Setting the Standard for Automation™

Eng. Felipe Sabino Costa, MSc, MBA

Moxa Product Marketing Manager Networking and Cybersecurity &
ISA Cybersecurity Director (District 4)

“Securing communications on industrial control systems with cognitive systems”

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

Presenter

Engr. Felipe Sabino Costa

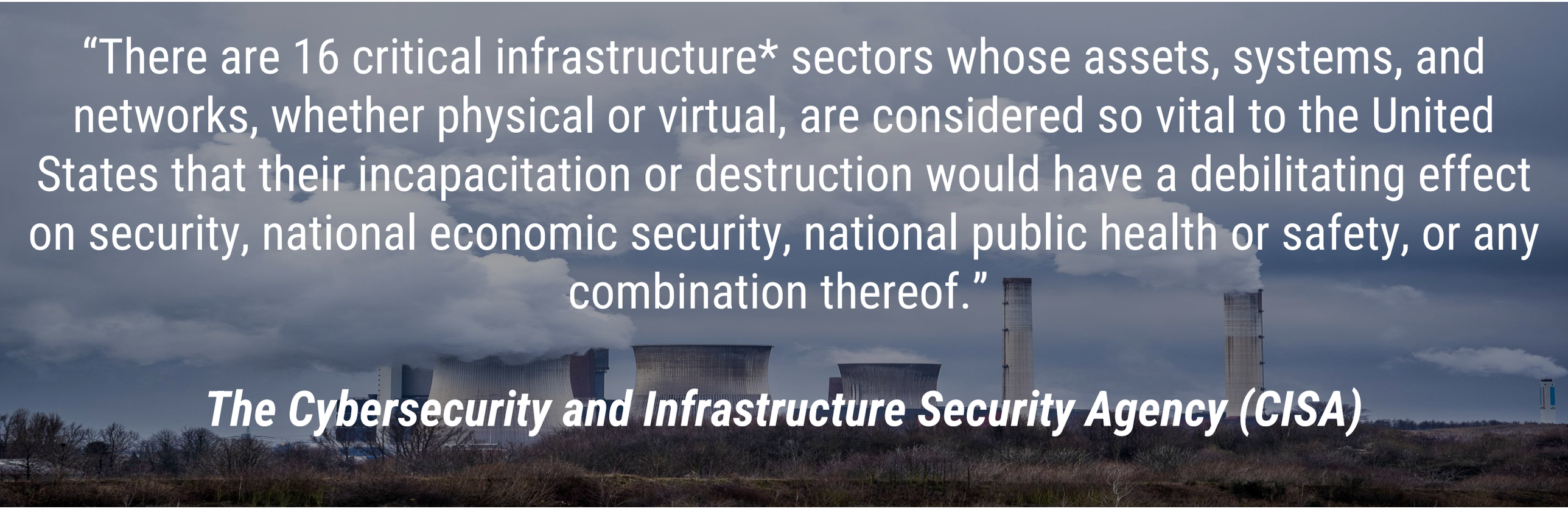
Moxa ICS Expert & ISA Cybersecurity Director (District 4)

- **+ 18 years** of Experience in Automation
- **+ 9 years** in Connectivity & Cybersecurity
- **ISA / IEC-62443 Official Instructor** and member of the Standard Committee
- Certifications: **US Defense, MIT, Stanford, IBM, NYU** and **Master's Degree in ICS in Spain**
- Specialization **in Innovation at Harvard** and **MBA** in Marketing, **Artificial Intelligence (AI)**

Let's Connect! https://www.linkedin.com/in/felipecybersecurity/

Mission-critical Applications

Mission-critical Applications (critical infrastructure)

