

PART 3C: Cyber Security

Session Contents

- Cyber Security Considerations for Power Utilities
- Key Lessons and Recommendations

Speaker:

Barry MacColl

Senior Regional
Manager

Electric Power Research
Institute (EPRI)

Everything is a Computer - And a Connected Device

- New equipment often comes with their own modems and connections to wide area networks that are out of the control of utilities

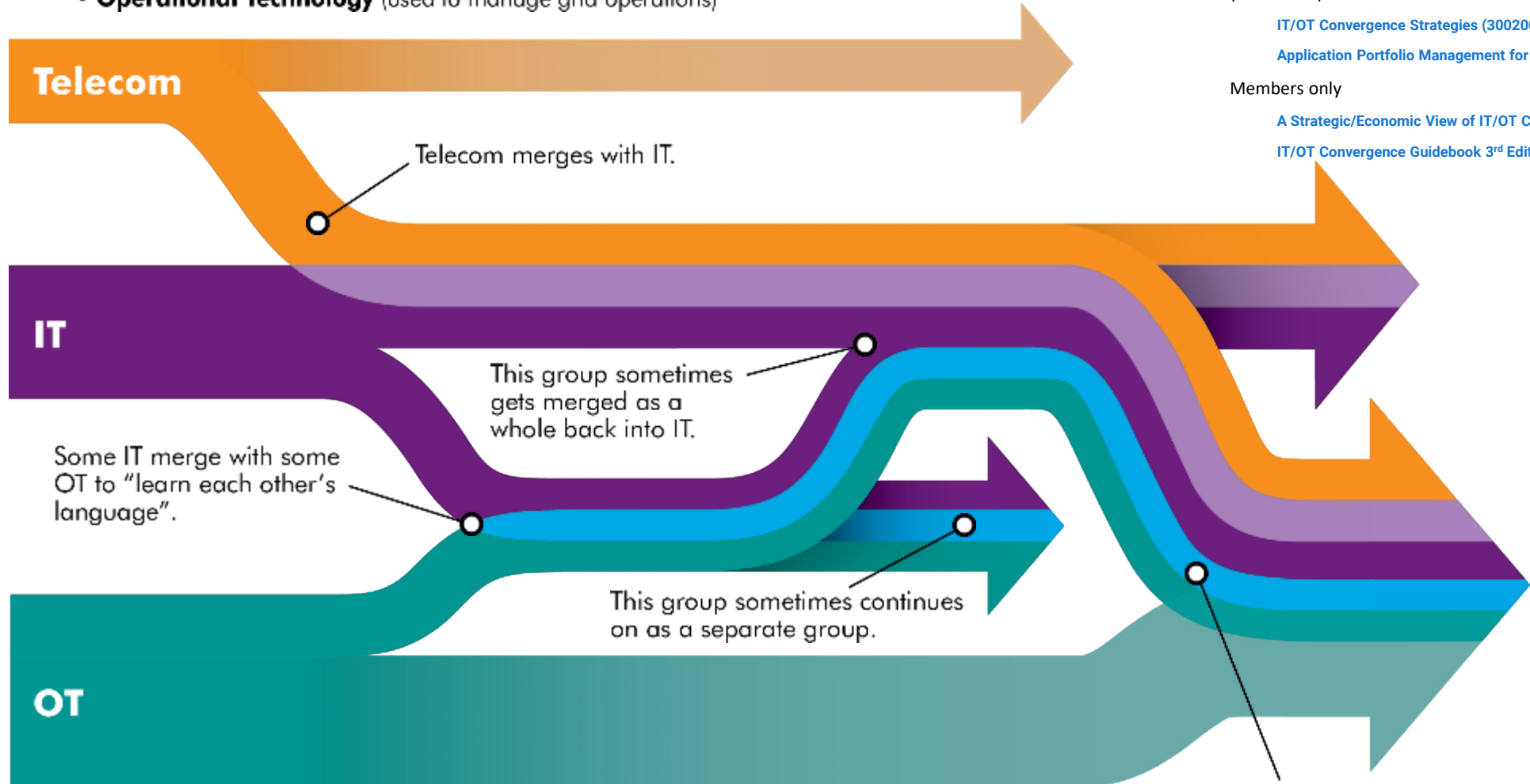


Workshop On Utility Digitalization And Performance Improvement In Africa - 12-14 February 2024 - Cape Town, South Africa

