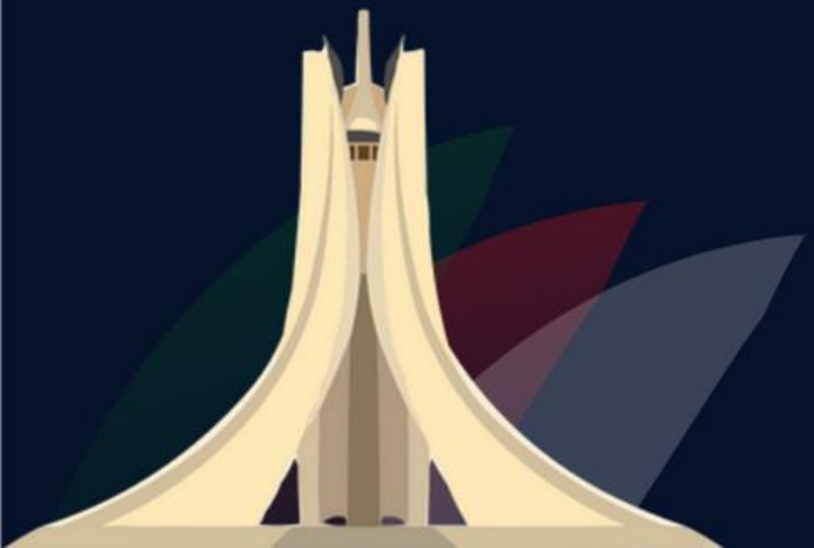
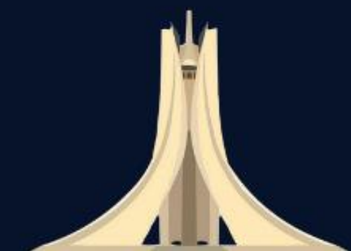
OWASP ALGIERS



OT Security & ISA/IEC 62443 Standards



Who am I ?

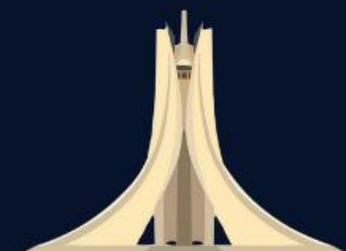
Mehdi Nacer KERKAR

IT/OT Cyber Security Consultant

- Cybersecurity Consultant Lead @ PwC Algeria
- Board Advisor @ OWASP Algiers Chapter
- Membership Director @ CSA Algeria
- Global Member @ ISC2
- Center of Cyber Safety & Education SASO Volunteer
- Global Member & Mentee @ ISA
- Guest Lecturer @ HIS University
- Cybersecurity Mentor @ TAP

Summary

- What is OT
- Automation Pyramid
- Challenges
- ISA/IEC 62443 Standards
- CSMS
- Bonus



What is OT / What is IACS

- Operational Technology is all what is used to control Physical Process
- A mix of Hardware & Software Systems
- Used to Monitor, Control and Supervise Physical Processes

- Including:
  - Sensors & Actuators
  - Programmable Logical Controllers (PLCs),
  - Human-Machine Interfaces (HMIs),
  - Supervisory Control & Data Acquisition (SCADA) Systems.

