



Cybersecurity

For Large Electrical Power Systems

```
010 010101 01111100111011 0011 10101010100 01010 010 1111 001 1001 01 11 0011001100 1 1
000 000000 01000001011000 0000 00000000000 00000 000 1000 011 011 00 01 1011000011 0 0
100 101011 00100011000100 0100 11001101011 01101 1 1 0100 10 00 0100110011 0 1
101 100101 10100000011000 1010 11011100101 1110010 1010 00 1000 01 10 0100110011 0 1
010 010100 01011100111011 0011 00100010100 000 0
100 101010 01000011001100 0100 010001010110001 0
101 101111 10100011100100 1100 1101110111101 1 1
011 010101 11111100111011 1011 111101 10011 0 1
010 011010 01011111011111 0010 0010 01 01 1 0
101 10101111010001100010001100 1101 10 01 0 1
111 11010111011110011001101001 1111 11 1 1 0
1000 01 10 0100110011 0 1
1011 11 11 010101100 1
0111 10 01 1110111101
0100 11 10 0100111101
1011 01 11 111101100
```

**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



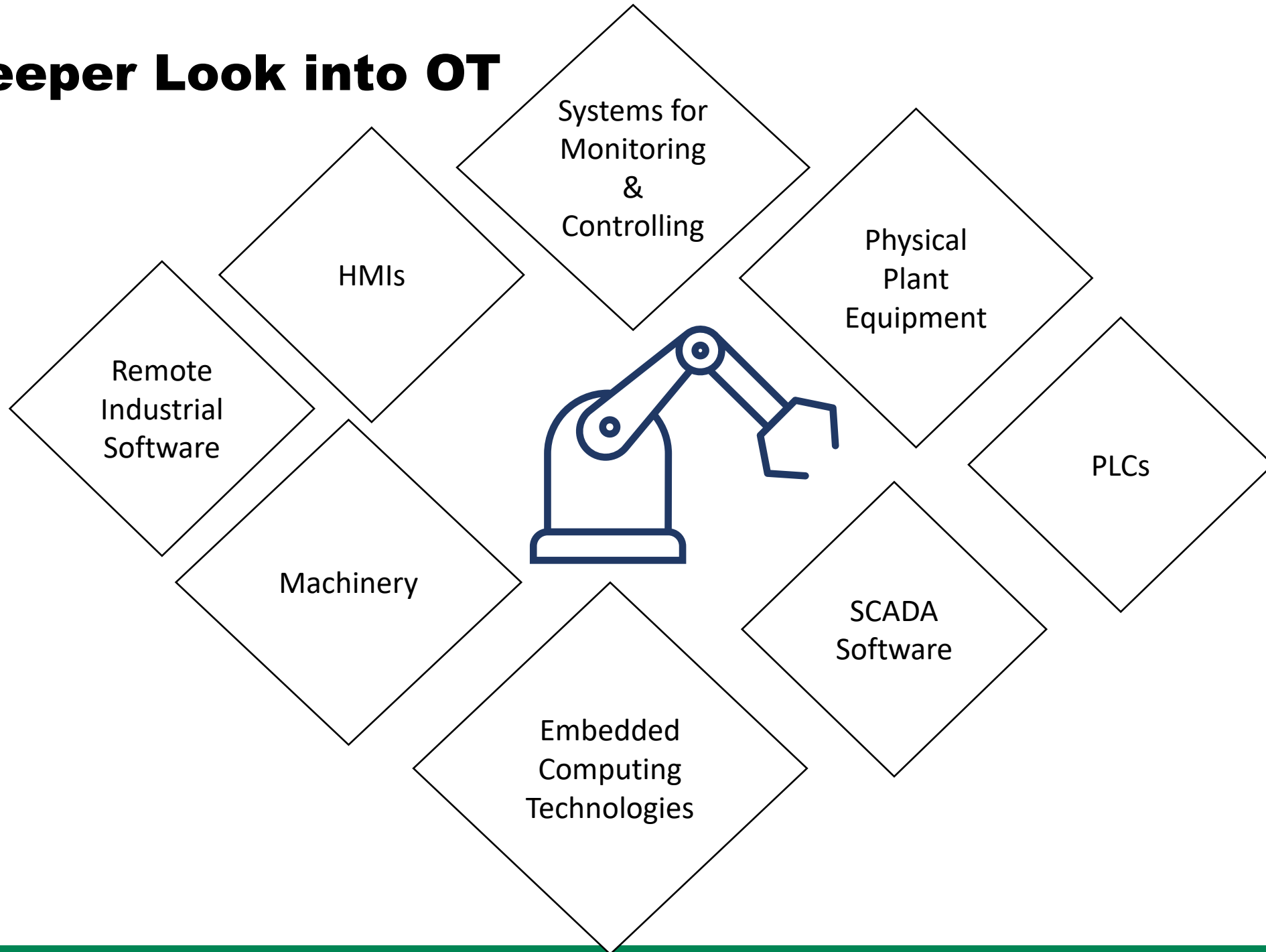
IT systems emphasis: confidentiality

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

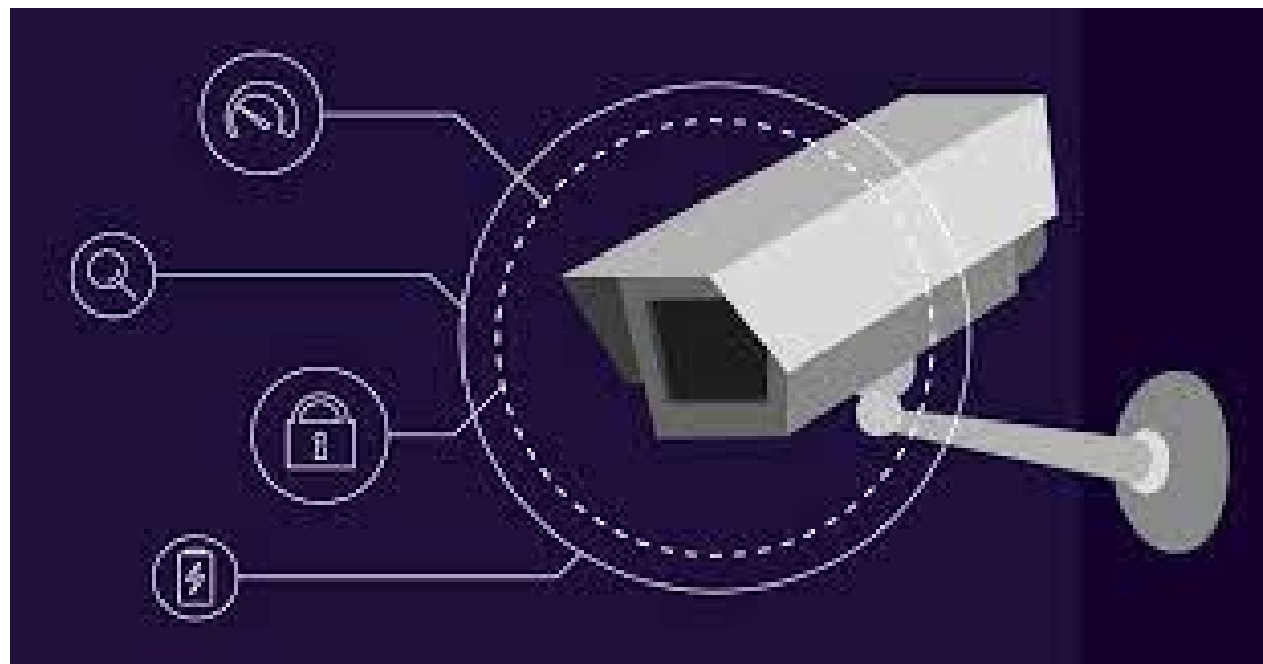
OT systems emphasis: availability

- ▶ 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

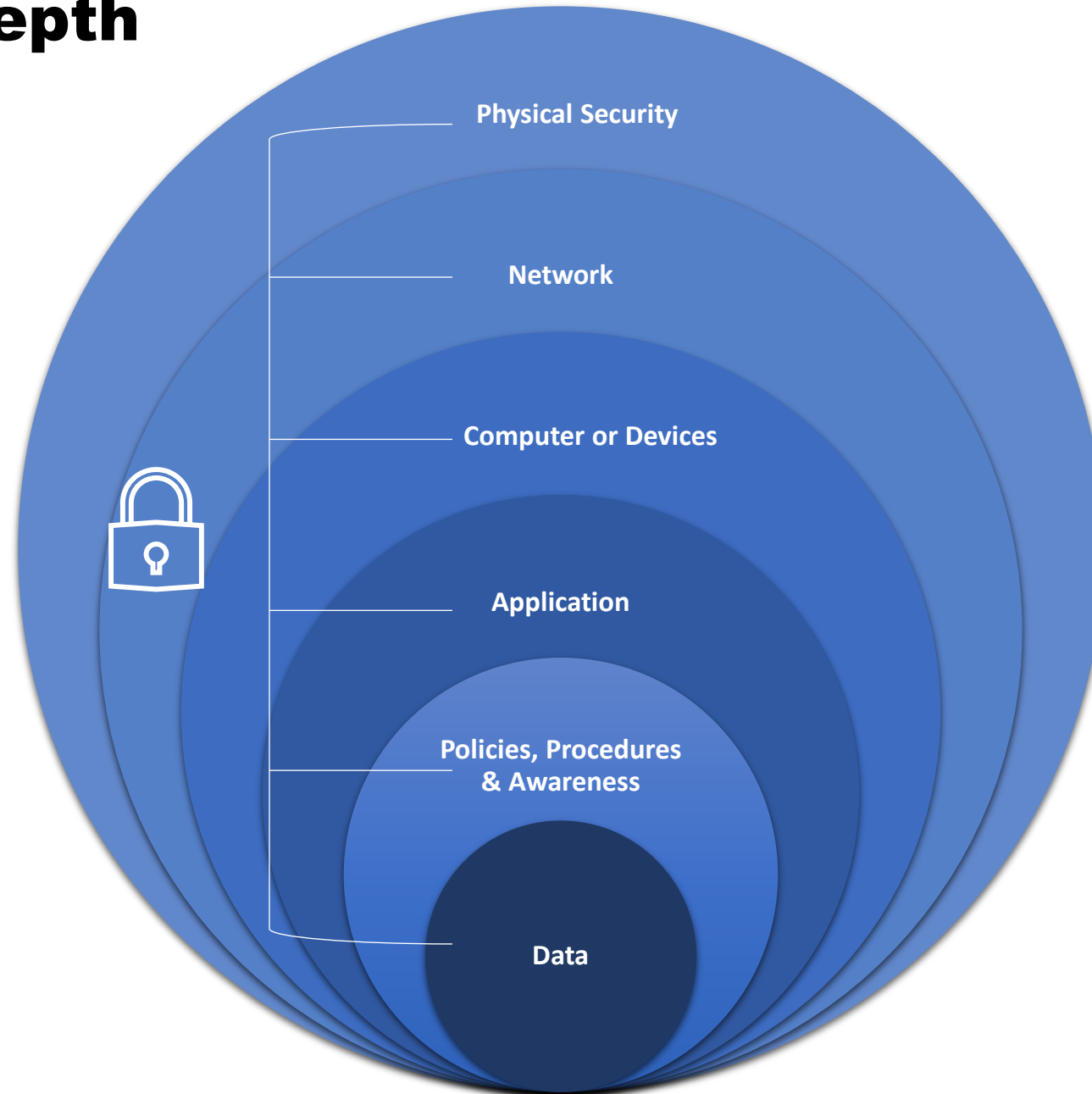


Monitoring & Physical Security on OT Systems



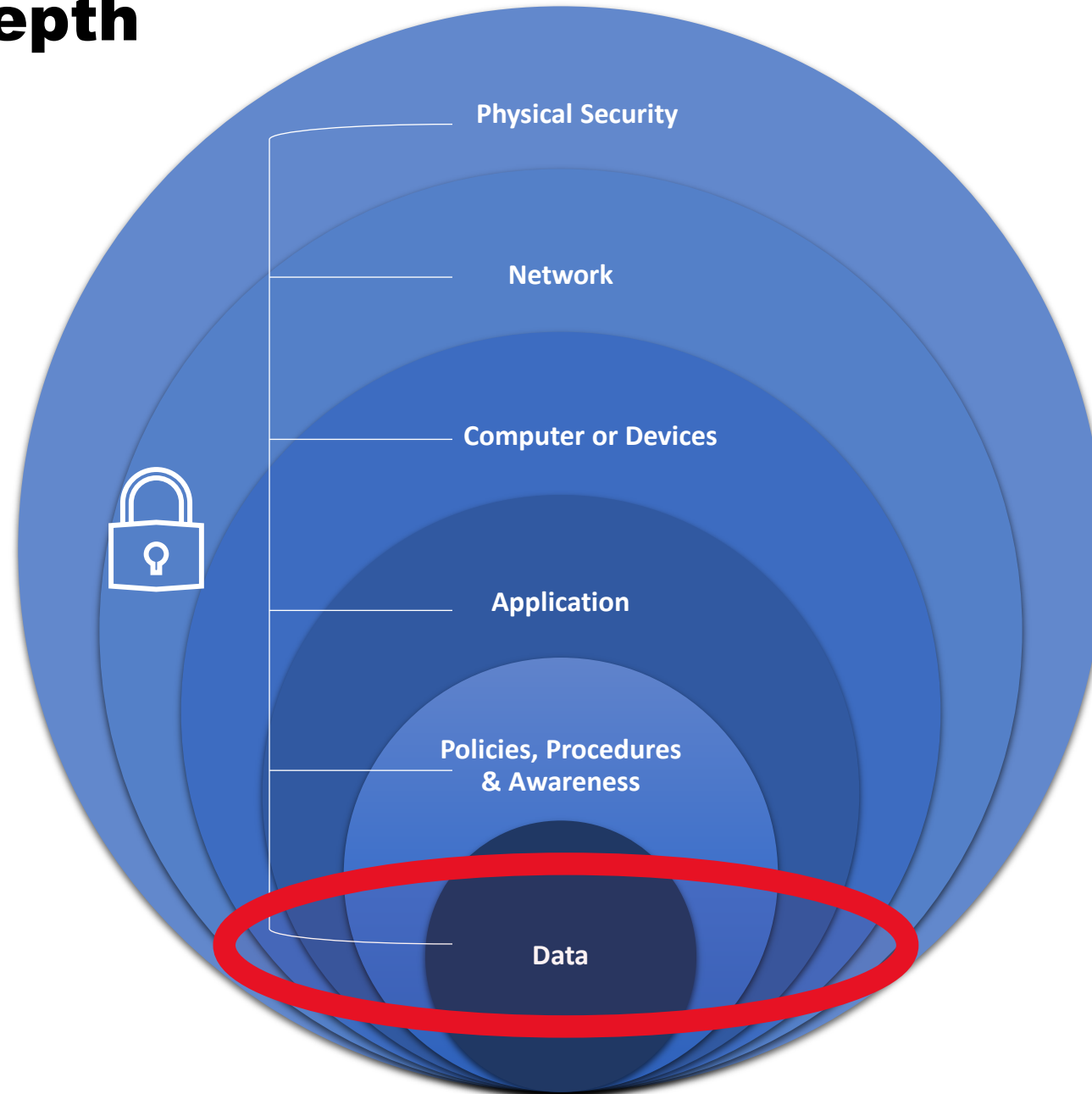
Defense in Depth

- What is it?



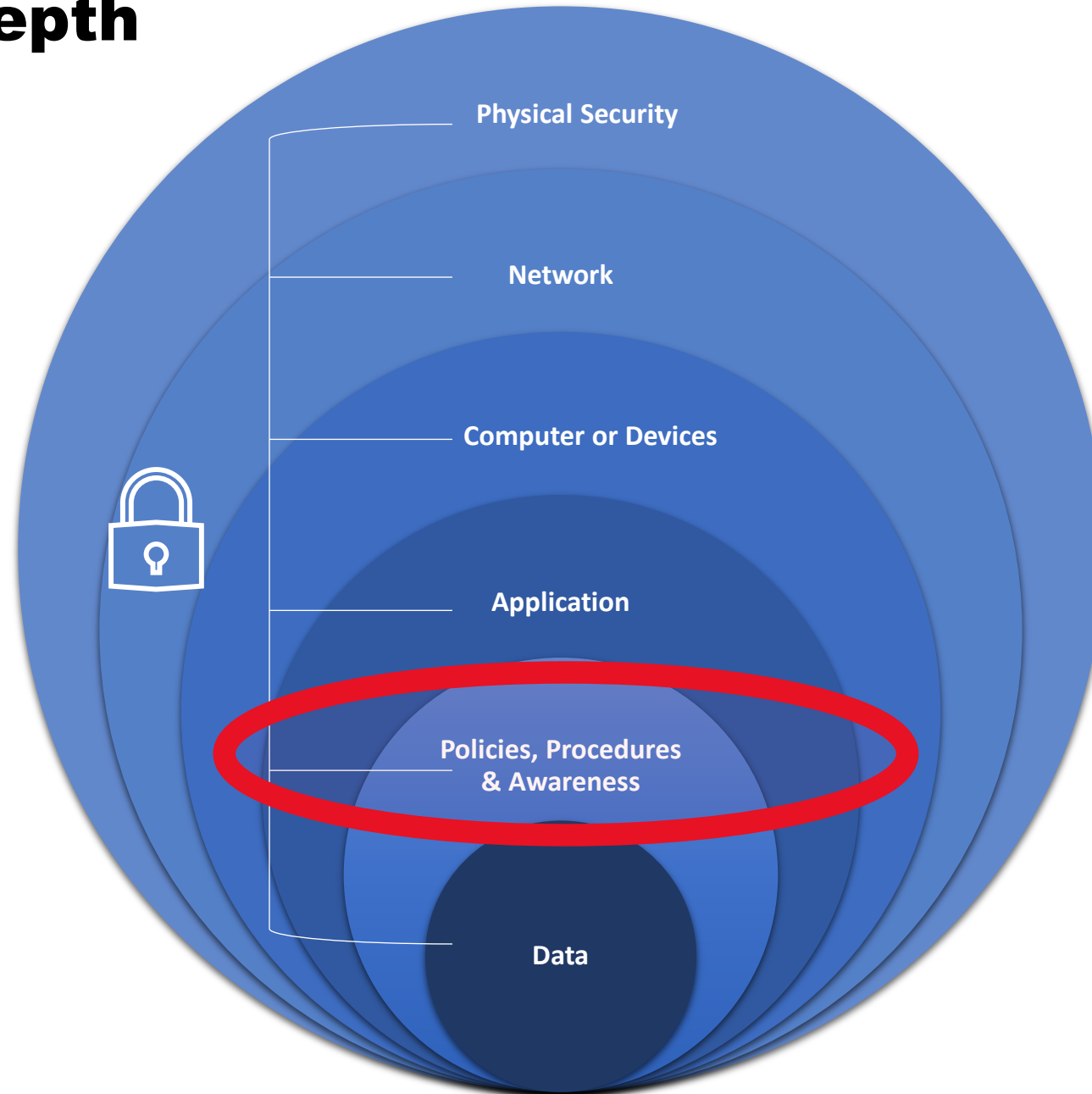
Defense in Depth

- What is it?



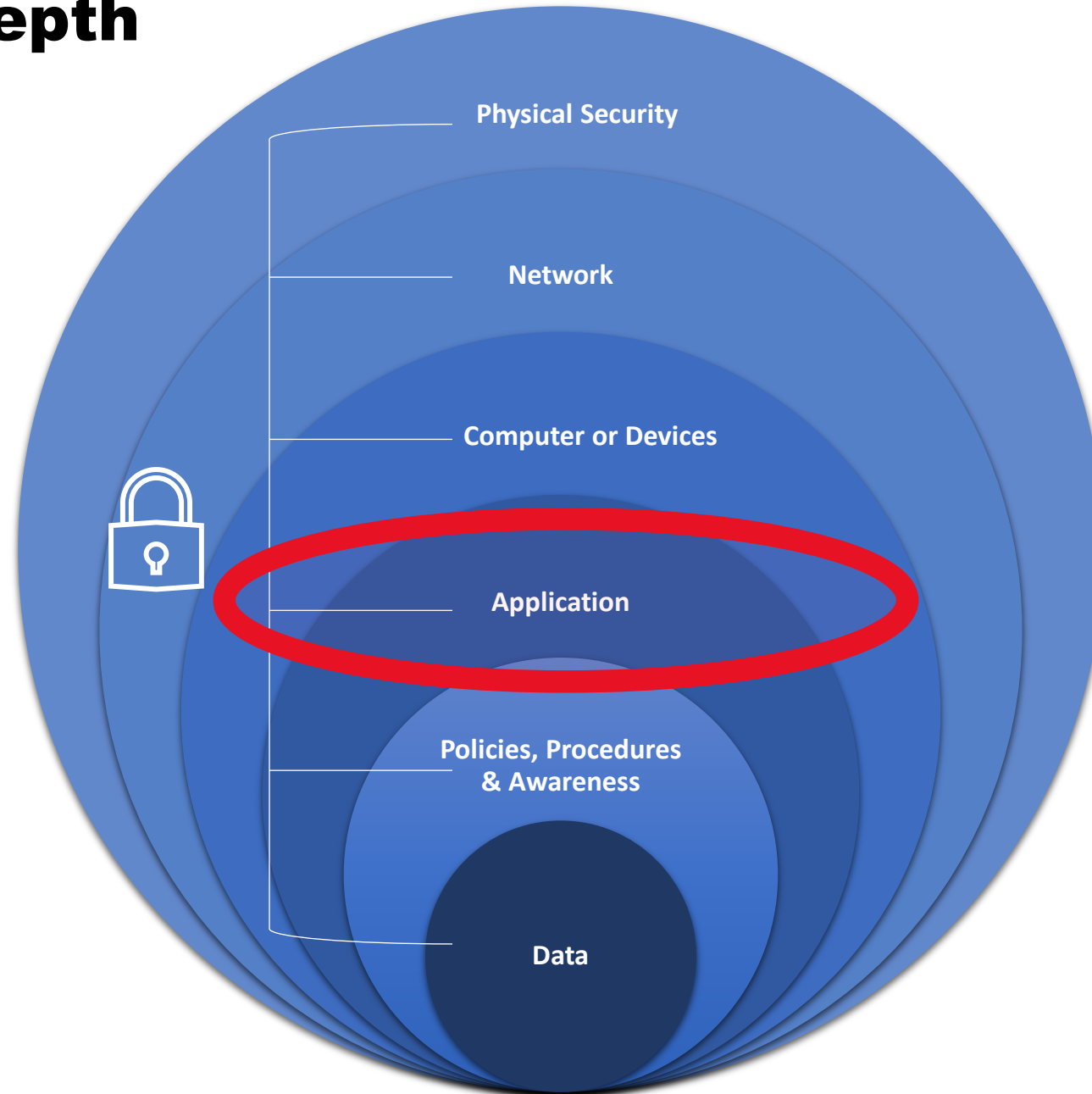
Defense in Depth

- What is it?