UTILITY CONVERGENCE PATHS

A utility usually has three technology related functions:

- **Telecom** (manages the wired/wireless networks)
- **Information Technology** (back-office, enterprise, and data center capabilities)
- **Operational Technology** (used to manage grid operations)

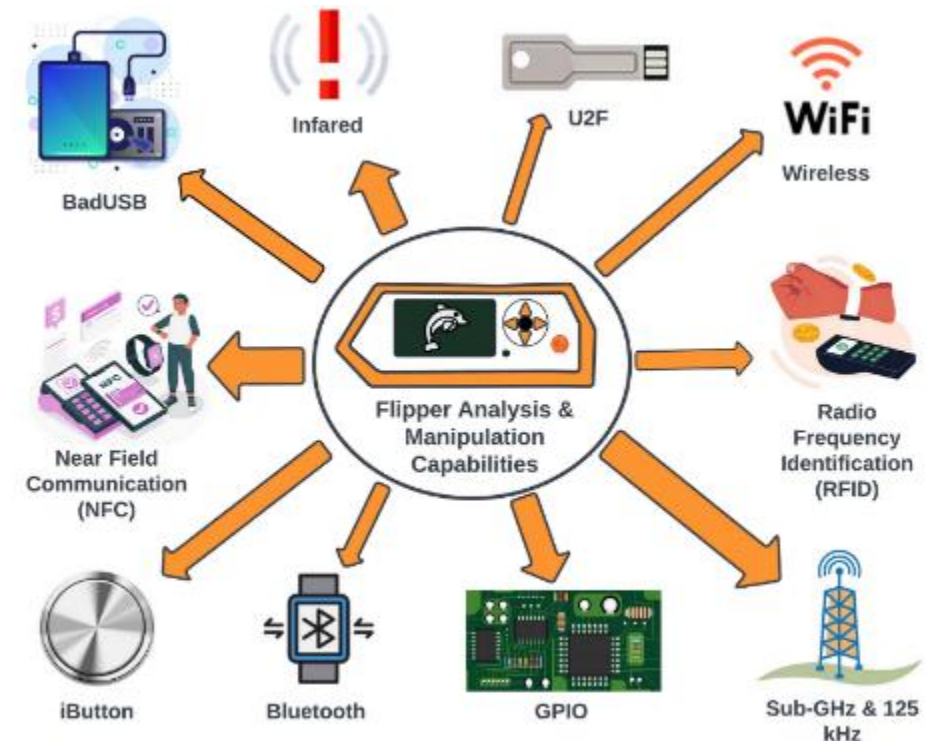


- Public
 - Toward a Utility Digital Transformation Maturity Model (3002017677)
 - EPRI Business Capability Model for IT-OT Alignment (<https://smartgrid.epri.com/htmlreport/>)
- (soon to be) Public
 - IT/OT Convergence Strategies (3002005249)
 - Application Portfolio Management for Aligning IT-OT (3002007877)
- Members only
 - A Strategic/Economic View of IT/OT Convergence (3002009979)
 - IT/OT Convergence Guidebook 3rd Edition (3002018638)

Sometimes IT and OT are merged in the end.

New Tools – New Threats, or at least new claims

- Tools like FlipperZero have created a world of new wireless attacks against everything from keycard systems, to cars, to smart meters, to cell phones.