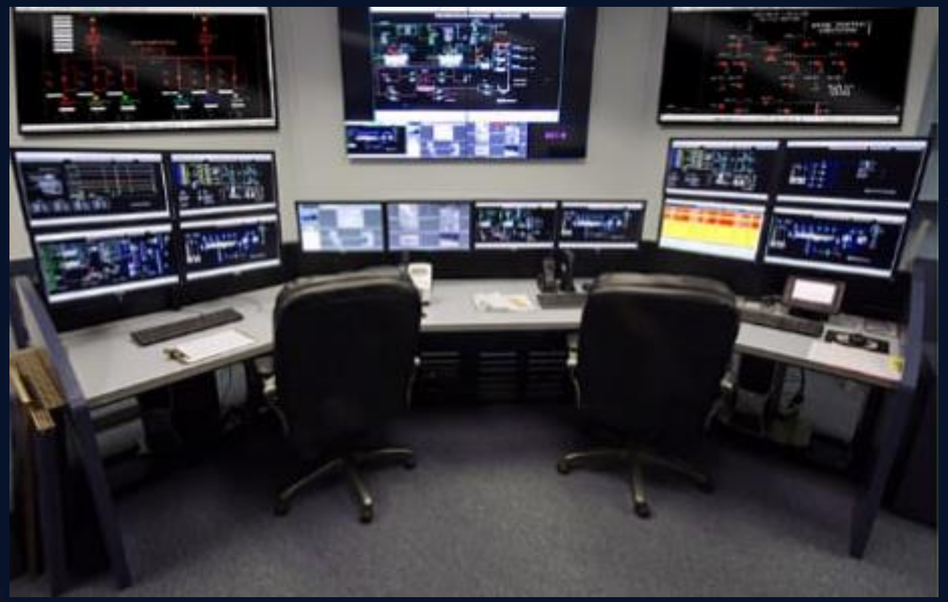
Industrial Automation & Control Systems



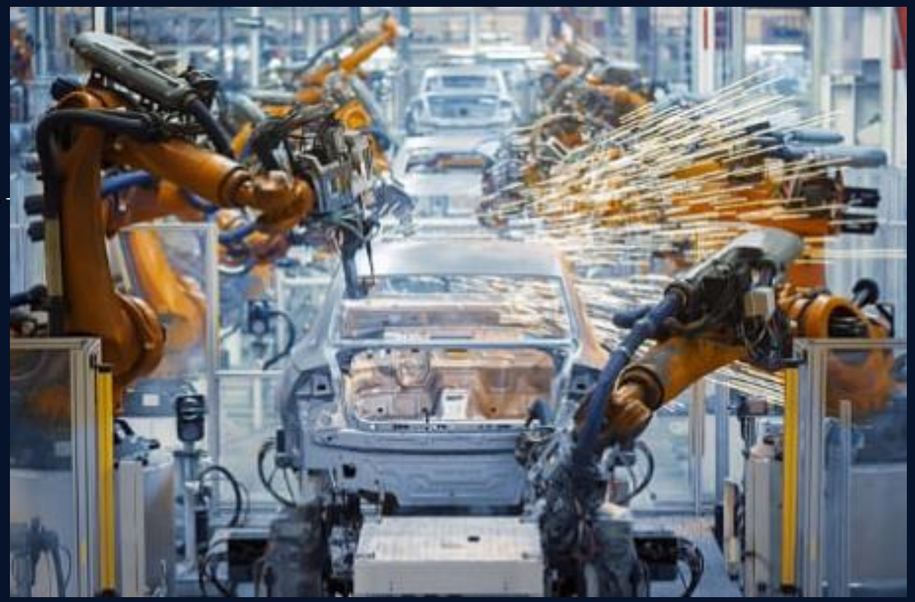


OT is used for ?

Monitoring, Control, Operation



Industrial Automation



Where is OT ?