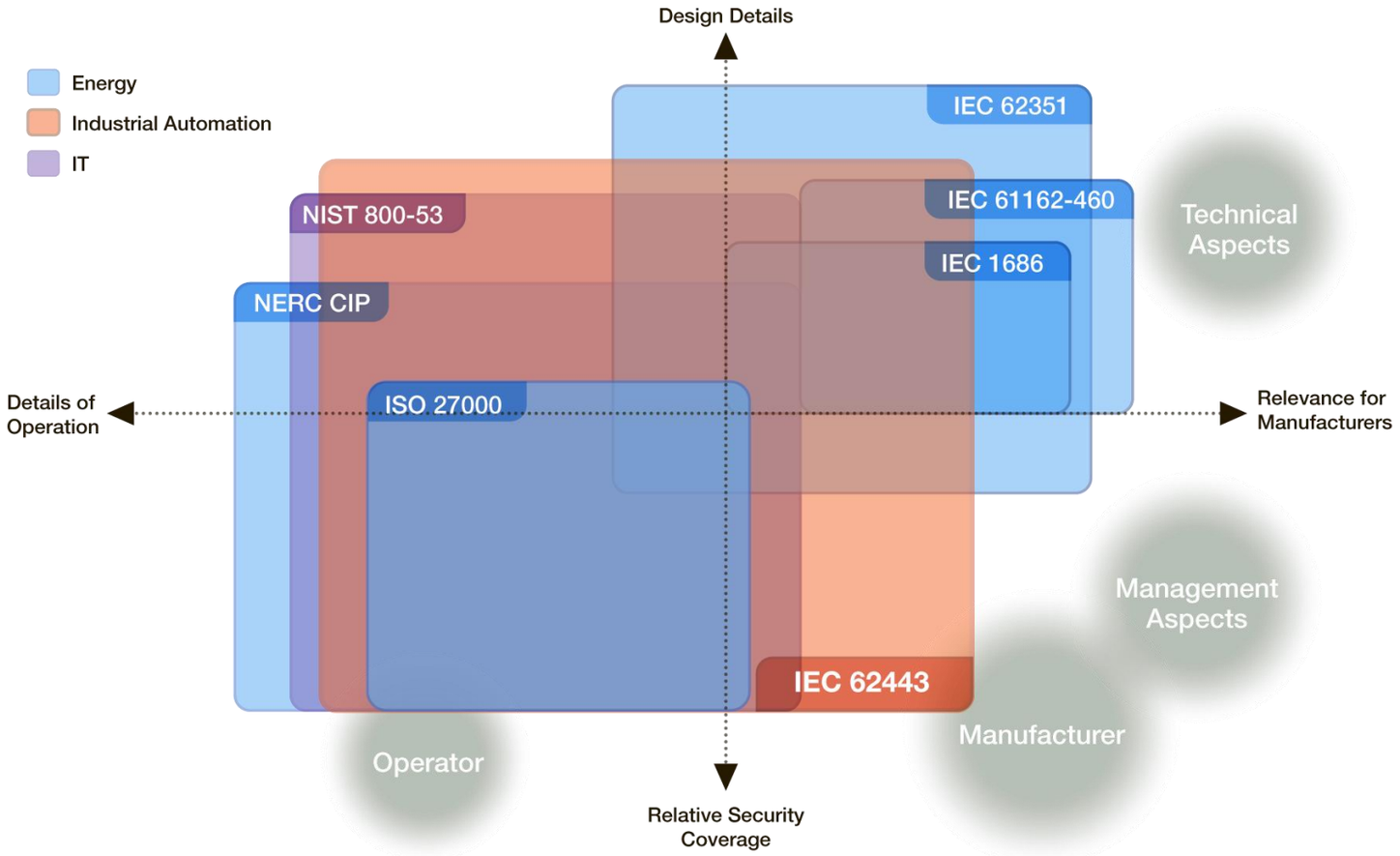


"There are 16 critical infrastructure* sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."

The Cybersecurity and Infrastructure Security Agency (CISA)

*Chemical Sector, Commercial Facilities Sector, Communications Sector, Critical Manufacturing Sector, Dams Sector, Defense Industrial Base Sector, Emergency Services Sector, Energy Sector, Financial Services Sector, Food and Agriculture Sector, Government Facilities Sector, Healthcare and Public Health Sector, Information Technology Sector, Nuclear Reactors, Materials, and Waste Sector ,Transportation Systems Sector, Water and Wastewater Systems Sector

Standards and Frameworks



General Industrial Automation
ISA 99 / IEC 62443

Power Automation
IEC 63351 / NERC CIP (U.S.)

