Cybersecurity

For Large Electrical Power Systems

IEEE TN Chapter
October 2021

Agenda

- Cybersecurity Basics
- Microgrids as an Example of a Large Electrical System
- Cybersecurity Principles Applied to a Microgrid
- Q&A

Cyber on an IT System vs Cyber on an OT System

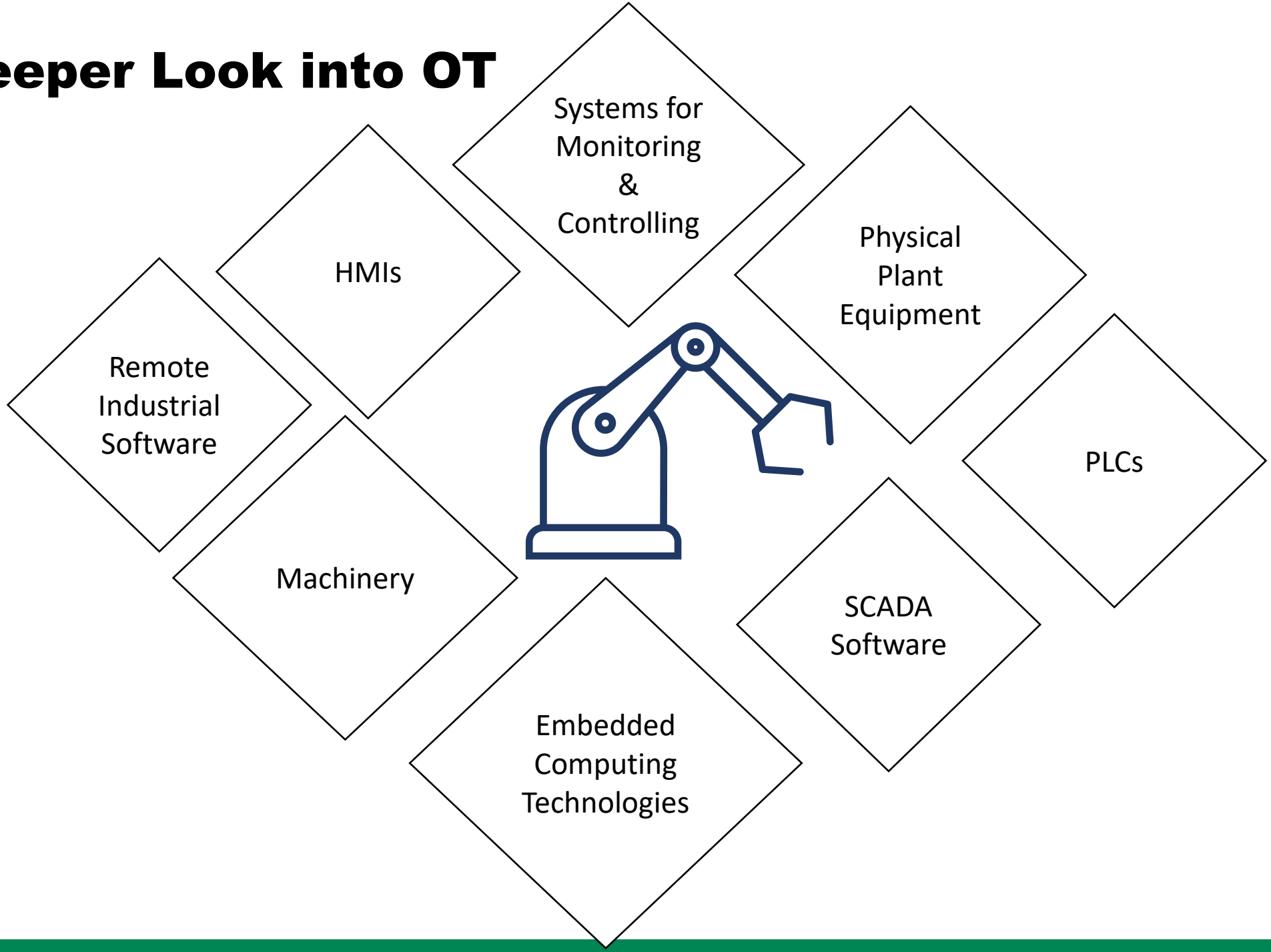
IT systems emphasis: confidentiality

- Enterprise information systems network
- ERP, CRM, email, financial systems
- Business-supporting applications
- Mature environment / routine patching & updates

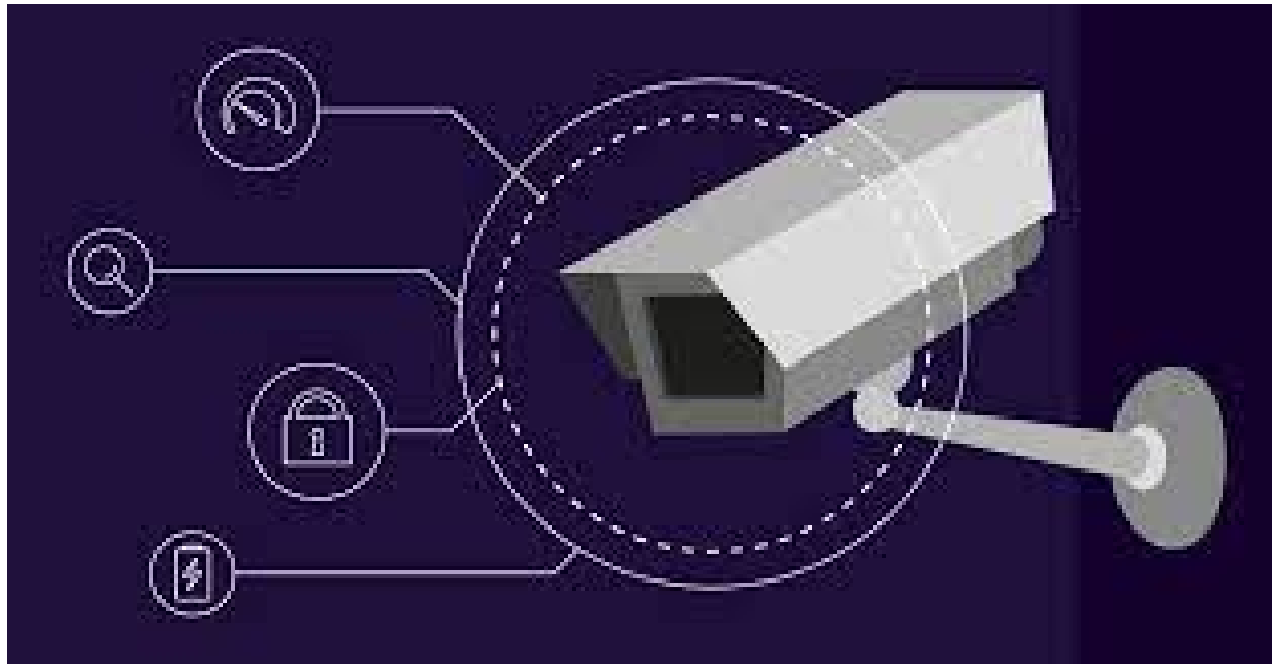
OT systems emphasis: availability

- Building management systems (BMS)
- Energy control (lights and efficiency)
- Environmental (heating, ventilation and air conditioning (HVAC)
- Security and safety (CCTV, access control, fire suppression)
- Ancillary systems (elevators, shade control, exterior lighting)
- PLC, SCADA, ICS, IIoT, HMI
- The *"forgotten network" / rare patches & updates*