Water & Sewage

Electricity

Transportation

Critical manufacturing

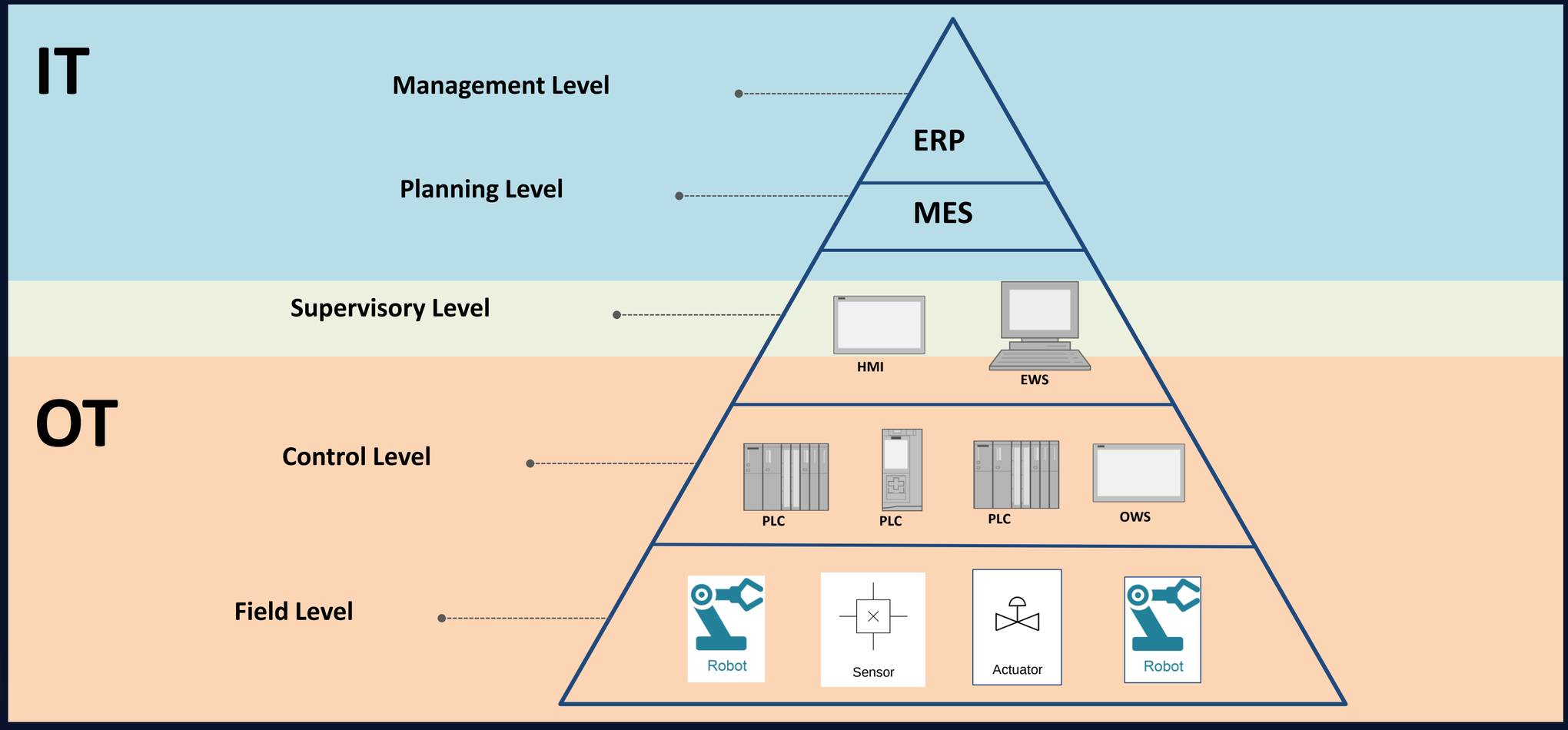
Industrial Automation

Oil & Gas

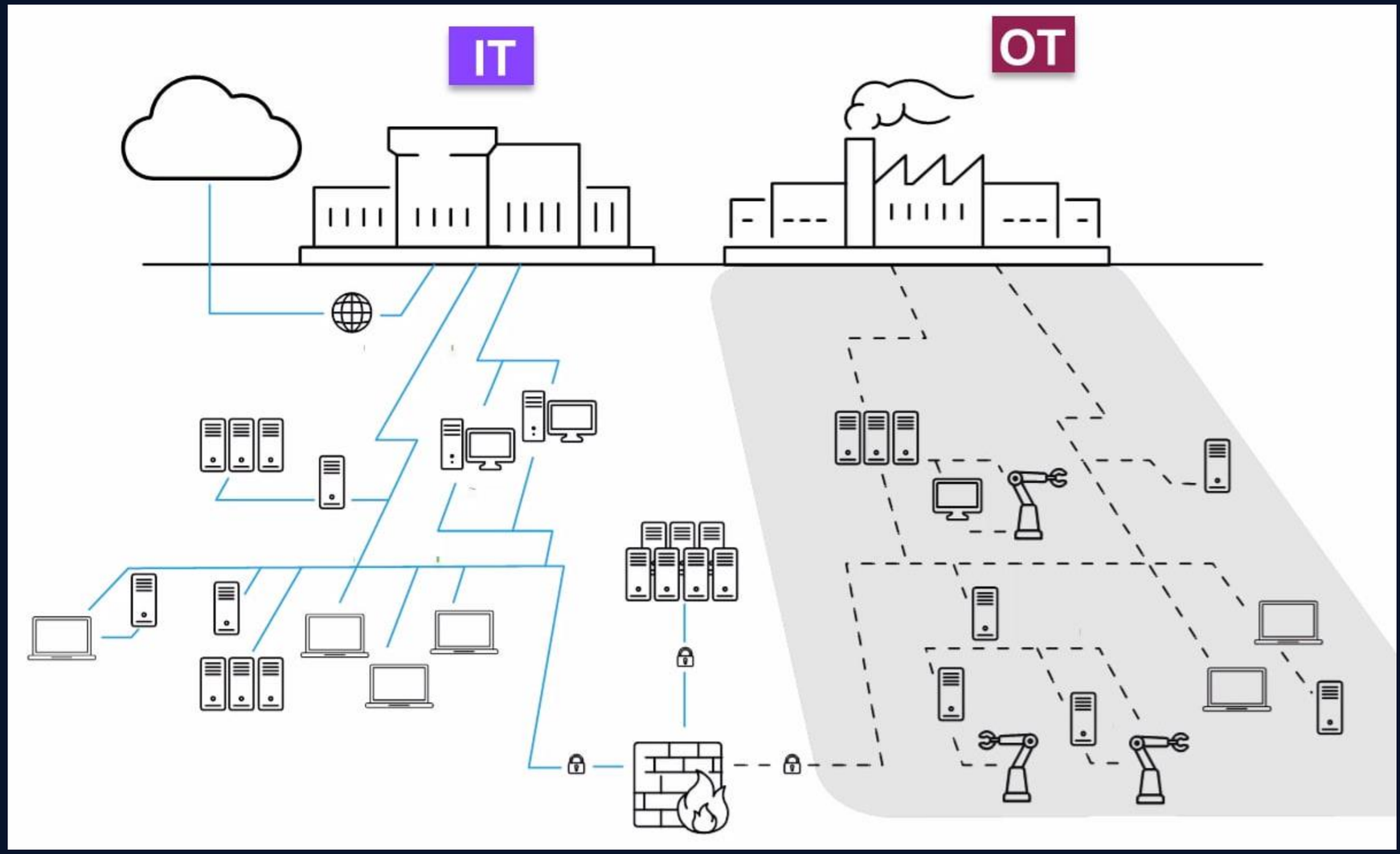
Building Management

All around Us !!