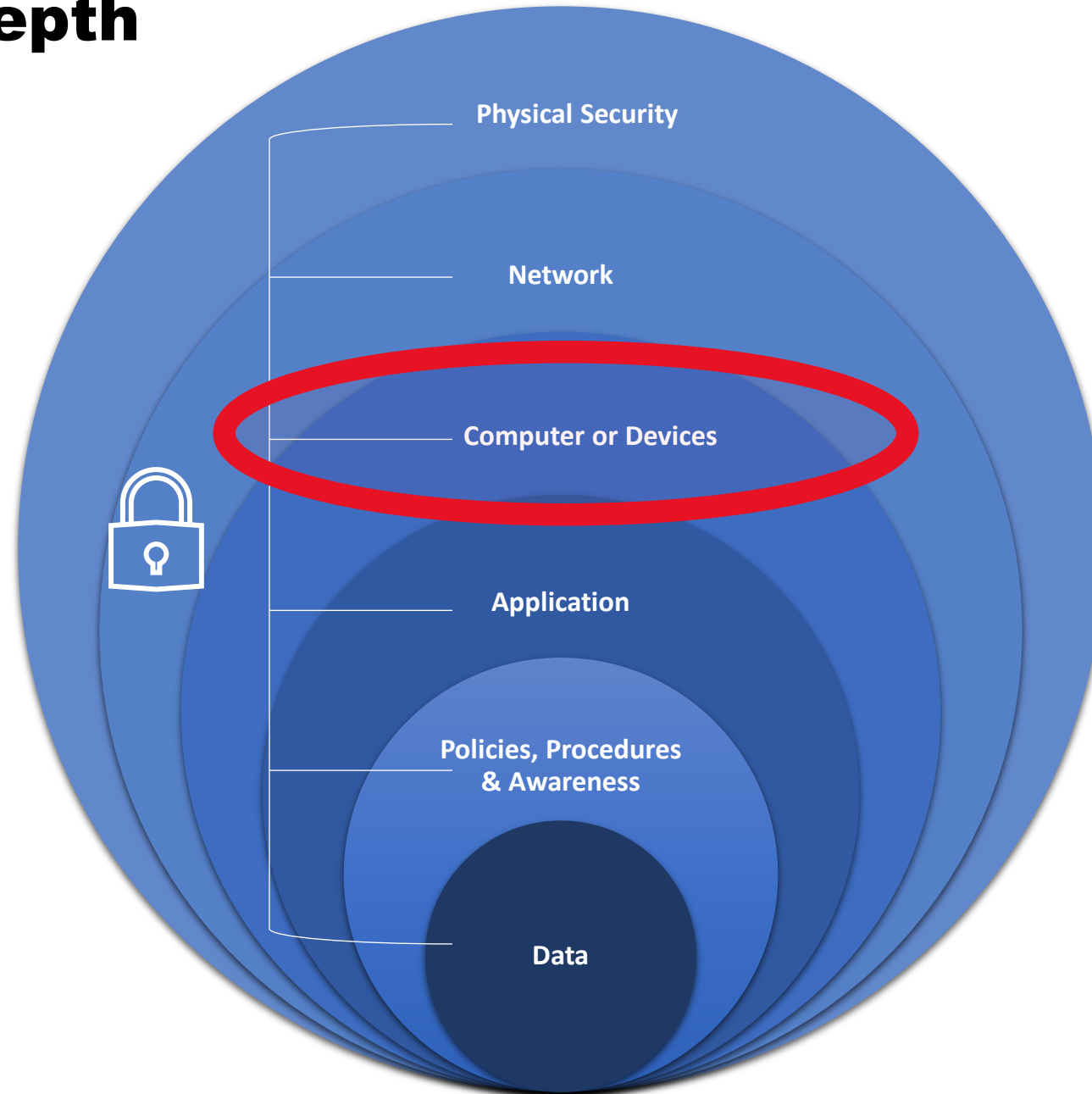
Defense in Depth

- What is it?



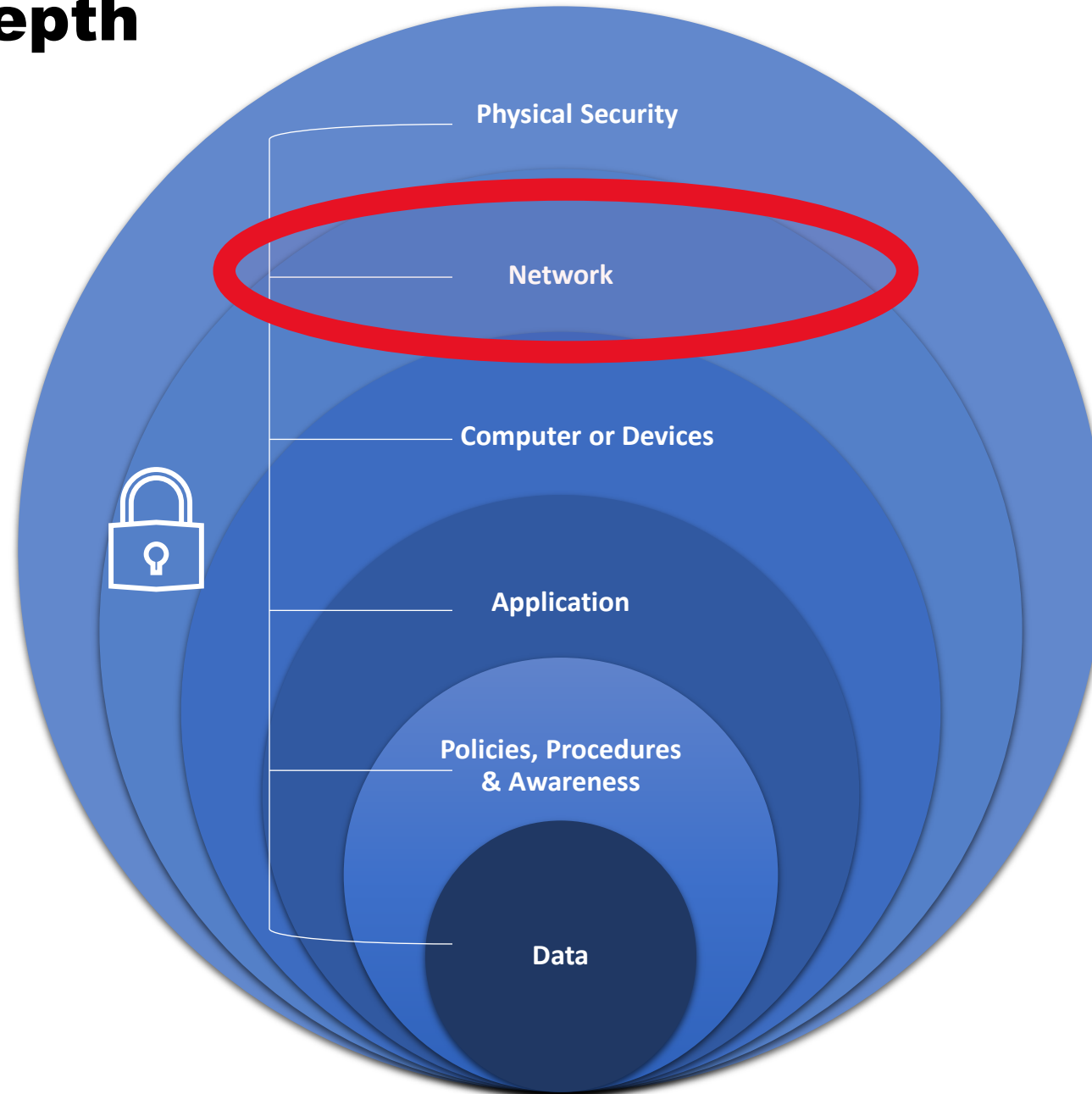
Defense in Depth

- What is it?



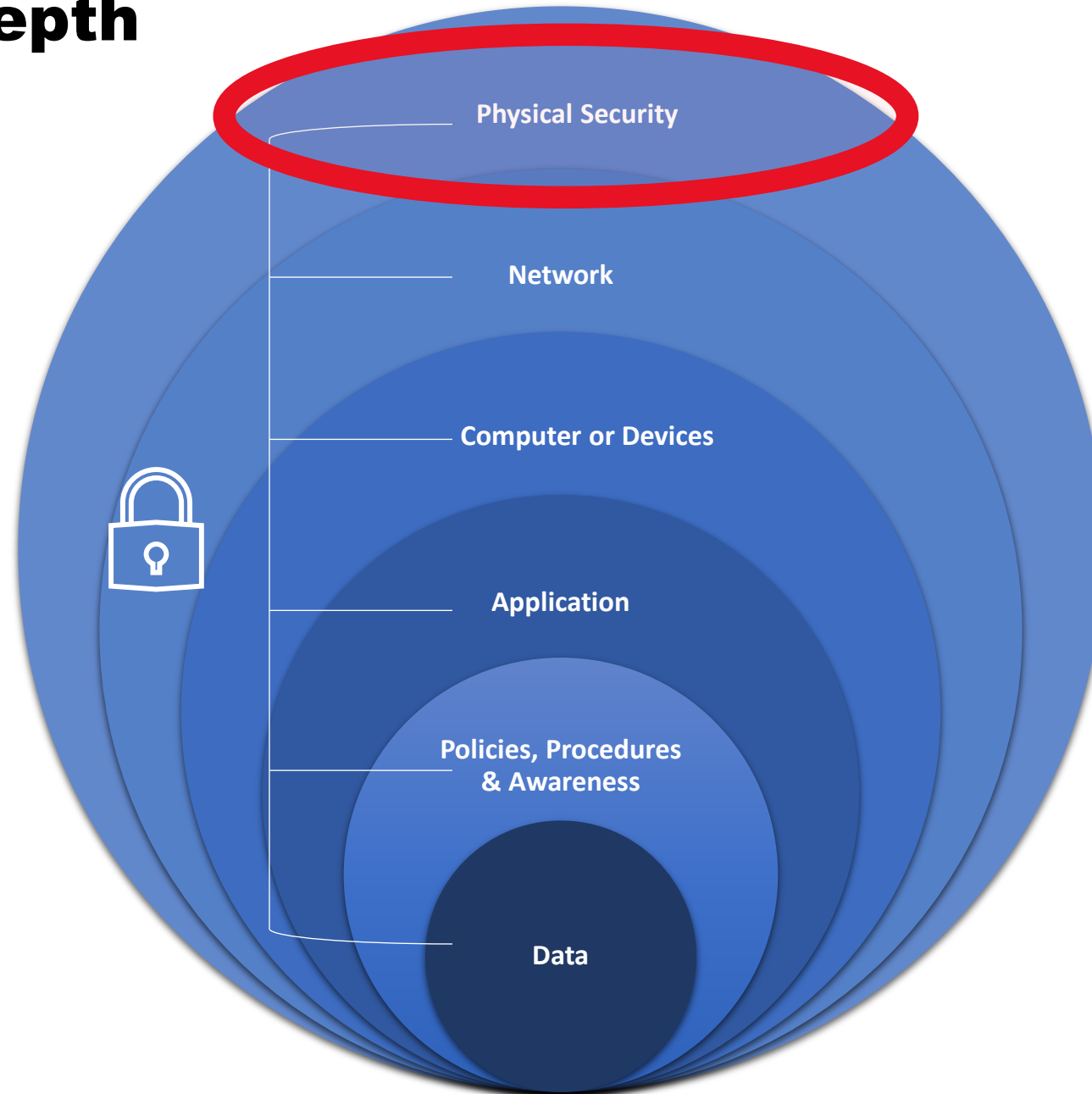
Defense in Depth

- What is it?



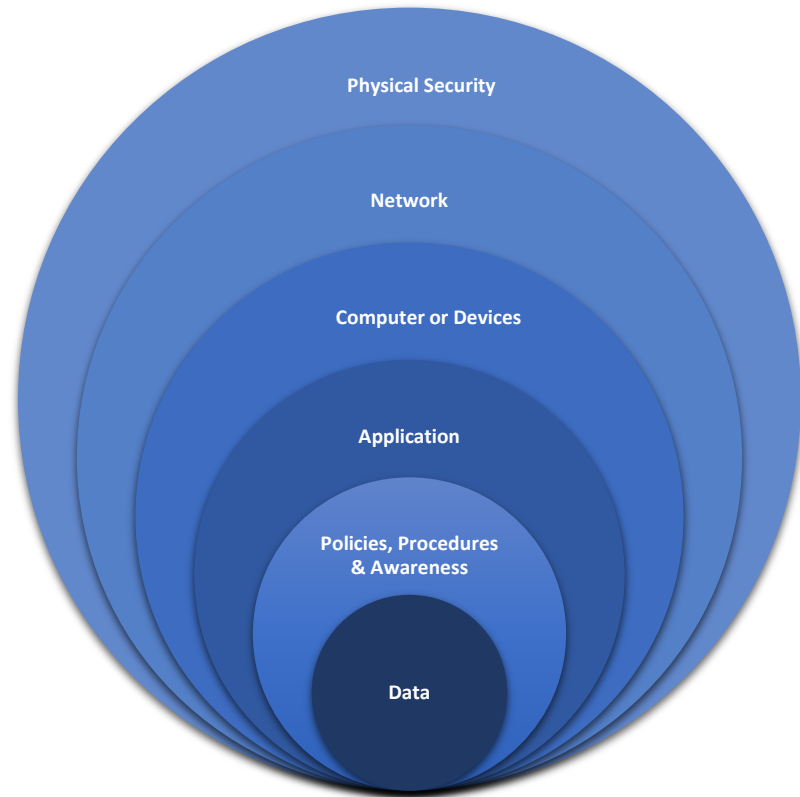
Defense in Depth

- What is it?



