector Cybersecurity Building Blocks: https://www.nrel.gov/docs/fy21osti/79396.pdf.
- Reach out for (free!) direct technical assistance through the Ask an Expert form.

Free NIST training: ttps://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content.

NIST SP-800-82: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

CIS Controls ICS Companion Guide: ttps://www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-industrial-control-systems/.

e USAID-NREL partnership can help with planning and/or execution of technical controls.

eferences and Resources, cont.

Resilient Energy Platform

History of Industrial Control System Cyber Incidents (INL and DOE, 2018)
nttps://www.osti.gov/servlets/purl/1505628.

SA/IEC 62443 Series of Standards:
nttps://gca.isa.org/blog/download-the-new-guide-to-the-isa/iec-62443-cybersecurity-standards.

Recommended Practices: Improving ICS Cybersecurity with Defense-in-Depth Strategies (DHS, 2016)
nttps://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

SCADA systems: Vulnerability assessment and security recommendations
nttps://www.sciencedirect.com/science/article/pii/S0167404819302068.

A Comprehensive Guide to Operational Technology (OT) Cybersecurity (Mission Secure, 2021)
nttps://www.missionsecure.com/ot-cybersecurity.

ne USAID-NREL partnership can help with planning and/or execution of technical controls.

Q&A

Please type questions into the Q&A on Zoom. Thanks!

Closing Thoughts

ow else can USAID & NREL help?

Presentations for utility:

- Board of directors
- Executives
- Technical staff
- Non-technical staff
- Regulators

New documents

New tools for

- Expanded assessments
- Cybersecurity investment ROI
- Other topics?

One-on-one technical assistance

https://resilient-energy.org/cyber

ow else can USAID & NREL help?

Resilient Energy Platform

Read the guidance document: *Power Sector Cybersecurity Building Blocks* report available at: https://resilient-energy.org/cyber

Access additional resources and information by visiting the Cybersecurity Resilience page on the Resilient Energy Platform website

Contact Us:

- Tami.Reynolds@nrel.gov
- Maurice.Martin@nrel.gov
- Anuj.Sanghvi@nrel.gov
- Steve.Granda@nrel.gov

ow else can USAID & NREL help?

coming Webinars in this Series:

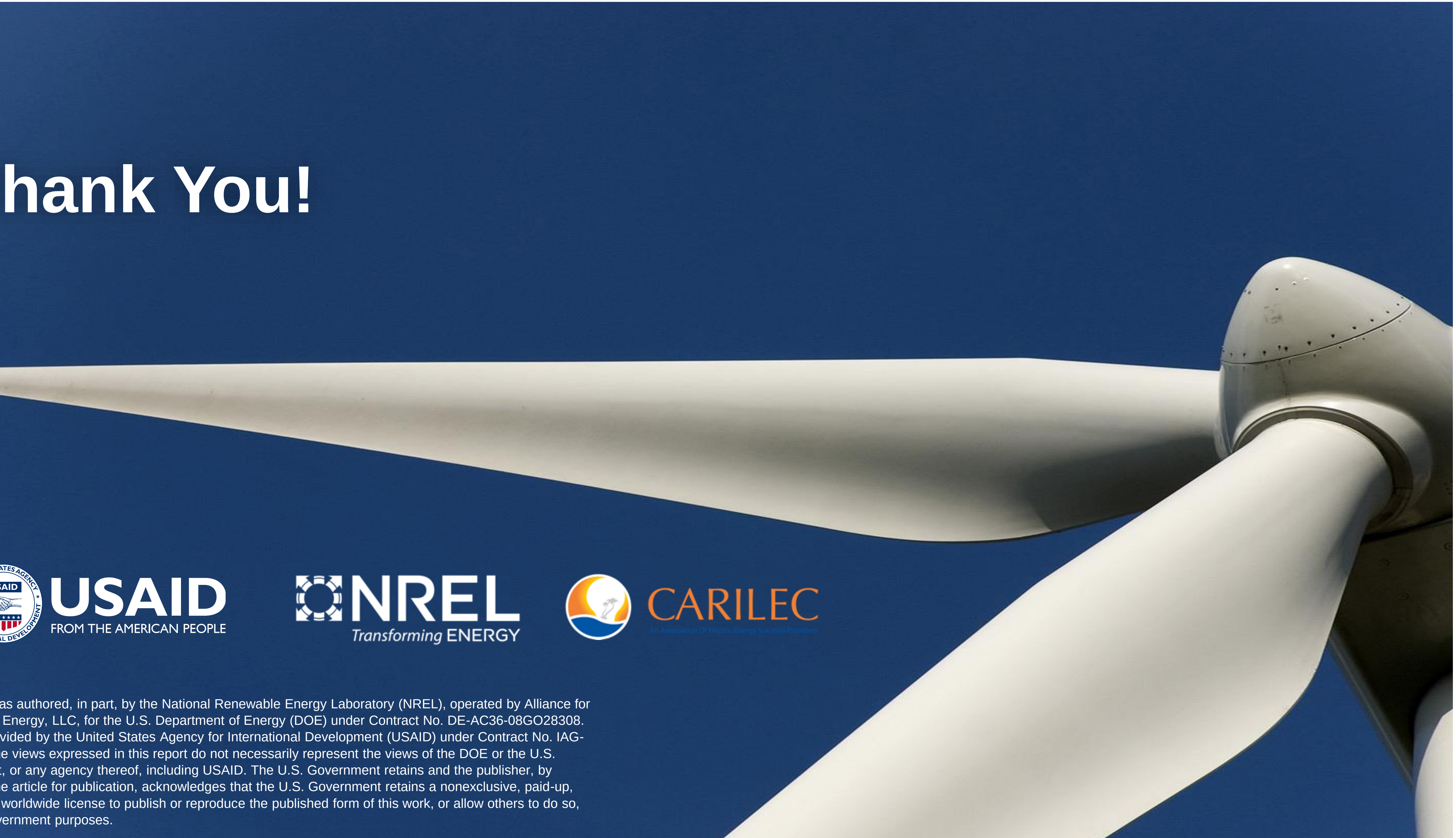
November 17, 2021: Regulatory Compliance

January 19, 2022: Risk Management

February 16, 2022: IT Network Security

To learn about additional webinars and resources, sign up for the quarterly **USAID-NREL Partnership Newsletter**!

Caribbean Cybersecurity Forum – March 2022



hank You!

as authored, in part, by the National Renewable Energy Laboratory (NREL), operated by Alliance for
Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308.
vided by the United States Agency for International Development (USAID) under Contract No. IAG-
e views expressed in this report do not necessarily represent the views of the DOE or the U.S.
, or any agency thereof, including USAID. The U.S. Government retains and the publisher, by
e article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up,
worldwide license to publish or reproduce the published form of this work, or allow others to do so,
vernment purposes.