BIRD ICRDE: Task 17 - **ICS Security by Design**

Empowering the Future:

Security by Design in the Energy Sector

Dr. Dov Shirtz - BGU

Israel-U.S. Energy Center
(Cyber Topic)

October 2023

Introduction

Task 17 deals with the future

= > We are not bound to current concepts

We are not trying to predict the future; we try to be visionary

We propose a framework for achieving the Security by Design goal

Assumptions and prerequisite

Law and regulations

Industry requirements will force the use computerized devices at all levels of the Purdue model

We do not negate any security standard, or best practice, but rather, we mandate them

Framework

We already propose a framework consists of

- **Constructing an ecosystem that includes all participants**
- **Non-technological Issues**
- **Technological Issues**

Presented in report meeting #4

Framework

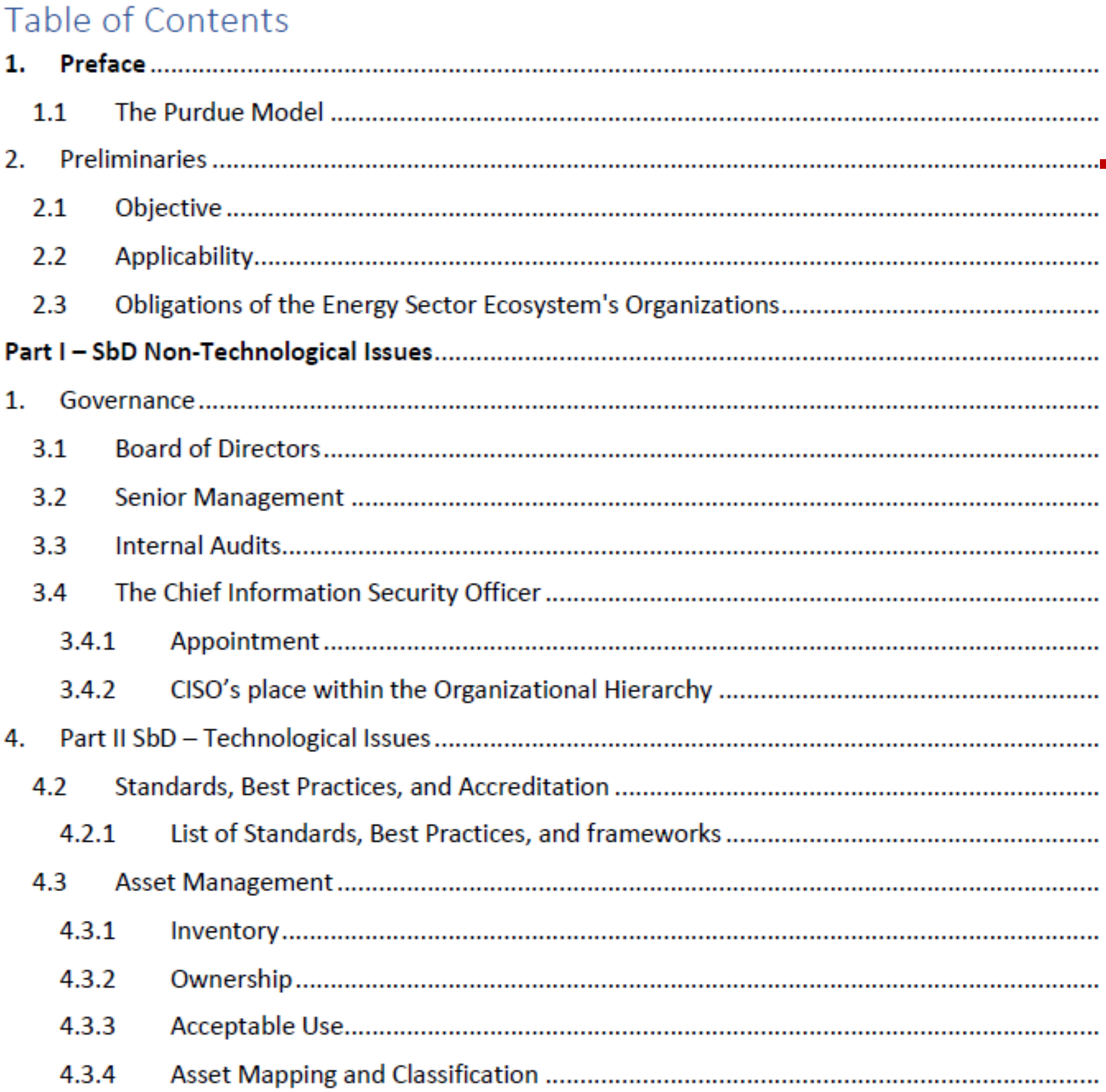
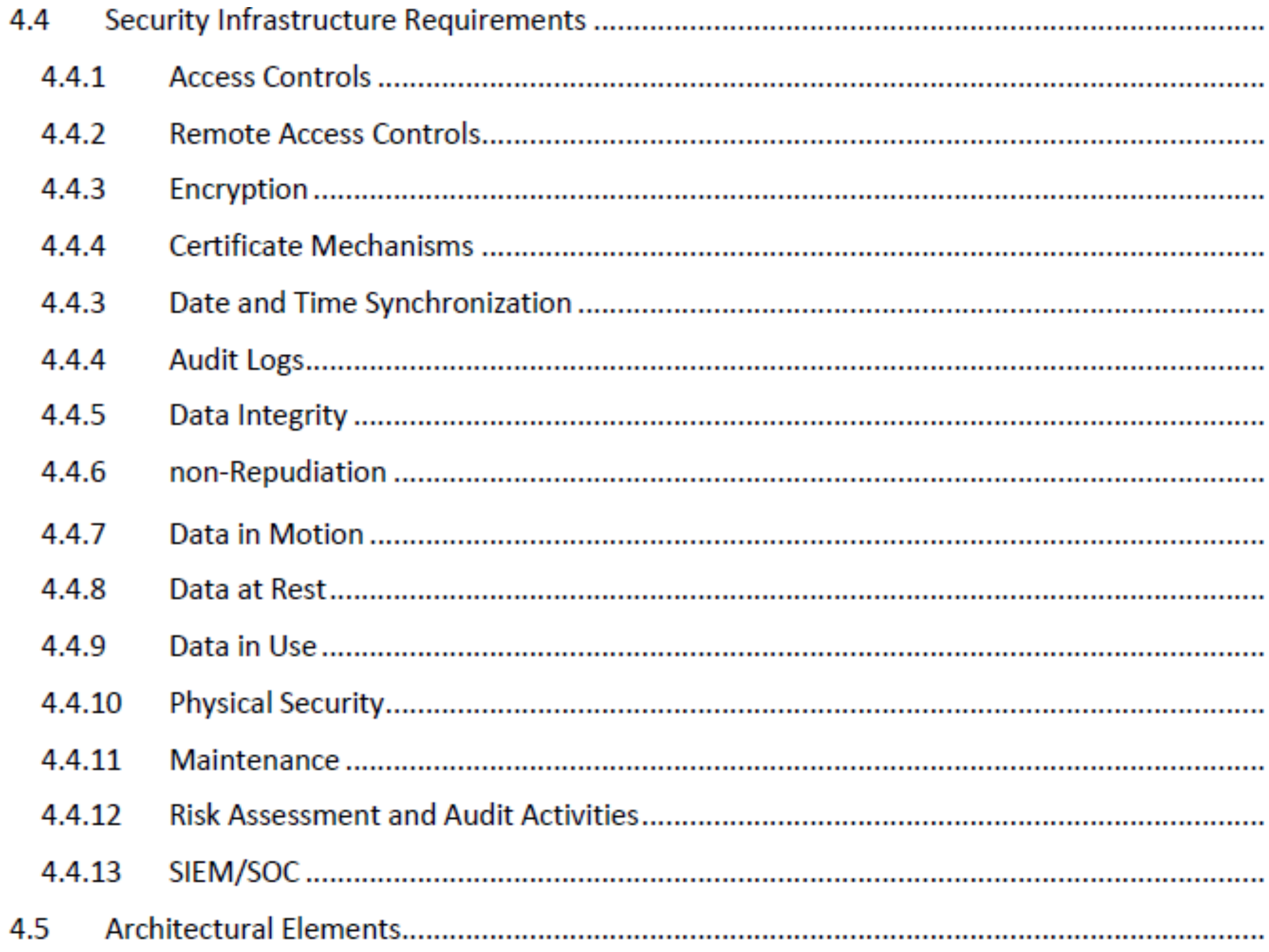
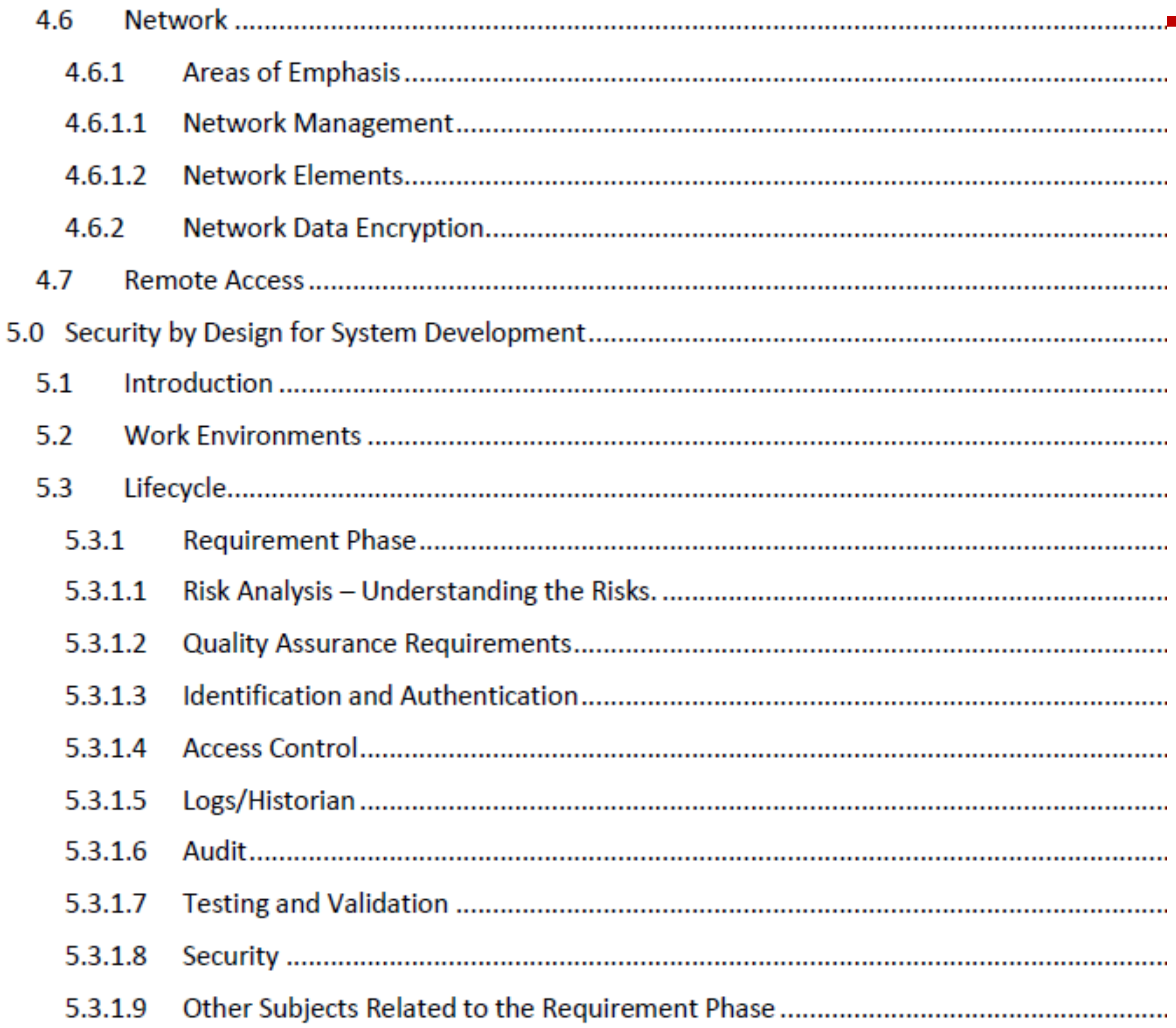