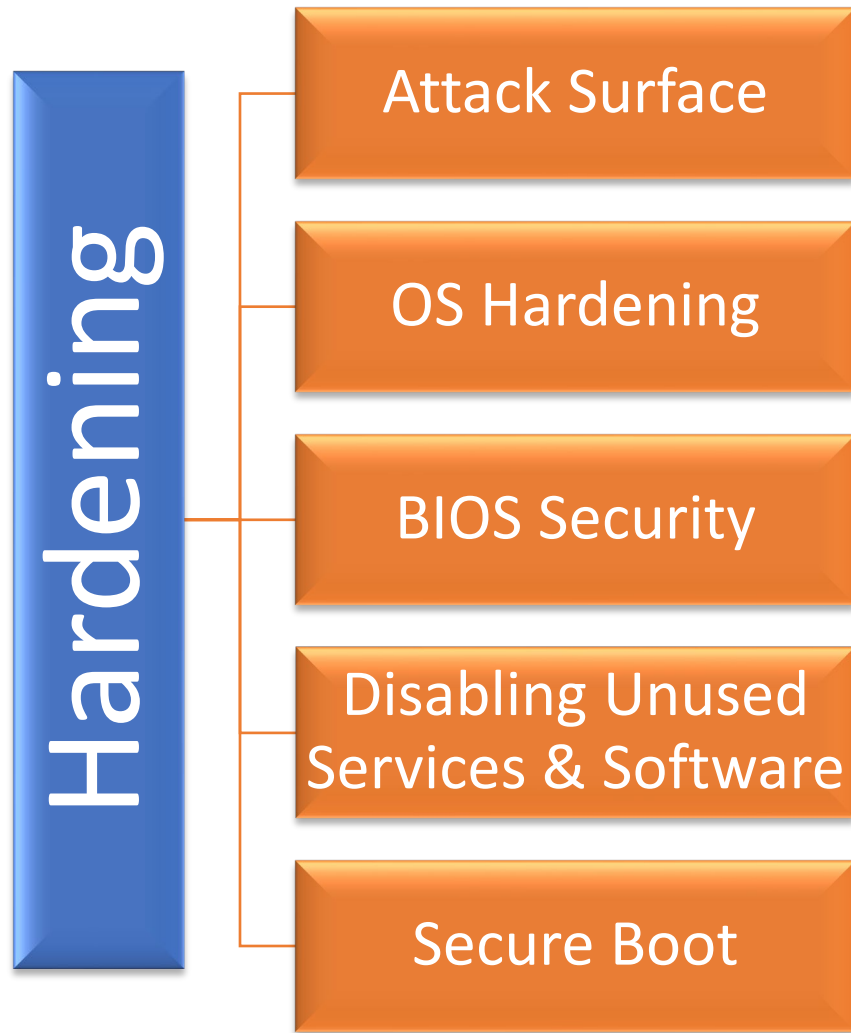
System Cybersecurity Design

- Designing the system with Defense in Depth



Device Hardening

What does it mean to “Harden” a computer?



How Do We Harden a Device

Best Practices

DISA STIG Viewer



Complex Passwords



Disabling unused/default accounts



Uninstalling unneeded software



Disabling unneeded services

The screenshot shows the DISA STIG Viewer interface. On the left, the 'STIG Explorer' pane shows a tree view with 'STIGs' expanded, listing 'Windows 10 Security Technical Implementa...'. Below this is a 'Filter Panel' with a search box and filter options. The main pane displays a table of rules:

Vul ID	Rule Name
V-63319	WN10-00-000005
V-63321	WN10-CC-000310
V-63323	WN10-00-000010
V-63325	WN10-CC-000315
V-63329	WN10-CC-000320
V-63333	WN10-CC-000325
V-63335	WN10-CC-000330
V-63337	WN10-00-000030
V-63339	WN10-CC-000335
V-63341	WN10-CC-000340
V-63343	WN10-00-000025
V-63345	WN10-00-000035
V-63347	WN10-CC-000345
V-63349	WN10-00-000040
V-63351	WN10-00-000045
V-63353	WN10-00-000050
V-63355	WN10-00-000055
V-63357	WN10-00-000060
V-63359	WN10-00-000065
V-63361	WN10-00-000070
V-63363	WN10-00-000075

The right pane shows details for rule V-63319:

Windows 10 Security Technical Implementation Guide :: Release: 13 Benchmark Date: 27 Apr 2018
Vuln ID: V-63319 **Rule ID:** SV-77809r3_rule **STIG ID:** WN10-00-000005
Severity: CAT II **Check Reference:** M **Classification:** Unclass

Group Title: WN10-00-000005

Rule Title: Domain-joined systems must use Windows 10 Enterprise Edition 64-bit version.

Discussion: Features such as Credential Guard use virtualization based security to protect information that could be used in credential theft attacks if compromised. There are a number of system requirements that must be met in order for Credential Guard to be configured and enabled properly. Virtualization based security and Credential Guard are only available with Windows 10 Enterprise 64-bit version.

Check Text: Verify domain-joined systems are using Windows 10 Enterprise Edition 64-bit version.

For standalone systems, this is NA.

Open "Settings".

Select "System", then "About".

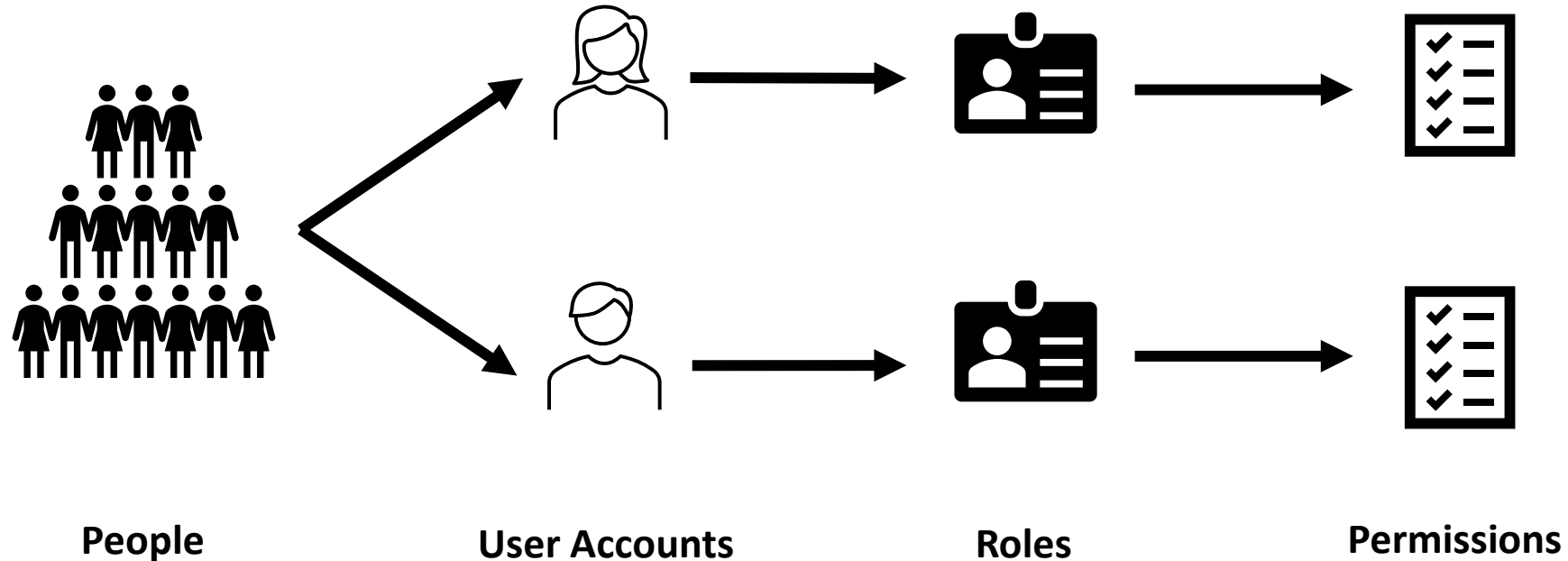
If "Edition" is not "Windows 10 Enterprise", this is a finding.

If "System type" is not "64-bit operating system...", this is a finding.

Fix Text: Use Windows 10 Enterprise 64-bit version for domain-joined systems.