A Deeper Look into OT

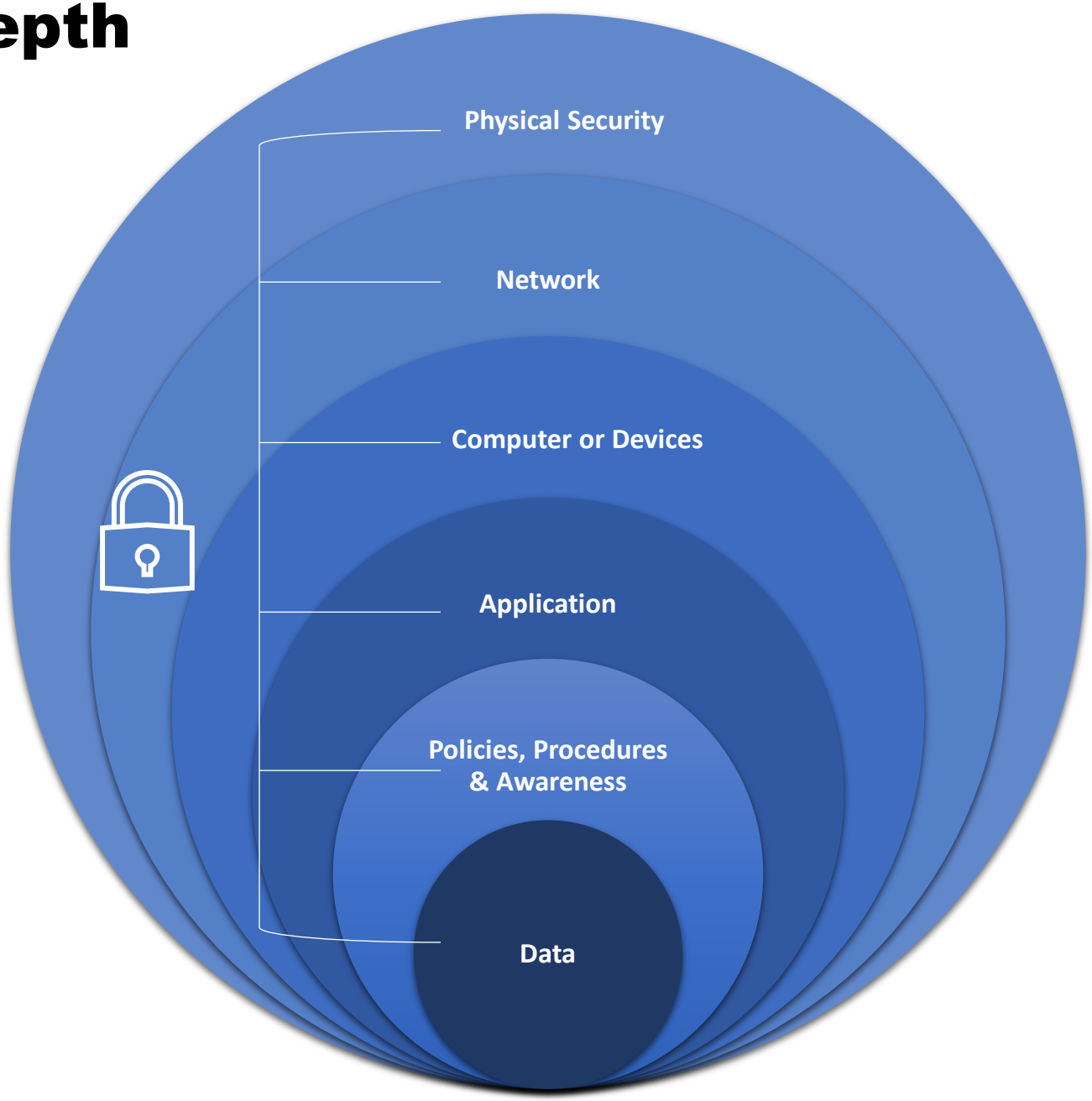


Monitoring & Physical Security on OT Systems



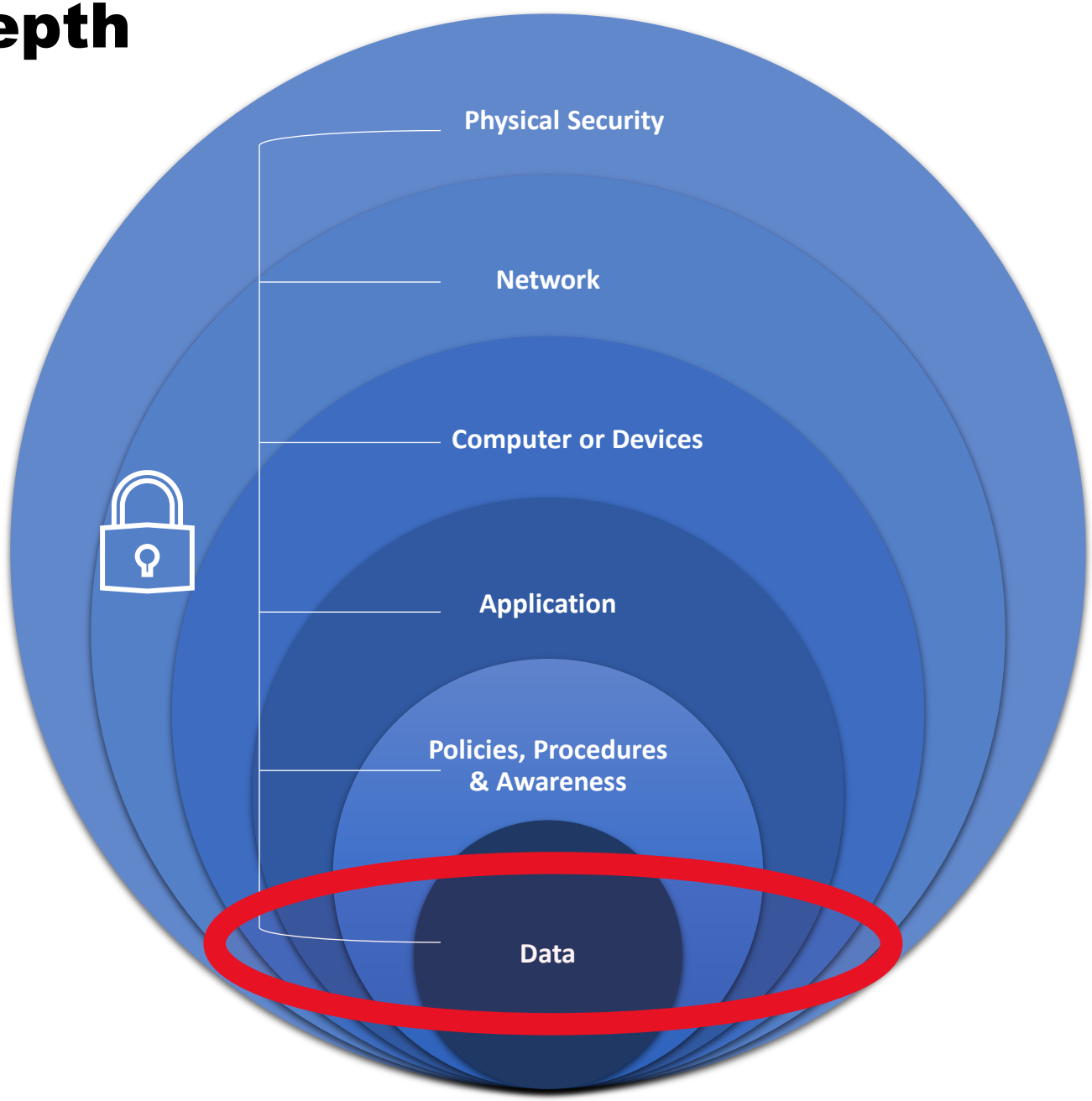
Defense in Depth

- What is it?



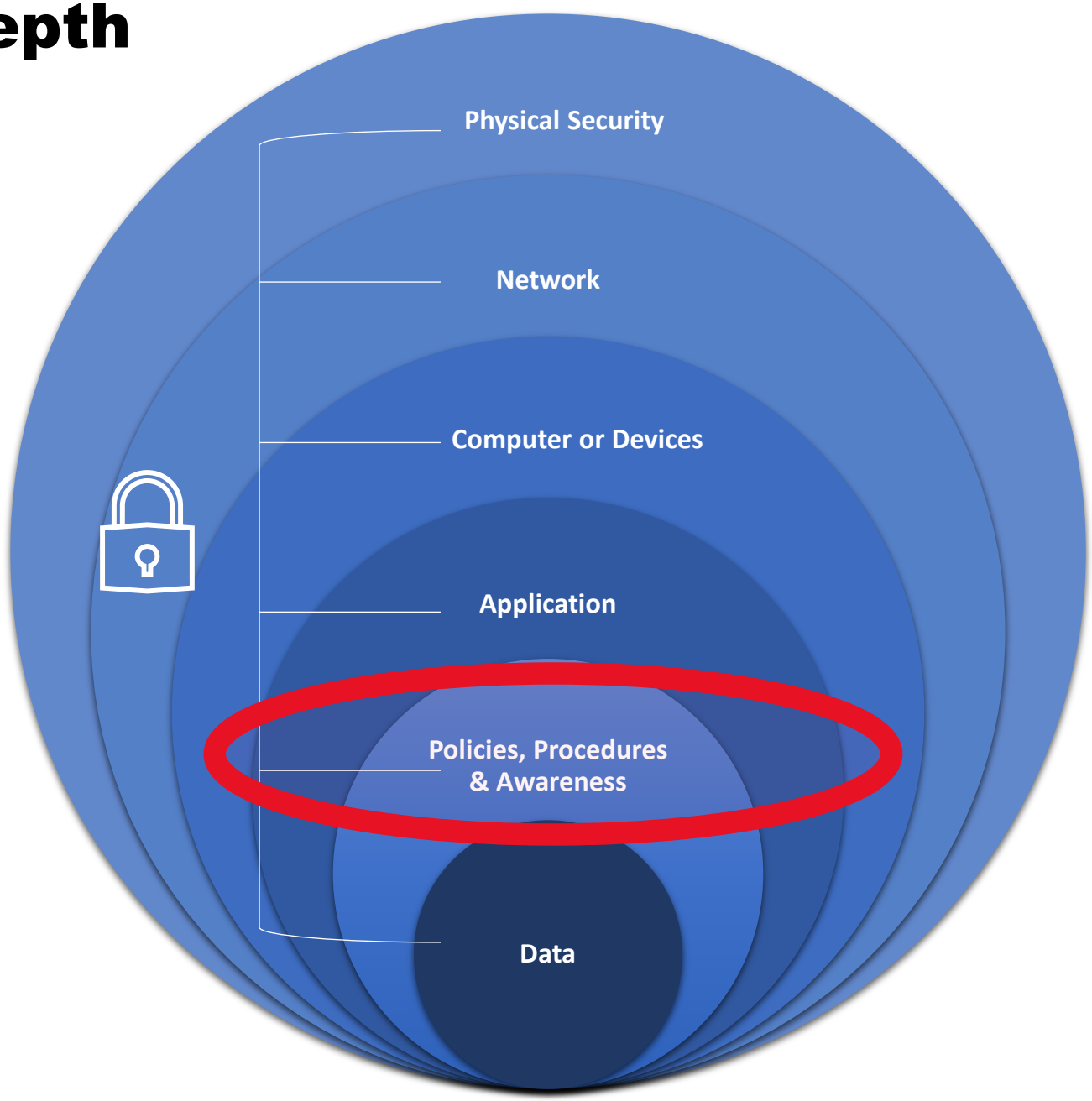
Defense in Depth

- What is it?



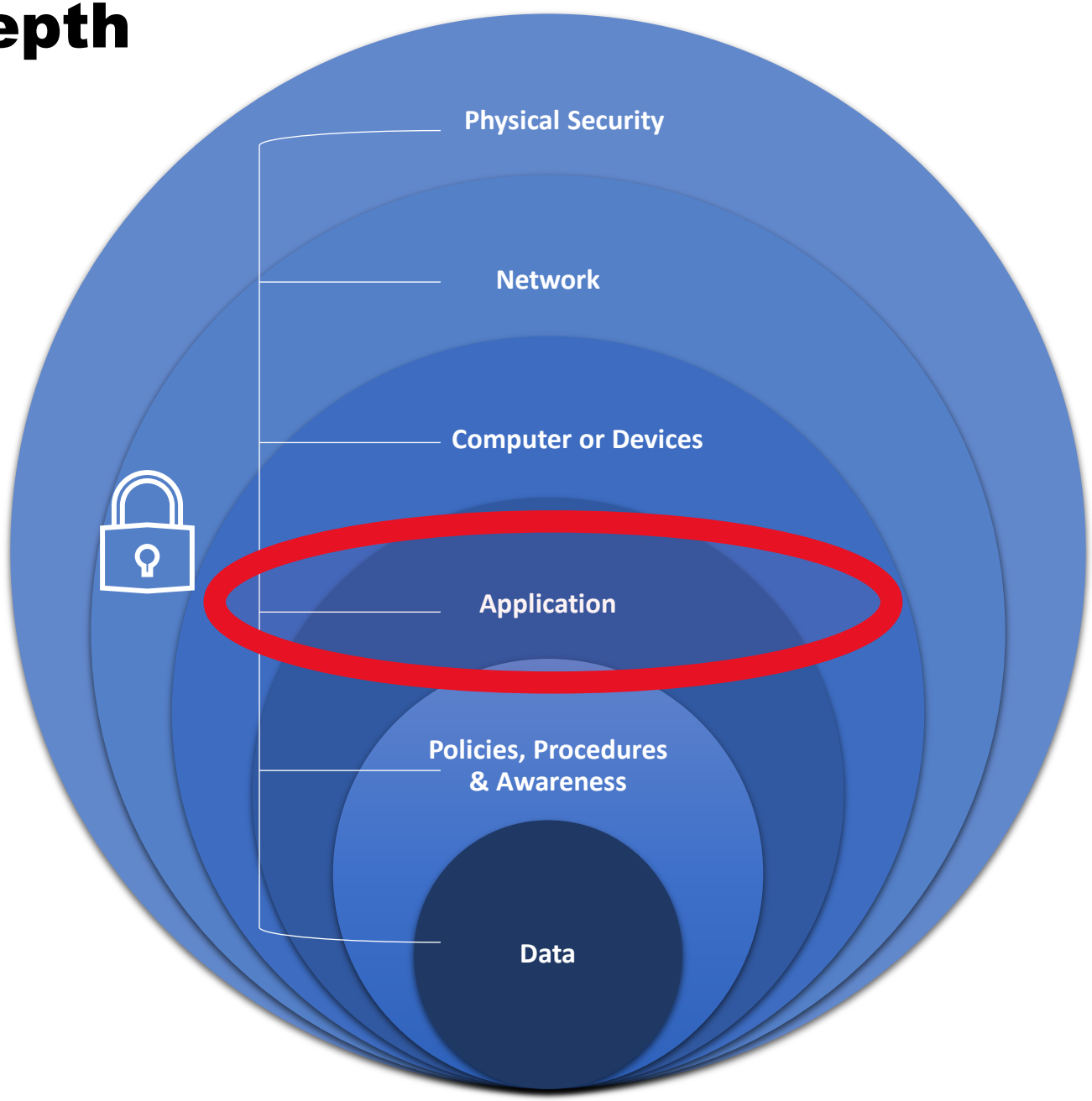
Defense in Depth

- What is it?