Automation Pyramid

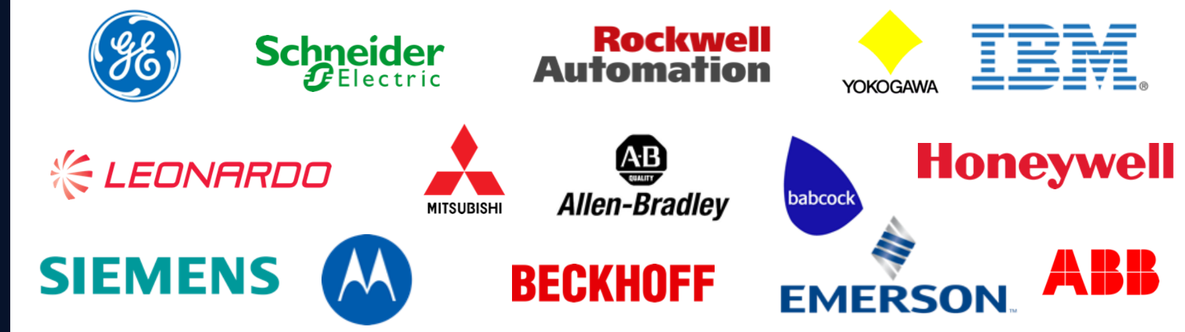


Same challenges of IT Professionals



OT Diversity

Industry Vendors

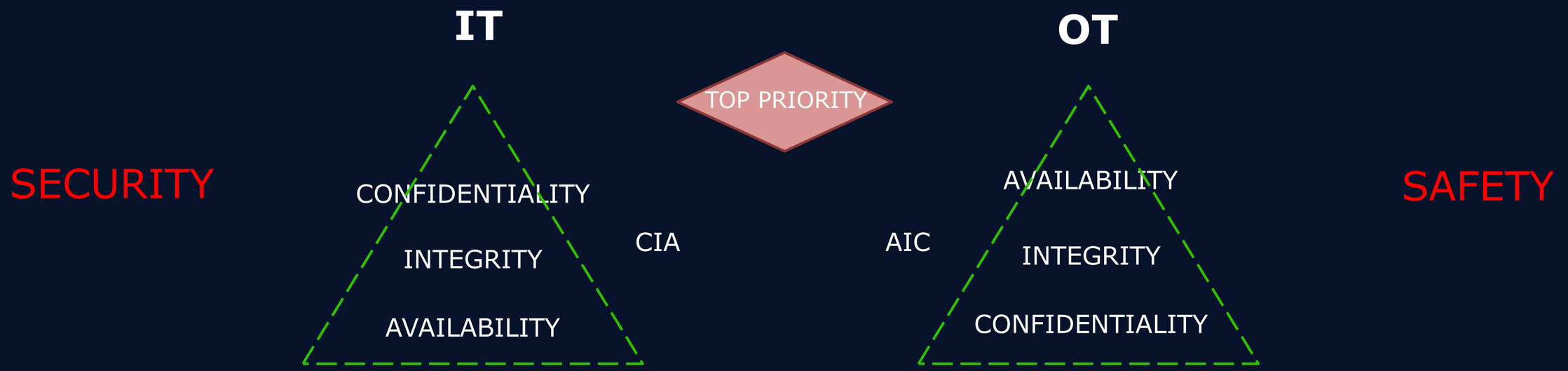


Industrial Protocols

ABB PGP2PGP, Aspentech Cim/IO, BACNet, Beckhoff ADS, BSAP IP, CC-LINK IE, CEI 79-5/2-3, COTP, DNP3, Emerson DeltaV, Enron Modbus, EtherCAT, EtherNet/IP - CIP, Foundation Fieldbus, Foxboro IA, Generic MMS, GE EGD, GE iFix2iFix, GE SRTP, GOOSE, Honeywell Experion protocols, Kongsberg Net/IO, IEC 60870-5-7 (IEC 62351-3 + IEC 62351-5), IEC 60870-5-104, IEC-61850 (MMS, GOOSE, SV), IEC DLMS/COSEM, ICCP, Modbus/RTU, Modbus/TCP, Modbus/TCP - Schneider Unity extensions, MQTT, OPC, PCCC, PI-Connect, Profinet/DCP, Profinet/I-O CM, Profinet/RT, ROC, Sercos III, Siemens S7, S7 Plus, Telvent OASyS DNA, Triconex TSAA, Vnet/IP

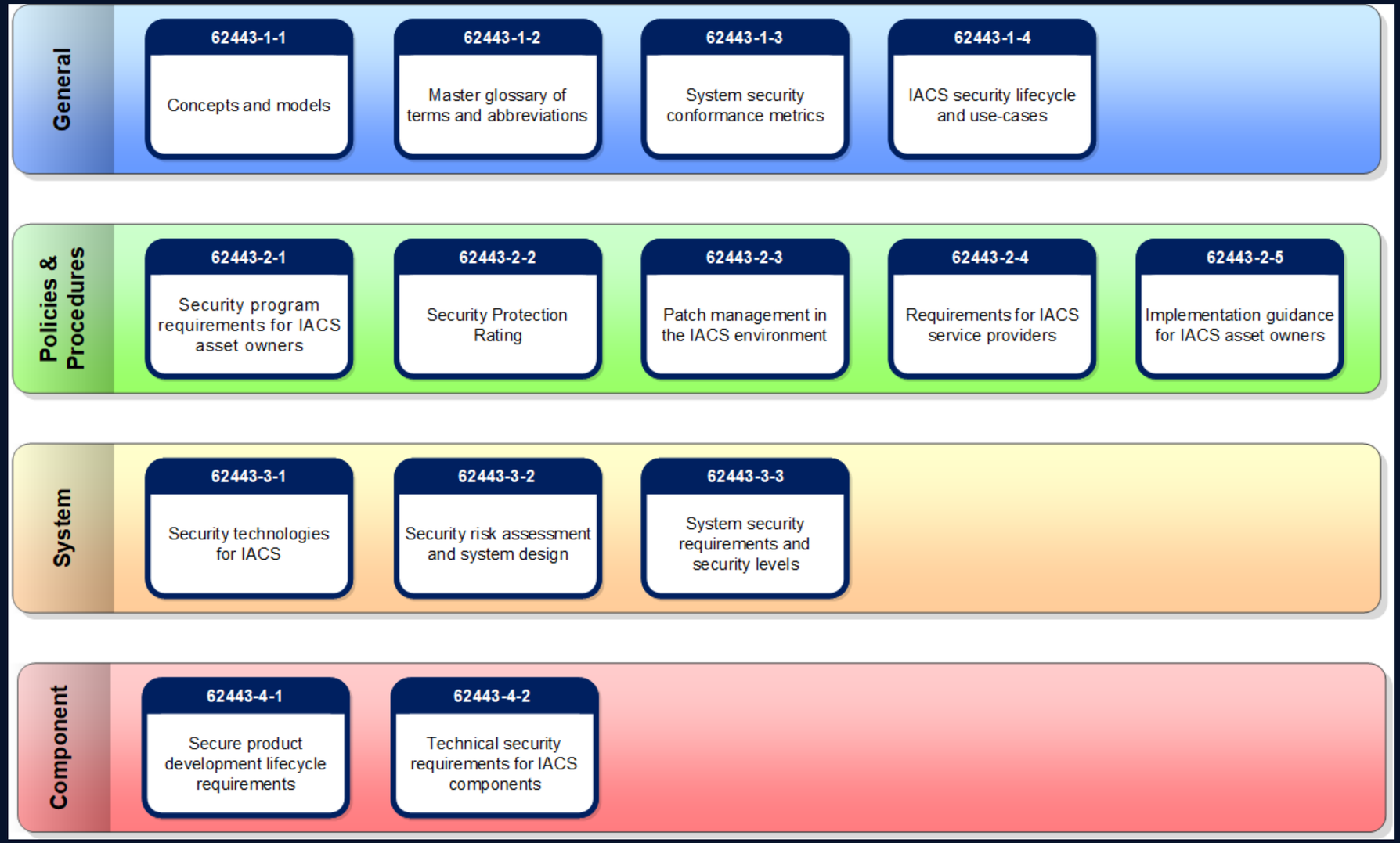
Standards Development Organization

How are IT and OT different ?