References

How Do We Harden a Device



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

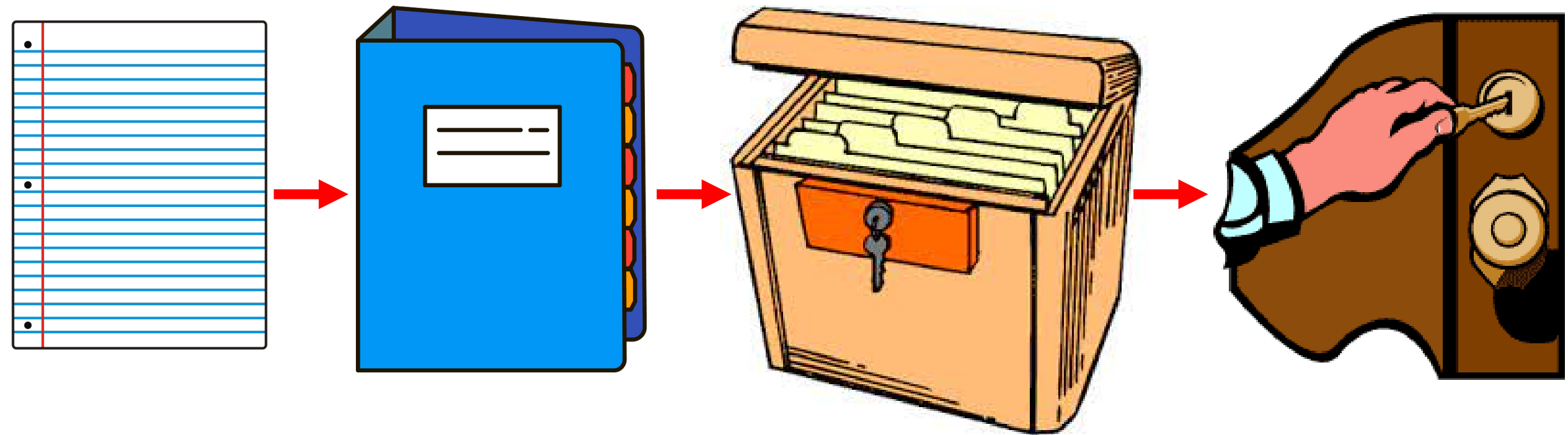
Now that the device is hardened



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

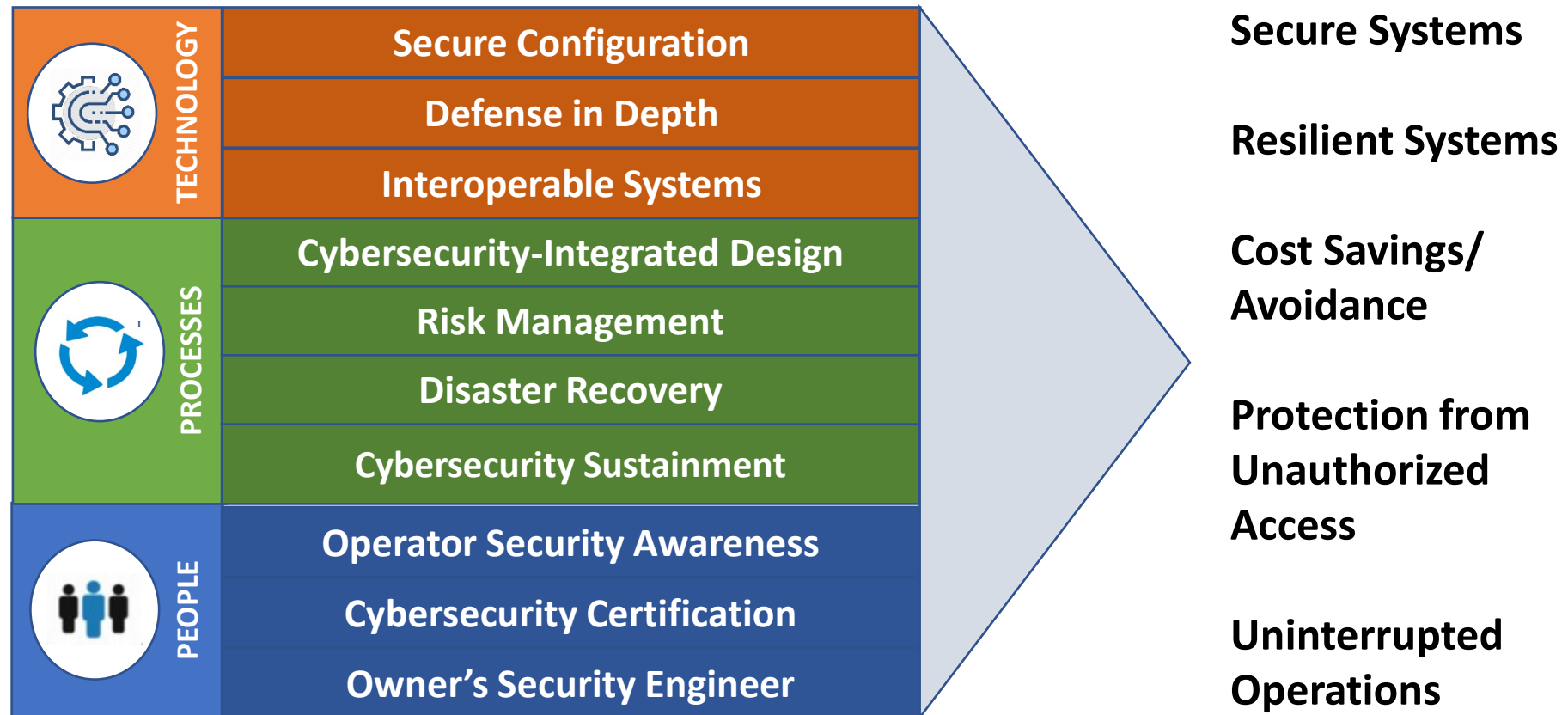
- Cybersecurity guidance for facility-related control systems

Controlled Unclassified Information (CUI)

- DFARS 252.204-7012
- NIST 800-171

Cybersecurity Integration Considerations

- People, Processes, Technology



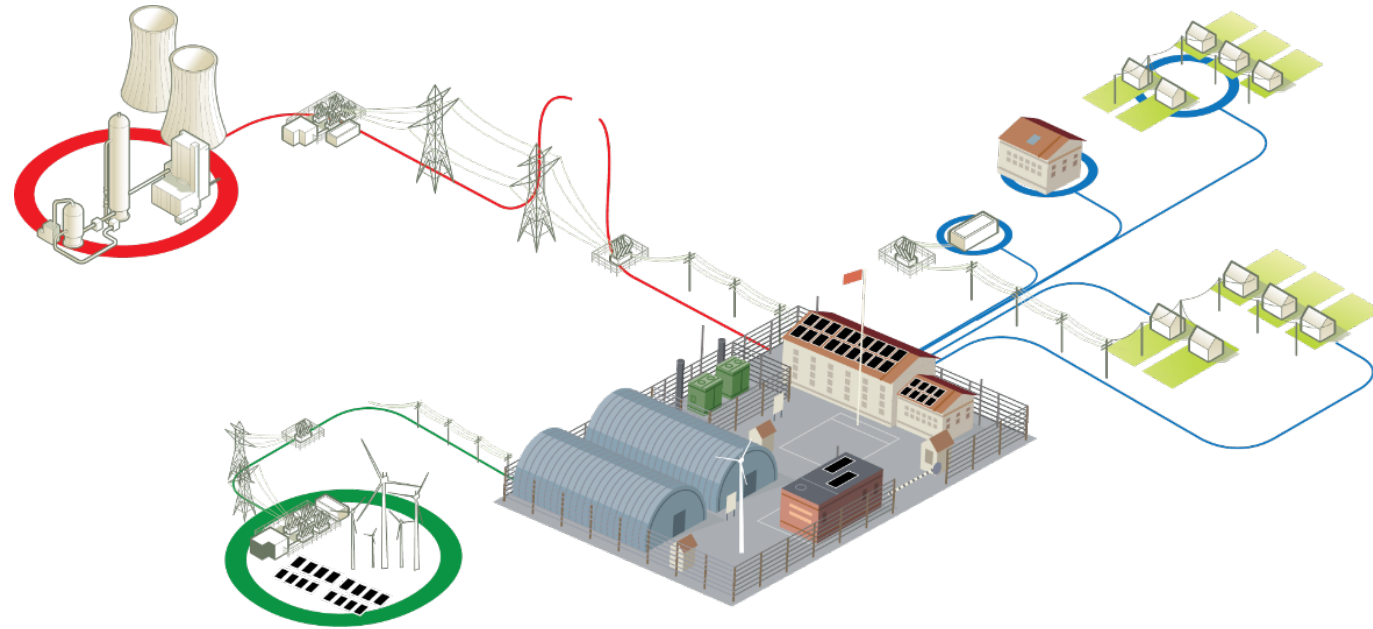
Microgrids as a Case Study

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

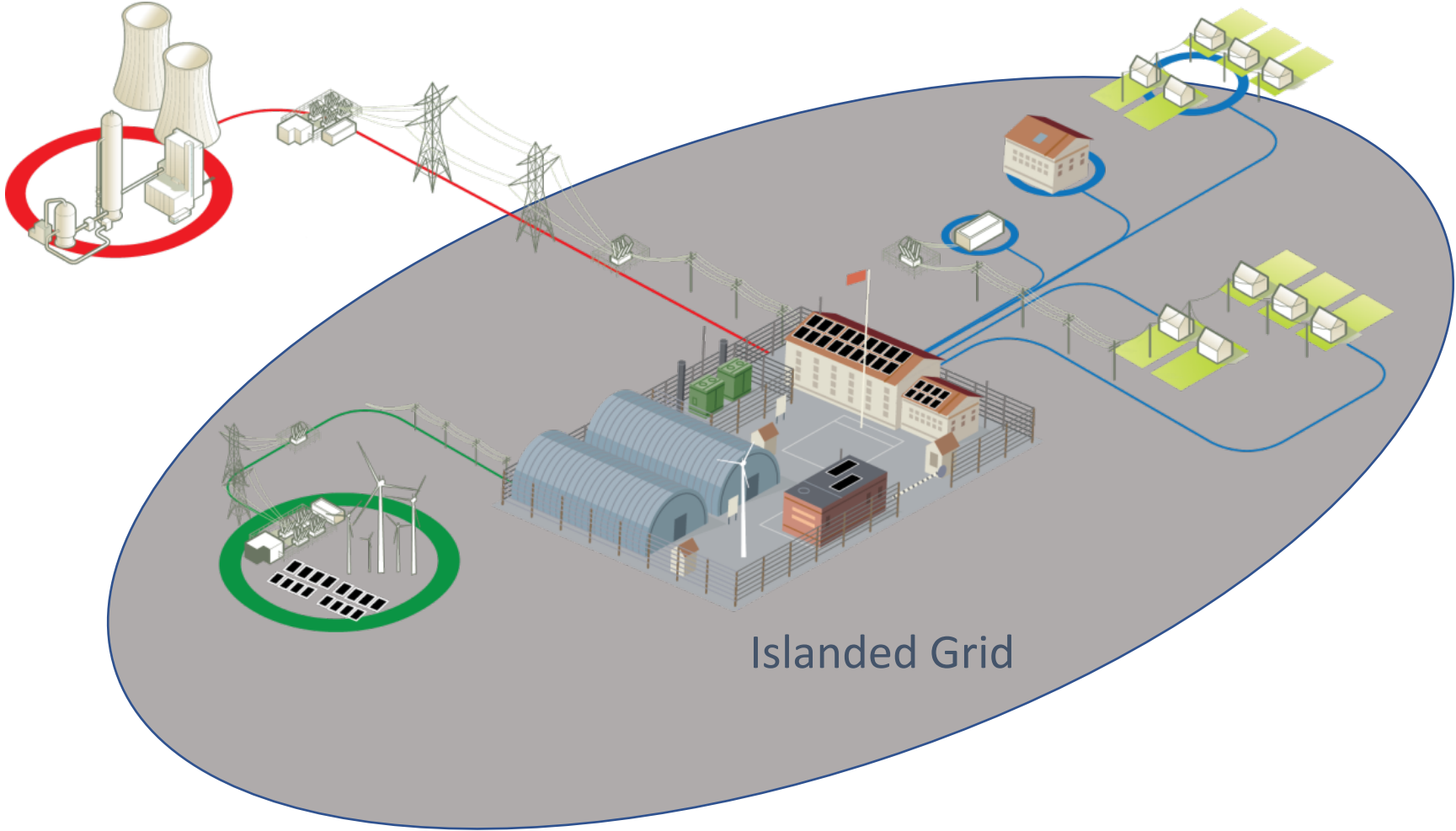
with **clearly defined electrical boundaries**

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



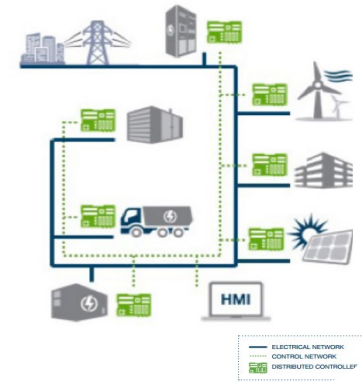
Microgrid Building Blocks



Distributed Energy Resources (DER)