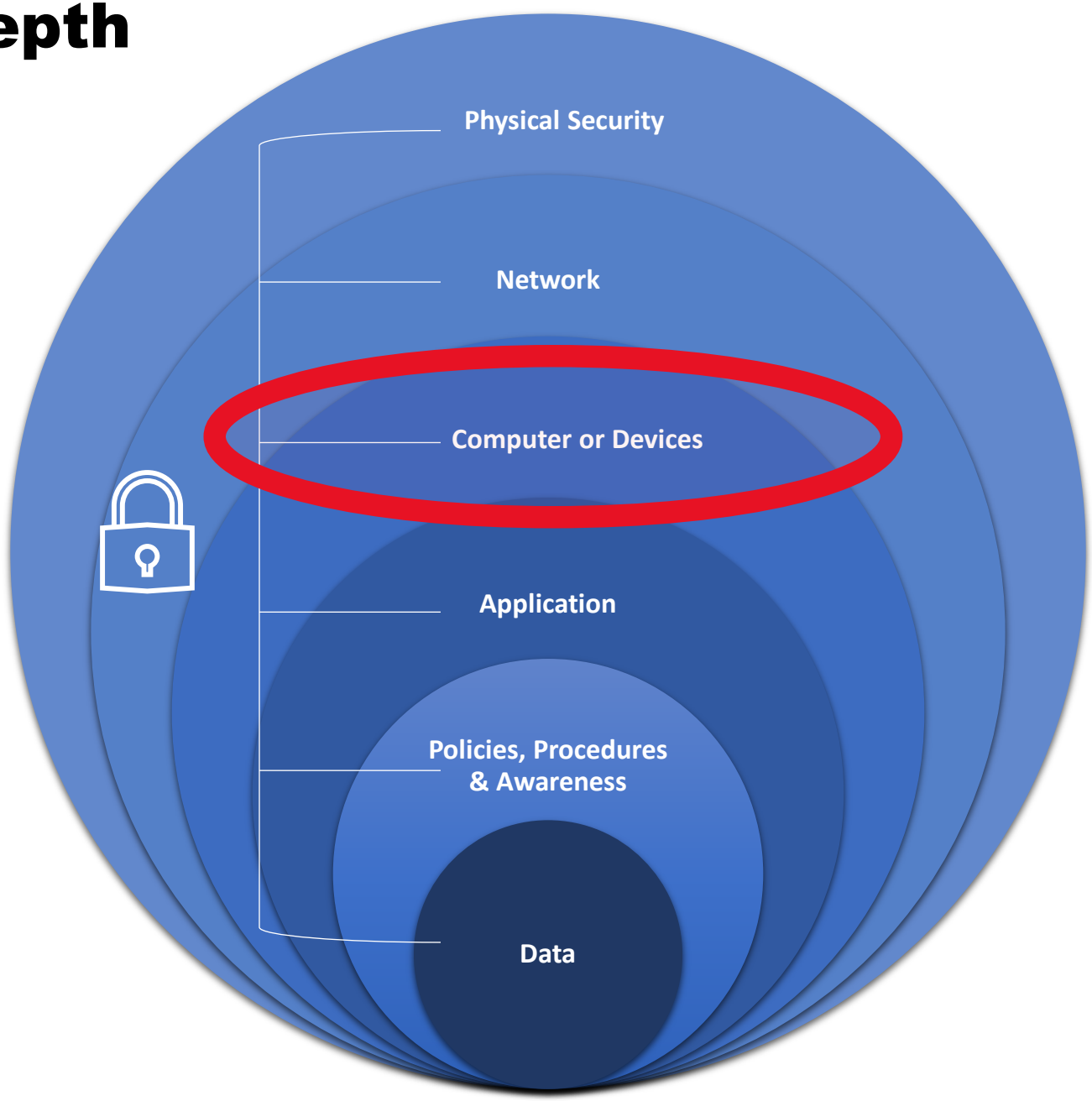
Defense in Depth

- What is it?



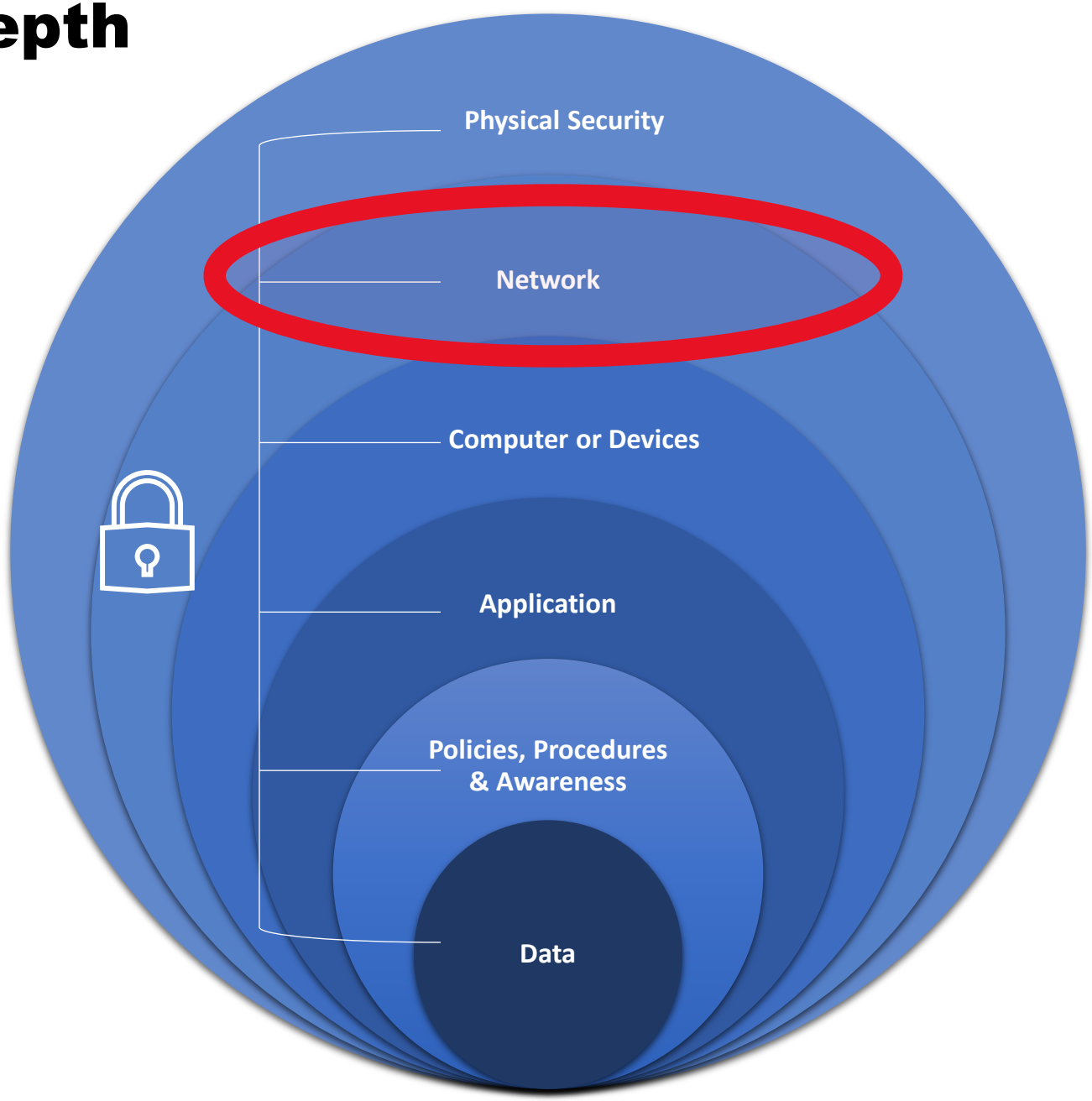
Defense in Depth

- What is it?



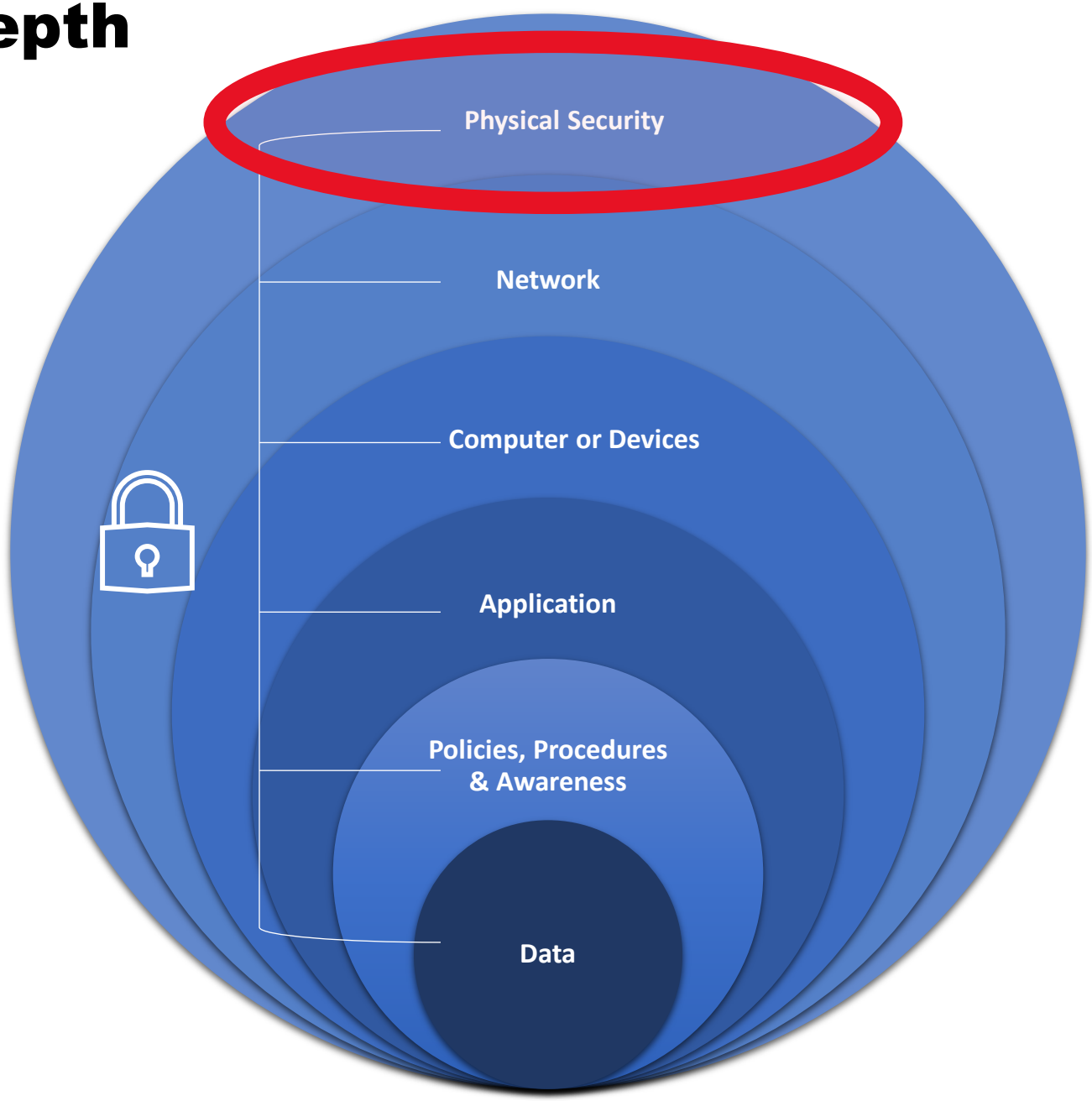
Defense in Depth

- What is it?



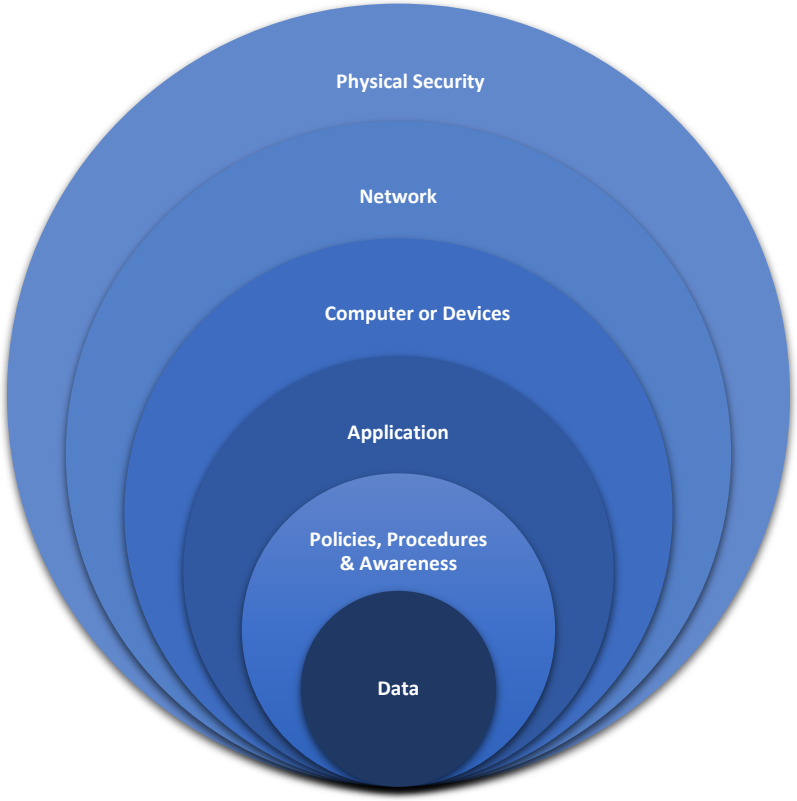
Defense in Depth

- What is it?



System Cybersecurity Design

- Designing the system with Defense in Depth



Device Hardening

What does it mean to “Harden” a computer?