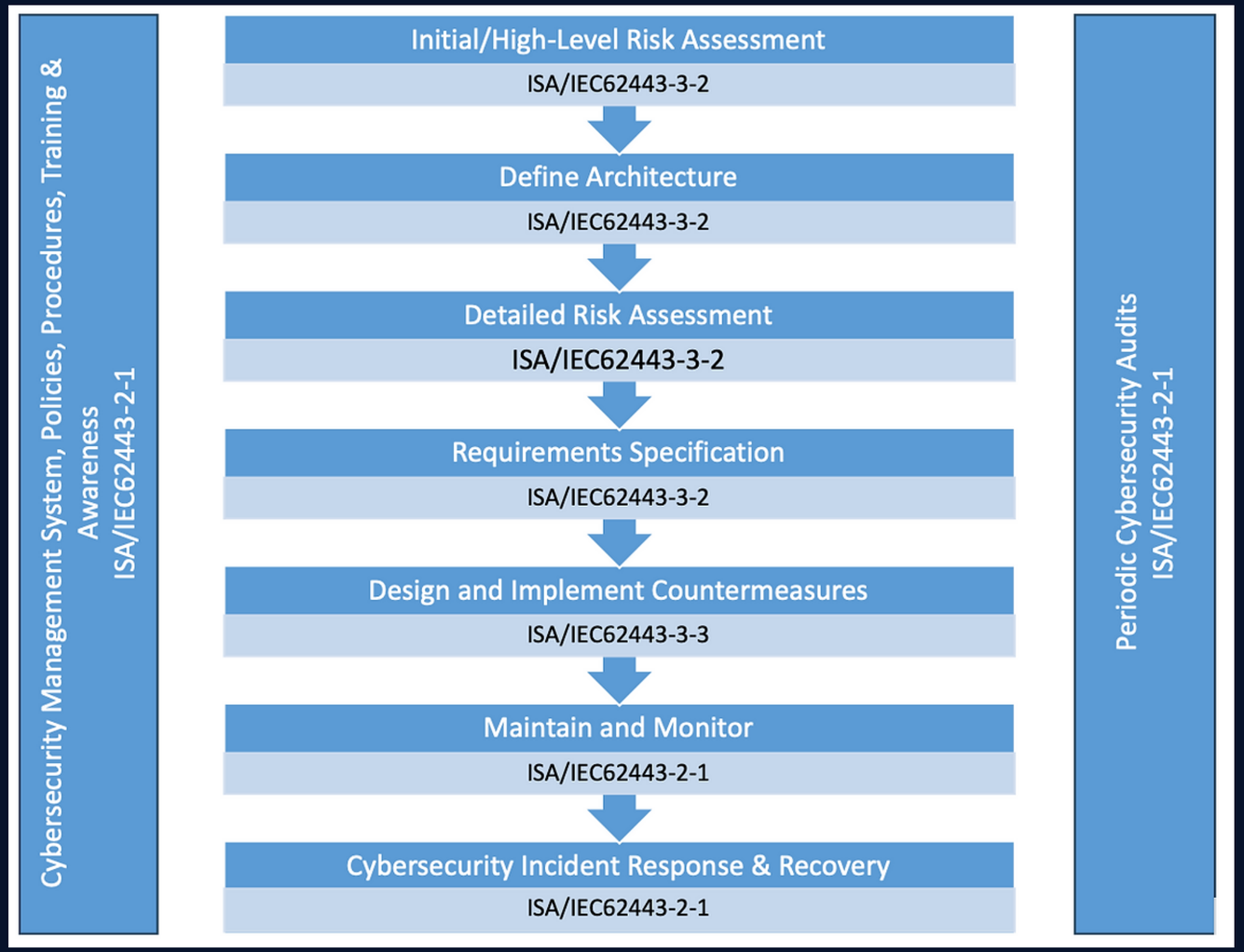


Characteristics Security objective priorities		
Medium, delays accepted	Availability requirement	Very High
Delays accepted	Real-time requirement	Critical
3-5 years	Component lifetime	Up to and 20 years
Regular / Scheduled	Application of patches	Slow / infrequent
Scheduled and mandated	Security testing / Audit	Occasional
High / mature	Security awareness	Increasing