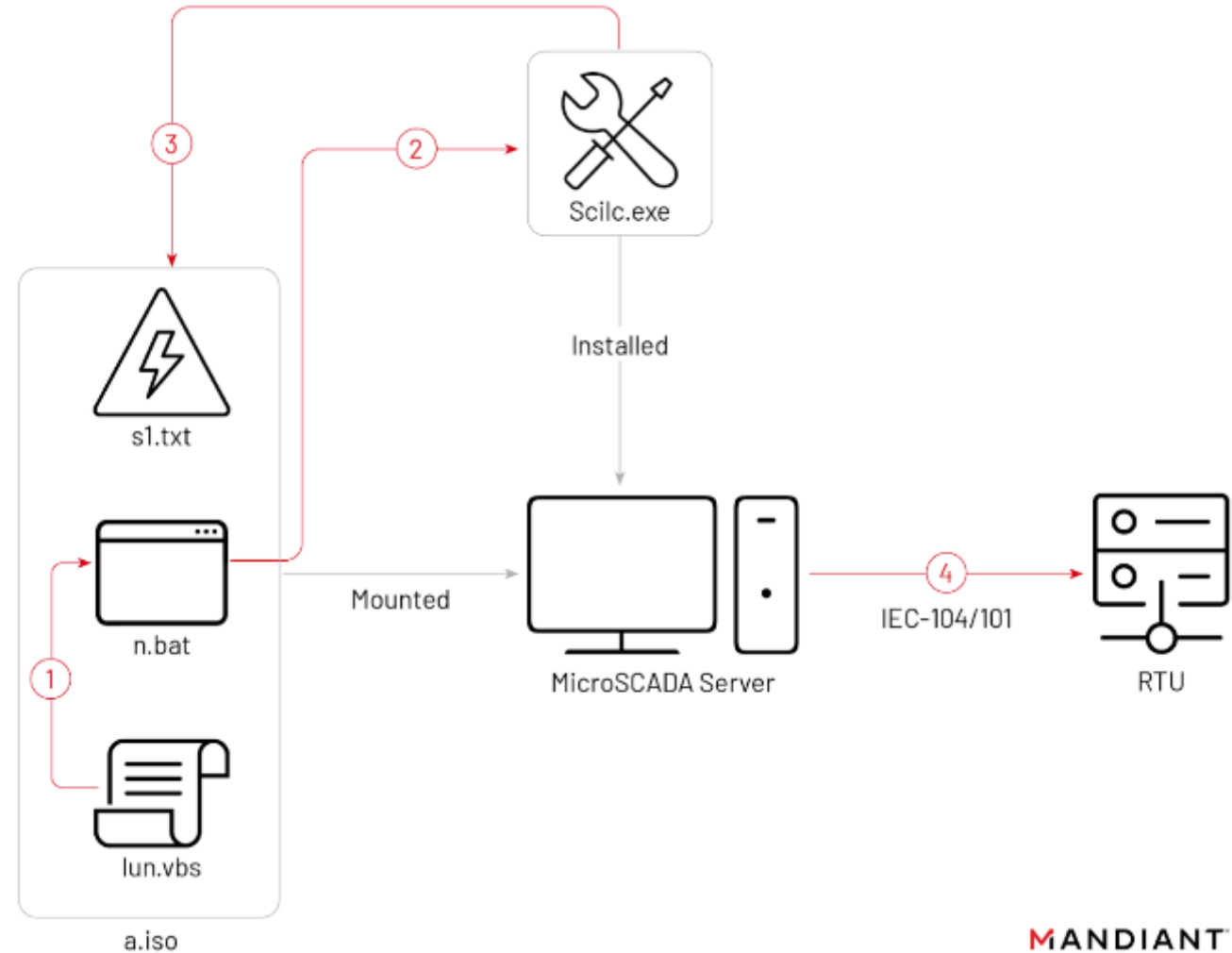


Recent Examples of State Level Cyber Attacks

- **April 2022.** Hackers targeted a Ukrainian energy facility, but CERT-UA and private sector assistance largely thwarted attempts to shutdown **electrical substations** in Ukraine.
- **April 2022.** Cybersecurity researchers observed hackers penetrating the networks of at least 7 Indian State Load Dispatch Centres (SLDCs) which oversee operations for **electrical grid control**
- **July 2022.** Hackers targeted Lithuania's **state-owned energy provider** in a DDoS attack.
- **August 2022.** A hacker group claimed responsibility for breaching a privately owned **UK water supply company** South Staffordshire Water and leaking files in an extortion attempt.
- **August 2022.** Hackers targeted Greece's largest **natural gas distributor** DESFA causing a system outage and data exposure.
- **August 2022.** Hackers breached Italy's **energy agency**, Gestore dei Servizi Energetici (GSE), compromising servers, blocking access to systems, and suspending access to the GSE website for a week.
- **March 2023:** (3/24) A hacking group targeted firms in China's **nuclear energy industry** in an espionage campaign.
- **December 2023:** Hackers hit Ukraine's largest **mobile phone provider**, Kyivstar, disabling access to its 24 million customers in Ukraine.
- **December 2023:** Hackers disrupted approximately 70% of **gas stations** in Iran.