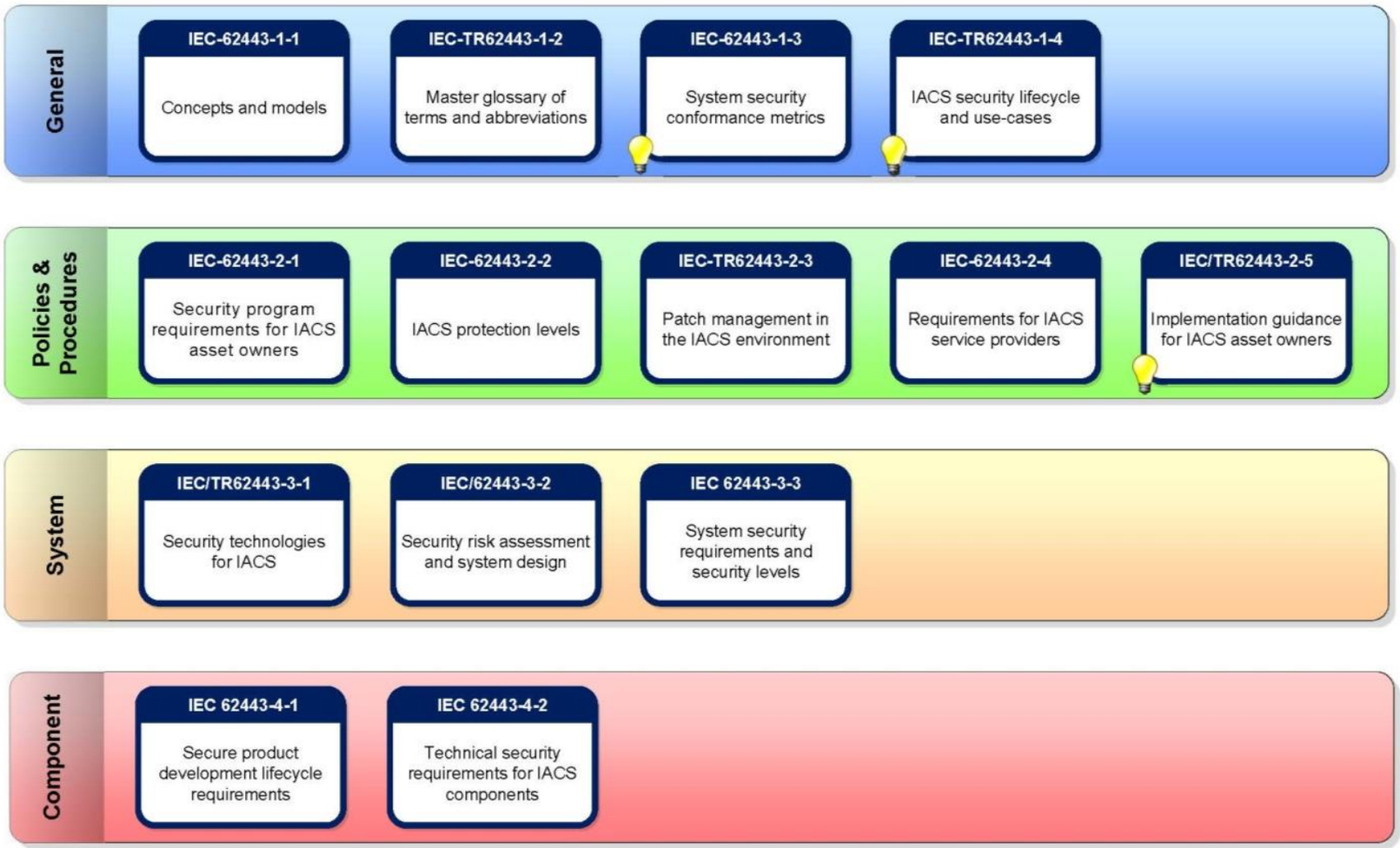
Guide to ICS Security
NIST SP 800-53 (U.S.)

