CESI

Shaping a Better Energy Future

EnerNex

A CESI Company

Cybersecurity OT
Focus on the Electrical Sector

Presented by:

Davide Piccagli, Automation & Innovative Solutions Product Leader, CESI Group

Kay Stefferud, Director of Implementation Services, EnerNex

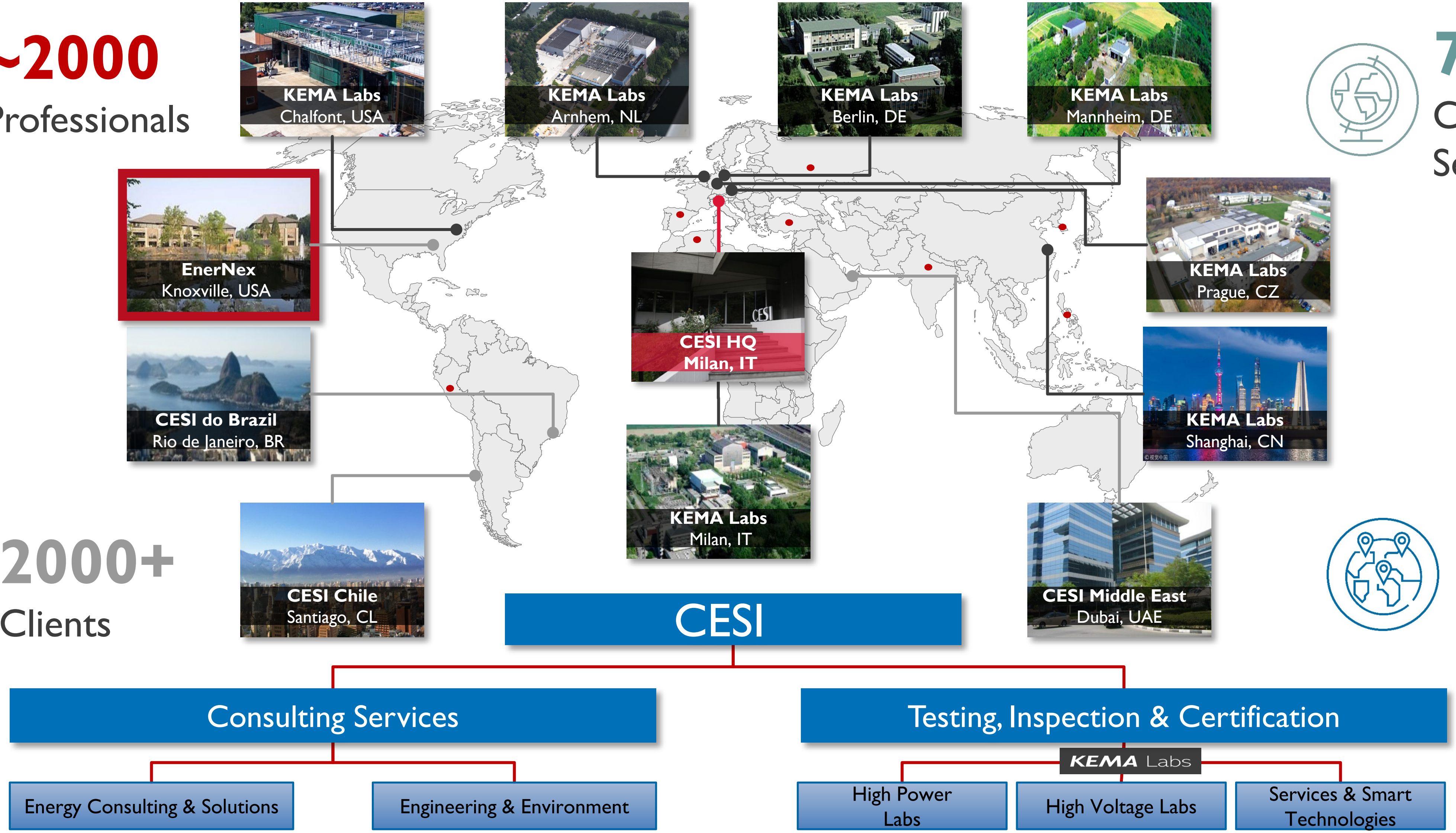
A Leading Global Player in Engineering, Testing, and Power Systems Consulting

~2000 Professionals

70+ Countries Served

2000+ Clients

11 Global Sites



CESI

Consulting Services

- Energy Consulting & Solutions
- Engineering & Environment

EnerNex

Testing, Inspection & Certification

KEMA Labs

- High Power Labs
- High Voltage Labs
- Services & Smart Technologies

© 2021 EnerNex. All Rights Reserved. www.enernex.com

Topics for Today's Discussion

Cybersecurity Challenges

Leading Cybersecurity Practices

Examples: Securing Third Party DER Systems, Smart Meter and Intelligent Devices

Cybersecurity Approaches

Our Cybersecurity Services

© 2021 EnerNex. All Rights Reserved. www.enernex.com

CESI

Shaping a Better Energy Future

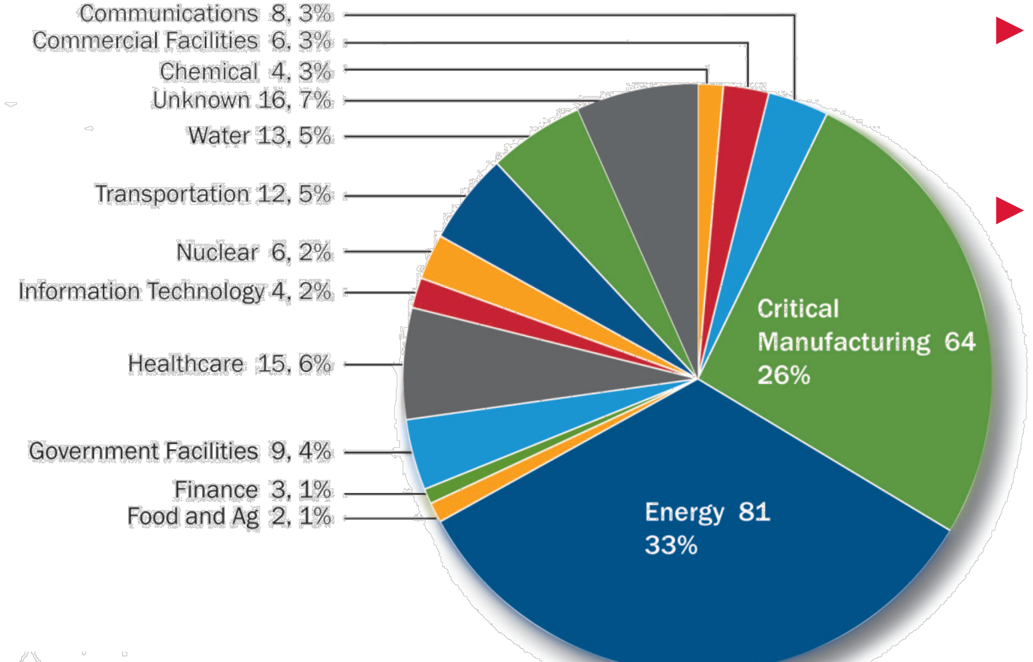
EnerNex

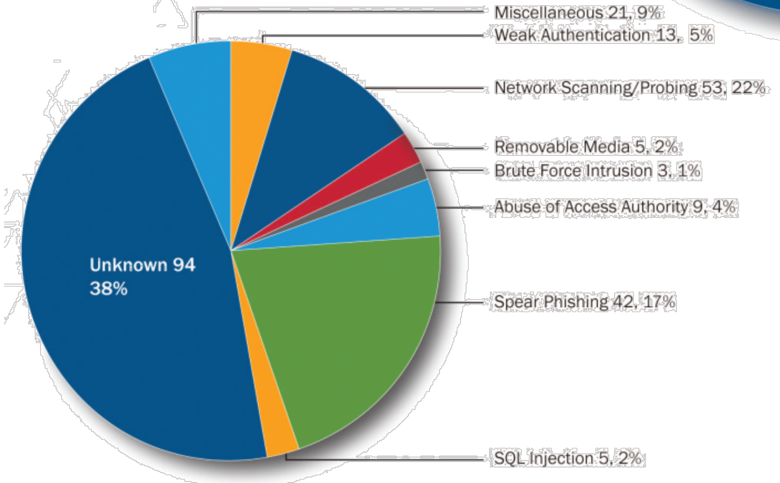
A CESI Company

1. Cybersecurity Challenges

Cybersecurity Challenges in the Energy Sector

Source: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf





- During 2014, **the Industrial Control Systems Cyber Emergency Response Team** (ICS-CERT) received and responded to 245 incidents reported by its associates who own industries and critical infrastructures.
- In 2017 **EU Energy Expert Cyber Security Platform** (EECSP) identified the main cybersecurity challenges for the Energy sector.

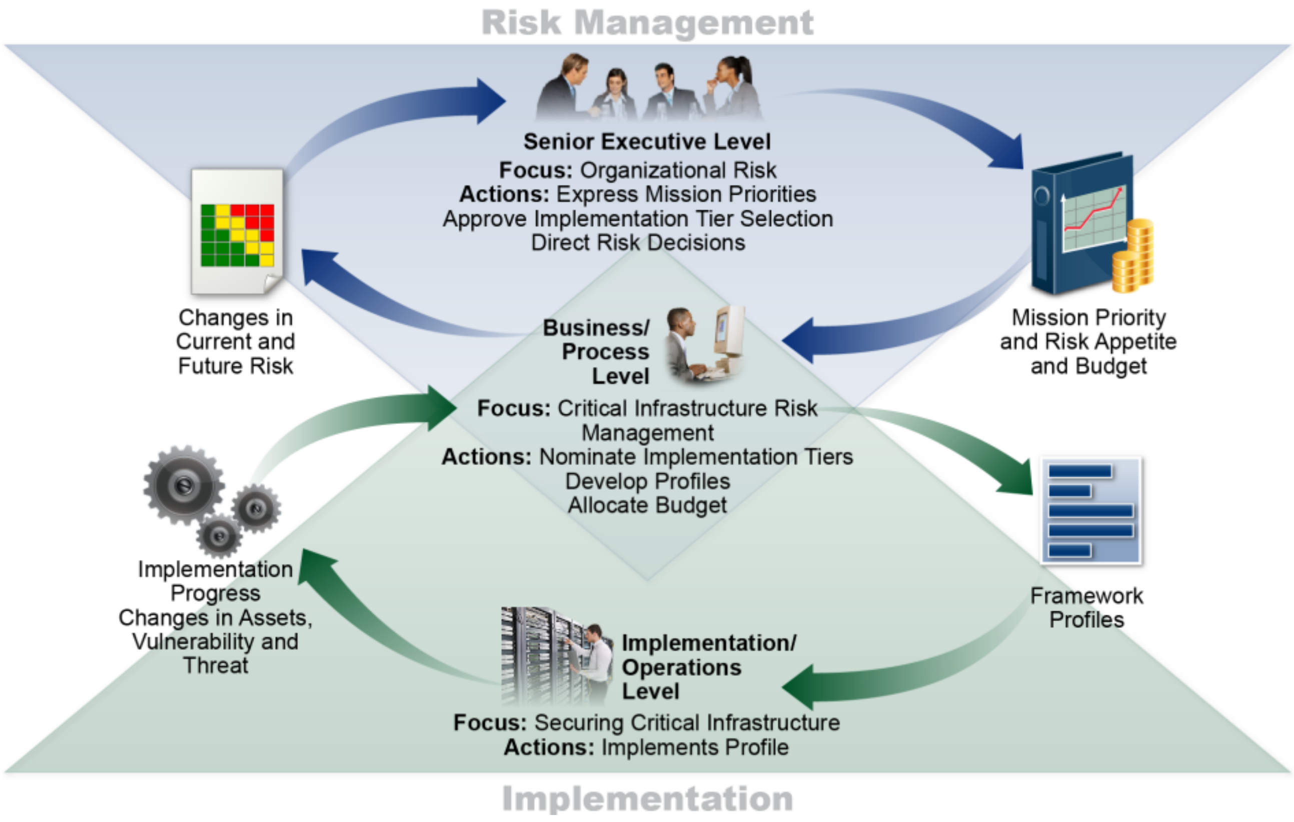
No.	Challenge	Electricity	Oil	Gas	Nuclear
1	Grid stability in a cross-border interconnected energy network.	x		x	x
2	Protection concepts reflecting current threats and risks.	x	x	x	x
3	Handling of cyber attacks within the EU.	x	x	x	x
4	Effects by cyber attacks not fully considered in the design rules of an existing power grid or nuclear facility	x			x
5	Introduction of new highly interconnected technologies and services.	x		x	
6	Outsourcing of infrastructures and services.	x		x	x
7	Integrity of components used in energy systems.	x		x	x
8	Increased interdependency among market players.	x			
9	Availability of human resources and their competences.	x	x	x	x
10	Constraints imposed by cyber security measures in contrast to real-time/availability requirements.	x		x	x