Hardening

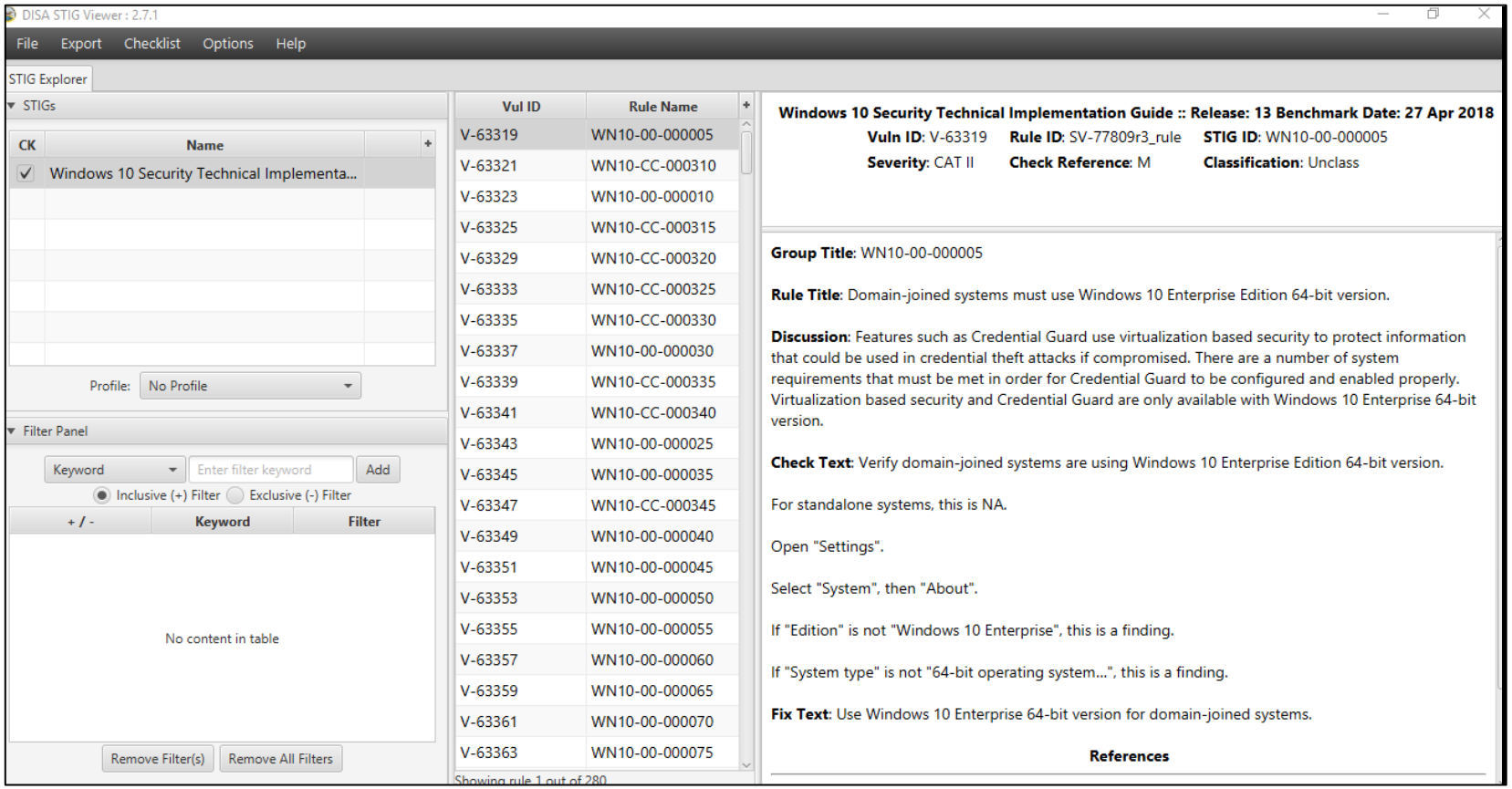
- Attack Surface
- OS Hardening
- BIOS Security
- Disabling Unused Services & Software
- Secure Boot

How Do We Harden a Device

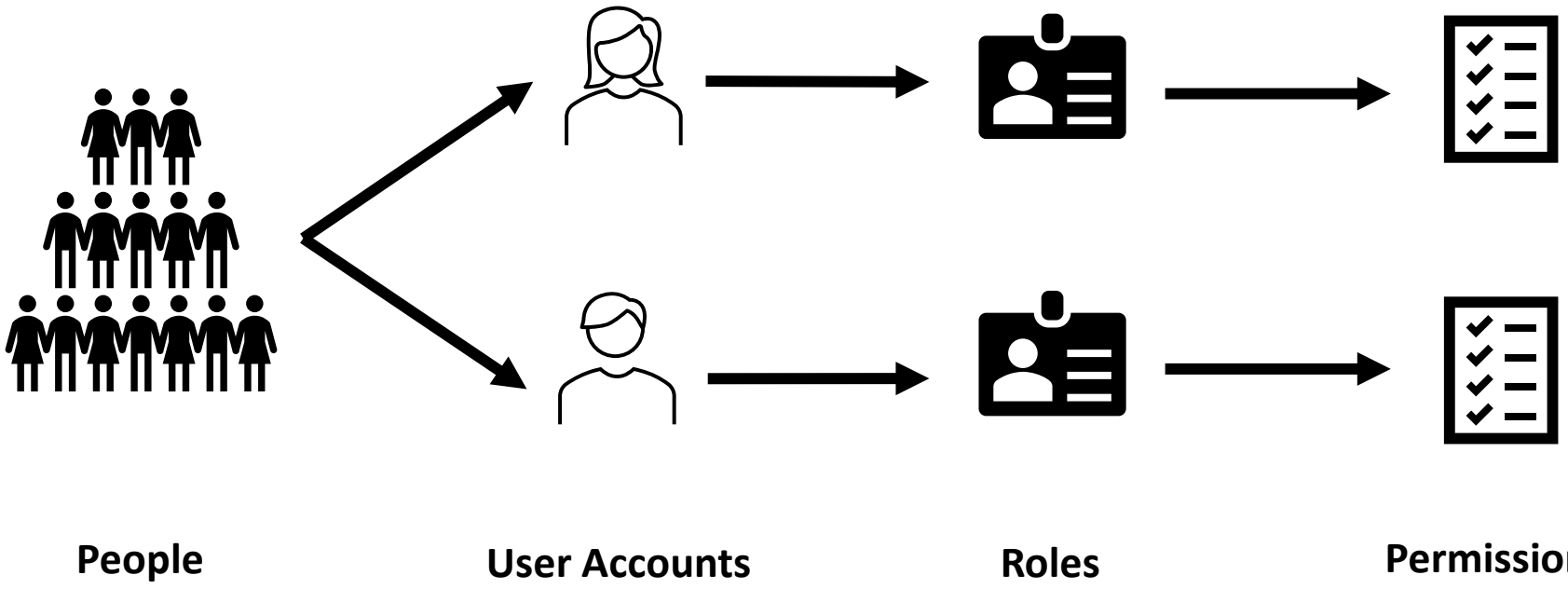
Best Practices

- Complex Passwords
- Disabling unused/default accounts
- Uninstalling unneeded software
- Disabling unneeded services

DISA STIG Viewer



How Do We Harden a Device

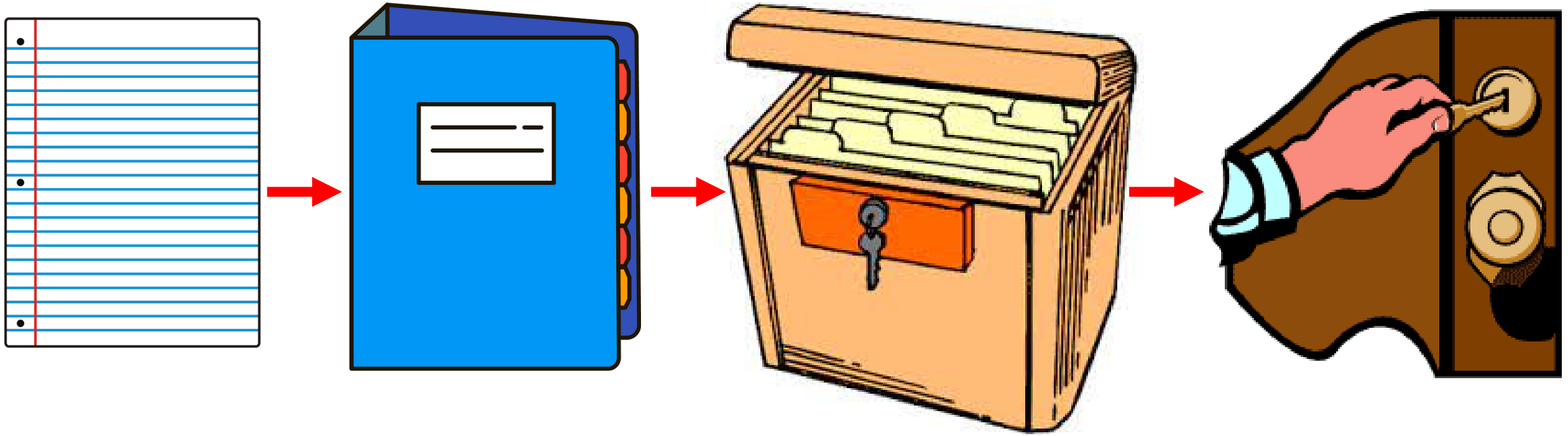


Implementing the principle of least privilege requires you to look at your systems, access methods, and permissions

Now that the device is hardened

Now That the Device is Hardened

DiD can be thought of in terms of "layers" like this piece of paper analogy



Cybersecurity Requirements

- Commercial/Utility, and Federal

Utility Requirements

NERC CIP

- Critical Infrastructure Protection (CIP)
- Bulk Electric System (BES) cyber standards
- Similar groupings as RMF “families”
- Future – Electronic security perimeters, Change Management, Supply Chain Risk

NISTIR 7628

- Smart Grid Cybersecurity
- Guidance for assessing risk, identifying and applying security requirements
- Focus on interconnections as attack vectors

Federal Requirements

Risk Management Framework (RMF)

- Security Categorization
- Security Control (Requirements) Baseline
- Overlays and guidance for “OT”

Unified Facilities Criteria

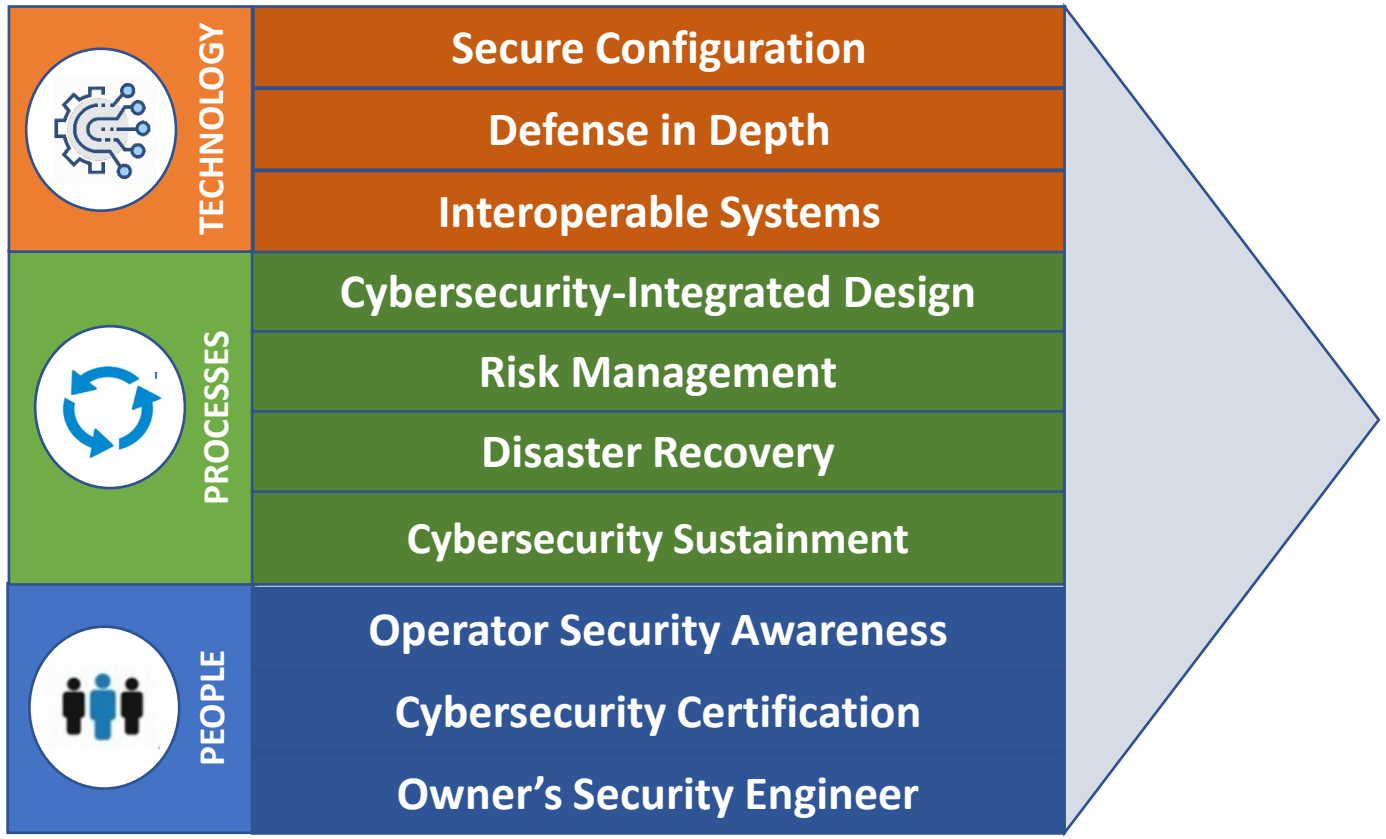
- Cybersecurity guidance for facility-related control systems