Table of Contents

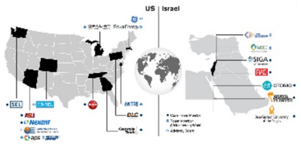
Framework

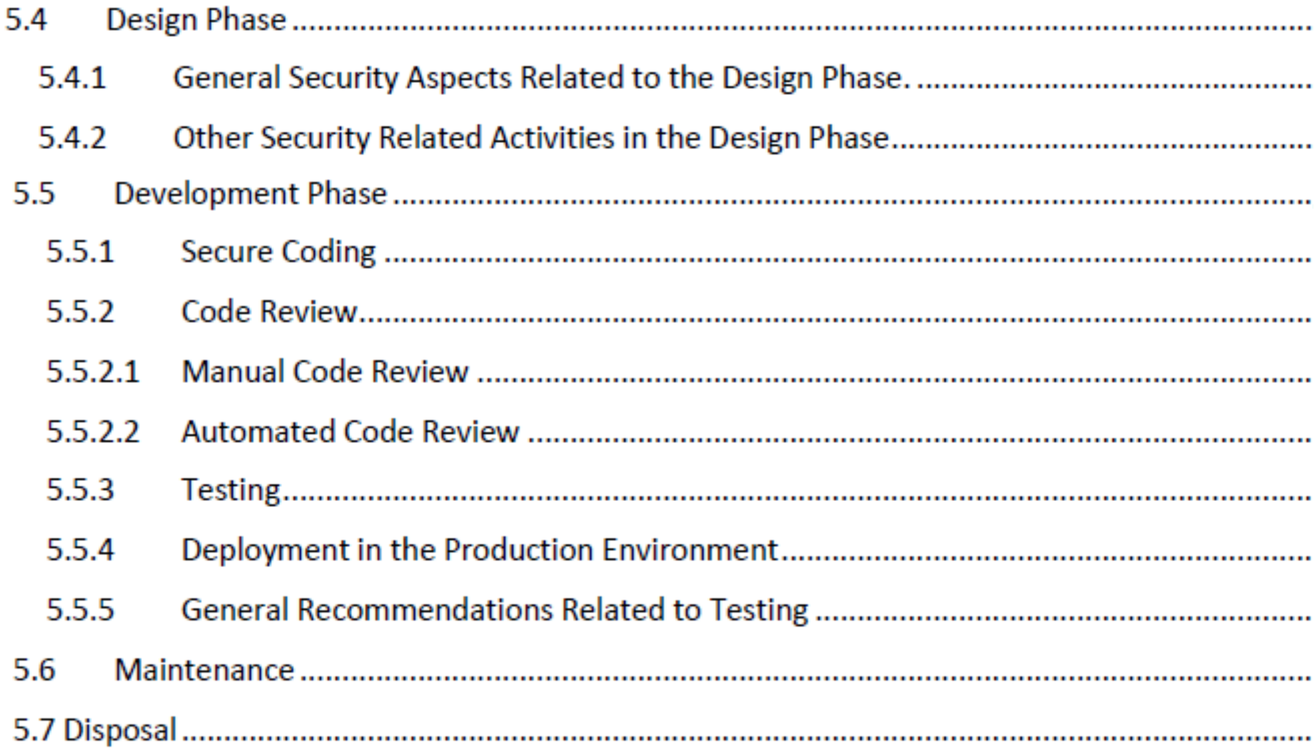


Framework

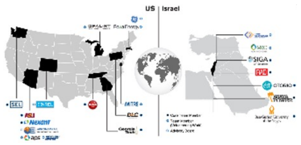


Framework

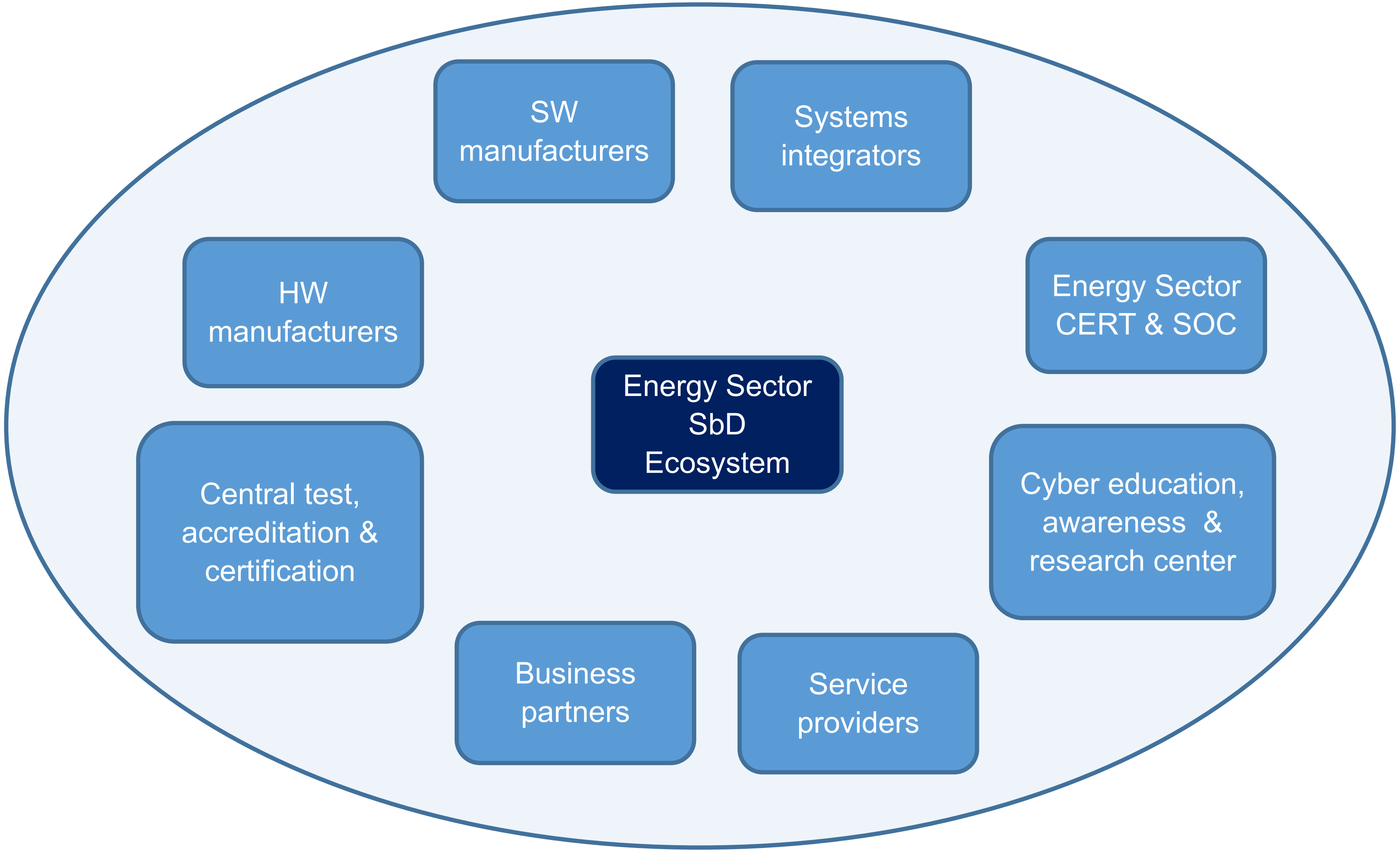




Framework - Ecosystem



Dov Shirtz



Energy Sector SbD Ecosystem

SW manufacturers

Systems integrators

HW manufacturers

Energy Sector CERT & SOC

Central test, accreditation & certification

Cyber education, awareness & research center

Business partners

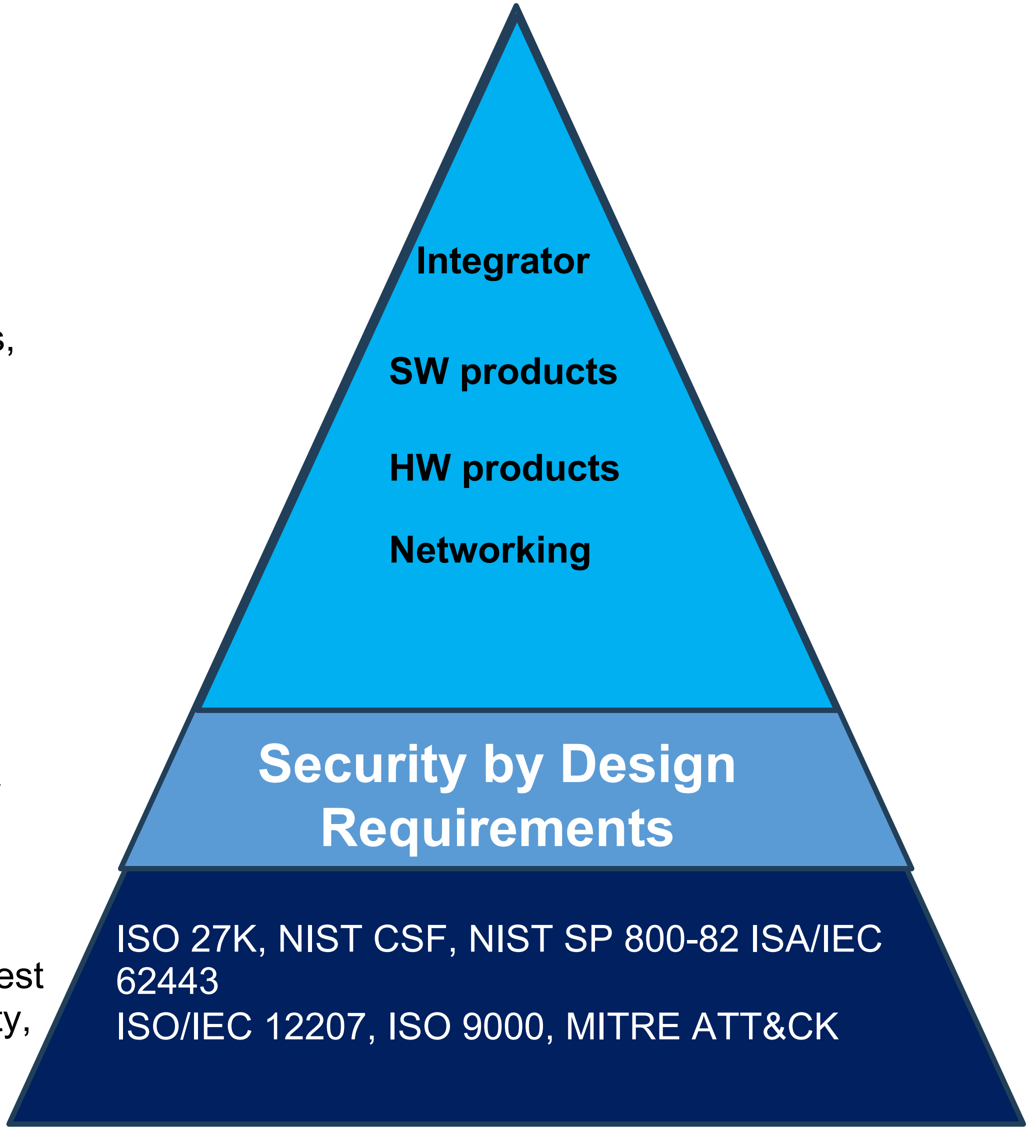
Service providers

Framework

Artifacts, Integrators,

SbD for the energy sector
May 2023