Switching and Protection



Microgrid Control

Microgrid Building Block: Distributed Energy Resources



DER Considerations



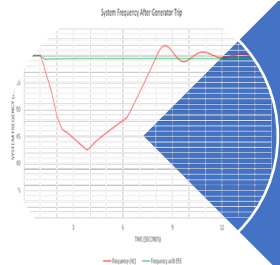
21, rue d'Artois, F-75008 PARIS

<http://www.cigre.org>

CIGRE US National Committee
2017 Grid of the Future Symposium



Power and
energy
capabilities



Response to
system events



Paralleling and
interconnection
limitations

Challenges and Considerations of DER Selection for Microgrid Applications

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

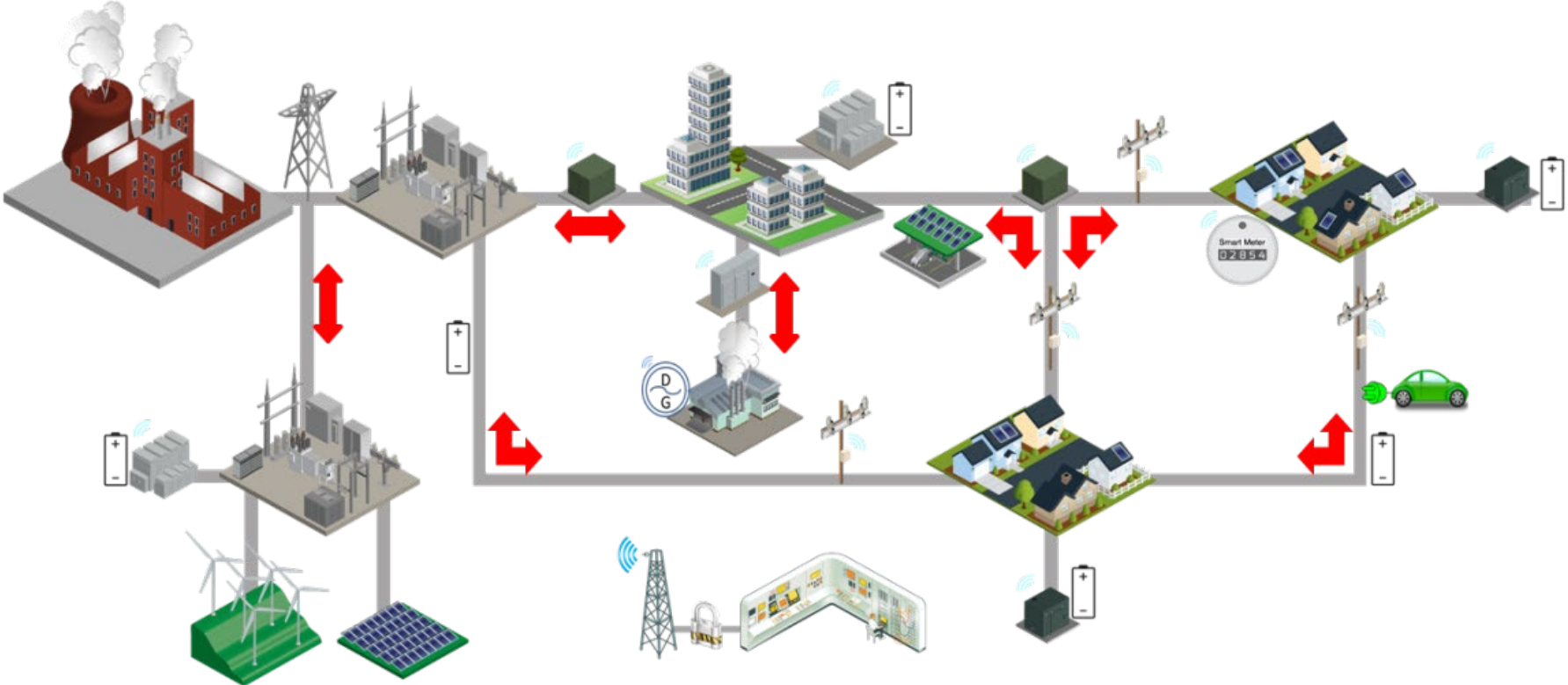
SUMMARY

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.

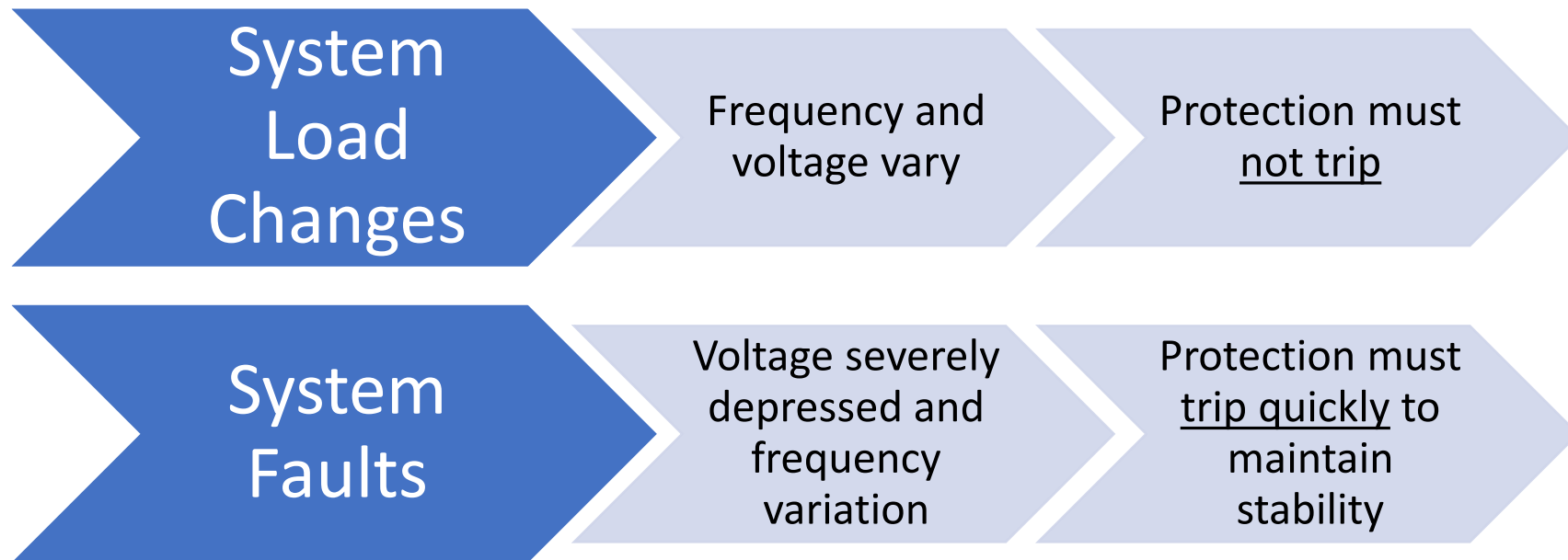
Microgrid Building Block: Switching and Protection



Microgrid Building Block: Switching and Protection



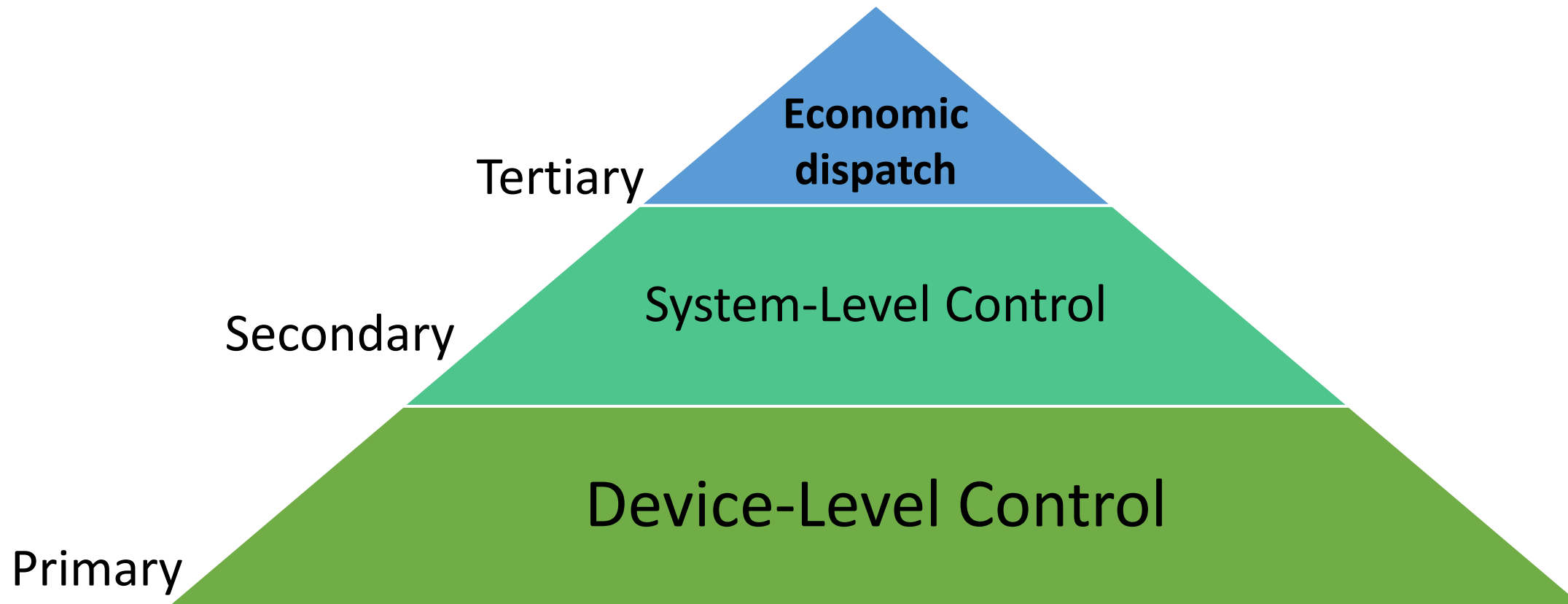
Microgrid Building Block: Switching and Protection