Controlled Unclassified Information (CUI)

- DFARS 252.204-7012
- NIST 800-171

Cybersecurity Integration Considerations

- People, Processes, Technology



Secure Systems

Resilient Systems

Cost Savings/ Avoidance

Protection from Unauthorized Access

Uninterrupted Operations

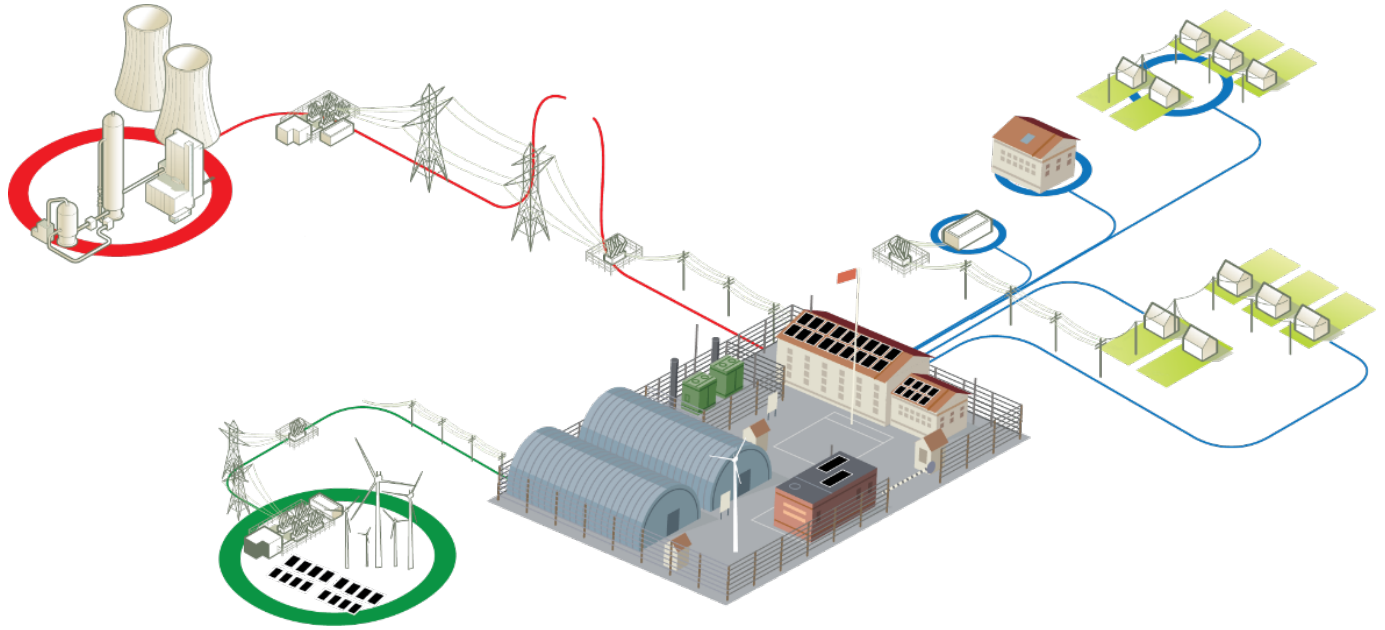
Microgrids as a Case Study

A group of **interconnected loads and distributed energy resources**

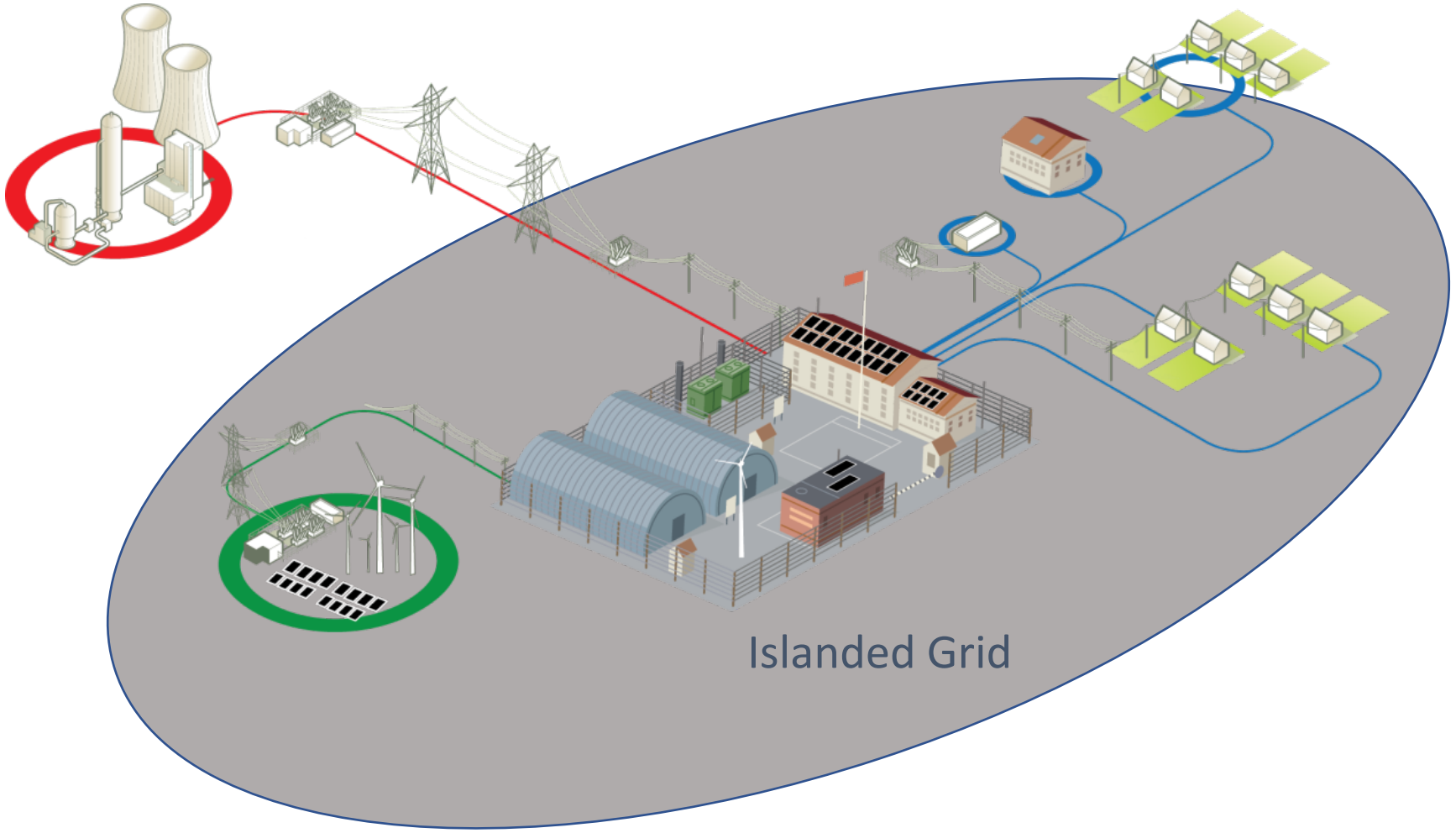
with **clearly defined electrical boundaries**

that acts as a **single controllable entity** with respect to the grid

and can **connect and disconnect from the grid** to enable it to operate in both grid-connected or islanded modes.



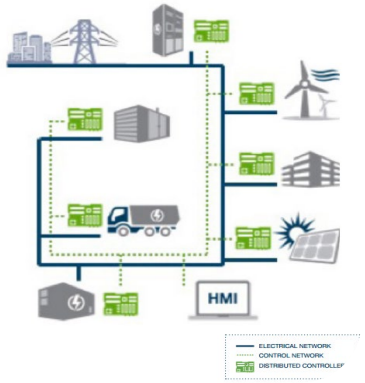
Benefits of a Microgrid



Microgrid Building Blocks

Distributed Energy Resources (DER)

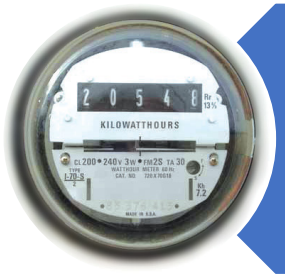
Switching and Protection



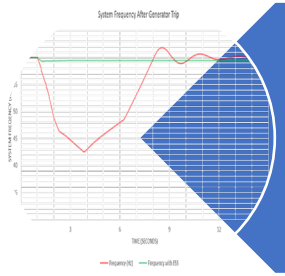
Microgrid Control

Microgrid Building Block: Distributed Energy Resources

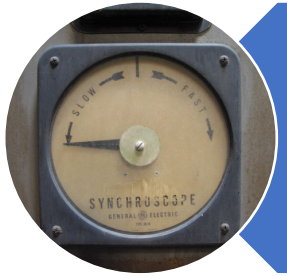
DER Considerations



Power and energy capabilities



Response to system events



Paralleling and interconnection limitations

21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2017 Grid of the Future Symposium

Challenges and Considerations of DER Selection for Microgrid Applications

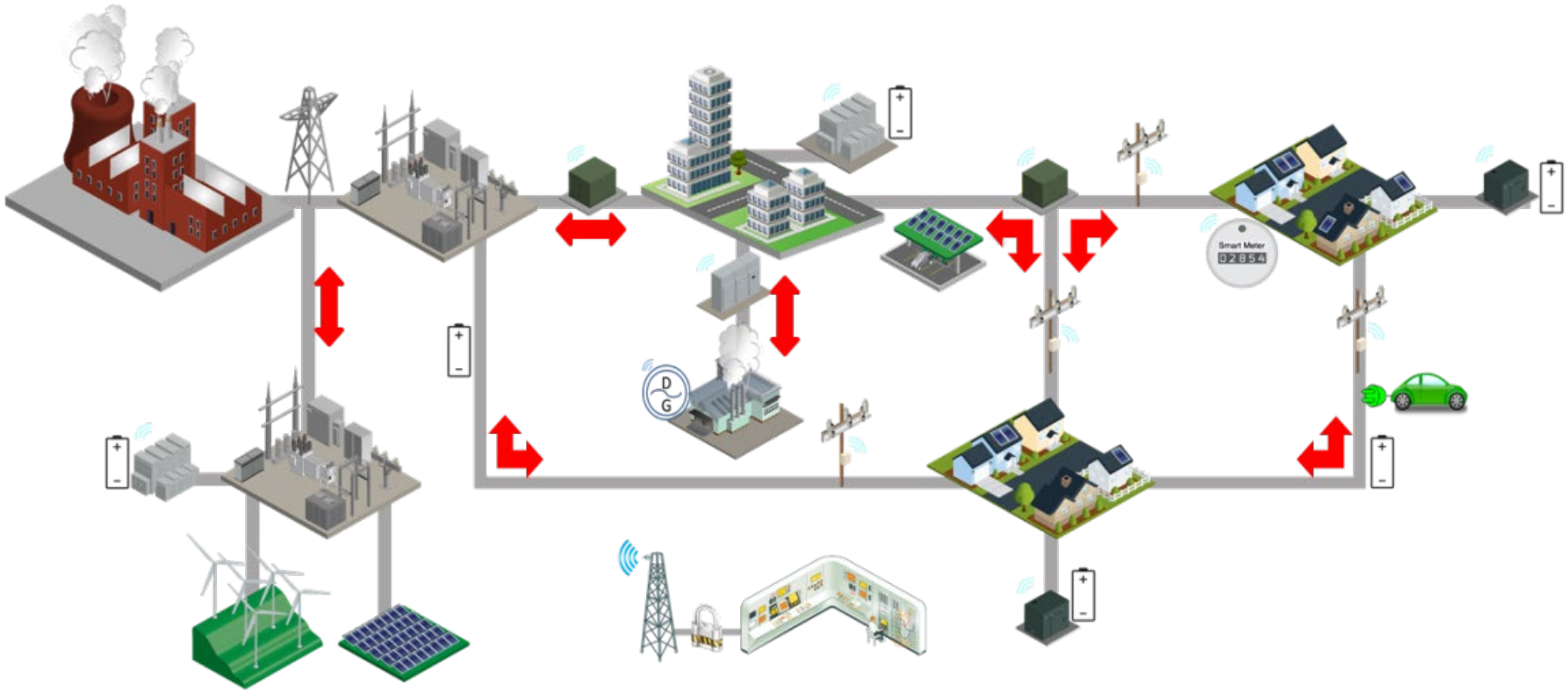
M. HIGGINSON, S. KAMALINIA
S&C Electric Company
USA