Source: Cyber Security in the Energy Sector - EU-EECSP - Report Feb 2017

© 2021 EnerNex. All Rights Reserved. www.enernex.com

Cybersecurity & Business a Challenge for All Company Levels: Risk Assessment and Ongoing Monitoring

- ***Main objective**: to determine the cause-and-effect relationships between cybersecurity protection level and company objectives.*
- *In the case of critical infrastructures, involvement must also be extended to **all the stakeholders**.*



Risk Management

Senior Executive Level
Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions

Changes in Current and Future Risk

Mission Priority and Risk Appetite and Budget

Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget

Implementation Progress
Changes in Assets, Vulnerability and Threat

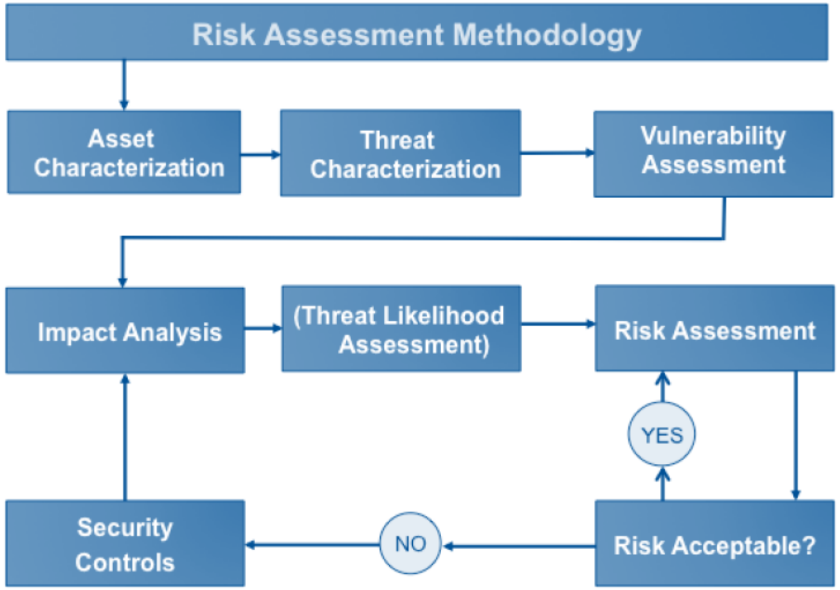
Framework Profiles

Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile

Implementation

Source: NIST - CyberSecurity Framework, January 2017

Phase 1: Risk Assessment



Risk Assessment Methodology

Asset Characterization

Threat Characterization

Vulnerability Assessment

Impact Analysis

(Threat Likelihood Assessment)

Risk Assessment

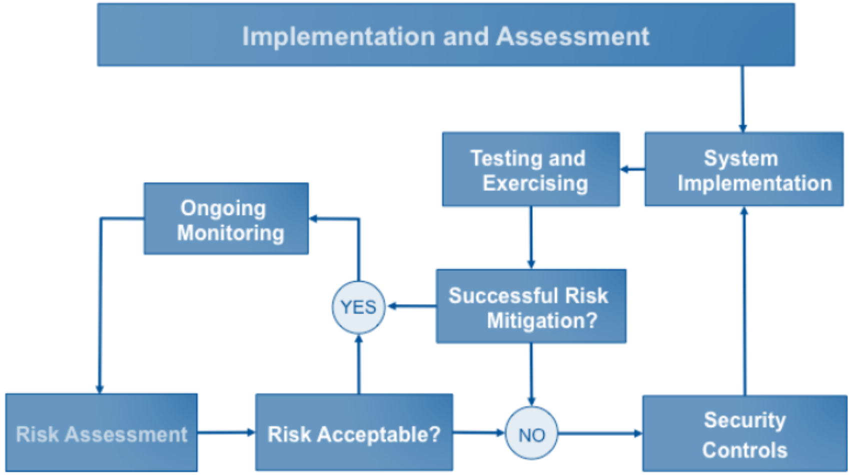
YES

Security Controls

NO

Risk Acceptable?

Phase 2: Implementation and Ongoing Monitoring



Implementation and Assessment

Testing and Exercising

System Implementation

Ongoing Monitoring

YES

Successful Risk Mitigation?

Risk Assessment

Risk Acceptable?

NO

Security Controls

EPRI: Cyber Security Strategy Guidance for the Electric Sector

CESI
Shaping a Better Energy Future

EnerNex
A CESI Company

© 2021 EnerNex. All Rights Reserved. www.enernex.com

Reasons for Cyber Attacks Detected in the Electrical Sector

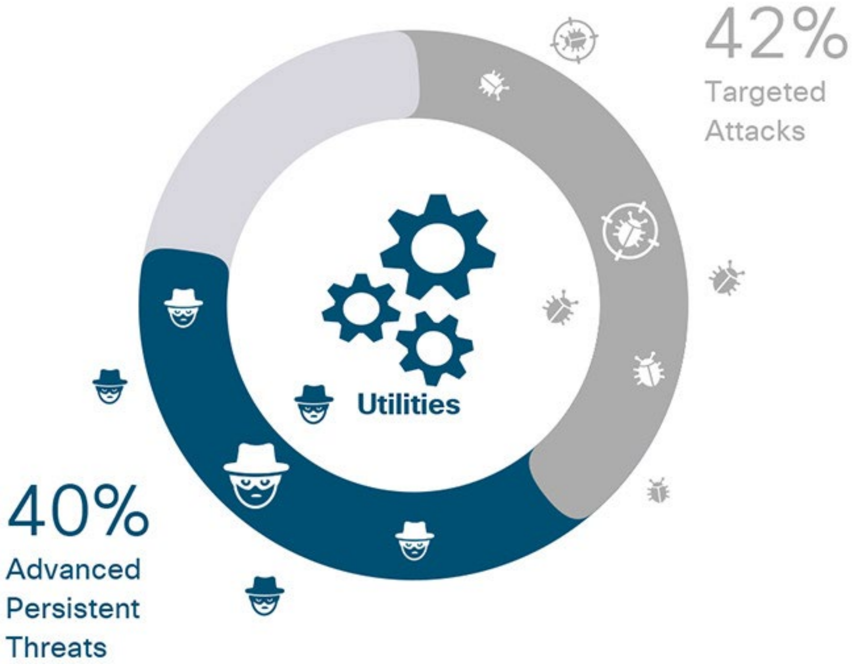
- ***Electric utilities*** *and related* ***critical infrastructures*** *have been the subject of many and varied cyber attacks.*

- *The data stolen from companies seems to some extent aimed at* ***mapping critical infrastructures*** *and collecting detailed information about them to create databases.*

- *If not adequately detected and contained, the cyber threats went on for a long time (****APT - Advanced Persistent Threats****) and involved components, networks, plants, monitoring systems and information relating to employees.*

- *The stolen data make it possible to* ***reconstruct the operating criteria*** *of companies, exposing them to ever greater risks.*

- *Most of the time, the attacks are aimed* ***at finding information rather than causing blackouts*** *on the network.*



Source: CISCO 2017 – Security Capabilities Benchmark Study

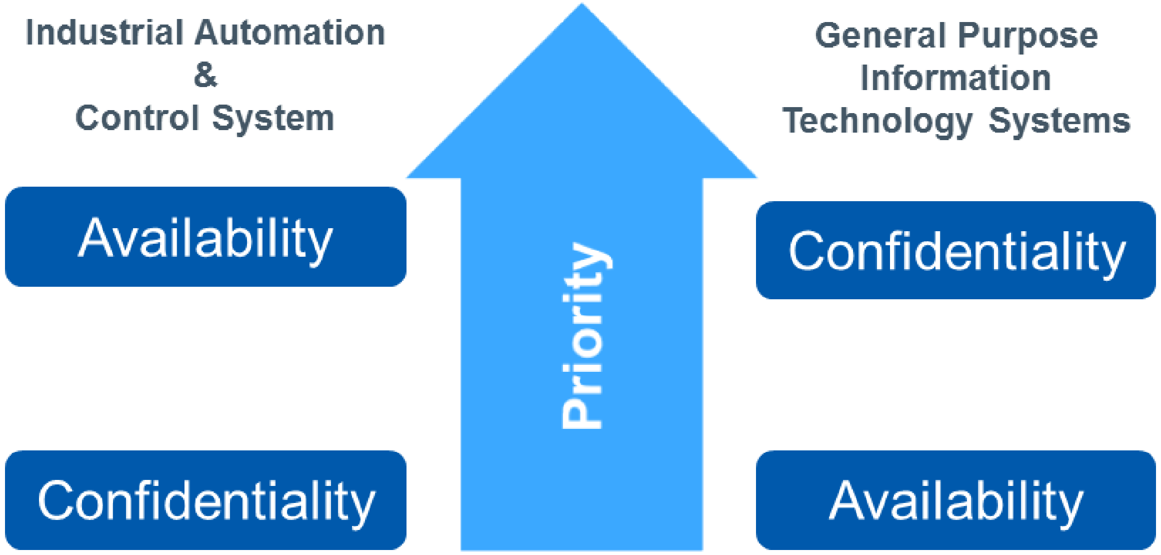
© 2021 EnerNex. All Rights Reserved. www.enernex.com

IT vs OT: Cybersecurity Assessment

- *For a long time, Information Technology (**IT**) and Operation Technology (**OT**) were **two completely distinct domains** of the utility business.*
- ***IT focused** on all the technologies necessary to **manage IT processes** (e.g. invoicing), with mainly economic-financial purposes.*
- ***OT focused on devices, sensors, networks and software** needed to manage operational processes (e.g. energy supply) with the main aim of reliability and safety.*
- *The **progressive opening and integration** of the OT world with the rest of the IT processes is changing this vision and the two domains are becoming more and more interconnected.*
- *The integration must be carried out in **compliance with the differences of the two domains**, bearing in mind however that the OT is often characterized by legacy systems and that **knowledge of the processes is essential**.*
- *The **security solutions** on traditional information systems must be **adequate** to deal with the Smart Grids environment considering:*
  - *the **legacy nature** of the infrastructure;*
  - *the **real-time nature** of the communication involved.*
- *Security must be built into the applications themselves (**Security by Design**).*

© 2021 EnerNex. All Rights Reserved. www.enernex.com

Security Requirements: Confidentiality, Integrity and Availability

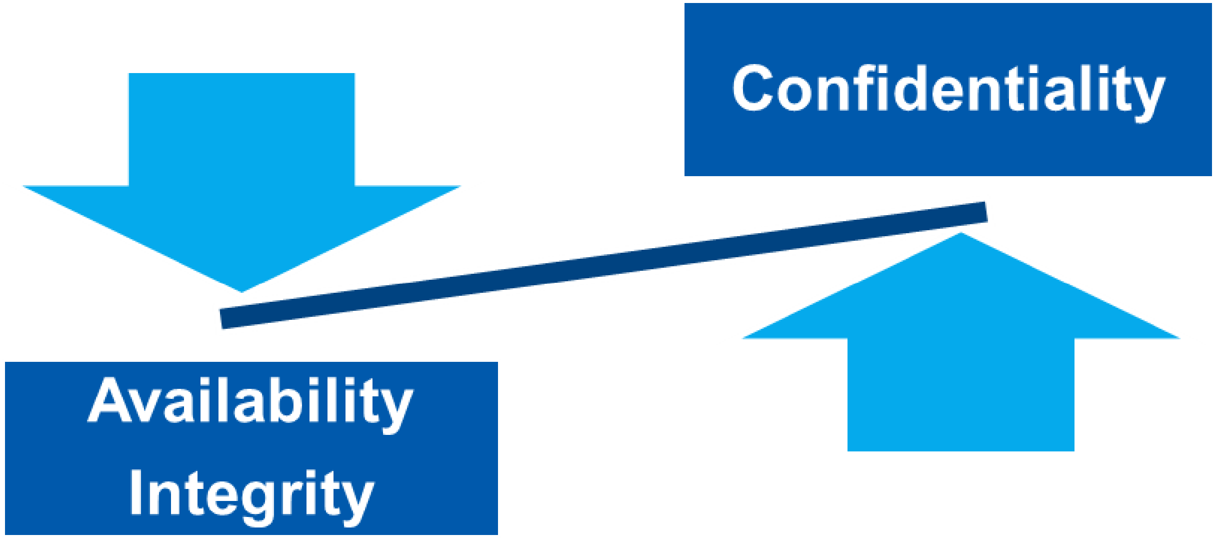


Different Priorities:

- ▶ ***IT*** *(Information Technology)*
- ▶ ***OT*** *(Operation Technology)*

Secure Sockets Layer (SSL) tunneling example:

- ▶ *SSL is used to secure data traffic from / to the internet (e.g. email) and* ***protect information***
- ▶ *SSL can provide an "****opaque tunnel****" within which malware can be introduced into a corporate network*



© 2021 EnerNex. All Rights Reserved. www.enernex.com

Smart Security Layers

- ***Applications in the electrical sector*** *(e.g. EMS, markets, etc.)* ***are designed to address random failures*** *that occur in the electrical system or on the information and communication systems connected to it.*

- *So, they are* ***not entirely inadequate*** *to deal with events caused by cyber attacks,* ***even coordinated*** *in order to hit multiple points in the system.*

- ***Smart Security*** *must have integrated security in all the following three layers*

  *(****Information*** *+* ***Infrastructure*** *+* ***System****)*

  to provide defense in depth to face cyber attacks

	Information Security	Infrastructure Security	System Security
NEEDS	• Information protection ○ Message confidentiality ○ Message integrity ○ Message authenticity	• Infrastructure protection ○ Routers ○ DNS servers ○ Links ○ Internet protocols • Service availability	• Generation control applications • Transmission control applications • Distribution control applications • Real-Time Energy Markets
MEANS	• Encryption/Decryption • Digital signature • Message Authenticity Codes • Public Key infrastructure	• Traffic monitoring • Statistical analysis • Authentication Protocols • Secure Protocols • Secure Servers	• **Attack-Resilient Control Algorithms** • **Model-based Algorithms** ○ Anomaly detection ○ Intrusion Tolerance ○ Bad data elimination • Risk modeling and mitigation

CESI

Shaping a Better Energy Future

EnerNex

A CESI Company

2. Leading Cyber Practices

© 2021 EnerNex. All Rights Reserved. www.enernex.com

Key Cybersecurity Frameworks and Standards for OT Systems

International Standards
International Organization for Standardization (ISO) 27001 Information security management systems
IEC 62443 Series of Standards (formerly ISA 99) - Industrial communication networks - IT security for networks and systems
IEC 62351 Series of Standards - Security for IEC 60870-5, IEC 60870-6, IEC 61850 IEC 61970 & IEC 61968 protocols

National Institute of Standards and Technology (NIST)
NIST Framework for Improving Critical Infrastructure Cybersecurity
NIST CSF Smart Grid Profile
NISTIR 7628 Guidelines for Smart Grid Cybersecurity
NIST Special Publication 800-53 Revision 4 Recommended Security Controls for Federal Information Systems and Organization
NIST Special Publication 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security
NIST National Cybersecurity Center of Excellence (NCCoE) Practice Guides/Use Cases

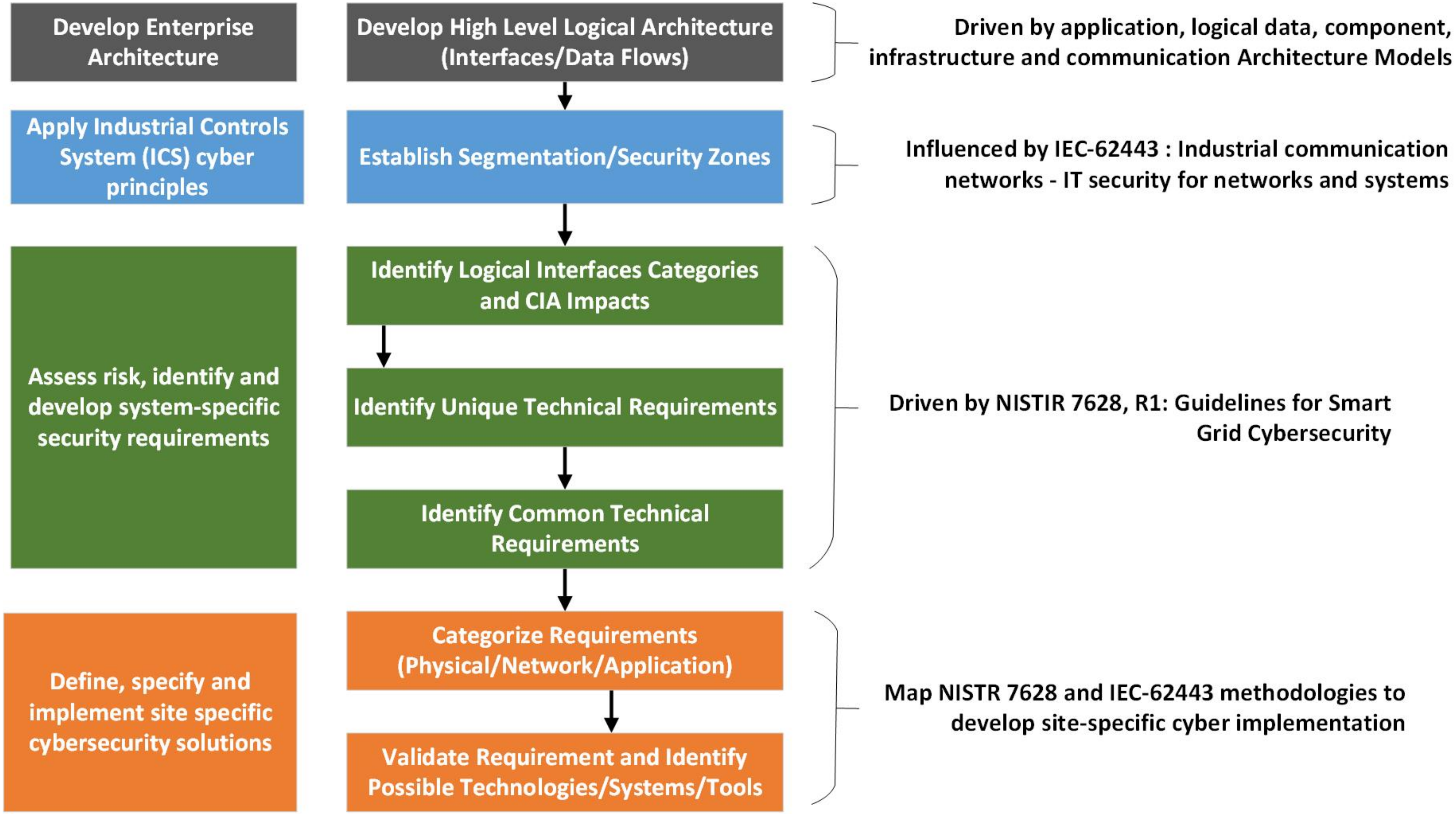
United States Department of Energy (DOE)
Electricity Subsector Cybersecurity Capabilities Maturity Model (ES-C2M2)
Cybersecurity Procurement Language for Energy Delivery Systems

National Rural Electric Cooperative Association (NRECA)
Assessing Your Cooperative's Cybersecurity Capabilities
Guide to Developing a Cyber Security and Risk Mitigation Plan

United States Department of Homeland Security (DHS)
Catalog of Control Systems Security: Recommendations for Standards Developers
Control Systems Cyber Security: Defence in Depth Strategies
Industrial Control Systems Cyber Emergency Response Team, Recommended Practice

© 2021 EnerNex. All Rights Reserved. www.enernex.com

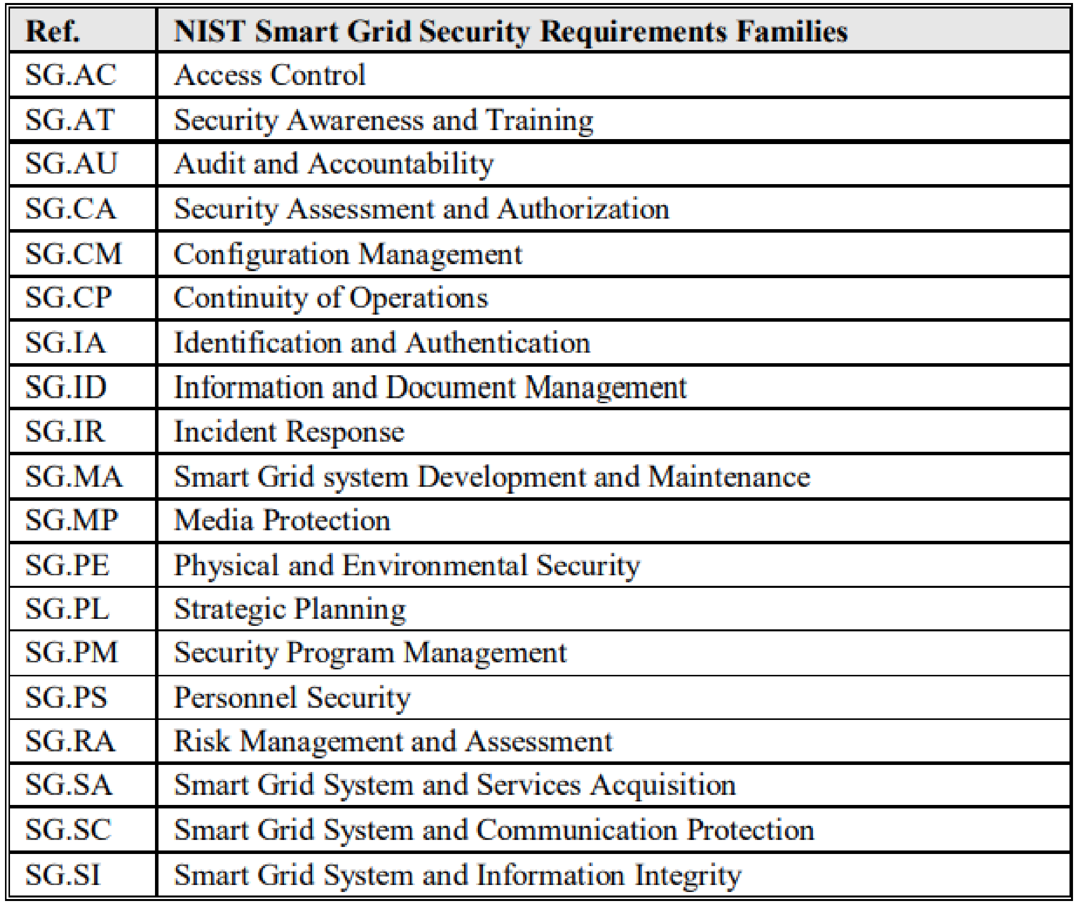
Leading Cybersecurity Practices


Develop Enterprise Architecture
Develop High Level Logical Architecture (Interfaces/Data Flows)
Driven by application, logical data, component, infrastructure and communication Architecture Models
Apply Industrial Controls System (ICS) cyber principles
Establish Segmentation/Security Zones
Influenced by IEC-62443 : Industrial communication networks - IT security for networks and systems
Assess risk, identify and develop system-specific security requirements
Identify Logical Interfaces Categories and CIA Impacts
Identify Unique Technical Requirements
Identify Common Technical Requirements
Driven by NISTIR 7628, R1: Guidelines for Smart Grid Cybersecurity
Define, specify and implement site specific cybersecurity solutions
Categorize Requirements (Physical/Network/Application)
Validate Requirement and Identify Possible Technologies/Systems/Tools
Map NISTR 7628 and IEC-62443 methodologies to develop site-specific cyber implementation

© 2021 EnerNex. All Rights Reserved. www.enernex.com

NISTIR 7628 Cybersecurity Requirements – A Comprehensive View of Cybersecurity

19 Requirement Categories



Ref.	NIST Smart Grid Security Requirements Families
SG.AC	Access Control
SG.AT	Security Awareness and Training
SG.AU	Audit and Accountability
SG.CA	Security Assessment and Authorization
SG.CM	Configuration Management
SG.CP	Continuity of Operations
SG.IA	Identification and Authentication
SG.ID	Information and Document Management
SG.IR	Incident Response
SG.MA	Smart Grid system Development and Maintenance
SG.MP	Media Protection
SG.PE	Physical and Environmental Security
SG.PL	Strategic Planning
SG.PM	Security Program Management
SG.PS	Personnel Security
SG.RA	Risk Management and Assessment
SG.SA	Smart Grid System and Services Acquisition
SG.SC	Smart Grid System and Communication Protection
SG.SI	Smart Grid System and Information Integrity

3 Requirement Types

Organizational Requirements

Governance Risk and Compliance (GRC)

- Centered around policy, procedure, and compliance-based activities

Technical Requirements

- Allocated to each Smart Grid system and not necessarily to every asset within a system, as the focus is on security at the system level
- Two Types:

Common Technical Requirements (CTR)

- Applicable to all interfaces

Unique Technical Requirements (UTR)

- Allocated to one or more interfaces based on impact and interface characteristics

Cybersecurity Evolution in EU: GDPR and NIS

General Data Protection Regulation (GDPR) - 2018

- *Regulation of the European Parliament and of the Council on the* ***protection of individuals*** *about processing of* ***personal data*** *and on the* ***free movement*** *of such data.*
- *Implies compliance duties in terms of* ***data privacy*** *for all the companies.*

The **EU General Data Protection Regulation (GDPR)** is the most important change in data privacy regulation in 20 years - we're here to make sure you're prepared.