Cyber Attacks on Ukraine Power Companies

- Based on evidence of lateral movement, the attacker potentially had access to the SCADA system for up to three months.
- On October 10 2022, the hacker **leveraged an optical disc (ISO) image** named “a.iso” to execute a native MicroSCADA binary in a likely attempt to execute malicious control commands to switch off substations.
- Unlike a physical optical disc, an image can be transferred over any data link or removable storage medium.
- An ISO image can be opened with almost every multi-format file archiver. The attack resulted in a power outage.



MANDIANT

Volt Typhoon

- Initial Access Techniques
 - **Entry Point: Internet-facing Fortinet FortiGuard devices** compromised for initial access.
 - Credential Harvesting: Extraction of Active Directory credentials from these devices for further network access
- Post-Compromise Activity
 - Command Line Usage: Direct hands-on-keyboard activity to explore and manipulate systems.
 - Credential Access: Dumping credentials through various Windows processes like LSASS and leveraging tools like Ntdsutil.exe.
 - Data Collection: Dumping information from local web browser applications and staging data in password-protected archives



Similar Cyber Attacks in Denmark

- Extensive cyber attack against Danish critical infrastructure in May 2023.
- 22 companies operating parts of the Danish energy infrastructure compromised.
- Attackers gained access to industrial control systems
 - Island mode operation initiated in several companies to prevent the attackers ability to launch an attack.



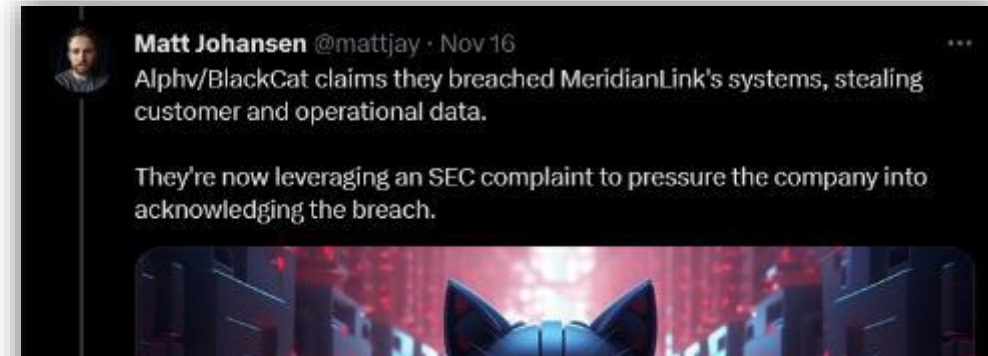
Mechanism of the Cyber Attack



- Initial Attack Phase:
 - On May 11, a coordinated attack against 16 carefully selected Danish energy companies was initiated.
 - Attackers targeted **a known vulnerability in Zyxel firewalls** used by the companies.
 - The attackers precisely knew which companies had the vulnerable firewalls, hitting every target without miss
- Vulnerability Exploitation:
 - Attackers exploited the vulnerability by sending a specially crafted data packet to port 500 on the vulnerable Zyxel devices.
 - Successful exploitation allowed attackers to execute commands with root privileges on the device without authentication
 - Actions: In most cases, the firewall remained operational for legitimate use, making it difficult to detect unauthorized access.
 - The attack was stealthy, intending to 'fly under the radar' and avoid detection

Ransomware Innovates Faster Than Us

- Ransomware payments were down 40% in 2022. But have dramatically rebounded in 2023, with current trends 154% of last years levels.



Henry Schein Inc - Henry's "LOST SHINE"

12/5/2023, 2:17:36 PM

Many of you recognize the name Henry Schein from recent weeks' posts and media outlets.