Marine Automation
IEC 61162-460

IT Security System
ISO / IEC 27000

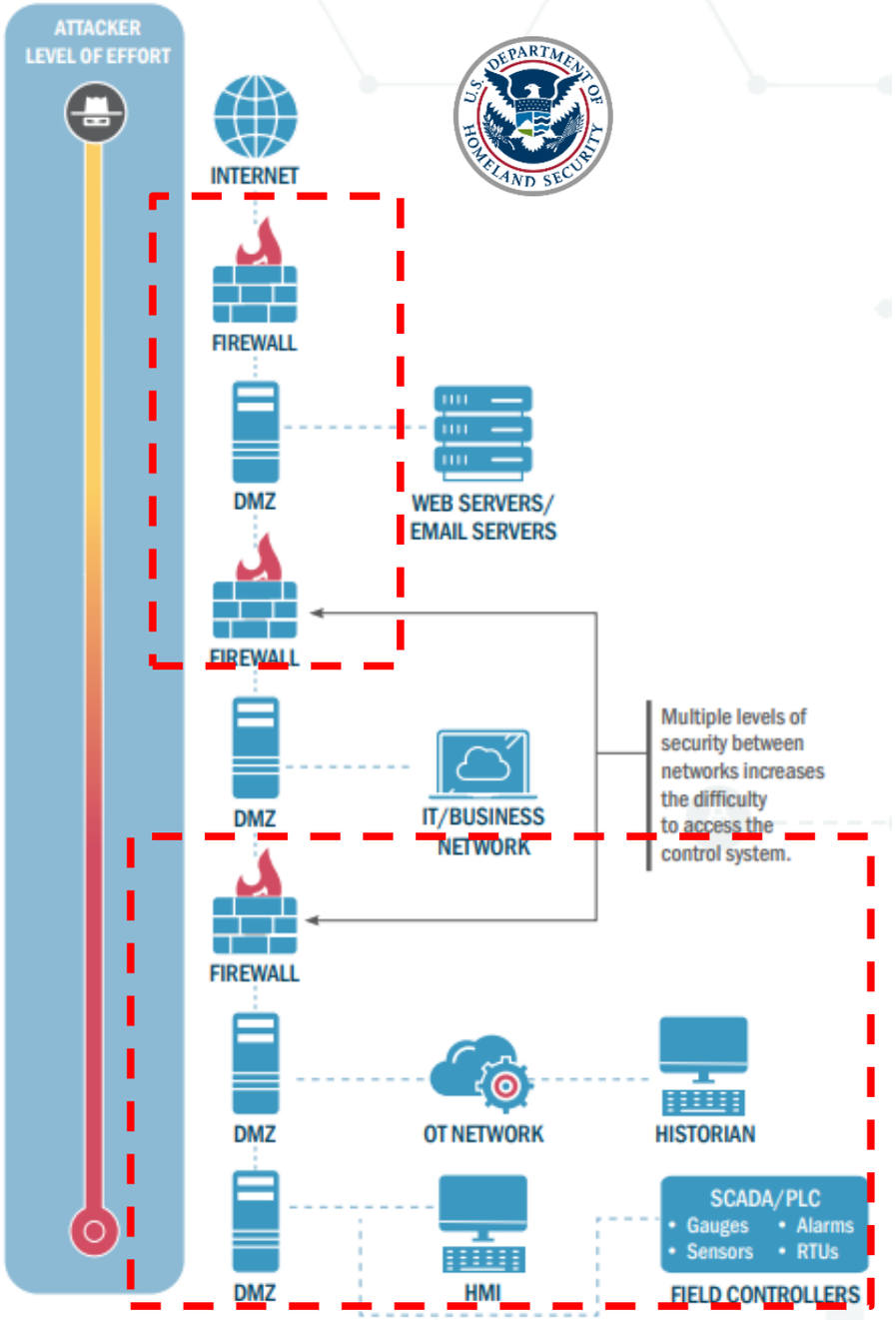
IEC-62443

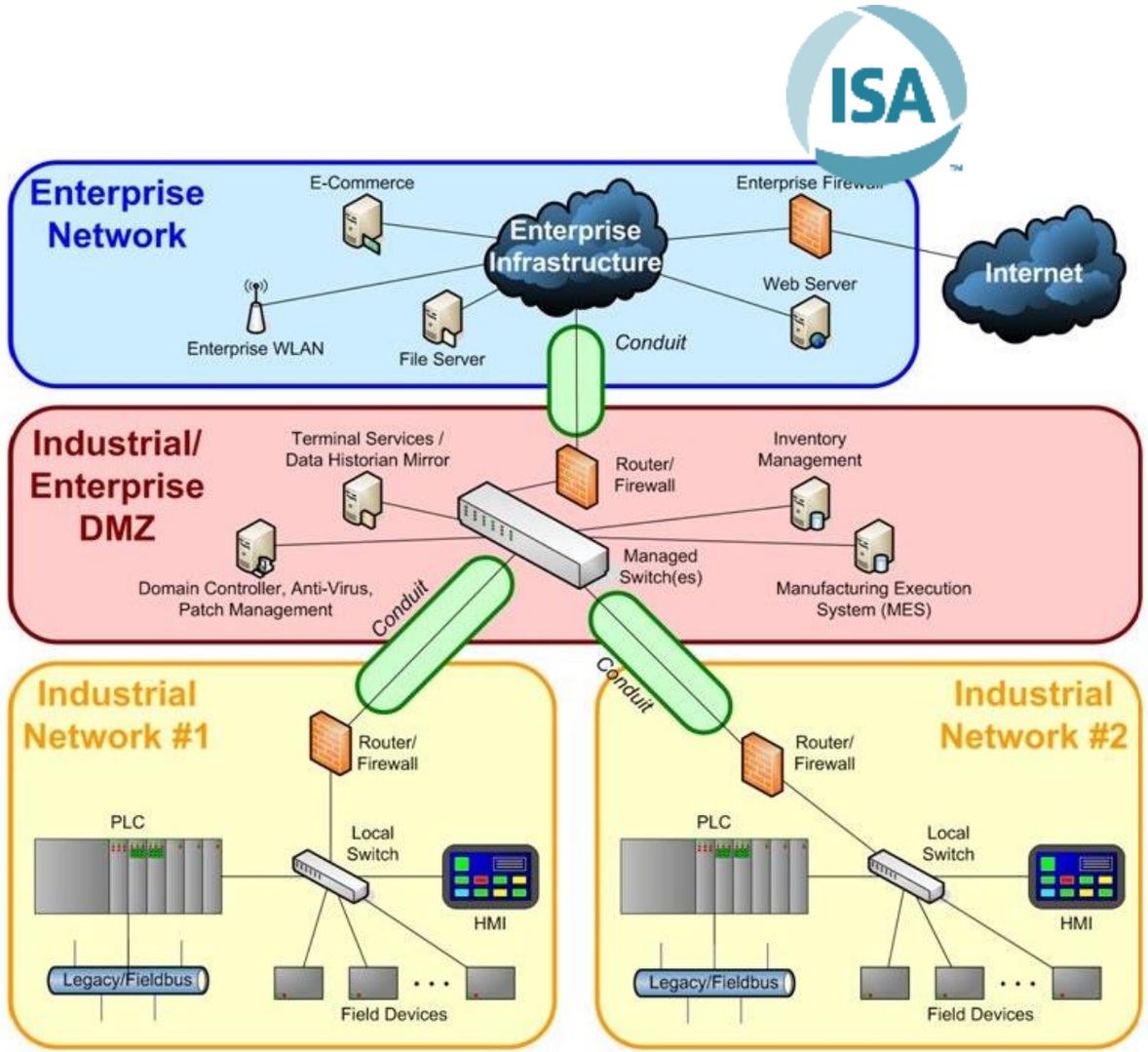
the 1000-foot view