Standards, regulations, Best Practices, Security, Quality, testing



Integrator

SW products

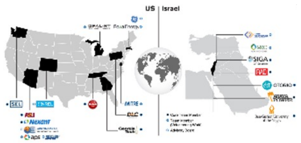
HW products

Networking

Security by Design Requirements

ISO 27K, NIST CSF, NIST SP 800-82 ISA/IEC 62443
ISO/IEC 12207, ISO 9000, MITRE ATT&CK

This presentation



The question was how do we see the future end node

Topics

- **End node**
- **Connectivity**

End Node

End nodes

Definition: End node

“a peripheral unit in a network, or a primary designated unit within that network. IT professionals and others use the term "end node" to specify a certain hardware component of a network that has its own role and properties within that network system.” [2]

[2] Technopedia. https://www.techopedia.com/definition/26122/end-node last accessed 15 Jul. 2023.

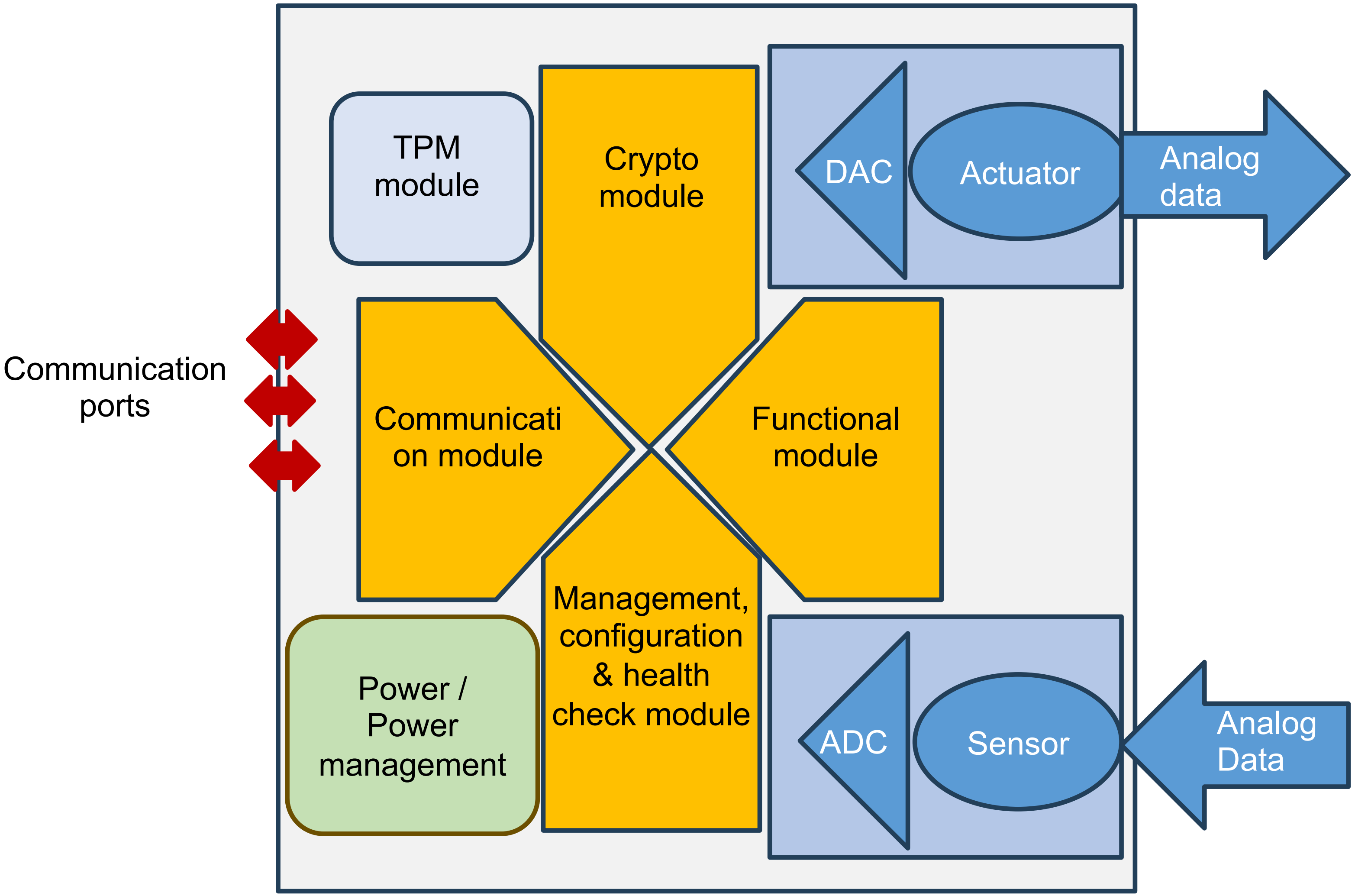
End nodes

Requirements

- **Functionality –** the physical functionality sensor, actuator, switch, …
- **Connectivity –** as today, not directly to the immediate upper layer, to the cloud,
- **Robustness -** to side channel attacks, “regular” cyber attacks
- **Security –** encryption of communication, digital signature
- **Visibility –** health check
- **Speed and Parallelism –** real time, near real time
- **Maintenance** – timely, secure and easy