The Network and Information Security (NIS) Directive:

- *The first piece of EU-wide legislation on cybersecurity; it provides legal measures to boost the overall* ***level of cybersecurity*** *in the EU.*
- *Member States had to transpose the Directive into their national laws and identify* ***operators of essential services*** *(2018).*
- *It ensure Member States' preparedness by requiring them to* ***be appropriately equipped via CSIRT*** *and a competent national* ***NIS authority.***
- *It guarantees a* ***culture of security across sectors*** *which are vital for our economy and society and moreover rely heavily on ICTs.*
- *It leverages on the* ***networking and the information exchange*** *among Member States.*

Cybersecurity Evolution in EU: Proposal for NIS 2

Reasons for revision

- *NIS Directive had notable **achievements** but by now has also proven its **limitations.***
- *The **digital transformation** of society (intensified by the COVID-19 crisis) has expanded the threat landscape and is bringing about new challenges.*
- *Any disruption, even one initially confined to one entity or one sector, can have **cascading effects more broadly** potentially resulting in **negative impacts in all the EU market.***

Key elements

- *It eliminates the distinction between **operators of essential services and digital service providers.***
- *It imposes a **risk management approach** providing a minimum list of basic security elements that must be applied.*
- *It introduces a more precise provisions on the **process for incident reporting.***
- *It address **security of supply chains and supplier relationships.***
- *It leverages on **coordination** to deal with **emerging technologies** and to manage **vulnerability disclosure.***

© 2021 EnerNex. All Rights Reserved. www.enernex.com

Cybersecurity Evolution in EU: Cyber Certification

- *The EU Cybersecurity Act establishes an* ***EU certification framework*** *for ICT digital products, services and processes.*
- *The European cybersecurity certification framework enables the creation of* ***tailored and risk-based EU certification schemes****.*
- *Certification plays a critical role in* ***increasing trust and security*** *in products and services that are crucial for the Digital Single Market.*

enisa
THE EU
CYBERSECURITY
AGENCY

Issues and challenges

- *Several* ***different*** *security certification schemes for ICT products exist in the EU, with an increasing* ***risk of fragmentation****.*
- *The certification framework will provide EU-wide* ***certification schemes as a comprehensive set of rules****, technical requirements, standards and procedures. Each European scheme should specify:*
  - *the* ***categories*** *of products and services covered,*
  - *the cybersecurity* ***requirements****, for example by reference to standards or technical specifications,*
  - *the type of* ***evaluation*** *(e.g. self-assessment or third-party evaluation), and*
  - *the intended* ***level of assurance*** *(e.g. basic, substantial and/or high).*

© 2021 EnerNex. All Rights Reserved. www.enernex.com

CESI

Shaping a Better Energy Future

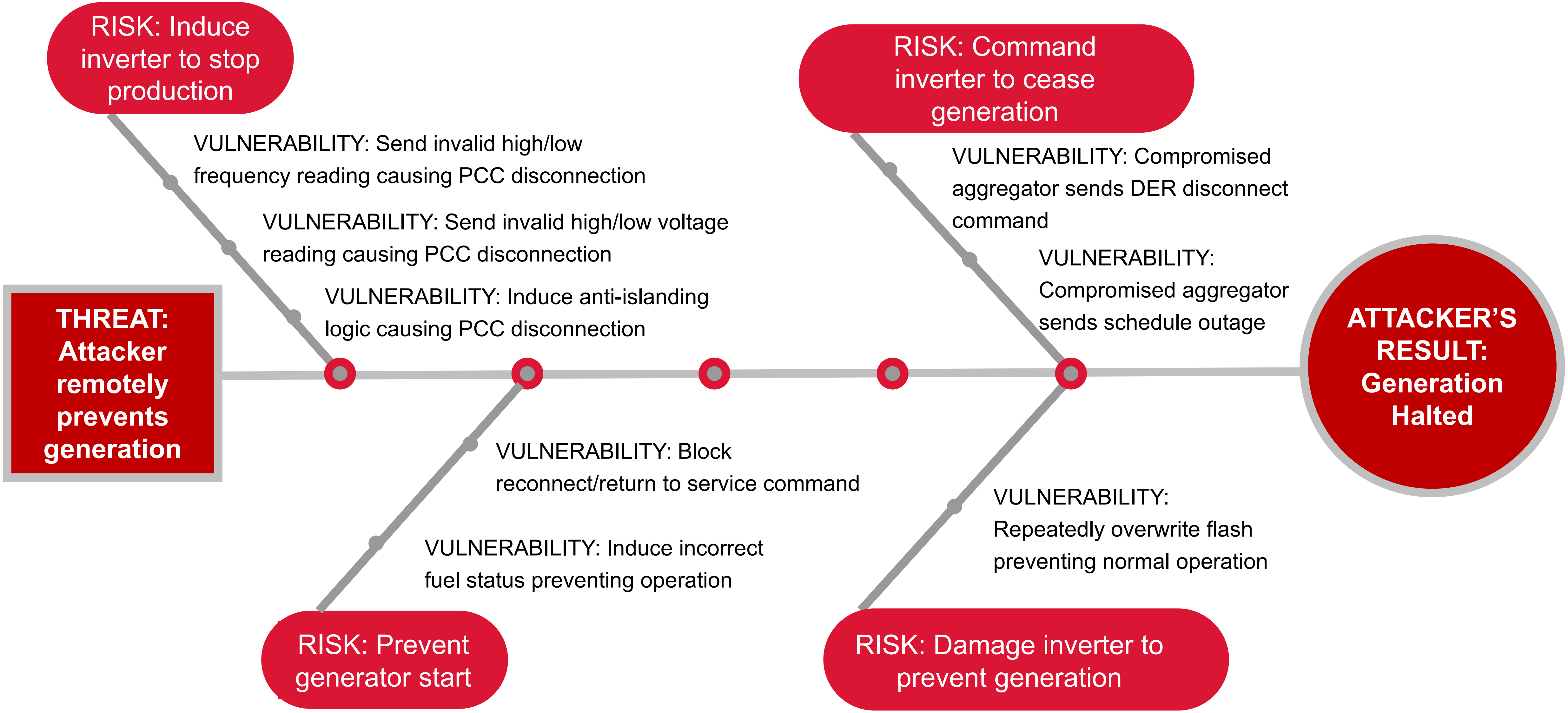
EnerNex

A CESI Company

3. EXAMPLES

© 2021 EnerNex. All Rights Reserved. www.enernex.com

Example: Microgrid Vulnerabilities, Risks & Threats



THREAT: Attacker remotely prevents generation

RISK: Induce inverter to stop production

VULNERABILITY: Send invalid high/low frequency reading causing PCC disconnection

VULNERABILITY: Send invalid high/low voltage reading causing PCC disconnection

VULNERABILITY: Induce anti-islanding logic causing PCC disconnection

RISK: Prevent generator start

VULNERABILITY: Block reconnect/return to service command

VULNERABILITY: Induce incorrect fuel status preventing operation

RISK: Command inverter to cease generation

VULNERABILITY: Compromised aggregator sends DER disconnect command

VULNERABILITY: Compromised aggregator sends schedule outage

RISK: Damage inverter to prevent generation

VULNERABILITY: Repeatedly overwrite flash preventing normal operation

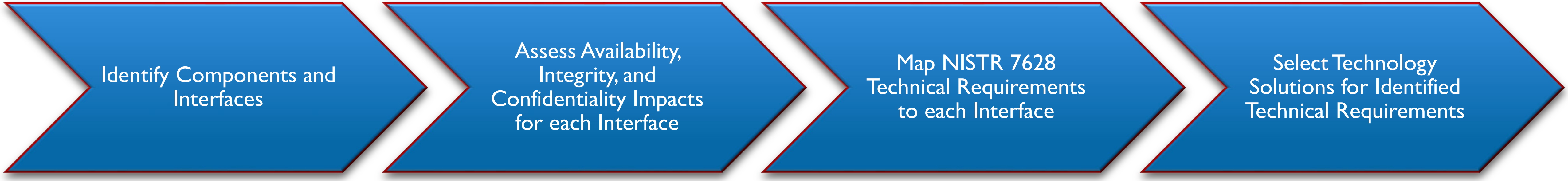
ATTACKER’S RESULT: Generation Halted

CESI
Shaping a Better Energy Future

EnerNex
A CESI Company

© 2021 EnerNex. All Rights Reserved. www.enernex.com

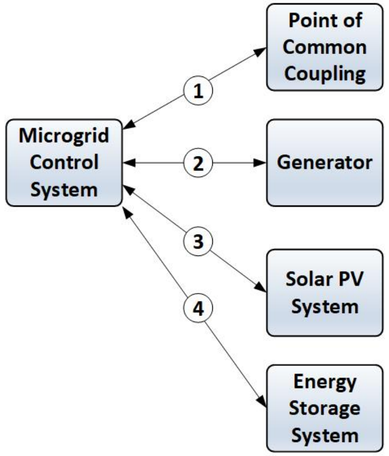
Recommended Practice: Example Process for Microgrid with DERs


Identify Components and Interfaces

Assess Availability, Integrity, and Confidentiality Impacts for each Interface

Map NISTR 7628 Technical Requirements to each Interface

Select Technology Solutions for Identified Technical Requirements



For OT systems, impact rankings should be relative to safety and system reliability

Logical Interface	Availability	Integrity	Confidentiality
1	High	Moderate	Low
2	High	Low	Low
3	Moderate	Moderate	Low
4	Moderate	Moderate	Low

Based on Logical Interface Category and Impact

NISTR 7628 Requirement	Applicable Interface Data Flows			
	1	2	3	4
SG.AU-3 Audit Logs	X		X	X
SG.PE-8 Emergency Power	X			X
SG.AC-15 Remote Access		X		X
SG.CM-7 Configuration for Least Functionality	X	X	X	X
. . .				