As you know, Henry was restored and back in operation after one month of silence, until now.

Aon's partner Stroz Friedberg and AVASEK teams thought they were doing a good job for HENRY, but they were just preparing for Henry's next catastrophe.

WE HAVE RE-ENCRYPTED HENRY SCHEIN TWICE AND THIRD COMING SOON.

We're proud to present the next level of attack.



594 43K


Defense is all about Cyber Security Governance


NIST Cybersecurity Framework 2.0 *draft*


- New core function – **Cyber security governance**
 - Risk Management Strategy
 - Supply Chain Management
 - Roles Responsibilities and Authorities
 - Global Partnerships
 - Policies, Processes, Procedures
- Inserts cybersecurity into enterprise risk management strategies




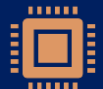
CIA Model of Security + Authentication

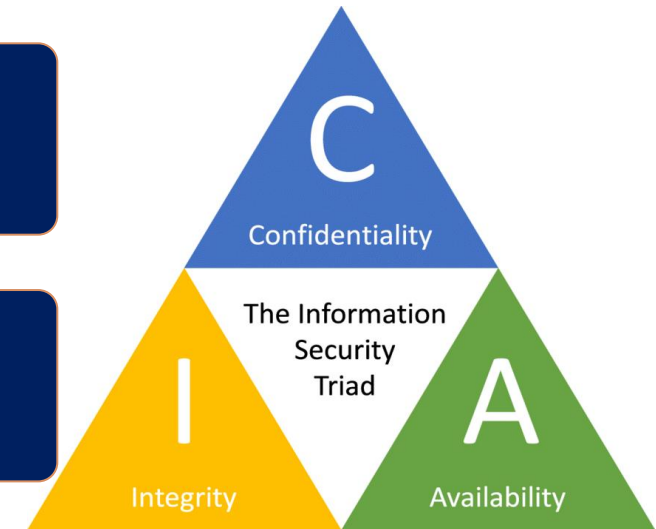
 The CIA (Confidentiality, Integrity, Availability) triad is a fundamental model in cyber security that guides policies for information security.

 *Confidentiality* ensures that data is restricted to only those who are authorized to access it. It involves measures such as encryption, access control, and data classification to prevent unauthorized access.

 *Integrity* refers to the completeness and accuracy of data, as well as the inability for it to be illegitimately altered. Measures such as hash functions and digital signatures are used to ensure data integrity.

 *Availability* ensures that authorized users have access to data whenever they need it. This involves maintaining hardware and technical infrastructure, implementing redundancy, and disaster recovery planning to minimize downtime.

 The CIA triad is a foundational model that helps organizations prioritize and implement security measures to protect their information and systems. It also directly interlinks with the concepts of authentication and authorization, which are essential components of a comprehensive cyber security strategy.



Vulnerability Assessment and Penetration Testing (VAPT)

Vulnerability Assessment

- Scans digital assets to identify pre-existing security vulnerabilities
- Provides a prioritized list of vulnerabilities
- Enables organizations to future-proof endpoints and strengthen security strategies
- Can help meet compliance with standards such as ISO 27001 and PCI DSS

Penetration Testing (aka Pen Testing)

- Determines the potential impact of a real attack
- Uses a combination of machine and human-led techniques
- Performs hacker-style evaluations and simulations
- Works to identify and address security weaknesses
- Can help meet compliance with various security benchmarks
- May be performed by internal staff or by an external (third-party) pen testing services company

Mitigation and Protection Guidance

- Exposure of Services
 - Verify only required services are exposed to the internet
- Update
 - Update edge devices as quickly as possible
- Contingency Plan
 - If a compromise happen, have a plan for possibility disconnecting equipment from the internet / network.
- Log Collection
 - Collect and analyze logs
- Map Network Inputs
 - Several members did not know that networks were attacked.
- Segmentation
 - Segment networks to reduce the ability for attackers to pivot to other areas of the network.
- Identify Devices
 - Members were not aware of vulnerable devices in some cases because they were installed and operated by third parties.
- Supplier Management
 - Some compromises happened because of confusion over who was responsible for patching.
- Emergency Preparedness
 - One member ran in island operation for 6 days. Making sure utilities have the ability to operate in degraded modes for extended periods is important.
- Vulnerability Scans
 - Vulnerability scans can be useful to identifying newly vulnerable devices when vulnerabilities are disclosed.