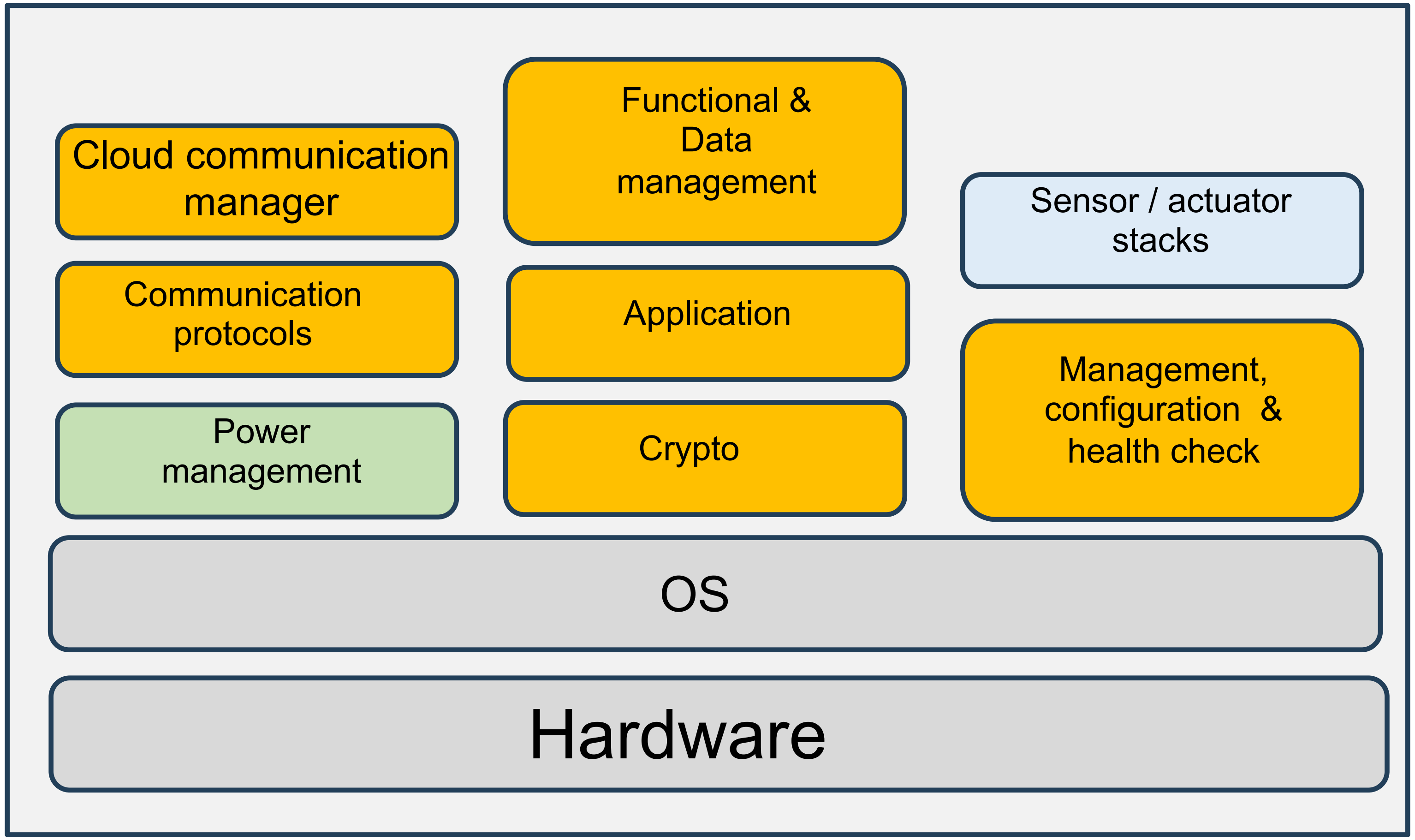
End nodes – hardware components HL diagram (partial)