SUMMARY

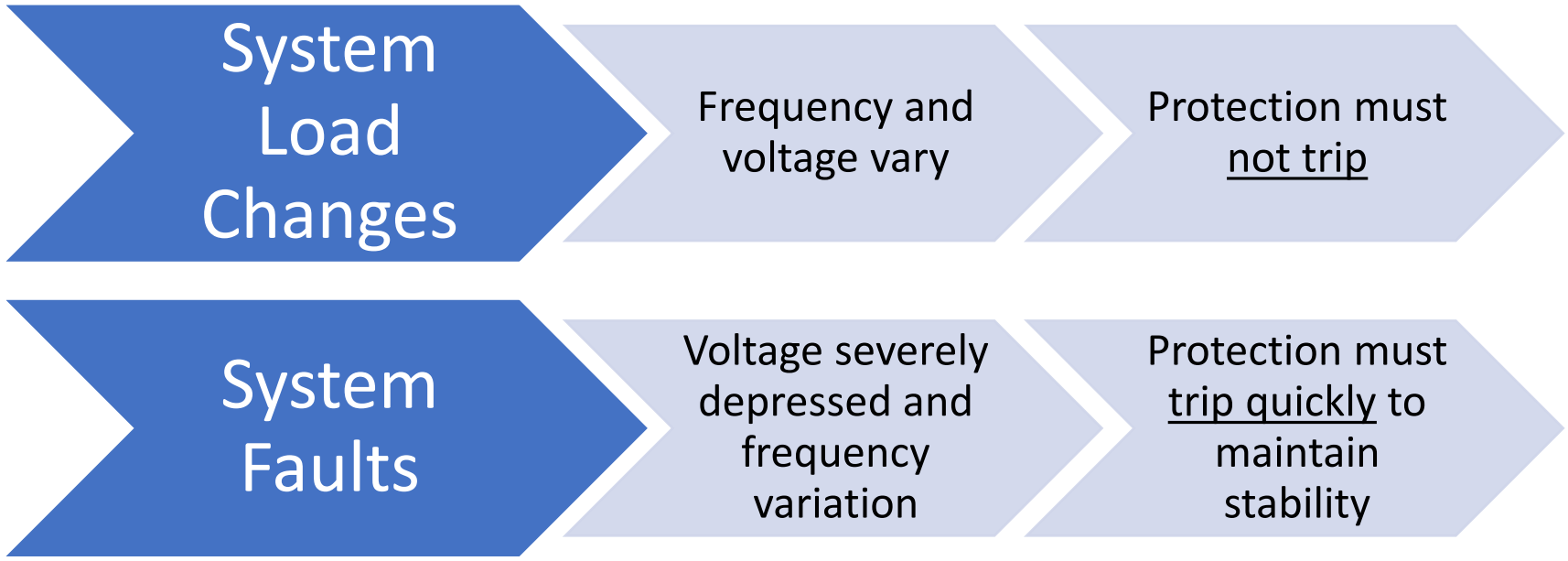
Adoption of Distributed Energy Resources (DERs) in microgrid applications can improve system reliability and power quality while reducing the cost of electricity through on-site generation. When selecting DERs for microgrid applications, several factors need to be considered. This paper will explore many technical considerations and challenges of DER selection based on real-world microgrid experience. Some of these challenges include the power and energy delivery capabilities of resources, steady-state performance, response to load variations, behavior during system faults, paralleling limitations, and power system grounding. In summary, this paper will enumerate challenges that must be considered when selecting DERs for integration in microgrid systems.