<https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/>

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a>

<https://www.wired.com/story/china-volt-typhoon-hack-us-critical-infrastructure/>

<https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf>

Information Sharing and Analysis Centers (ISACs)

What an ISAC is



- Sector-specific nonprofit organizations that serve as central resources for gathering, analyzing, and disseminating actionable threat information to their members
- Trusted entities established by critical infrastructure owners and operators to foster information sharing and good practices about physical and cyber threats and mitigation

What an ISAC does



- Collect, analyze, and share threat information to protect critical infrastructure, personnel, and customers from cyber and physical security threats
- Provide members with tools to mitigate risks and enhance resiliency
- Collaborate to maintain situational awareness across various critical infrastructure sectors
- Provide risk mitigation, incident response, technical exchanges, workshops, and webinars
- Promote cyber security by sharing threat information and collaborating on effective security measures

E-ISAC works with energy companies



- Offers membership to North American electricity and natural gas industry asset owners and operators
- Encourages physical and cyber security professionals at these organizations to benefit from their services
- Australia, Canada, Europe, India, Japan, Singapore, US

Use Intrusion Detection Systems (not limited to)



Capabilities

- Alert Methodology
- Rule Customization
- Asset Management

Implementation Considerations

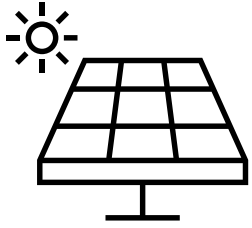
- Placement / Location
- Data Collection Methods
- Resource / Bandwidth Requirements
- SIEM Integrations and Data Forwarding

Performance Management

- Tuning
- Data Forwarding

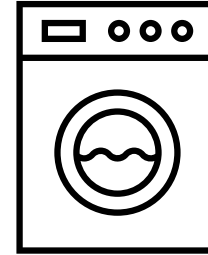
Cyber Risk in Distributed Energy Resources (DER)

DER Technologies



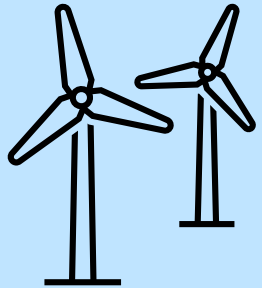
Solar

Photovoltaic (PV) technologies produce intermittent energy through the absorption of sunlight.



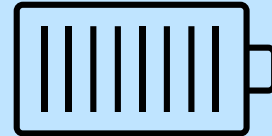
Controllable Loads

Customer devices that can be managed and adjusted to vary its power consumption based on utility demand response requests.



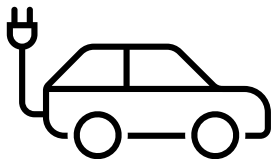
Wind

Wind turbines used as a DER. Also known as distributed wind.



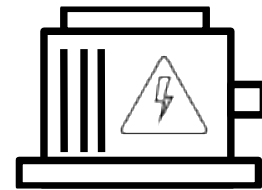
Energy Storage

Energy storage systems (ESS) can store excess electricity when it is not needed and supplies it back to a customer or the grid when in demand.