Tailoring solutions for specific system components may be necessary

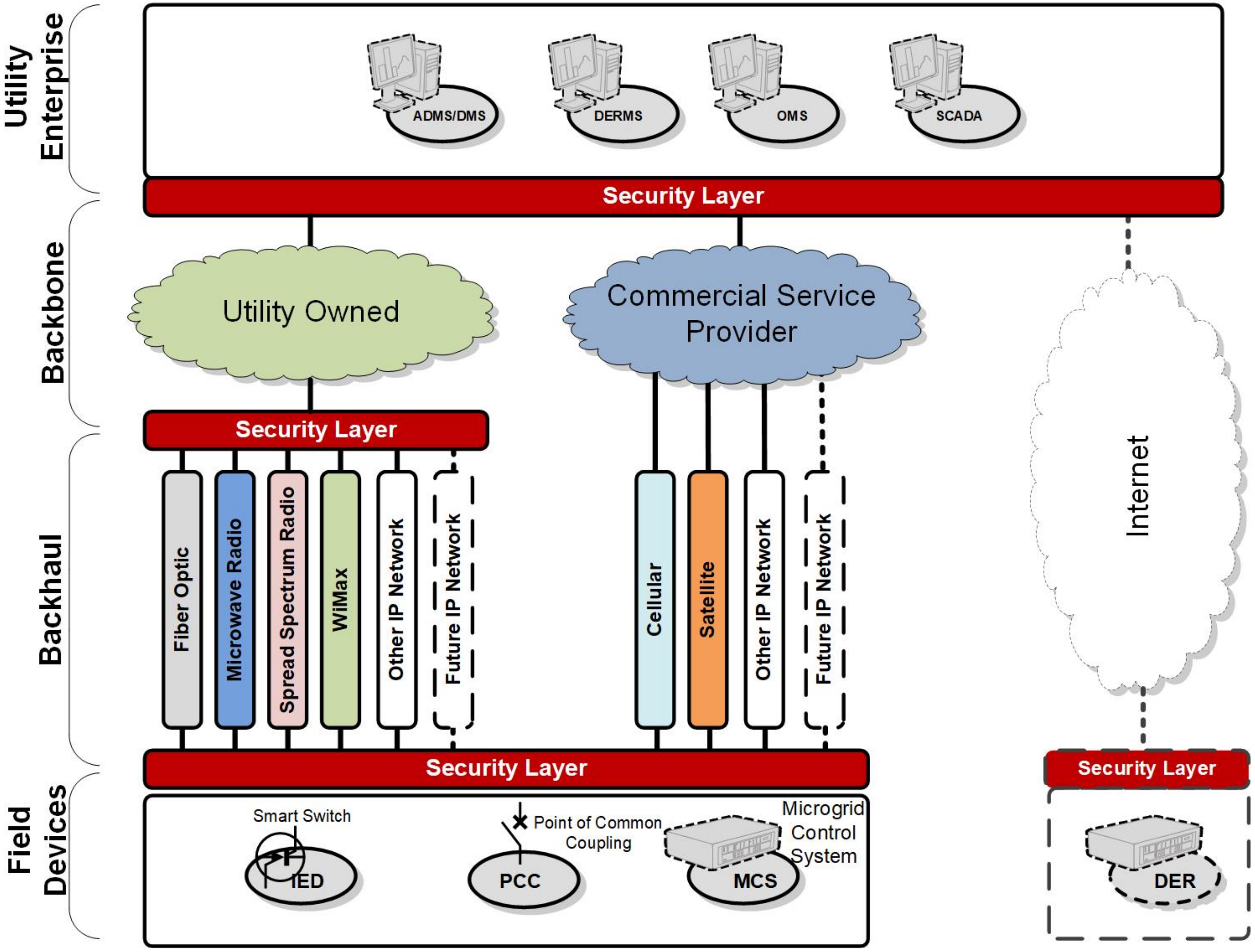
Solutions
• Implement Syslog from all system components to central log aggregator
• Battery backup for critical system components
• Jump server implemented within DMZ using Virtual Desktop Infrastructure (VDI) • VPN encryption
• Disable unused ports & services on hosts • Configure network firewalls to allow only necessary inbound/outbound traffic

CESI Shaping a Better Energy Future

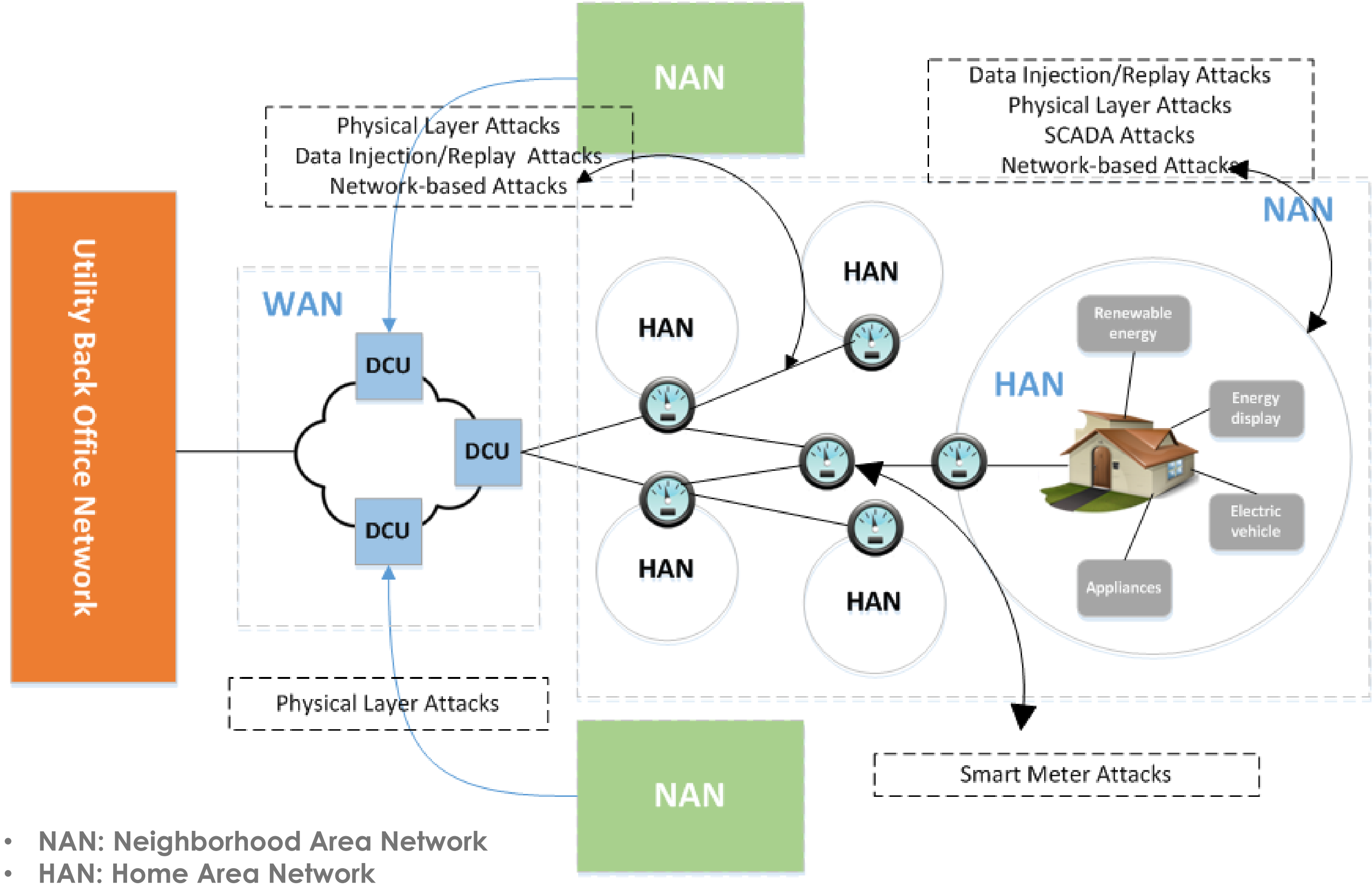
EnerNex A CESI Company

© 2021 EnerNex. All Rights Reserved. www.enernex.com

Example: Securing Microgrid with Third Party DER Systems Security Architecture



Smart Meter Example: Attacks and Security Requirements

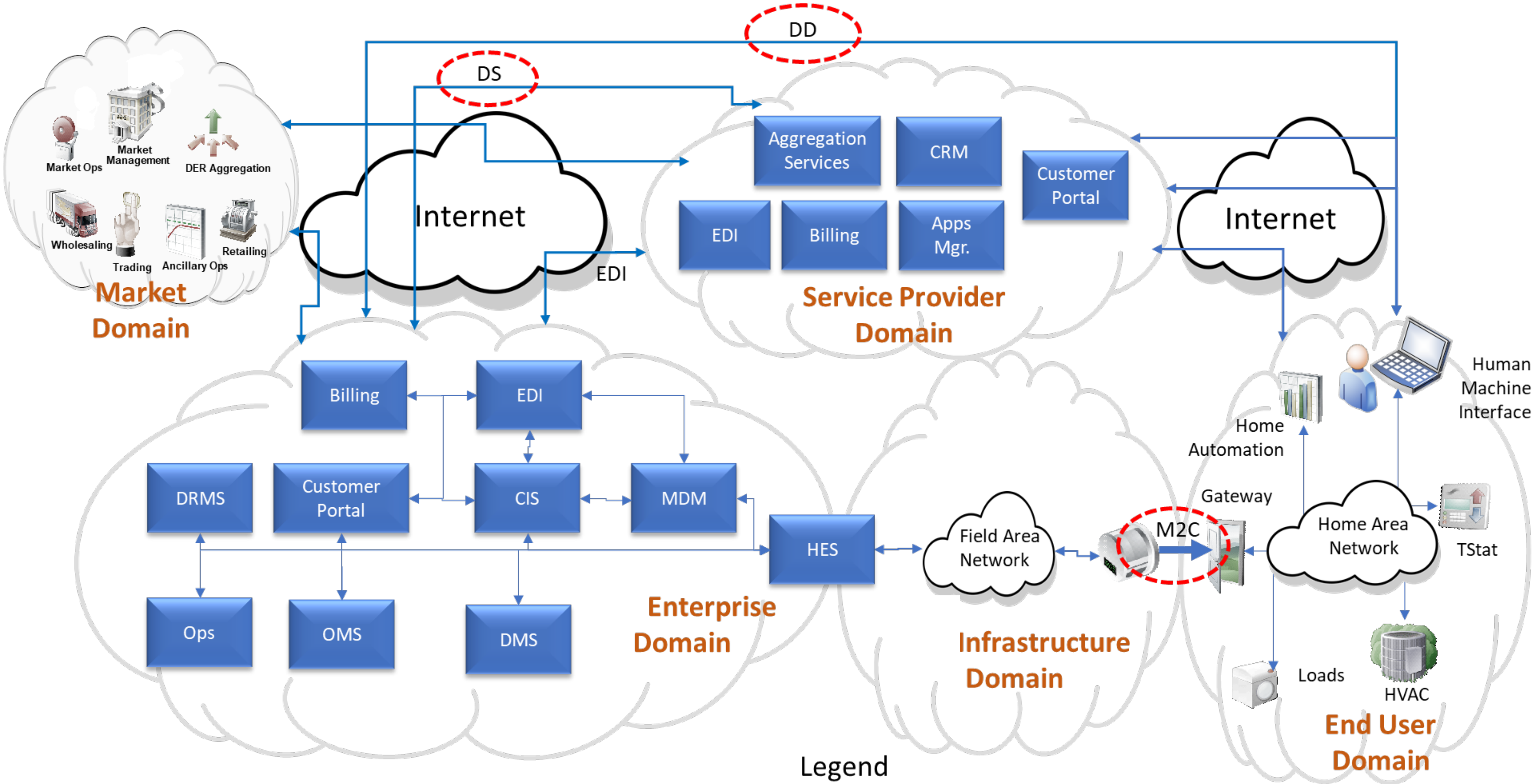


- NAN: Neighborhood Area Network
- HAN: Home Area Network
- WAN: Wide Area Network
- DCU: Data Collection Unit

Attack target	Security requirements violations
SCADA	Confidentiality, Availability, Integrity
Smart meter	Integrity, Availability, Confidentiality
Physical layer	Availability, Integrity, Confidentiality
Data injection / Reply attacks	Confidentiality
Network	Availability, Confidentiality

© 2021 EnerNex. All Rights Reserved. www.enernex.com

AMI to Home Area Network Architecture Options



Legend

OMS	Outage Management System	CIS	Customer Information System	MDM	Meter Data Management System	DS	Data Sharing
DMS	Distribution Management System	OPS	Engineering/Operations Center	DRMS	Demand Response Management System	M2C	Meter to Customer
HES	Headend System	EDI	Electronic Data Interchange	DD	Data Download		