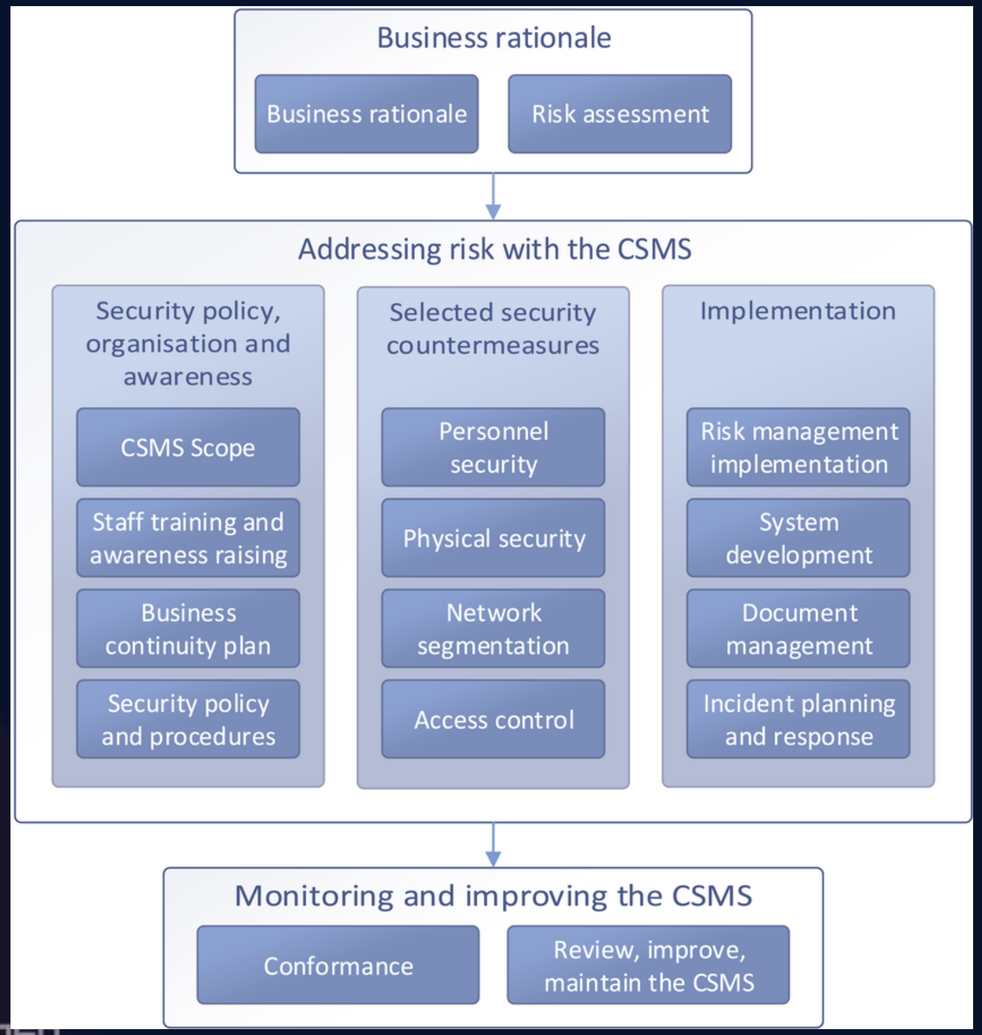
ISA/IEC 62443 Standards



Cybersecurity Management System



Addressing risk with the CSMS



Calculating Risk

	Target Security Level	Capability Security Level	Achieved Security Level
Acronym	(SL-T)	(SL-C)	(SL-A)
Definition	The security level equipment should reach according to the system-level risk assessment	The security level equipment is capable of according to the CRs it supports as per IEC 62443-4-2	The security level that equipment achieves
Objective	SL-T ≥ level defined by risk assessment	SL-C ≥ SL-T	SL-A ≥ SL-T

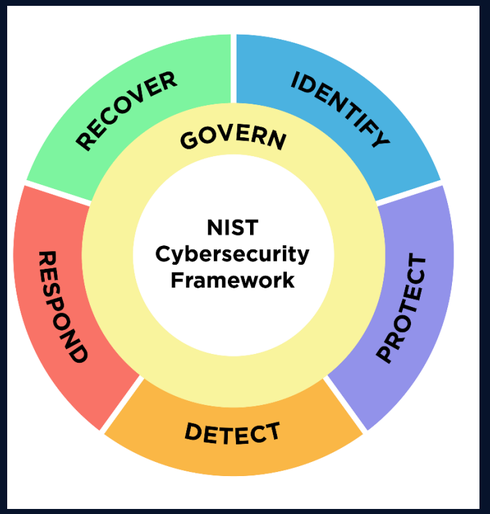
Risk	SL-T
Low	1
Medium	2
Medium High	3
High	4

Mapping ISA/IEC standards with NIST CSF & ISO 27001

PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	· **CIS CSC** 1, 5, 15, 16 · **COBIT 5** DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.5.1 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Physical access to assets is managed and protected	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 · **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: Remote access is managed	· **CIS CSC** 12 · **COBIT 5** APO13.01, DSS01.04, DSS05.03 · **ISA 62443-2-1:2009** 4.3.3.6.6 · **ISA 62443-3-3:2013** SR 1.13, SR 2.6 · **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	· **CIS CSC** 3, 5, 12, 14, 15, 16, 18 · **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.7.3 · **ISA 62443-3-3:2013** SR 2.1 · **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	· **CIS CSC** 9, 14, 15, 18 · **COBIT 5** DSS01.05, DSS05.02 · **ISA 62443-2-1:2009** 4.3.3.4 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8 · **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7