Electric Vehicles (EVs) & Chargers

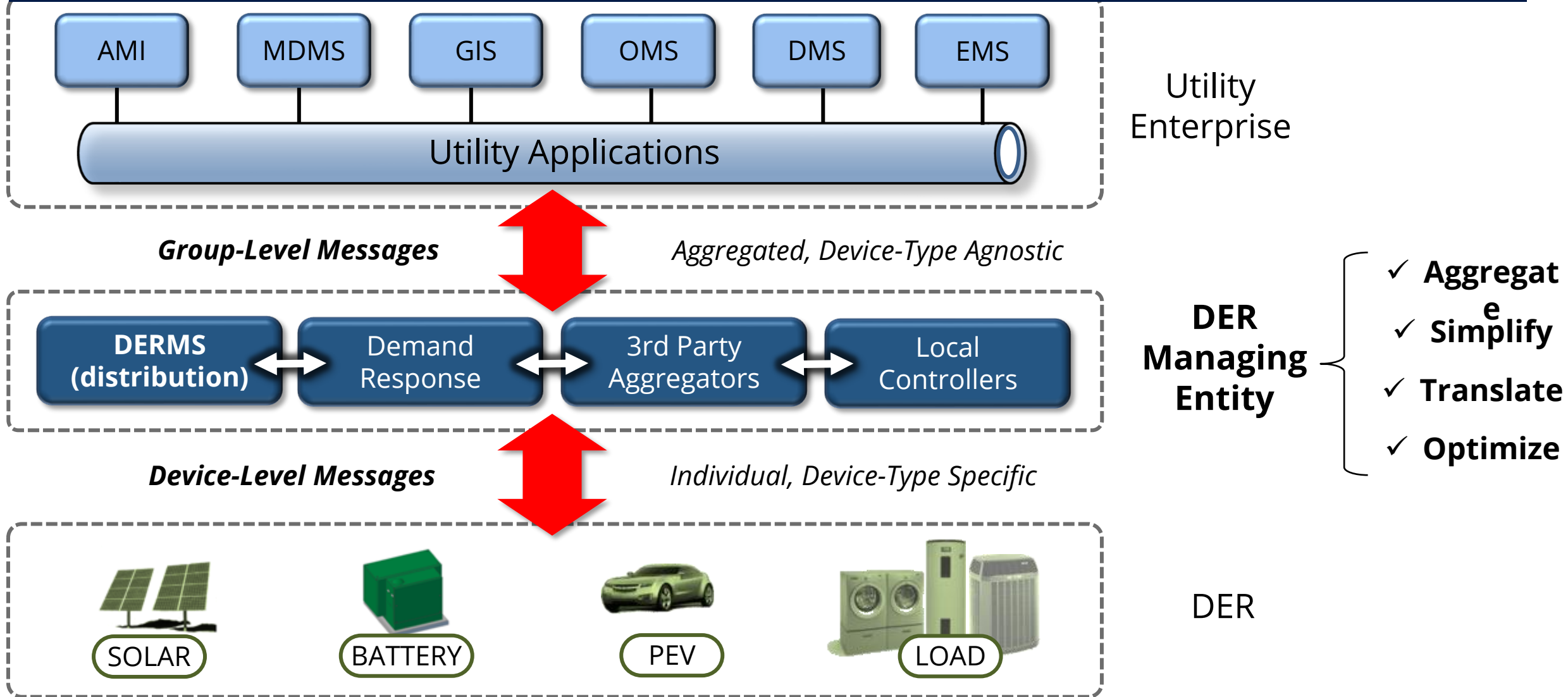
Regarded as mobile energy storage systems because of their ability to both consume and supply energy to the grid. Interconnection is through a charger.



Backup Generation

Typically, carbon-based generation (diesel) used as a power backup in case main source of electricity (the grid) is not available.

DERMS Architecture







Guidebook for DER Cyber Security

EPRI

2023 TECHNICAL UPDATE

Distributed Energy Resources (DER)
Cyber Security Guidebook for Utility
Architects and Engineers

3rd Edition

Chapter	Chapter Overview	Target Audience
Chapter 2: Understanding DER General Operating Concepts	Basic definitions of DERs, their operating concepts, interoperability use cases for the integrated DER Grid.	 Cyber Security Personnel new to DER systems.
Chapter 3: Current State of DER Standards & Certifications	Overviews of relevant interoperability, protocol, and certification standards to-date.	 All Utility Personnel, including cyber security personnel and grid application owners.
Chapter 4: Understanding DER Cyber Security Risks	Overviews of the various drivers to DER risks and possible risk scenarios of concern.	
Chapter 5: Understanding DER Reference Architectures	Summaries of various interoperability, cyber security, and DER technology architectures.	 Cyber Security Architects
Chapter 6: Cyber Security Engineering Guidance	Detailed guidance on technological considerations, challenges, and implementation requirements.	 Cyber Security Engineers or Technology Specialists

<https://www.epri.com/research/products/000000003002027325>

Some Homework to get you thinking...