Microgrid Building Block: Switching and Protection

Microgrid Building Block: Switching and Protection

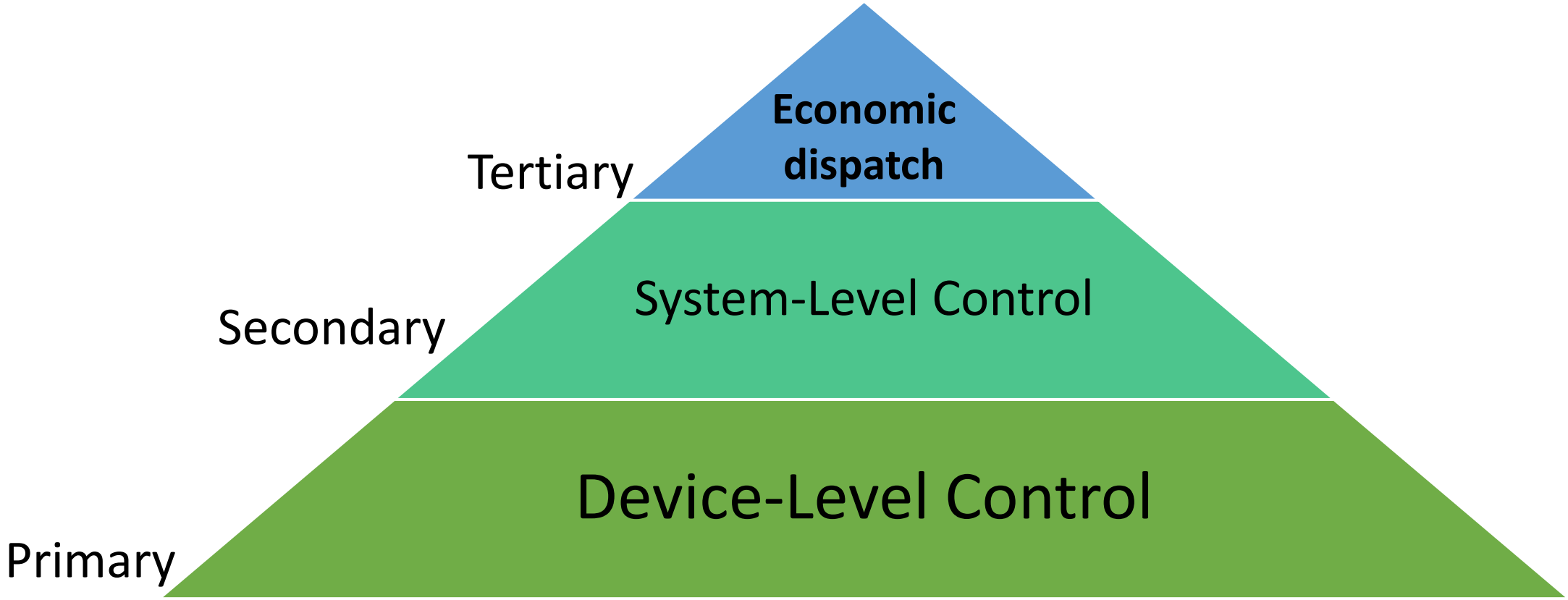


Microgrid Building Block: Switching and Protection



Microgrid Building Block: Control

Tiered Control in Microgrids

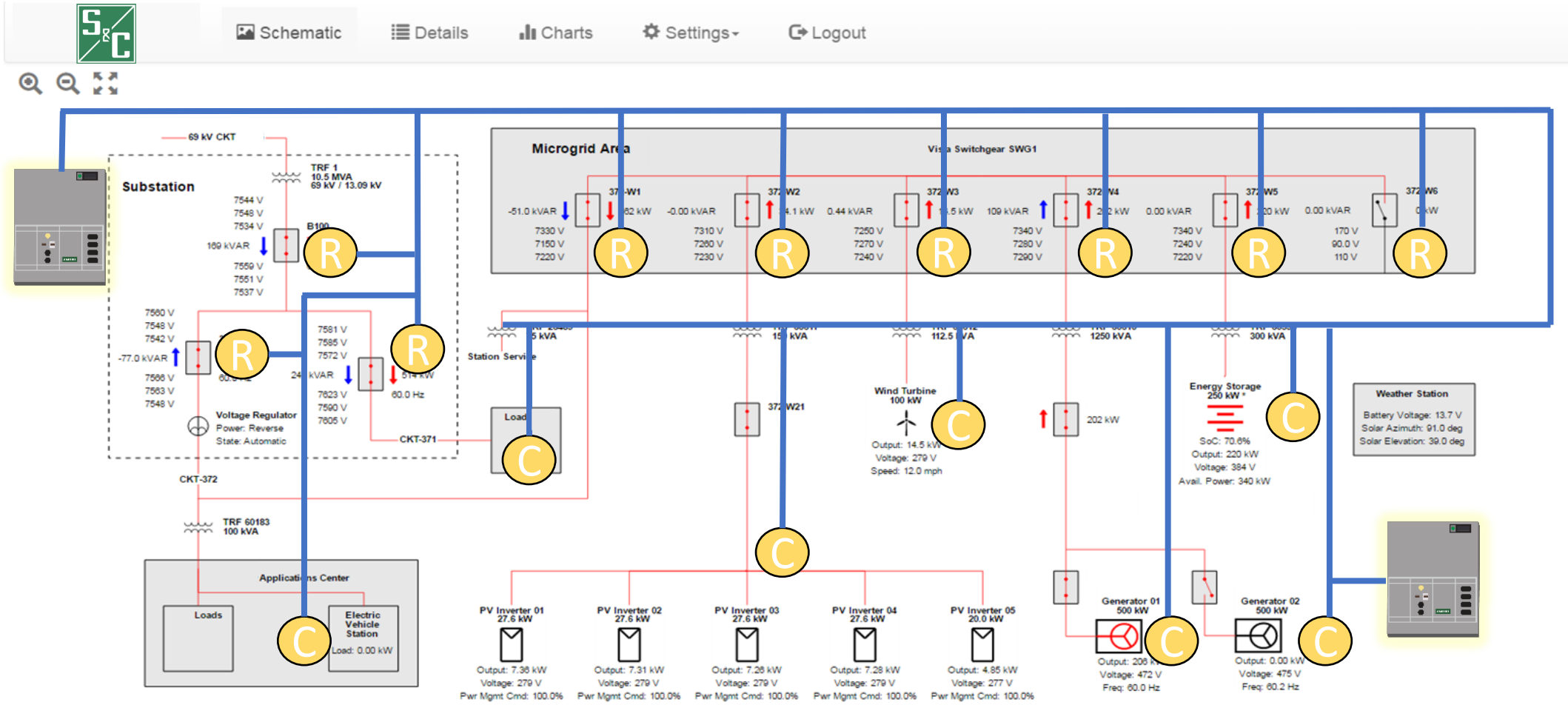


Microgrid Control Visualization

C Local Controller

R Microprocessor Relay

Microgrid Controller



Ameren TAC Microgrid

Ameren TAC Microgrid

- Project Information

Champaign, IL

15 kV POI

Research Loads

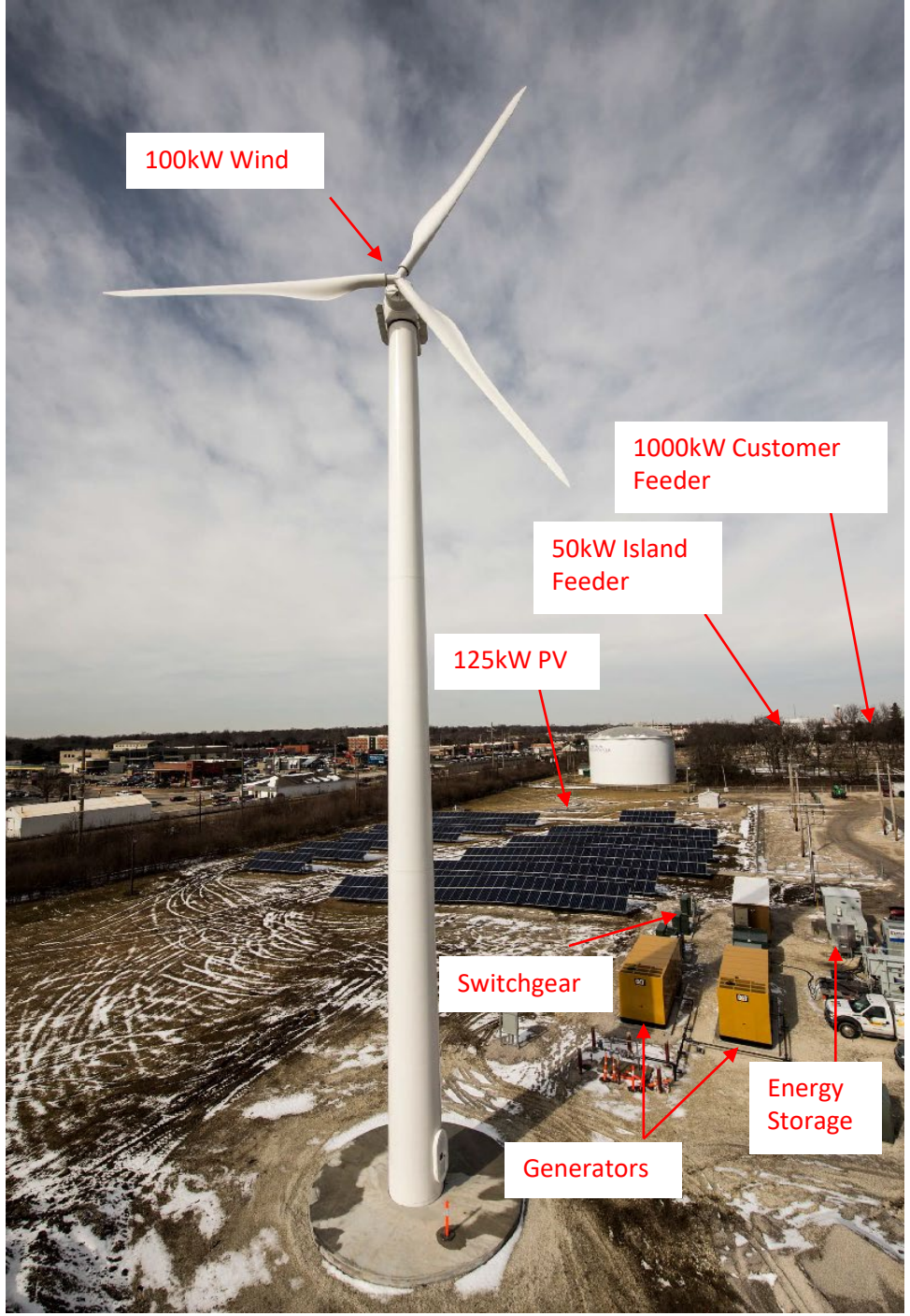
1000 kW Rate-Paying Customer Loads

(2) 500 kW Natural Gas Gens

(1) 250 kW / 500 kWh Li-On Energy Storage

125 kW PV Solar

100 kW Wind



Ameren Project Overview

- Use Cases

- DER Monitoring, Control, & Integration
- DER Optimal Power Flow
- Integrating with existing SCADA System
- Islanding – Synchronous Transition to Island
- Islanding – Synchronous Transition to Grid Tied
- Islanding – Black Start Capability
- Islanding – 100% Renewable Operation
- Volt/VAR Control
- Power Quality
- Demand Response
- EV Integration
- Peak Load Shaving
- Optimal Economic Dispatch
- Storm Preparedness

Ameren TAC Microgrid

- Communication and Control

- Primary:
  - Protective Devices
  - DERs and DER controllers
- Secondary:
  - GridMaster microgrid control system
- Tertiary:
  - Utility ADMS
  - Economic Dispatch

Cybersecurity Design Drivers

- Starts during System Concept & Design

Key Considerations:

1.

Risk Assessment – system and supported loads criticality, interconnections as attack vectors, encryption needs

2.

Network device selection – perimeter security, environment, protocols, network switches, syslog server

3.

Communication options and limitations – geography, cost of media, available protocols

4.

Data visualization & system operations – HMI locations, remote HMIs, Vendor connections, Cyber monitoring

Security Categorization

- Risk Assessment

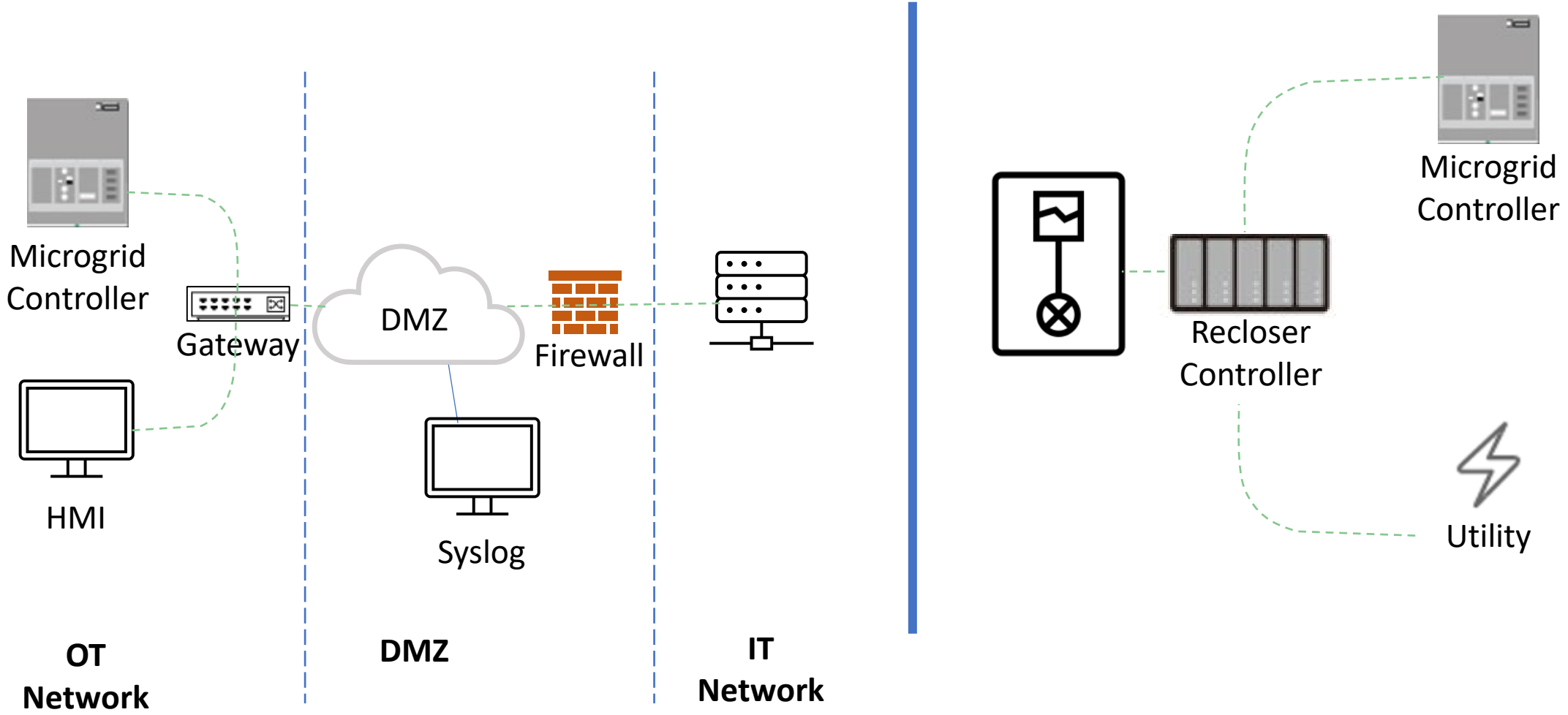
Information Types,
Confidentiality, Integrity,
Availability
Impact Values