IoT



End nodes – logic perspective diagram

IoT



Cloud communication manager

Functional & Data management

Sensor / actuator stacks

Communication protocols

Application

Management, configuration & health check

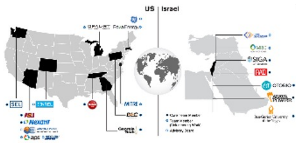
Power management

Crypto

OS

Hardware

End nodes – benefits from the suggested infrastructure

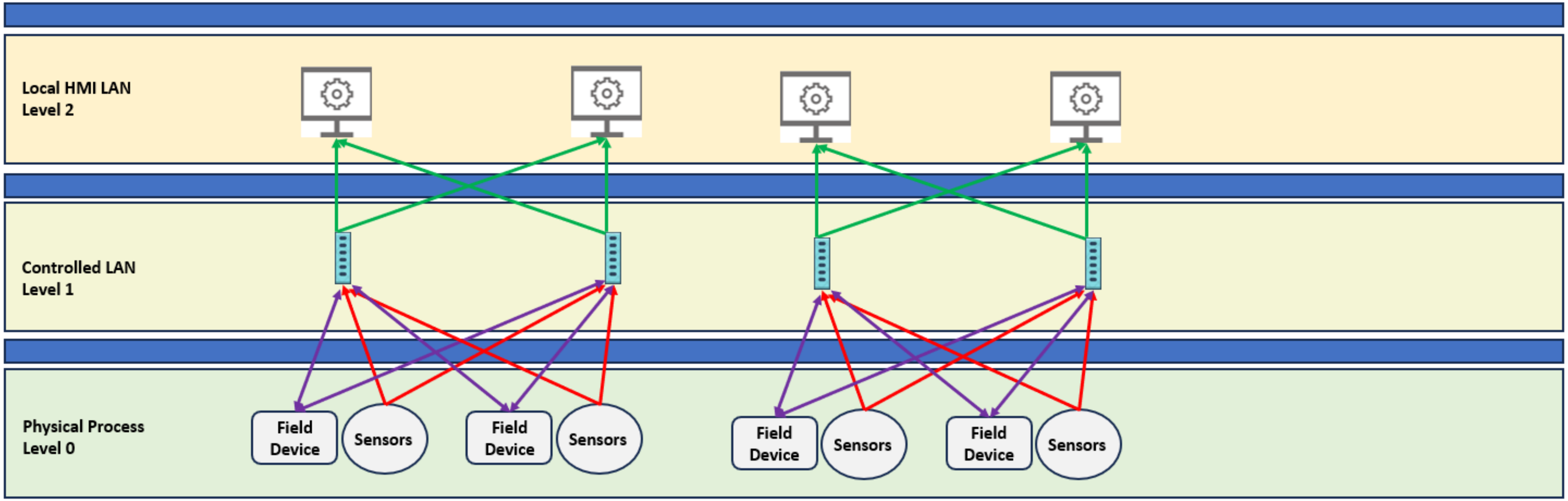


- Higer level of cyber security
- Potential edge computing capabilities
- Simultaneous cloud and non-cloud connectivity
- Potential of using Zero trust (ZT) and moving target defense (MTD) capabilities
- Certificate access control

Connectivity

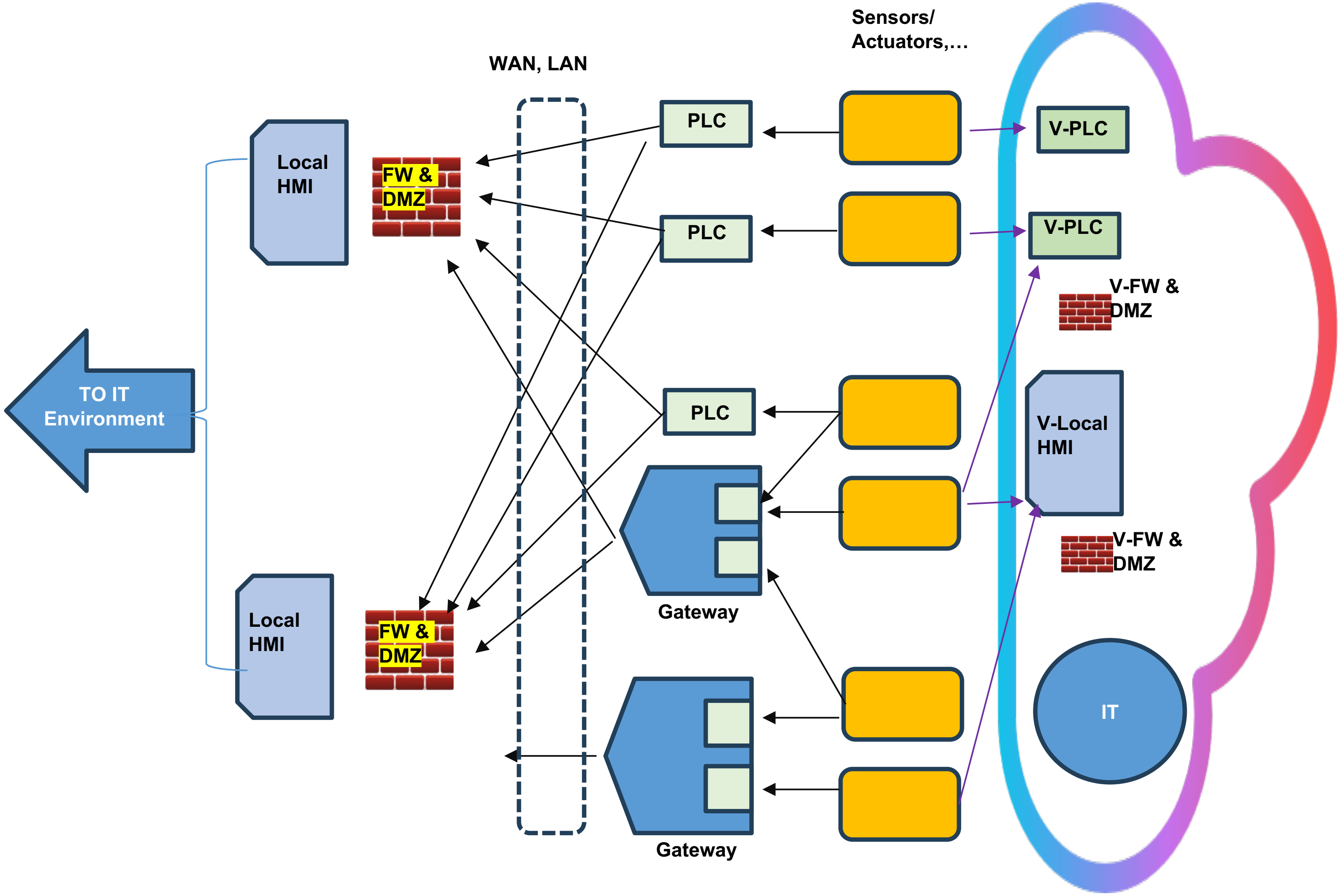
Connectivity

Duplication

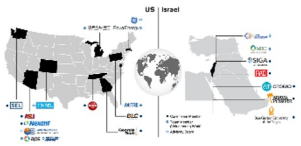


Duplication is the name of the game

Connectivity - variants

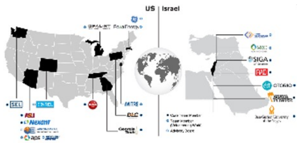


Connectivity - variants



#	Connection 1	Connection 2	Remarks
1	Physical PLC	Physical PLC	Same as today except the requirement to duplicate the number of connections
2	Physical PLC	Gateway	We assume a gateway with PLC capability. Moreover, we assume that the gateway converges the Physical PLC and the gateway that communicate to the upper levels of the Purdue model, e.g., HMI
3	Gateway	Gateway	We assume a converge of PLC and gateway that communicate to the HMI.
4	Physical PLC	Virtual PLC (V-PLC)	Virtual PLC is a software code that resides in the cloud. Communication to it may be set in various protocols, e.g., 5G, Wi-Fi, etc.
5	Virtual PLC (V-PLC)	Virtual PLC (V-PLC)	See (4) above. The connectivity can be done to the very same cloud to different PLCs, or to two different clouds.