https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62443/

IEC-62443 - Examples of Zones and Conduits



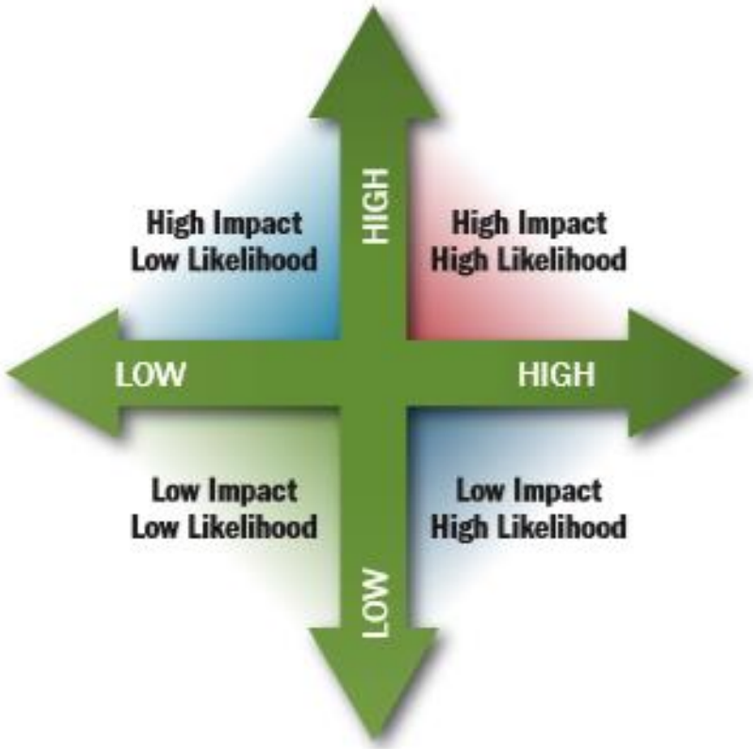


Current Challenge

How create the zones properly?