Mapping ISA/IEC standards with NIST CSF & ISO 27001

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



OWASP ALGIERS

Operation Profile

Asset Owner

- Responsible on the IACS Environment
- Operate IACS, equipment under control

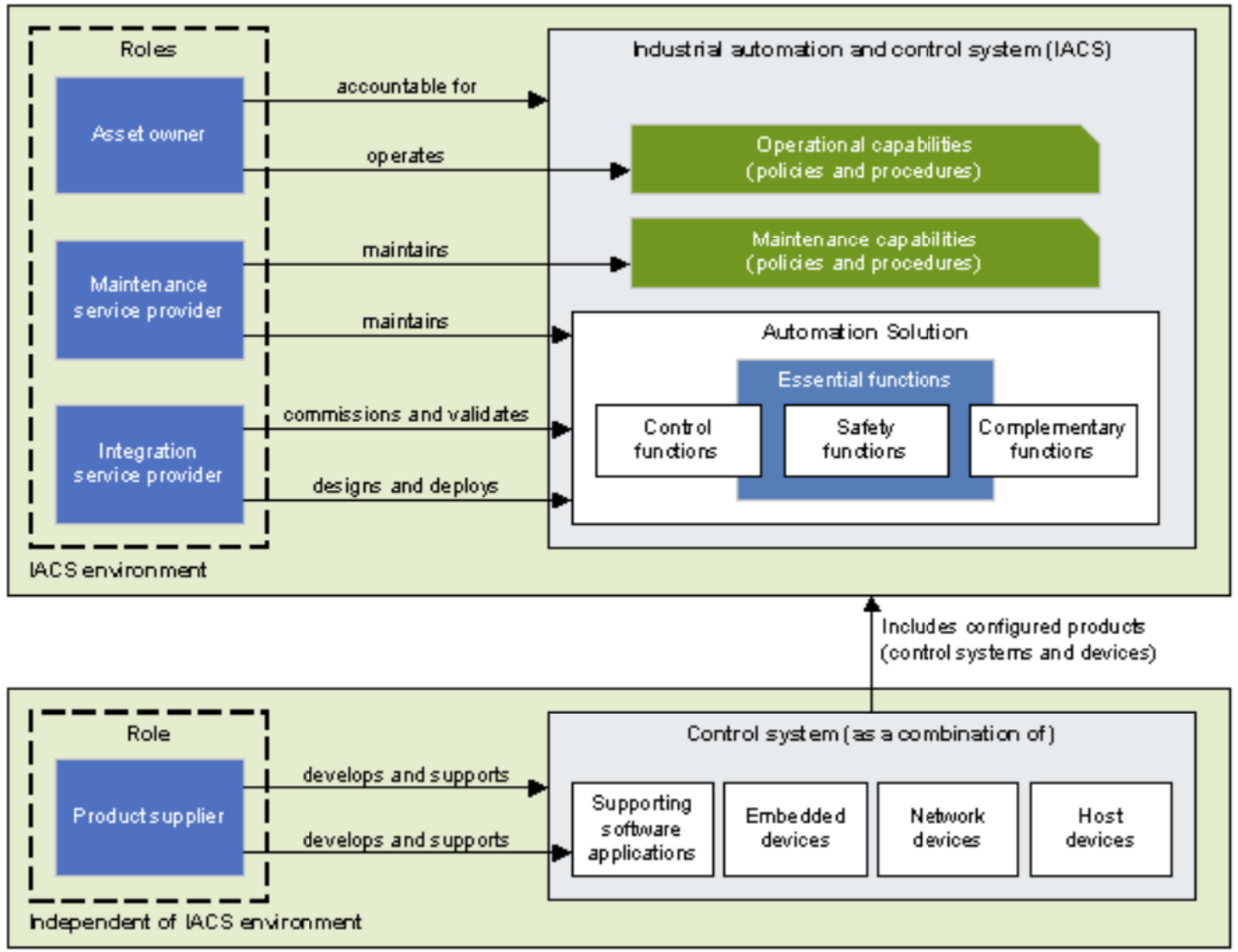
Product Supplier

- Manufacture, Develop and Support IACS hardware & Software problems

Service Provider
Maintenance & Integration

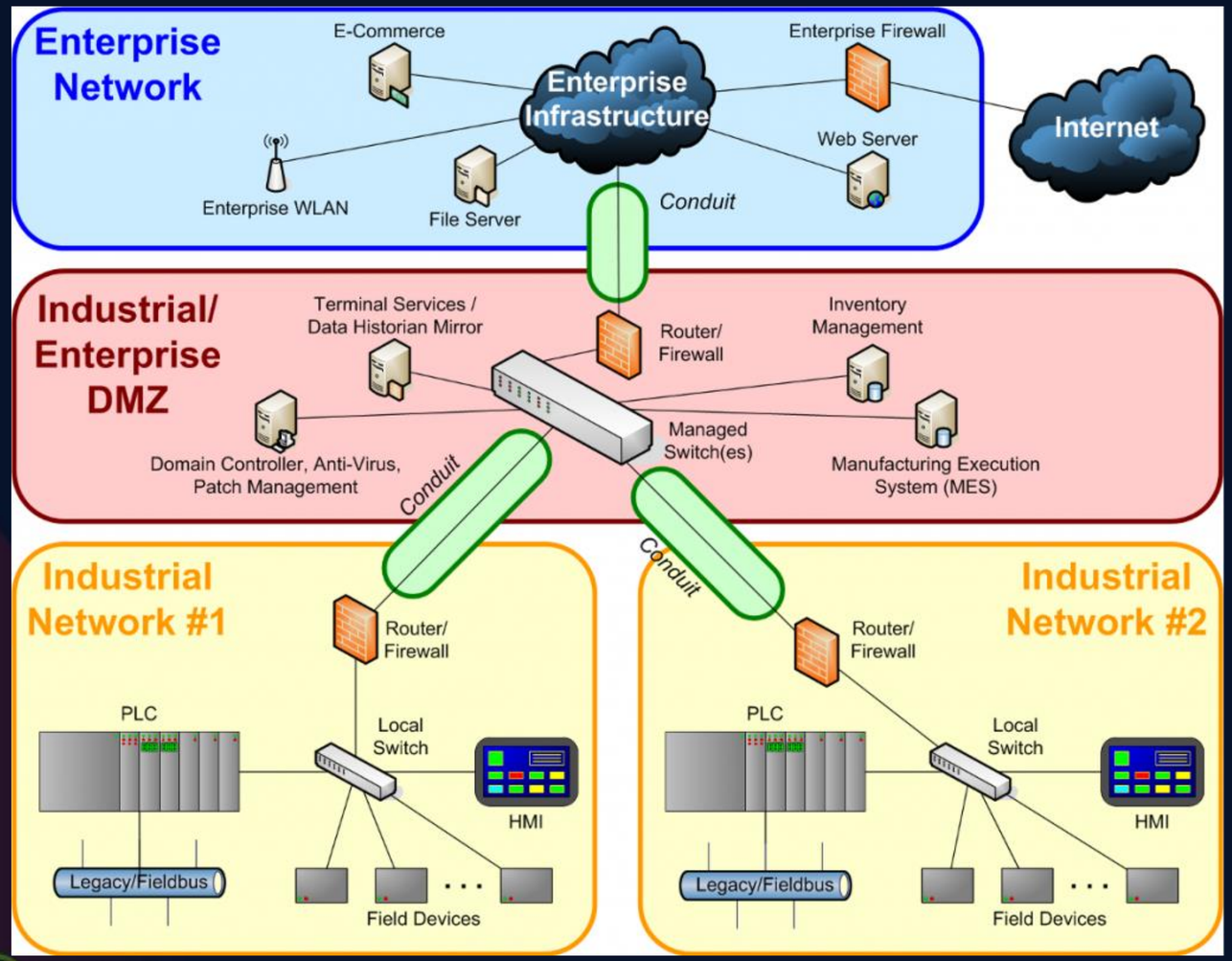
- Integrate, Maintain and Concept
- Analyze, Install, Configure and Test

Stakholders Roles, Responsibilities and relevant 62443 standards



- Asset Owner
  - Part 1-1 – Concepts and models
  - Part 2-1 – Security program requirements
  - Part 2-2 – Security protection rating
  - Part 2-3 – Patch management
  - Part 3-2 – Risk assessment and system design
- Maintenance Service Provider
  - Part 1-1 – Concepts and models
  - Part 2-4 – Service providers
- Integration Service Provider
  - Part 1-1 – Concepts and models
  - Part 2-4 – Service providers
  - Part 3-2 – Risk assessment and system design
  - Part 3-3 – System requirements and security levels
- Product Supplier
  - Part 1-1 – Concepts and models
  - Part 3-3 – System requirements and security levels
  - Part 4-1 – Security development lifecycle
  - Part 4-2 – Component requirements

Zones & Conduits per ISA/IEC 62443-3-2



ISA/IEC 62443-3-2: Security Risk Assessment for System Design

This standard defines the concept of zones and conduits as a methodology for segmenting industrial systems to reduce security risks.