Connectivity – Derived benefits

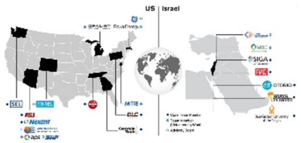


- **Edge computing**
- **Maintenance**
- **Cloud**
- **Cyber robustness and resilience**
- **Using advance cyber security methods**

  Zero Trust (ZT)

  Moving target defense (MTD)

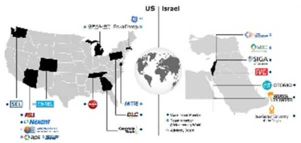
Connectivity – Derived changes



Issues derived from the new form of connectivity

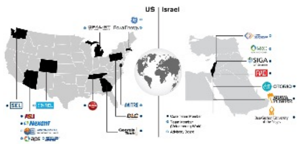
- **Algorithm changes**
- **Work method change**

Conclusion



- It’s a long way
- Cost
- Better Cyber security
- Security by Design

Conclusion



We achieve

- **Encryption**
- **Authentication**
- **Visibility**
- **Blockchain**
- **Zero trust**
- **Digital twin**
- **Network segmentation**

BIRD ICRDE: Task 17 - **ICS Security by Design**

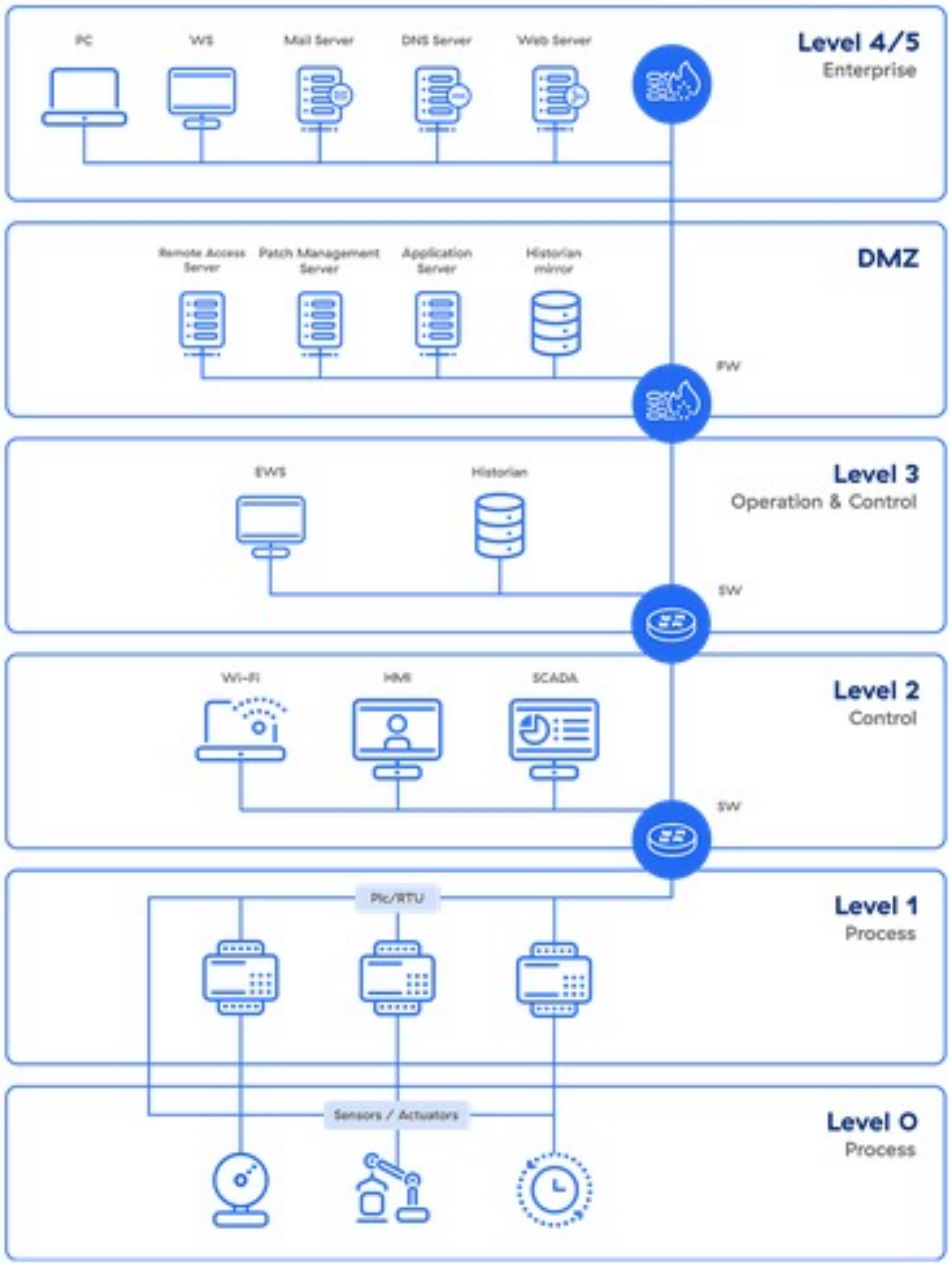
End of

Empowering the Future:

Security by Design in the Energy Sector

Questions Please

Purdue – basic model



https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security