- Who is ultimately accountable for Cyber Security in our organization?
- Are we testing our capabilities to recover in case of a cyberattack?
- How do we measure our cyber and data resiliency? Risk?
- What guidance does our data governance policy provide about data backups for recovery of systems after cyberattack?
- What are the most critical systems to support cyber security?
- Do we have redundant equipment or replacements for the most critical systems?
- Is there a backup of critical data for those systems?
- What is the frequency of the data backup?
- Where are backups located?
- What would be an acceptable Recovery Time Objective to achieve the target Recovery Point Objective?
- Etc.

Last Word - Key element of cyber resiliency: Data resiliency

Resiliency of data is focused on **ability** to **anticipate** attacks, **identify** the most important data to utility operations and cyber security operations, and have a robust data **recovery plan** focused on four essential areas.

1. Inventory and assessment of data

- Categorize data and applications based on priority of operational restoration – what data is important to conduct cyber security operations and restore protection of grid assets
- Establish goals to measure performance
 - Determine Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) for each data type
 - Engage stakeholders to understand restoration speed and acceptable data loss levels

2. Planning and Prioritization

- Assess vulnerabilities for prioritized data in storage, transit, and use
 - Identify and prioritize weaknesses in likelihood and potential damage
 - Evaluate external threats and insider risks
 - Prioritize recovery time over backup speed

3. Backup and Recovery Strategy

- Include Active Directory
 - Recognize Active Directory as critical data
 - Invest in dedicated tools for streamlined recovery
- Protect backups
 - Safeguard backup systems against interference, encryption, or corruption
 - Employ the 3-2-1 backup strategy: three copies, two storage media, one off-site

4. Review and Testing

- Regular testing
 - Test and revise the recovery plan regularly

Thank you

- Barry MacColl
- bmaccoll@epri.co.za
- +27 83 440 2169
- www.epri.com



Annexes

Some Definitions

- Information Technology
 - Office automation
 - Back-office applications; Payroll, Billing etc
 - Analytics/reporting
 - Data center
- Operational Technology
 - Used to manage the grid
 - Sensors and control devices: meters, telemetry, cap banks, transformers
 - Sensing and control applications: SCADA, EMS, Dispatch

Cyber Security Standards for Power Systems

NIST Cyber Security Framework

A framework built around five functions within cyber security: identify, protect, detect, respond, and recover

NIST 800-53

A standard promoting security and privacy controls for all U.S. federal information systems except national security systems

NERC CIP

A set of standards for securing the Bulk Electric System (BES) in North America

The ISO/IEC 27000 Family of Standards

A series of mutually supporting information security standards that can be combined to provide a comprehensive approach to managing and protecting organizational information and sets out the specification for an Information Security Management System (ISMS)

IEC 62443

A series of standards that provide guidelines for securing industrial control systems, including network and system security, security management, and security technologies

IEC 62351

A standard that provides guidelines and requirements that are focused on the security of power systems management and associated information exchange within industrial automation and control systems

Cyber Security Standards for Power Systems

NIST - National Institute of Standards and Technology

Non-regulatory federal agency within the U.S. Department of Commerce. NIST 800-53 standard provides a catalog of controls that support the development of secure and resilient federal information systems. NIST CSF is a cybersecurity framework of guidelines, standards and best practices

NERC - North American Electric Reliability Corporation

The Electric Reliability Organization (ERO) for North America, responsible for assessing and reporting on the reliability and adequacy of the North American bulk power system. NERC CIP standards are a set of mandatory security regulations and guidelines designed to protect the Bulk Electric System (BES) from cyber threats.

The ISO/IEC 27000 Family of Standards

A series of mutually supporting information security standards that can be combined to provide a comprehensive approach to managing and protecting organizational information and sets out the specification for an Information Security Management System (ISMS)

IEC 62443

A series of standards that provide guidelines for securing industrial control systems, including network and system security, security management, and security technologies

IEC 62351

A standard that provides guidelines and requirements that are focused on the security of power systems management and associated information exchange within industrial automation and control systems