Interfaces,
Interconnections,
Load Criticality,
Attack Vectors

Downstream DER &
Endpoint Communications,
Data-in-Transit Protections

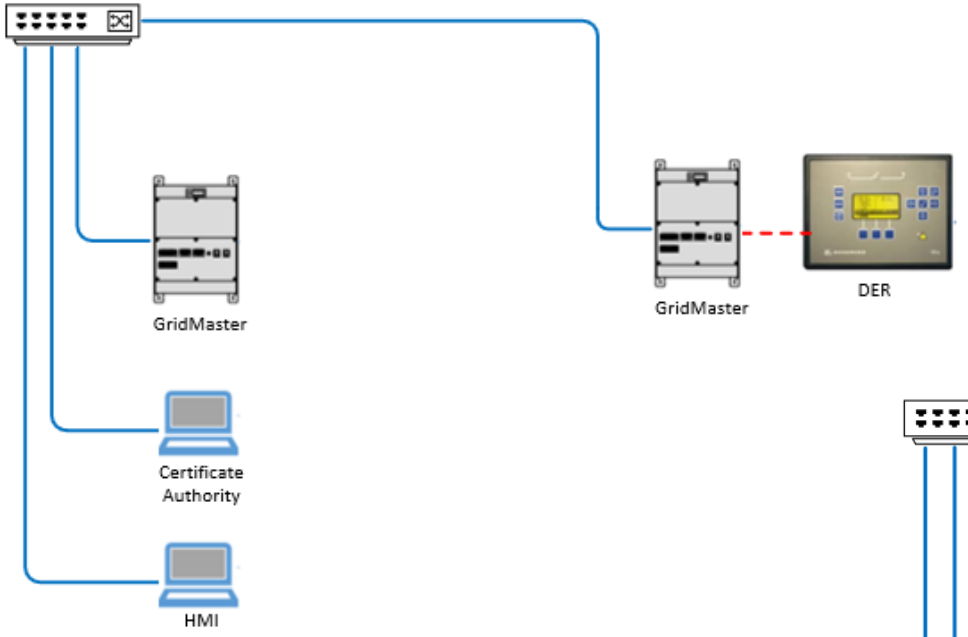
Segregated Communications

- Perimeter and Host-based Protections

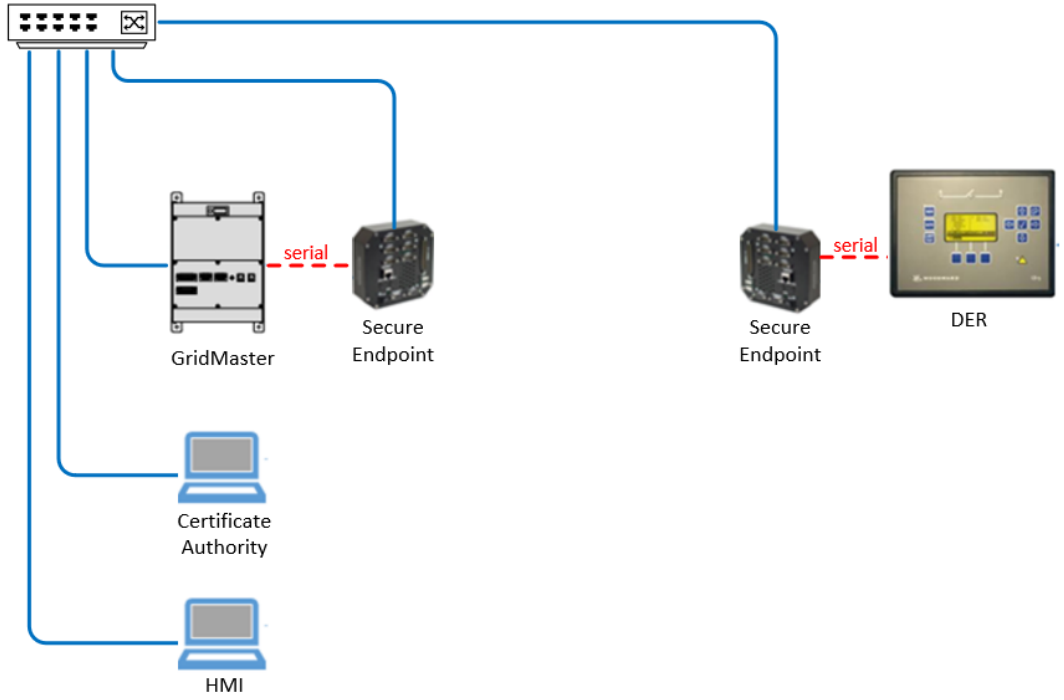


Microgrid DER Security

- Extending encrypted communication paths



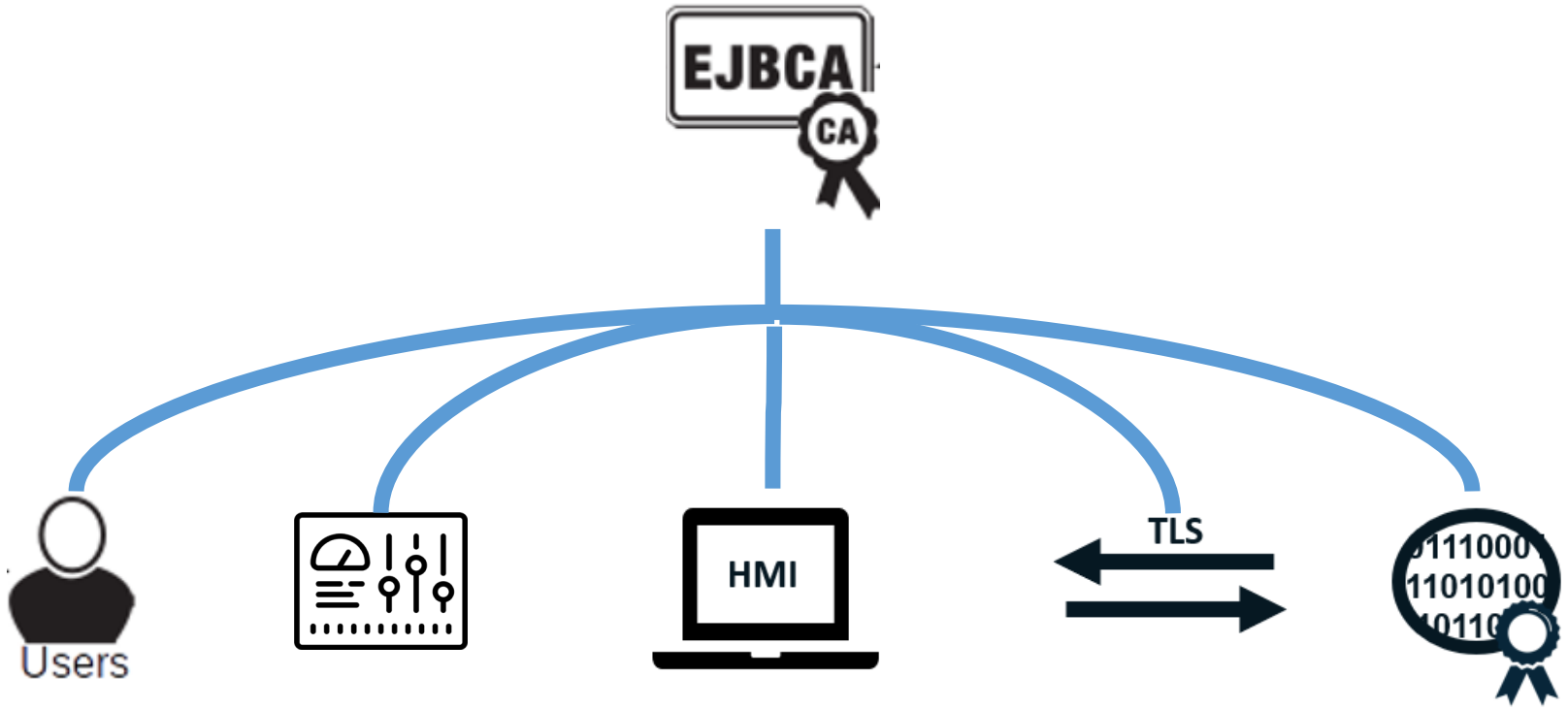
Collocate controller with DER point of connection



EST capable endpoints connected to DER point of connection

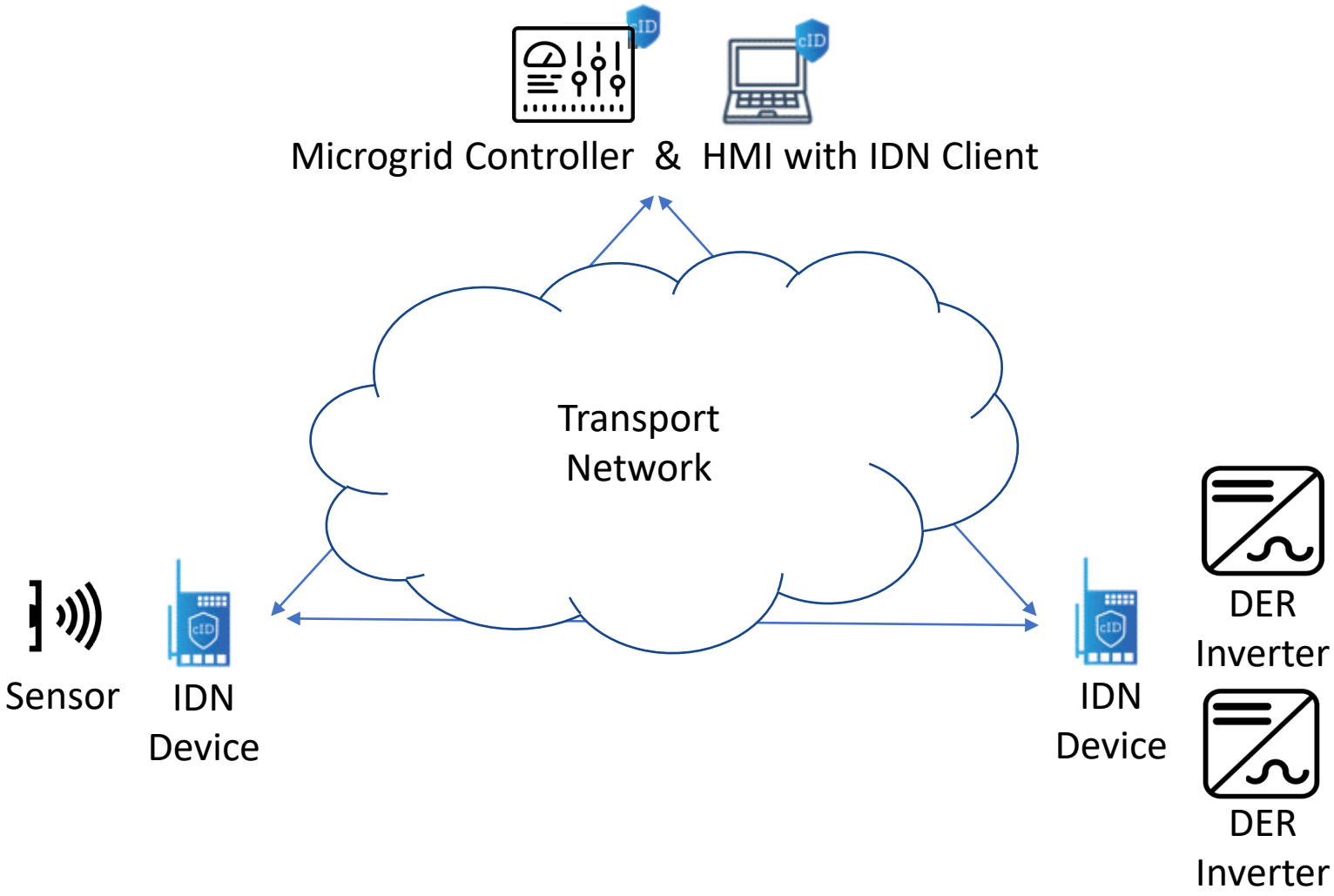
Microgrid PKI

- Enterprise Java Beans Certificate Authority



Identity Defined Network

- Protecting Power System Communications



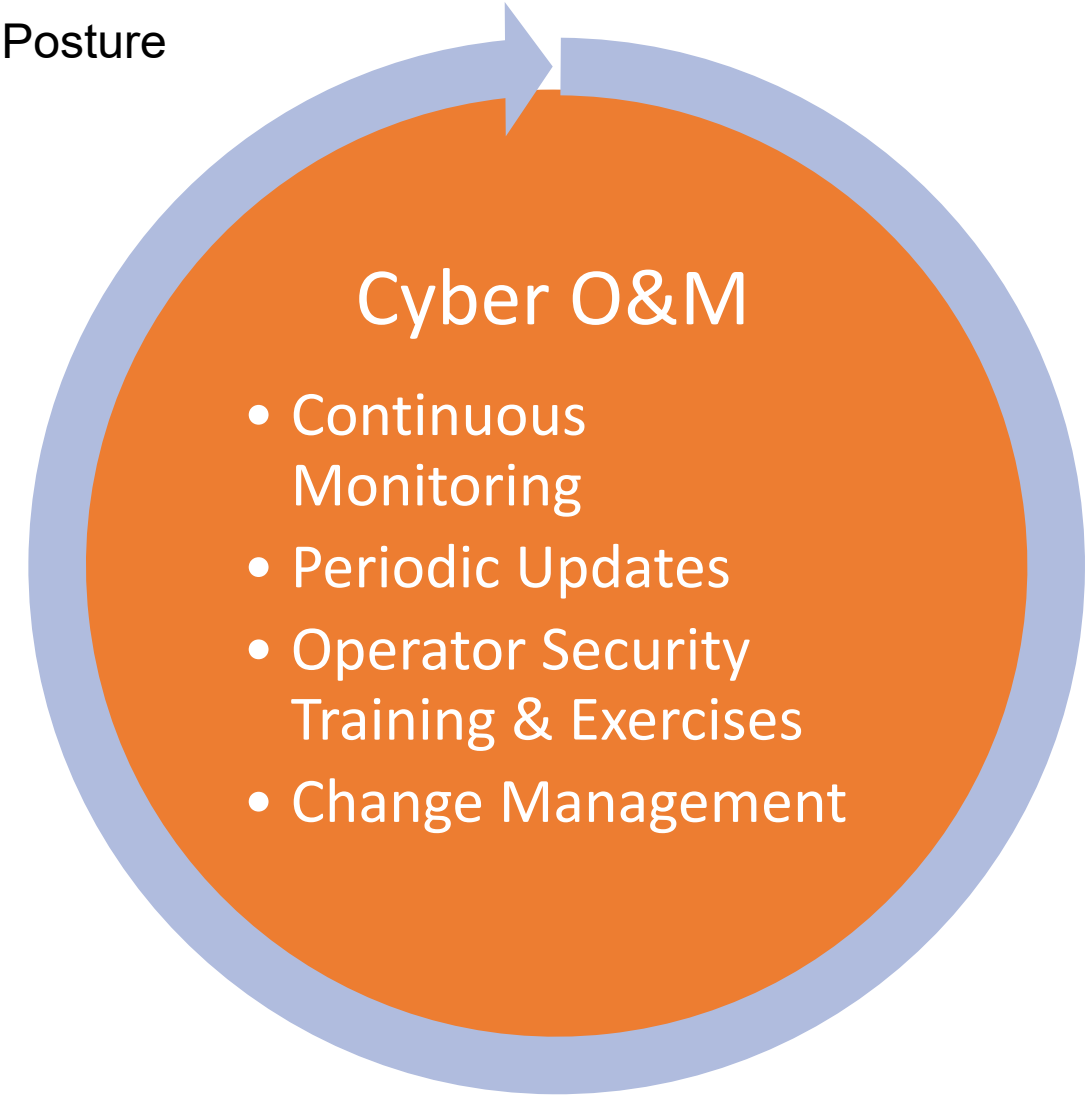
DER endpoints and TCP/IP footprint are hidden

No complex firewall rules, routing policies, VLANs and ACLs

Serial-over-IP communications protected

Cyber Sustainment

- Maintaining Cybersecurity Posture




Questions??
IEEE TN Chapter
October 2021

Thank You

Chad.Douglas@sandc.com

James.Lee@sandc.com

Michael.Higginson@sandc.com

AuraLee.Keating@sandc.com