- Zones: Logical or physical groupings of assets with common security requirements.
- Conduits: Secure communication paths that connect different zones while enforcing security policies.

The zone & conduit model helps organizations structure security controls, limit attack surfaces, and ensure defense-in-depth. It's essential for risk assessment and secure system design in OT environments.

OWASP ALGIERS

Bonus

Career option in OT Security

Career Evolution

Manufacturing	Research/Product Development	Advisor/Consulting
CISO	Head of OT Technology	IT/OT Sr Manager
Head of OT Cybersecurity Operations	Head of OT Research	IT/OT Sr Consultant
OT Cybersecurity Engineer	OT Architect	OT Risk Specialist
OT Cybersecurity Maintenance Specialist	OT Architect/Expert	OT Consultant
OT System Analyst	OT Researcher	OT Analyst

OT Certifications

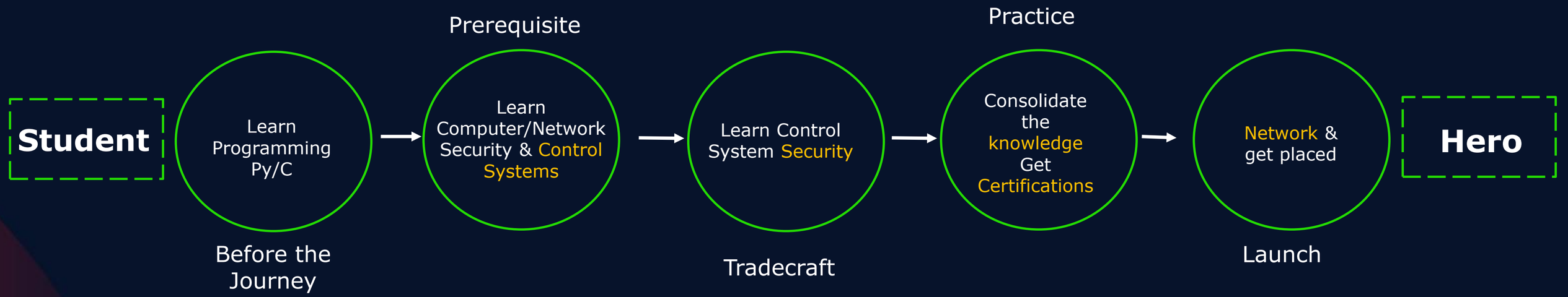
CISSP
CISM / COSM
ICS410 GICSP
ICS515 GRID
ICS610

ISA/IEC 62443 Expert
COSP
ISA/IEC 62443 Maintenance Specialist
ISA/IEC 62443 Design specialist
ISA/IEC 62443 Risk Assessment Specialist

ISA/IEC 62443 Fundamental Specialist

OWASP ALGIERS

OT Security: Zero to Hero



Transition to OT Security

From OT (Industrial) Background

OT Security

1. Build a strong foundation in cybersecurity
   - Cybersecurity principles, practices, and technologies
   - Network security, security architecture, Cryptography and risk management
2. Gain hands-on experience OT Security
   - Network security, security architecture and risk management
3. Pursue relevant certifications

From IT Security Background

OT Security

1. Build a strong foundation in Operational Security
   - System Architecture, Network Architecture
   - Communication Protocols (Modbus, DNP3, Profibus Ethernet/IP etc.,)
2. Gain hands-on experience OT Security
   - Network security, security architecture and risk management
3. Pursue relevant certifications

OWASP ALGIERS

Platform to practice

ControlThings.io

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

https://www.cisa.gov/ics-training-available-through-cisa

https://github.com/dark-lbp/isf

https://github.com/nsacyber/ELITEWOLF

CSET®
CYBER SECURITY EVALUATION TOOL

FORTIPHYD LOGIC GRFICSv2

https://github.com/Fortiphyd/GRFICSv2

Training Game
FACILITY CYBERSECURITY

https://facilitycyber.labworks.org/training/trainingGame/landing

IAAE®
International Academy of Automation Engineering®

Low-cost ICS Testbed
https://github.com/thainnos/LICSTER

opendnp3

https://dnp3.github.io/

Try Hack Me
Attacking ICS Plant

OWASP ALGIERS

Learning & Certifications

OT Security Certifications

GICSP – GIAC Industrial Cyber Security Professional

GRID – GIAC Response and Industrial Defense

GCIP – GIAC Critical Infrastructure Protection

COSP – LIMES SECURITY – Certified OT Security Practitioner TÜV®

COSM – LIMES SECURITY – Certified OT Security Manager TÜV®

EC-Council ICS/SCADA CYBER SECURITY CERTIFIED

Vendors Trainings

DRAGOS ICS/OT CYBERSECURITY TRAINING

FORTINET CERTIFIED SOLUTION SPECIALIST OT Security

NOZOMI NETWORKS Engineer CERTIFIED

ISA/IEC 62443 Standard Certifications

OWASP ALGIERS

Q/A
&
Thank you

Mehdi Nacer KERKAR

IT/OT Cyber Security Consultant