Microgrid Building Block: Control

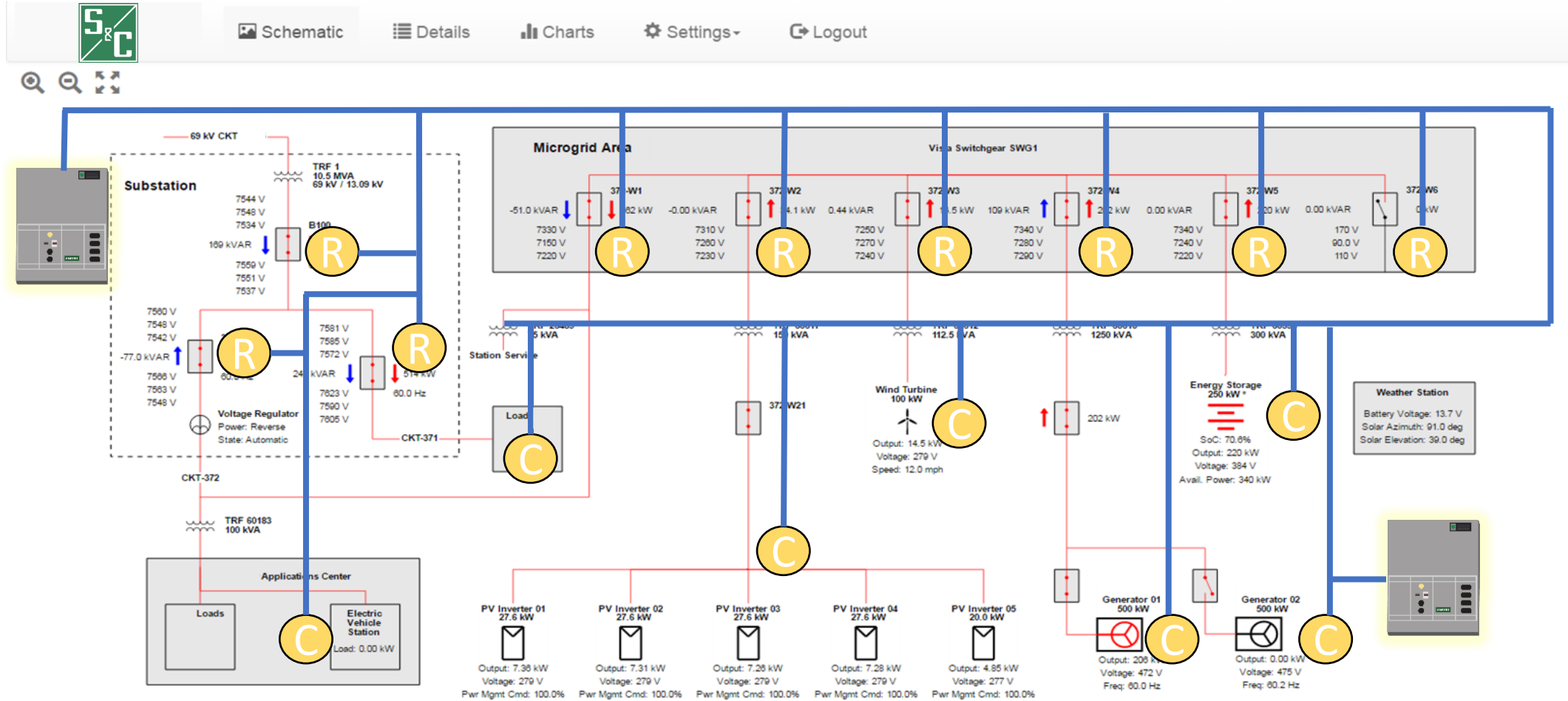


Tiered Control in Microgrids



Microgrid Control Visualization

-  Local Controller
-  Microprocessor Relay
-  Microgrid Controller



Ameren TAC Microgrid



Ameren TAC Microgrid

■ Project Information

Champaign, IL

15 kV POI

Research Loads

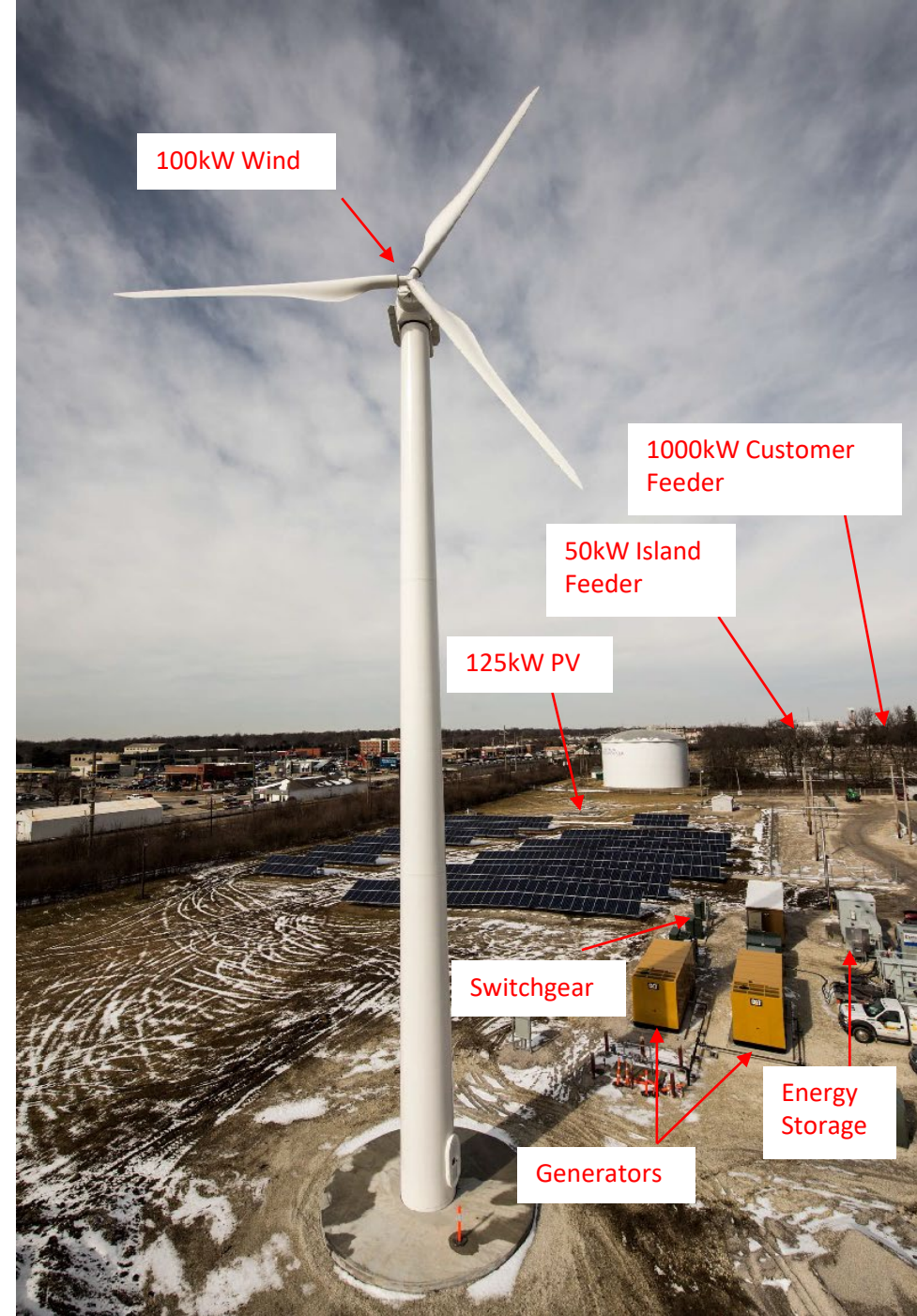
1000 kW Rate-Paying Customer Loads

(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



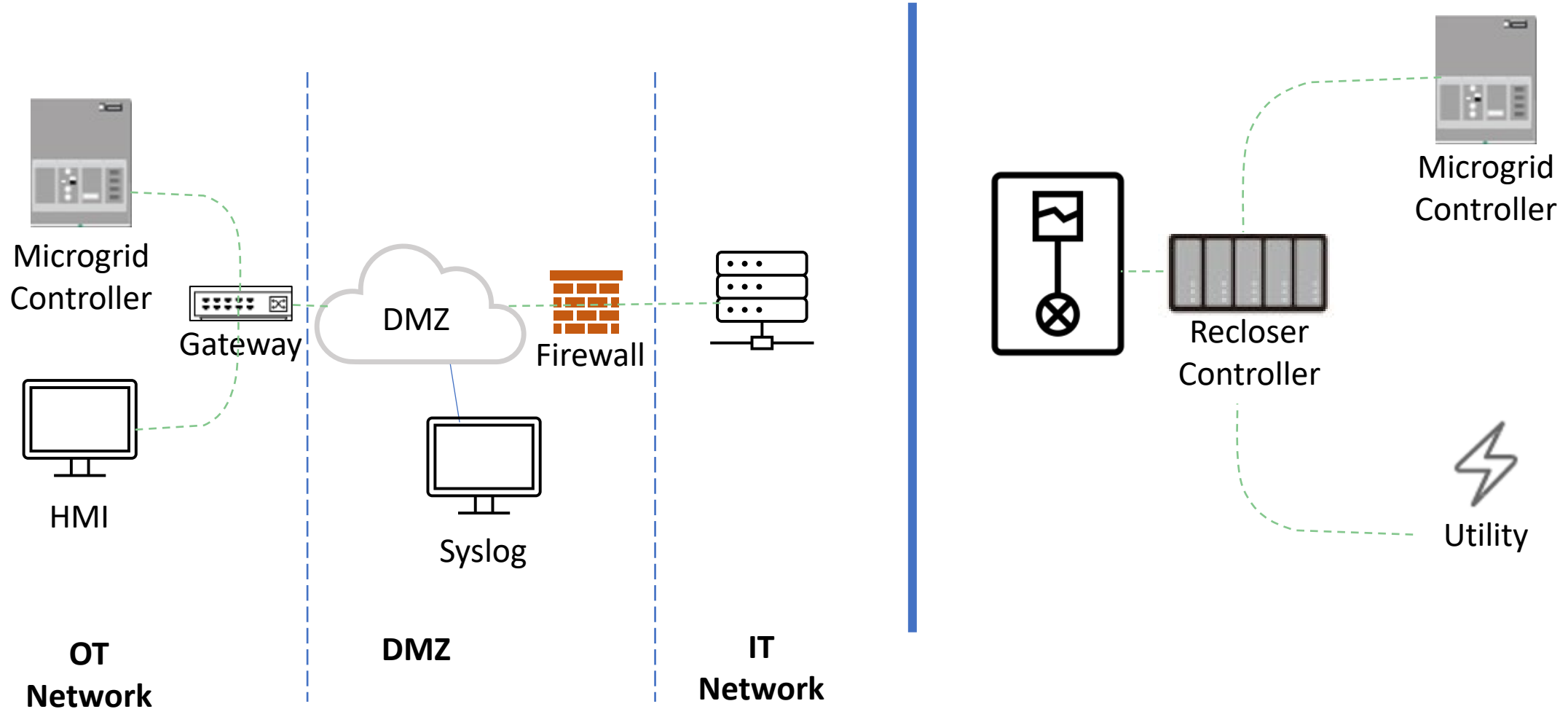
Interfaces,
Interconnections,
Load Criticality,
Attack Vectors