CESI
Shaping a Better Energy Future

EnerNex
A CESI Company

© 2021 EnerNex. All Rights Reserved. www.enernex.com

CESI

Shaping a Better Energy Future

EnerNex

A CESI Company

4. CYBERSECURITY APPROACHES

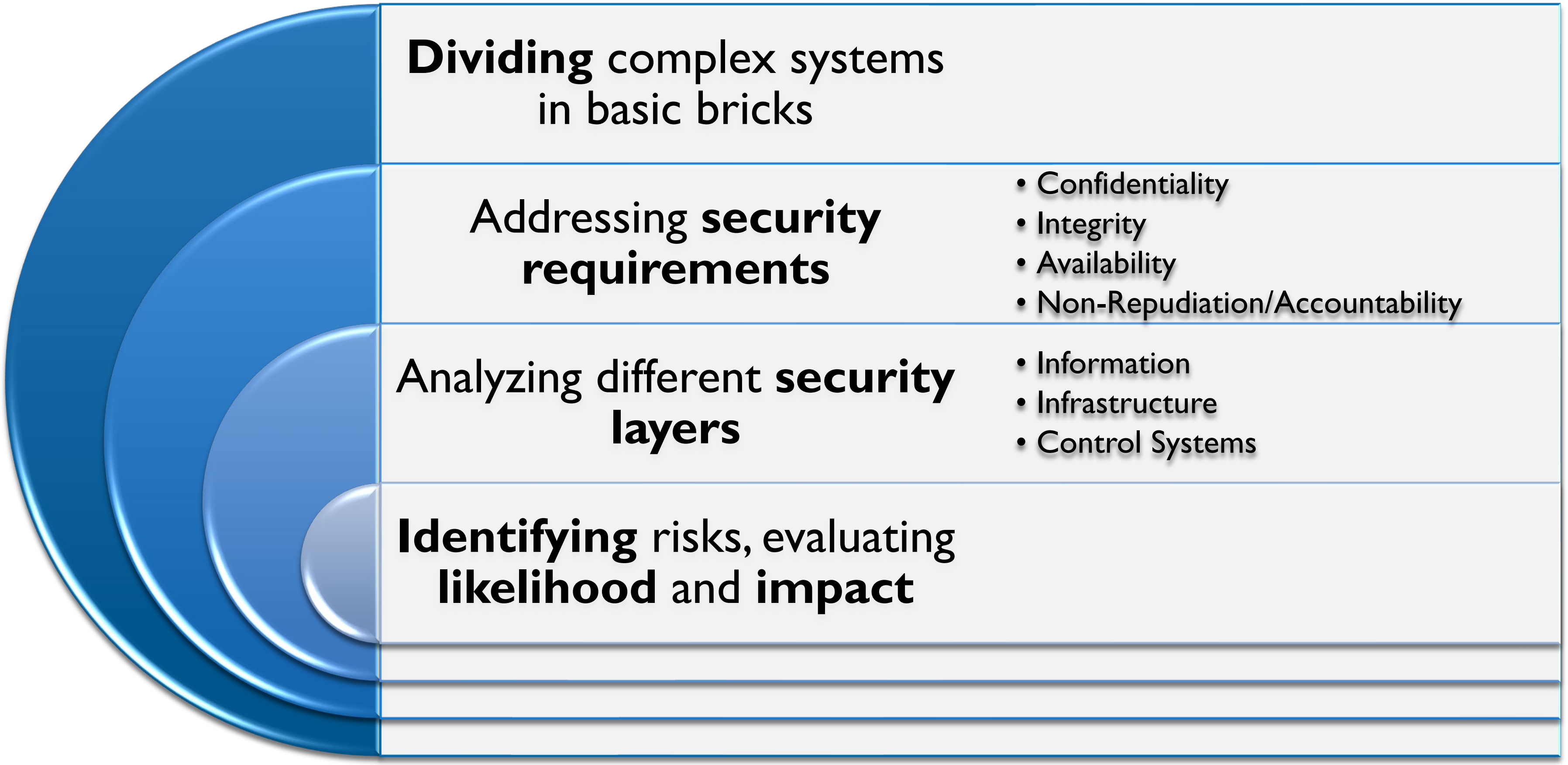
***Technical Specifications & Cyber-Requirements**: security must be considered in the design phase of systems and processes*

Specific environment

Specific needs

Development of technical specifications that cover both functional and cybersecurity requirements

Systems and processes knowledge and experience in the electrical sector is crucial



Dividing complex systems in basic bricks

Addressing **security requirements**

- Confidentiality
- Integrity
- Availability
- Non-Repudiation/Accountability

Analyzing different **security layers**

- Information
- Infrastructure
- Control Systems

Identifying risks, evaluating **likelihood** and **impact**

Guiding Principle

Security by design: if security is not projected from the beginning surely there will be problems

Source: NIST - Guidelines for Smart Grid Cybersecurity

© 2021 EnerNex. All Rights Reserved. www.enernex.com

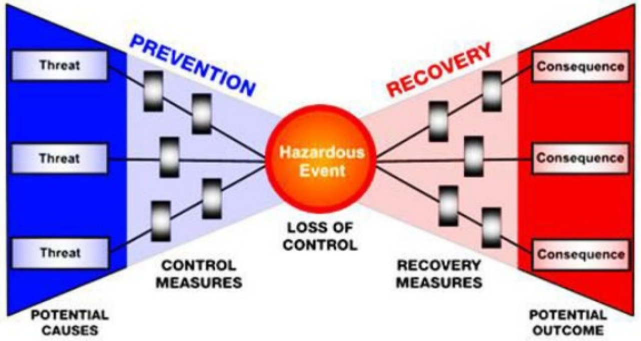
***Cyber Risk System Assessment**: risk evaluation activity and possible approaches to address cybersecurity requirements*

- ***CyberRisk Assessment** is a complete security consultancy service, which involves all engineering processes and not just software and IT management.*
- ***Identify, evaluate and estimate** the level of risk considering threats as well as their consequences.*

Risk Assessment Matrix

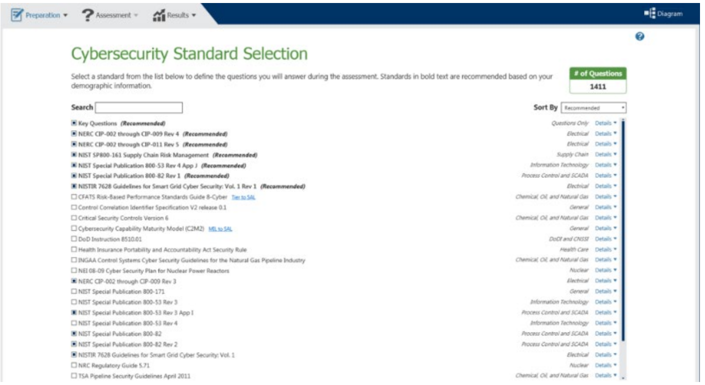
		Likelihood of Incident Scenario				
		Very Low	Low	Medium	High	Very High
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Bow-Tie models used for process risk evaluation



- *An **acceptable level of risk** is determined both by the achieved security levels, but also by the application context of the systems and infrastructures concerned.*

- ***Q&A approach:** consisting of an appropriate list of questions (typically based on one or more international standards); based on related answers it is possible to build summary reports useful for highlighting the critical points of the system.*



Cybersecurity Standard Selection

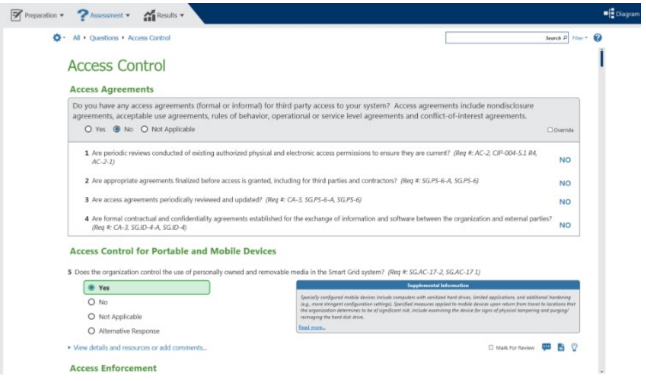
Select a standard from the list below to define the questions you will answer during the assessment. Standards in bold text are recommended based on your demographic information.

# of Questions: 1411

Search

Sort By: Recommended

☒ **Key Questions *(Recommended)***	*Questions Only*	Details ▾
☒ **NERC CIP-002 through CIP-009 Rev 4 *(Recommended)***	*Electrical*	Details ▾
☒ **NERC CIP-002 through CIP-011 Rev 5 *(Recommended)***	*Electrical*	Details ▾
☒ **NIST SP800-161 Supply Chain Risk Management *(Recommended)***	*Supply Chain*	Details ▾
☒ **NIST Special Publication 800-53 Rev 4 App J *(Recommended)***	*Information Technology*	Details ▾
☒ **NIST Special Publication 800-82 Rev 1 *(Recommended)***	*Process Control and SCADA*	Details ▾
☒ **NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1 Rev 1 *(Recommended)***	*Electrical*	Details ▾
☐ CFATS Risk-Based Performance Standards Guide 8-Cyber Tier to SAL	*Chemical, Oil, and Natural Gas*	Details ▾
☐ Control Correlation Identifier Specification V2 release 0.1	*General*	Details ▾
☐ Critical Security Controls Version 6	*Chemical, Oil, and Natural Gas*	Details ▾
☐ Cybersecurity Capability Maturity Model (C2M2) MIL to SAL	*General*	Details ▾
☐ DoD Instruction 8510.01	*DoDI and CNSSI*	Details ▾
☐ Health Insurance Portability and Accountability Act Security Rule	*Health Care*	Details ▾
☐ INGAA Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry	*Chemical, Oil, and Natural Gas*	Details ▾
☐ NEI 08-09 Cyber Security Plan for Nuclear Power Reactors	*Nuclear*	Details ▾
☒ NERC CIP-002 through CIP-009 Rev 3	*Electrical*	Details ▾
☐ NIST Special Publication 800-171	*General*	Details ▾
☐ NIST Special Publication 800-53 Rev 3	*Information Technology*	Details ▾
☒ NIST Special Publication 800-53 Rev 3 App I	*Process Control and SCADA*	Details ▾
☐ NIST Special Publication 800-53 Rev 4	*Information Technology*	Details ▾
☒ NIST Special Publication 800-82	*Process Control and SCADA*	Details ▾
☒ NIST Special Publication 800-82 Rev 2	*Process Control and SCADA*	Details ▾
☒ NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1	*Electrical*	Details ▾
☐ NRC Regulatory Guide 5.71	*Nuclear*	Details ▾
☐ TSA Pipeline Security Guidelines April 2011	*Chemical, Oil, and Natural Gas*	Details ▾



Access Control

Access Agreements

Do you have any access agreements (formal or informal) for third party access to your system? Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, operational or service level agreements and conflict-of-interest agreements.

○ Yes ● No ○ Not Applicable ☐ Override

1 Are periodic reviews conducted of existing authorized physical and electronic access permissions to ensure they are current? *(Req #: AC-2, CIP-004-5.1 R4, AC-2-1)* NO

2 Are appropriate agreements finalized before access is granted, including for third parties and contractors? *(Req #: SG.PS-6-A, SG.PS-6)* NO

3 Are access agreements periodically reviewed and updated? *(Req #: CA-3, SG.PS-6-A, SG.PS-6)* NO

4 Are formal contractual and confidentiality agreements established for the exchange of information and software between the organization and external parties? *(Req #: CA-3, SG.ID-4-A, SG.ID-4)* NO

Access Control for Portable and Mobile Devices

5 Does the organization control the use of personally owned and removable media in the Smart Grid system? *(Req #: SG.AC-17-2, SG.AC-17 1)*

● Yes
○ No
○ Not Applicable
○ Alternative Response

Supplemental Information

Specially configured mobile devices include computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel to locations that the organization determines to be of significant risk, include examining the device for signs of physical tampering and purging/reimaging the hard disk drive.

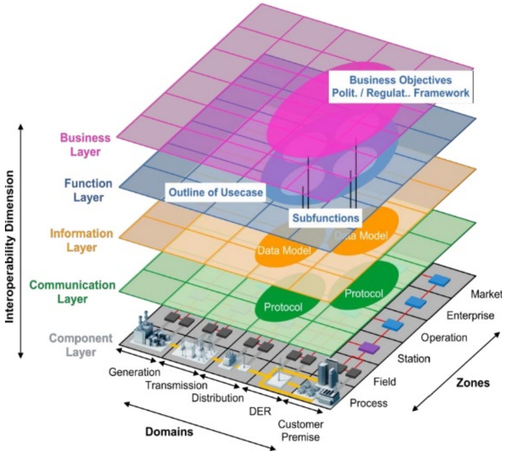
Read more...

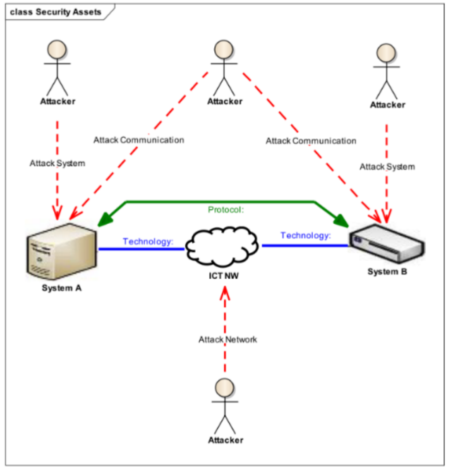
▸ View details and resources or add comments...

☐ Mark For Review

Access Enforcement

- ***Modeling approach**: a system model is constructed using a standard modeling language (i.e. UML) also describing the possible vulnerabilities and sources of risk directly connected to the elements of the system.*





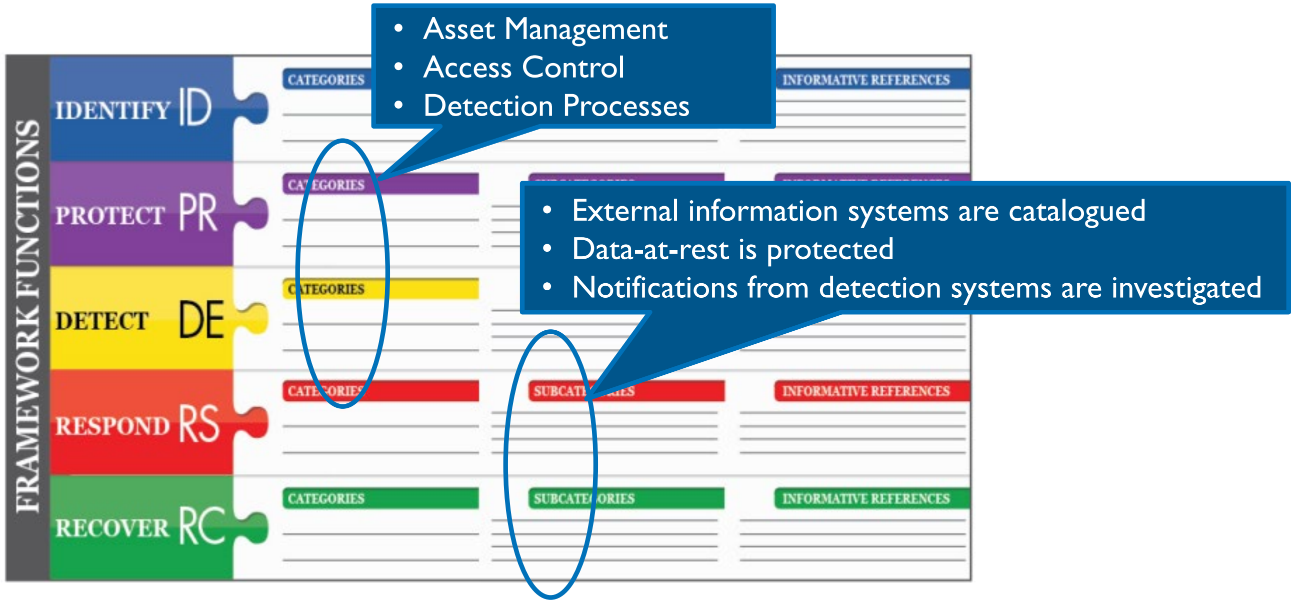
Sources:

- **CSET** (U.S. Department of Homeland Security)
- **SGAM Toolbox** (UML Language)

CESI Shaping a Better Energy Future
EnerNex A CESI Company

© 2021 EnerNex. All Rights Reserved.

***Cybersecurity Procedures**: deploy risk assessment outcomes in the operating process*



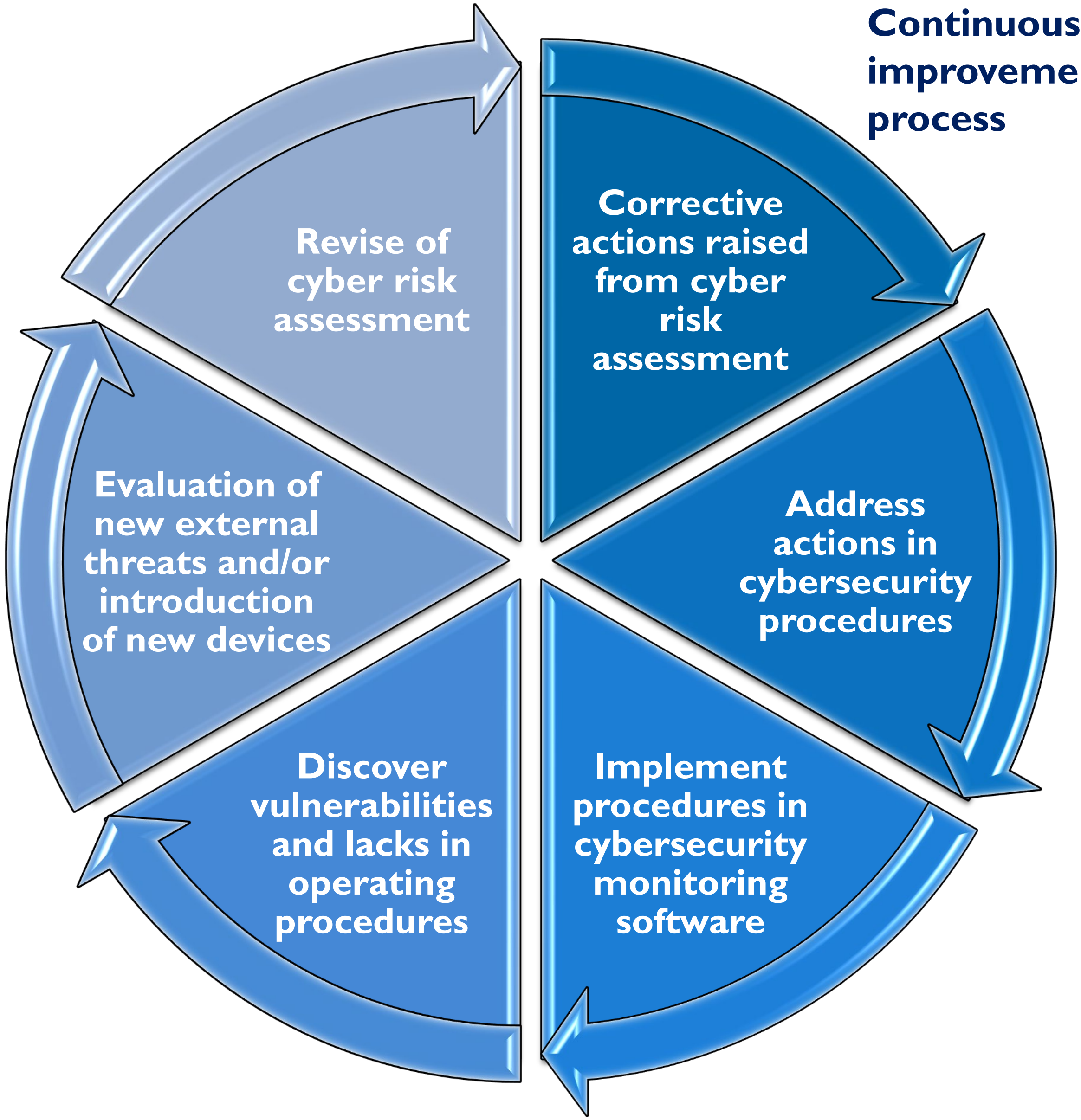
- Asset Management
- Access Control
- Detection Processes

- External information systems are catalogued
- Data-at-rest is protected
- Notifications from detection systems are investigated

- ***Functions*** *organize basic cybersecurity activities at their highest level.*
- ***Categories*** *are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities.*
- ***Subcategories*** *further divide a Category into specific outcomes of technical and/or management activities.They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category.*
- ***Informative References*** *are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory.*

Source: NIST - CyberSecurity Framework, January 2017

Continuous improvement process

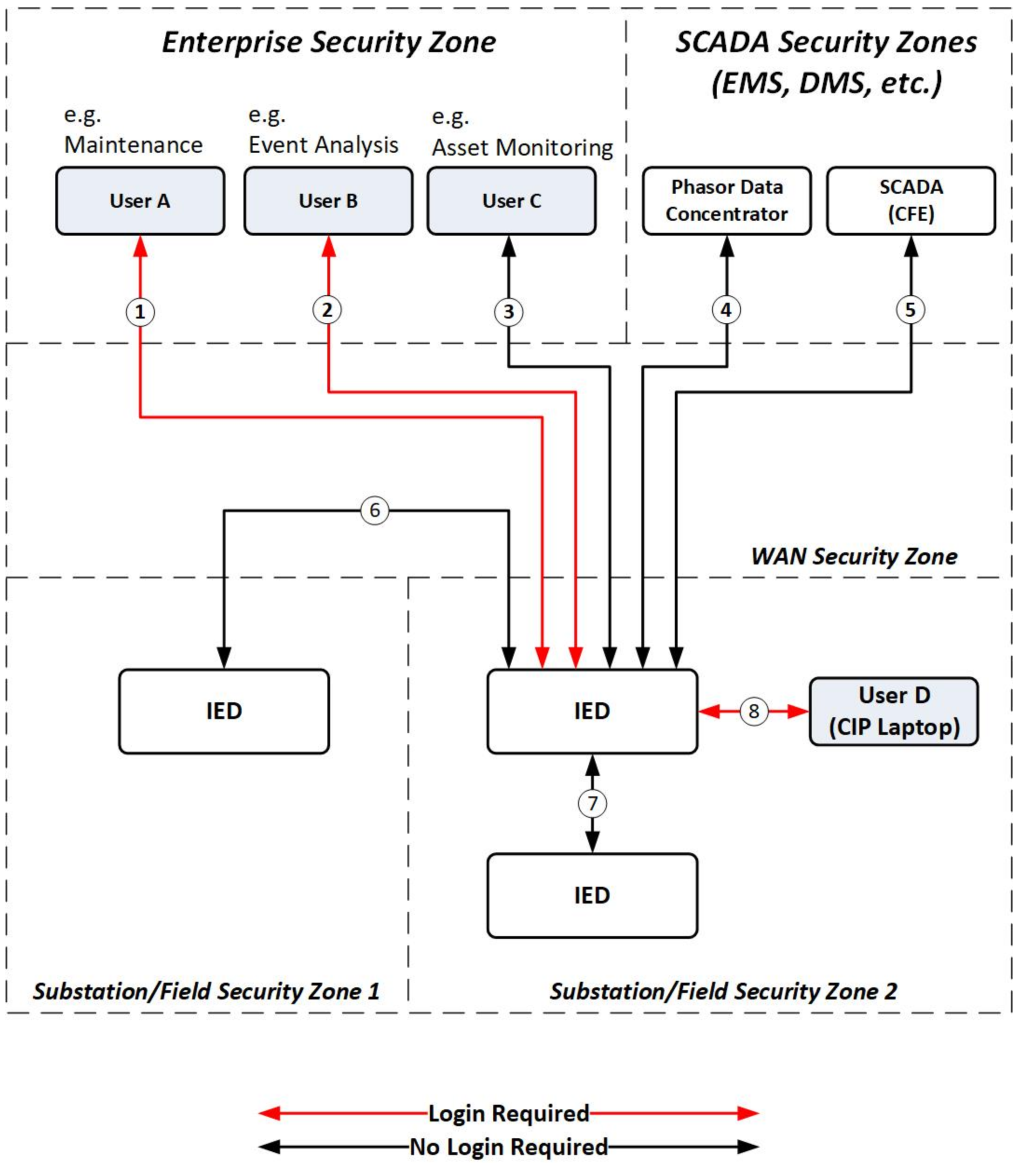

Revise of cyber risk assessment
Corrective actions raised from cyber risk assessment
Address actions in cybersecurity procedures
Implement procedures in cybersecurity monitoring software
Discover vulnerabilities and lacks in operating procedures
Evaluation of new external threats and/or introduction of new devices