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

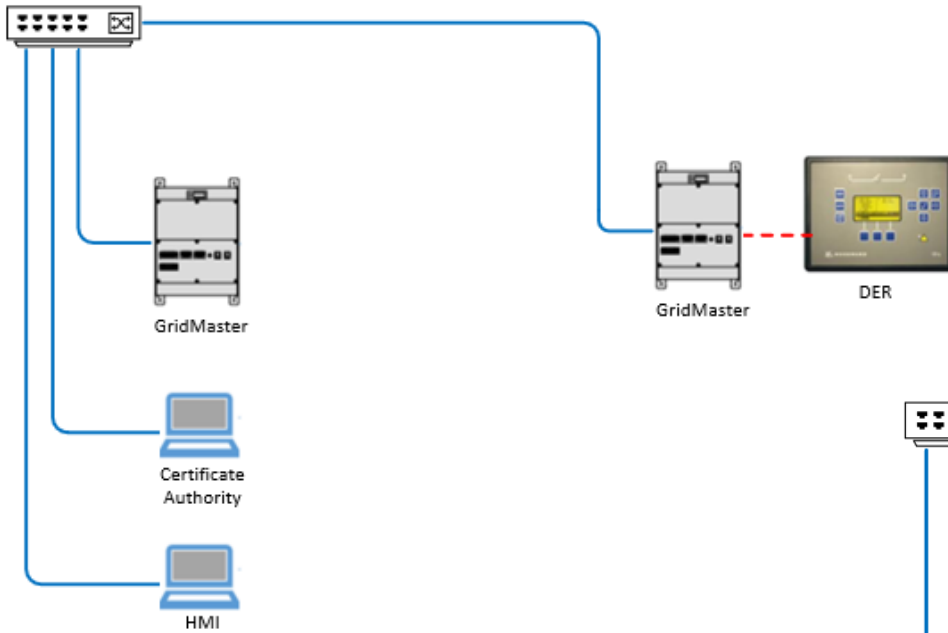
Segregated Communications

- Perimeter and Host-based Protections



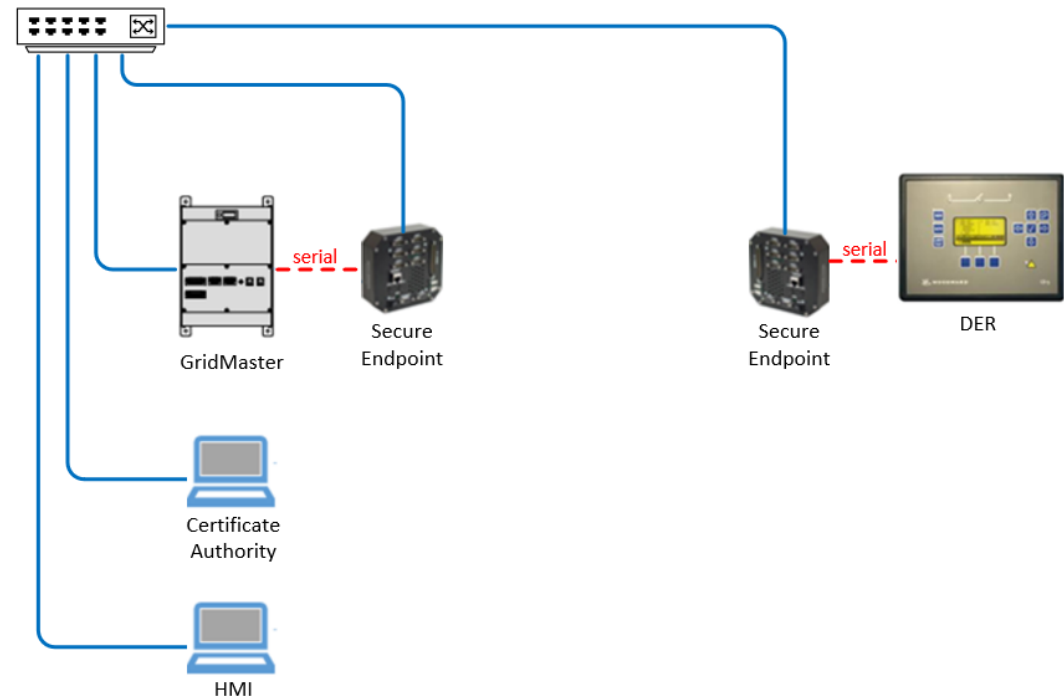
Microgrid DER Security

- Extending encrypted communication paths



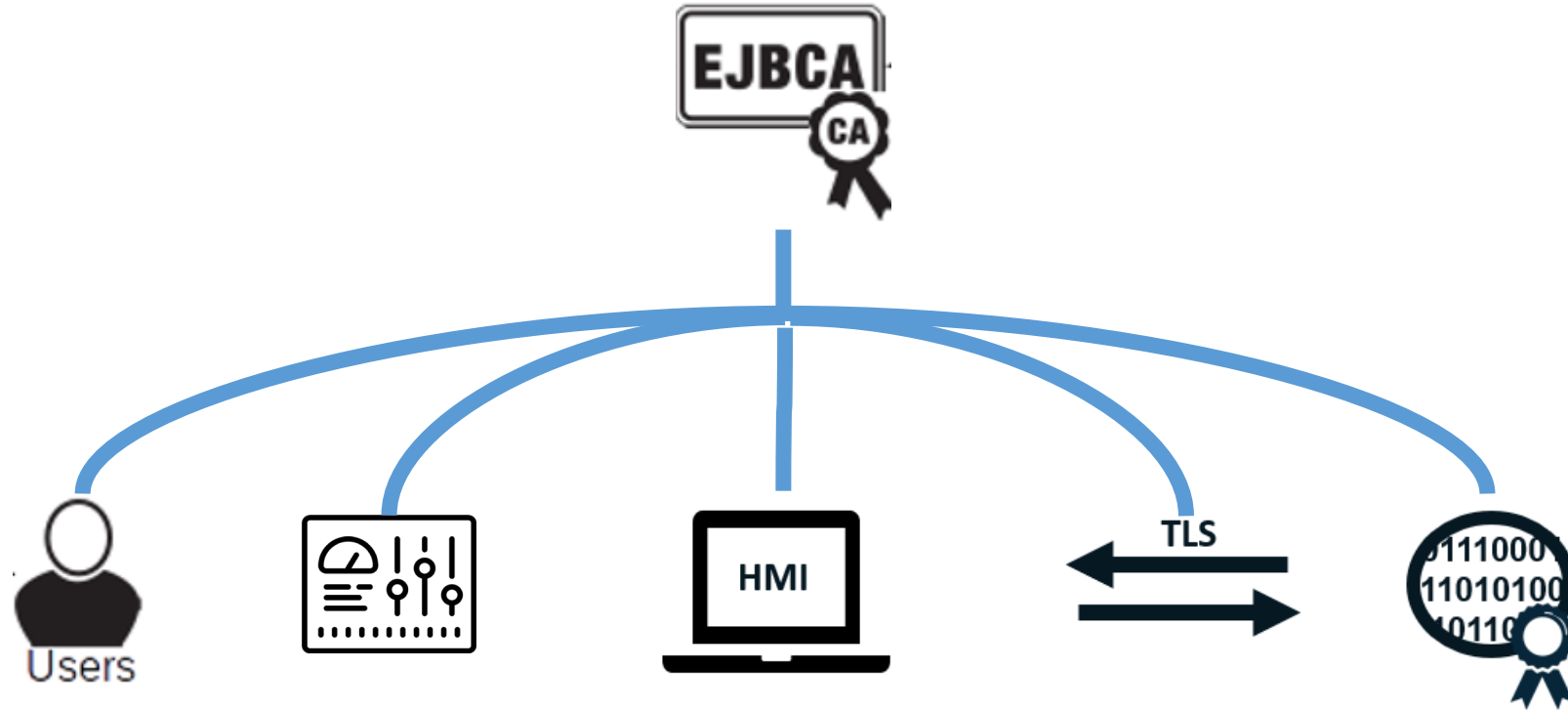
Collocate controller with DER point of connection

EST capable endpoints connected to DER point of connection



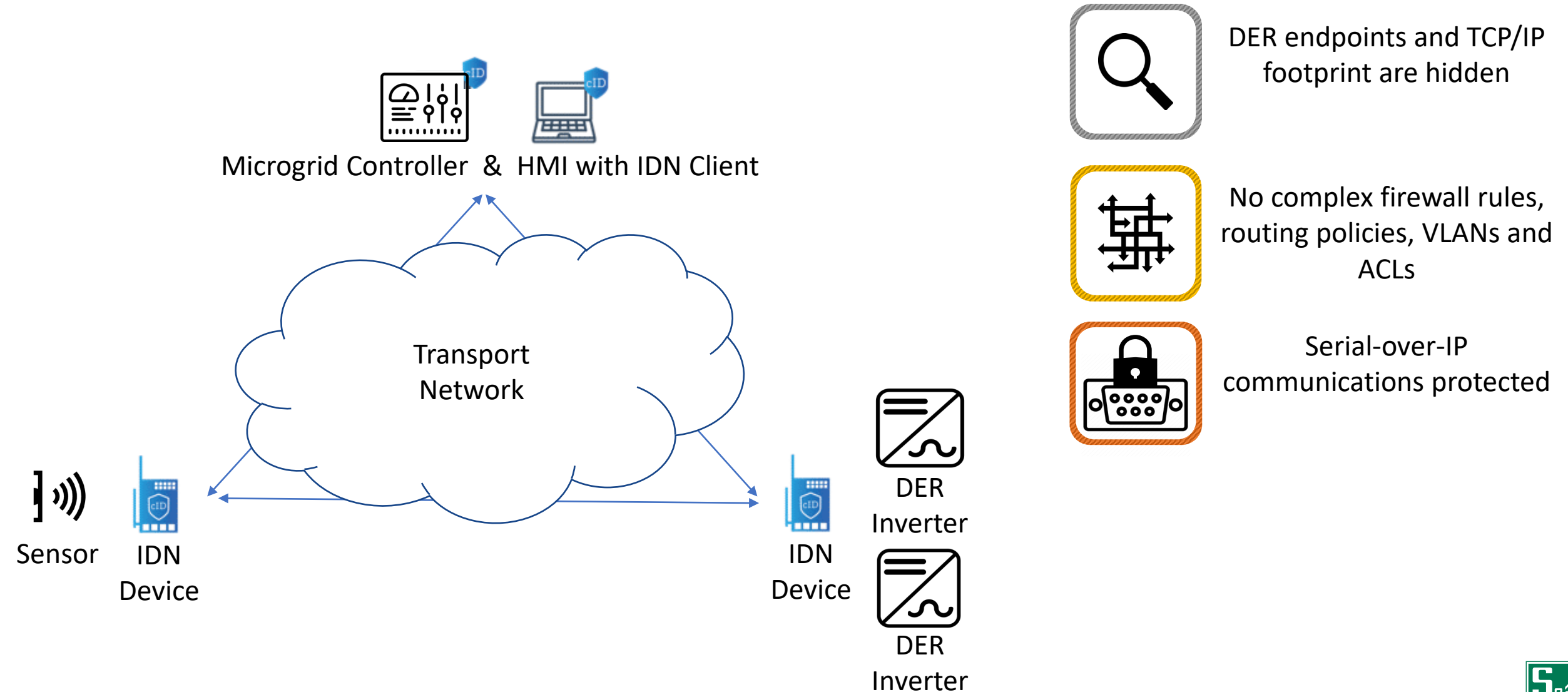
Microgrid PKI

- Enterprise Java Beans Certificate Authority



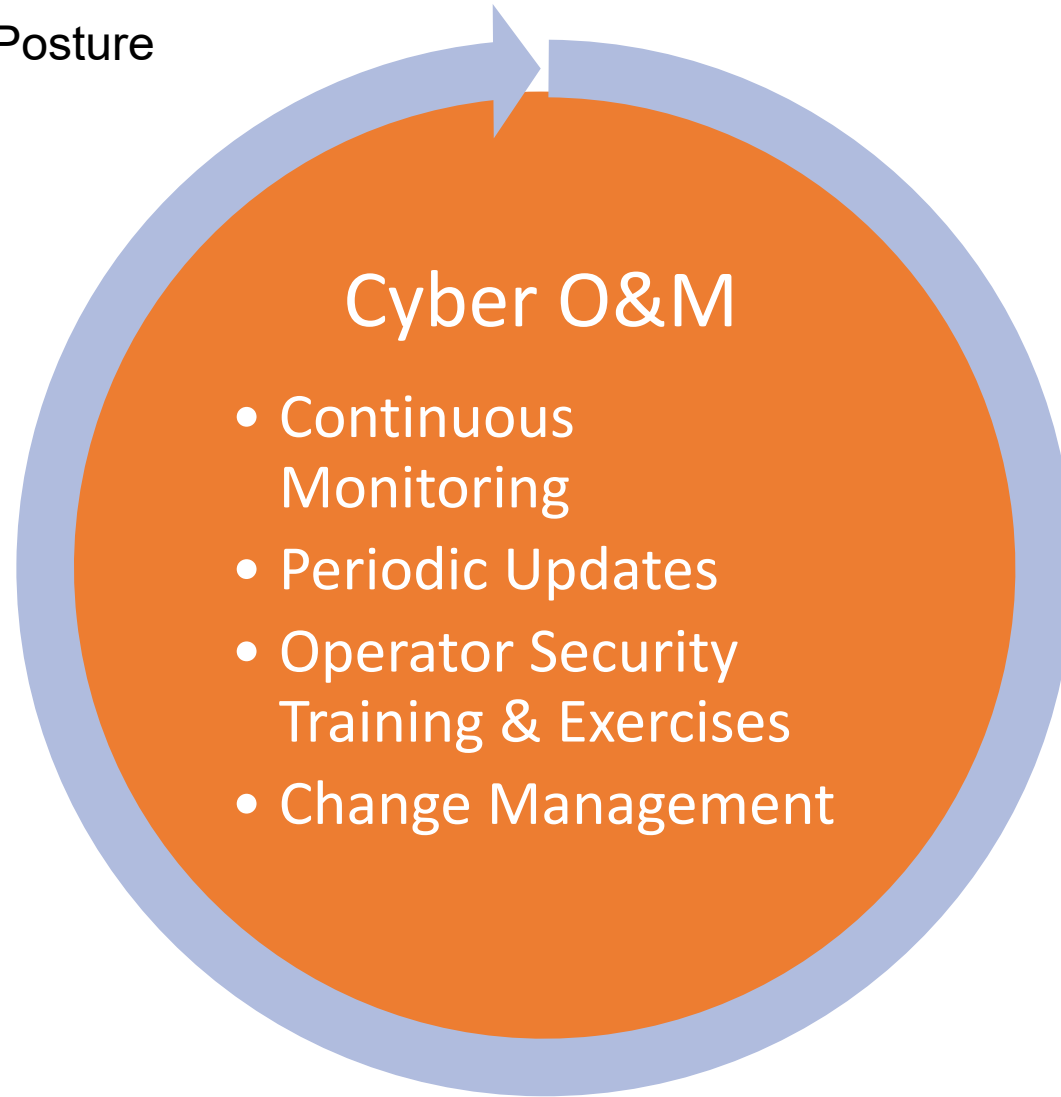
Identity Defined Network

Protecting Power System Communications



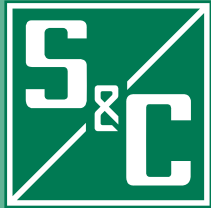
Cyber Sustainment

- Maintaining Cybersecurity Posture



Questions??

```
010 010101 01111100111011 0011 10101010100 01010 010 1111 001 1001 01 11 0011001100 1 1
000 000000 01000001011000 0000 00000000000 00000 000 1000 011 011 00 01 1011000011 0 0
100 101011 00100011000100 0100 11001101011 01101 1 1 0100 10 00 0100110011 0 1
101 100101 10100000011000 1010 11011100101 1110010 1010 00 1000 01 10 0100110011 0 1
010 010100 01011100111011 0011 00100010100 000 0
100 101010 01000011001100 0100 010001010110001 0
101 101111 10100011100100 1100 1101110111101 1 1
011 010101 11111100111011 1011 011101 10011 0 1
010 011010 01011111011111 0010 0010 01 01 1 0
101 10101111010001100010001100 1101 10 01 0 1
111 11010111011110011001101001 1111 11 1 1 0
1000 01 10 0100110011 0 1
1011 01 11 010101100 1
0111 10 01 1110111101
0100 11 10 0100111101
1011 01 11 111101100
```



Thank You

Chad.Douglas@sandc.com

James.Lee@sandc.com

Michael.Higginson@sandc.com

AuraLee.Keating@sandc.com