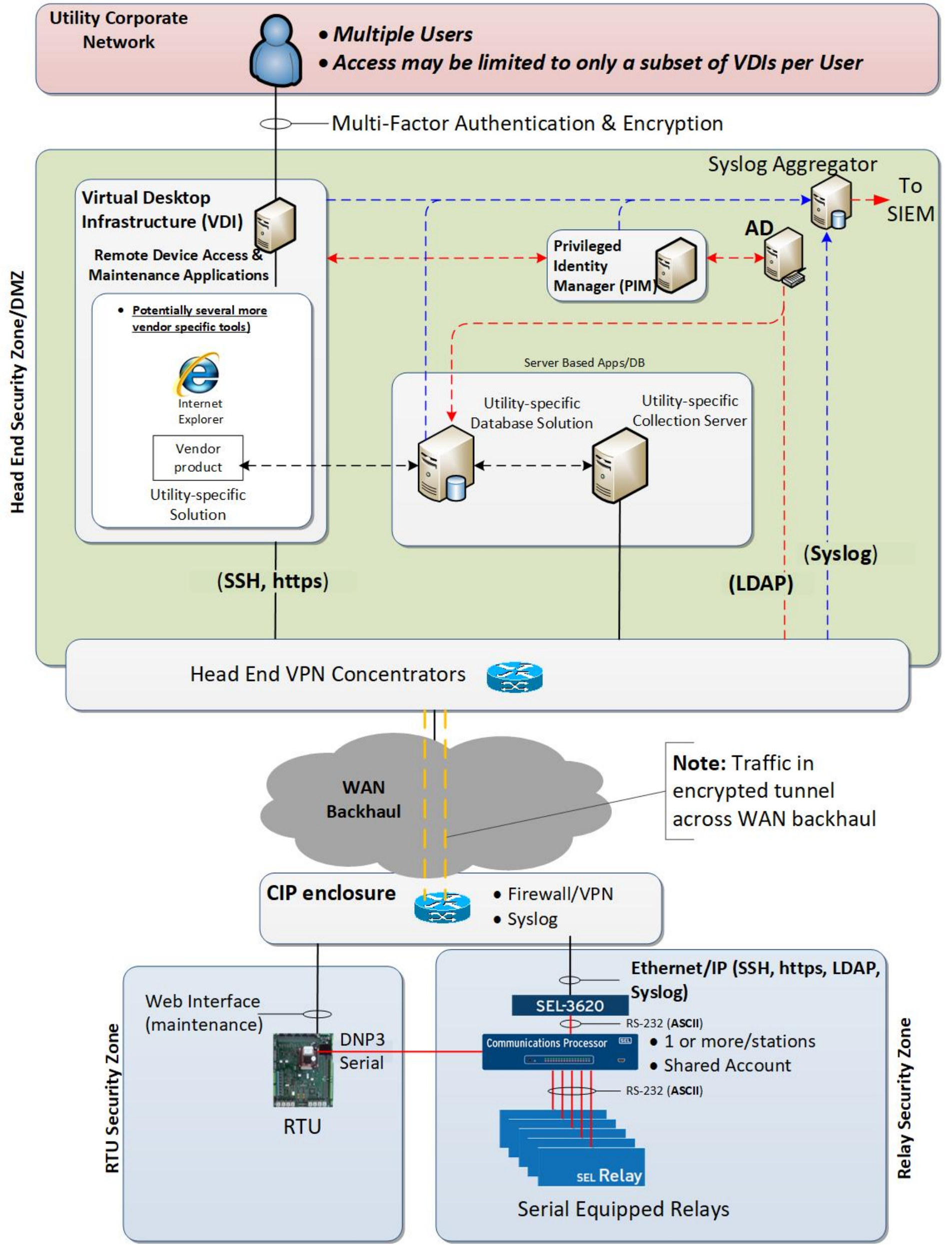
CESI Shaping a Better Energy Future

EnerNex A CESI Company

© 2021 EnerNex. All Rights Reserved. www.enernex.com

Cybersecurity Architecture Zones



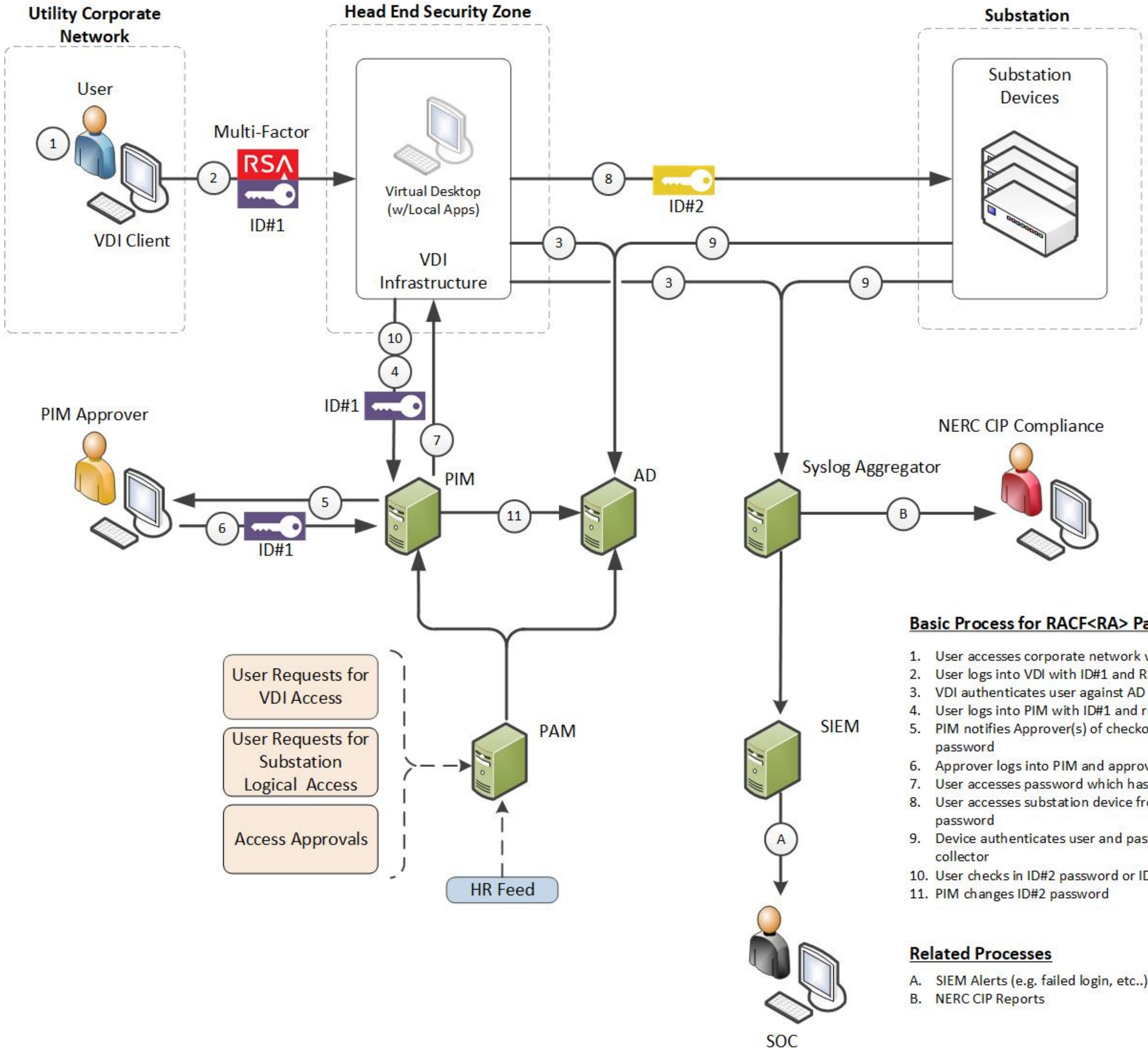

Utility Corporate Network
• Multiple Users
• Access may be limited to only a subset of VDIs per User
Multi-Factor Authentication & Encryption
Head End Security Zone/DMZ
Syslog Aggregator
To SIEM
Virtual Desktop Infrastructure (VDI)
Remote Device Access & Maintenance Applications
• Potentially several more vendor specific tools)
Internet Explorer
Vendor product
Utility-specific Solution
Privileged Identity Manager (PIM)
AD
Server Based Apps/DB
Utility-specific Database Solution
Utility-specific Collection Server
(Syslog)
(SSH, https)
(LDAP)
Head End VPN Concentrators
WAN Backhaul
Note: Traffic in encrypted tunnel across WAN backhaul
CIP enclosure
• Firewall/VPN
• Syslog
RTU Security Zone
Web Interface (maintenance)
DNP3 Serial
RTU
Ethernet/IP (SSH, https, LDAP, Syslog)
SEL-3620
RS-232 (ASCII)
Communications Processor
• 1 or more/stations
• Shared Account
RS-232 (ASCII)
SEL Relay
Serial Equipped Relays
Relay Security Zone

CESI Shaping a Better Energy Future

EnerNex A CESI Company

© 2021 EnerNex. All Rights Reserved. www.enernex.com

Cybersecurity Architecture Data Flow for IEDs and Substation Devices



Basic Process for RACF<RA> Password Checkout and Use

1. User accesses corporate network with ID#1
2. User logs into VDI with ID#1 and RSA
3. VDI authenticates user against AD and sends logs to Log collector
4. User logs into PIM with ID#1 and requests checkout of ID#2 password
5. PIM notifies Approver(s) of checkout request of User's assigned ID#2 password
6. Approver logs into PIM and approves User's PIM checkout request
7. User accesses password which has been approved for checkout in PIM
8. User accesses substation device from VDI and logs in with ID#2 account and password
9. Device authenticates user and password against AD and sends logs to Log collector
10. User checks in ID#2 password or ID#2 password auto expires after 8 hours
11. PIM changes ID#2 password

Related Processes

A. SIEM Alerts (e.g. failed login, etc..)
B. NERC CIP Reports

CESI
Shaping a Better Energy Future

EnerNex
A CESI Company

© 2021 EnerNex. All Rights Reserved. www.enernex.com

CESI

Shaping a Better Energy Future

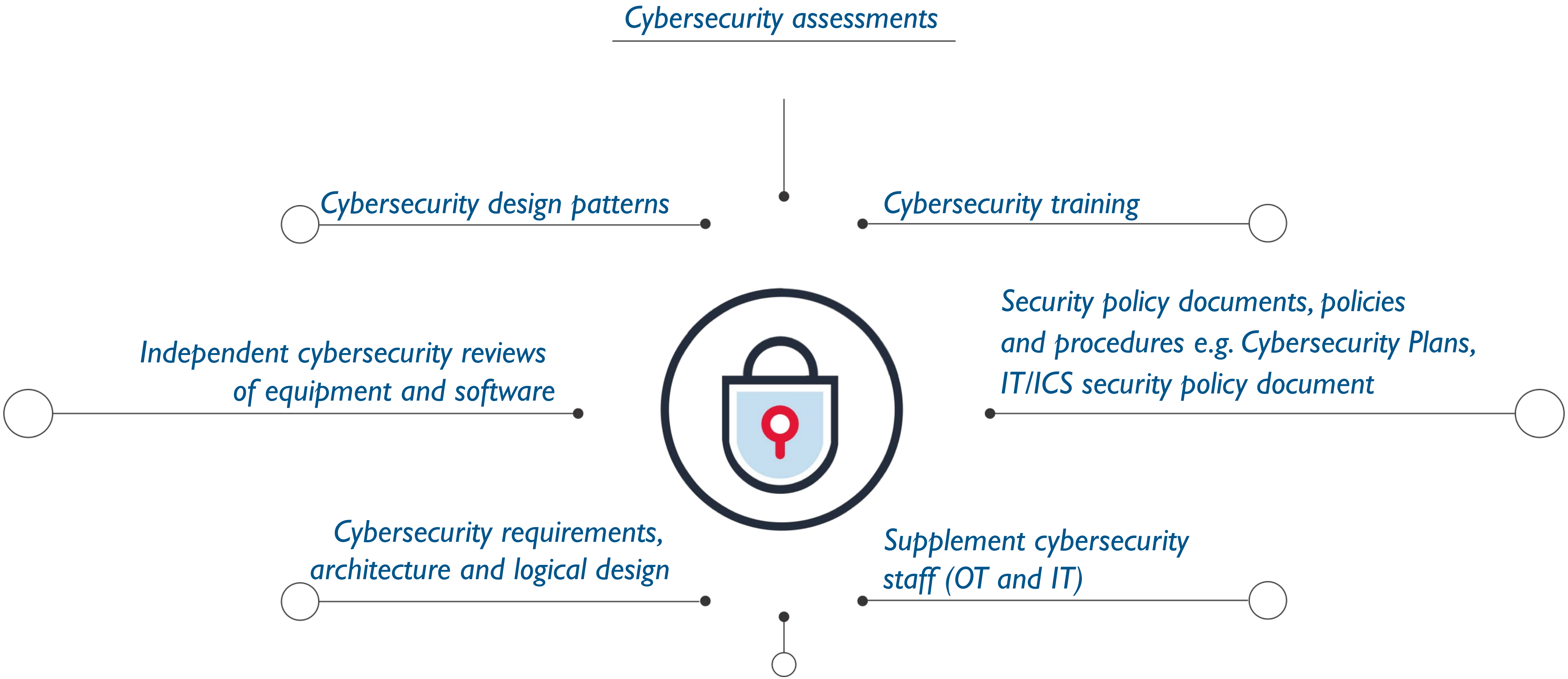
EnerNex

A CESI Company

5. CYBERSECURITY OFFERINGS

© 2021 EnerNex. All Rights Reserved. www.enernex.com

Our Cybersecurity Offerings



Cybersecurity assessments

Cybersecurity design patterns

Cybersecurity training

Independent cybersecurity reviews of equipment and software

Security policy documents, policies and procedures e.g. Cybersecurity Plans, IT/ICS security policy document

Cybersecurity requirements, architecture and logical design

Supplement cybersecurity staff (OT and IT)

© 2021 EnerNex. All Rights Reserved. www.enernex.com

CESI

Shaping a Better Energy Future

EnerNex

A CESI Company

Q&A

© 2021 EnerNex. All Rights Reserved. www.enernex.com

CESI

Shaping a Better Energy Future

cesi.it

EnerNex

A CESI Company

enernex.com

Thank you for attending! Keep in touch with us.