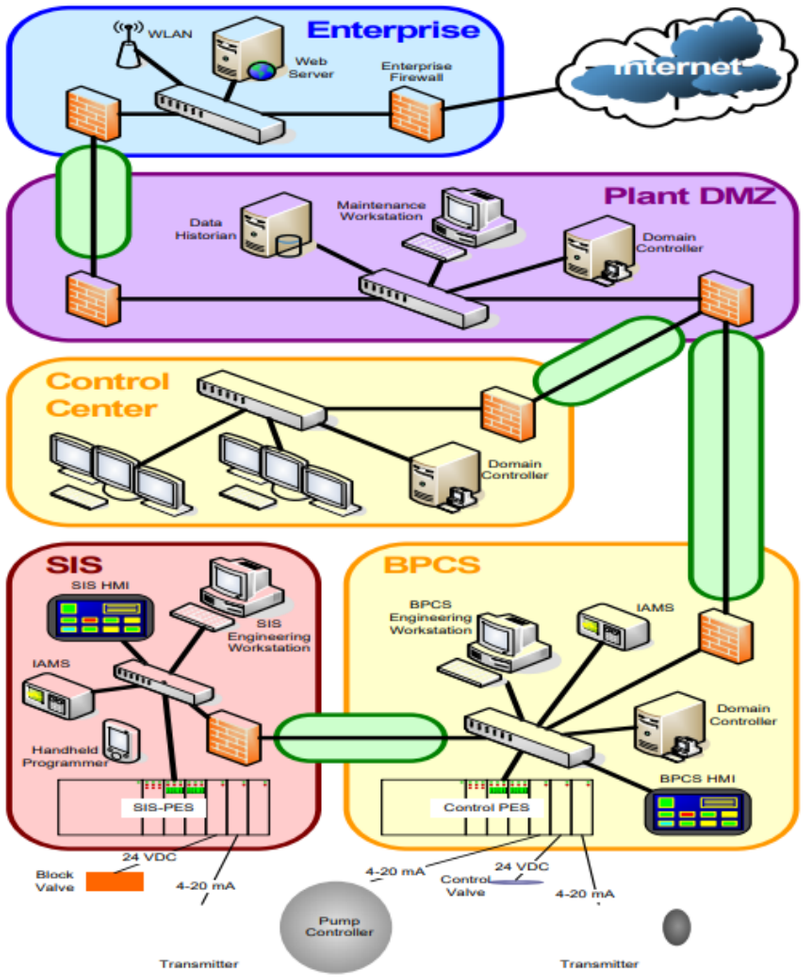
Planning

Risk Assessment



"Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies"

		Likelihood				
		1 Remote	2 Unlikely	3 Possible	4 Likely	5 Certain
Impact	1 Trival	1	2	3	4	5
	2 Minor	2	4	6	8	10
	3 Moderate	3	6	9	12	15
	4 Major	4	8	12	16	20
	5 Critical	5	10	16	20	25



High/Detailed Level Risk Assessment & Zone and conduits*

*https://automationinstrumentationsummit.files.wordpress.com/2017/07/037-prosalus-easton.pdf

Cognitive System Applied to Cybersecurity

How to suggest automatically a security zone?

Determining Communication Patterns

1) 'Source IP',
2) 'Source Port',
3) 'Destination IP',
4) 'Destination Port',
5) 'Protocol' and
6) 'Timestamp' to determine the distance, it considers the transmission time of each packet; *

* CICDDoS2019 dataset

Reference Topology*

1) Normalization**

2) Tested 3 different classes of algorithms

1. unsupervised learning using the k-means clustering,
2. supervised learning using the Support vector machine (SVM) and
3. neural networks using the convolutional neural network (CNN).

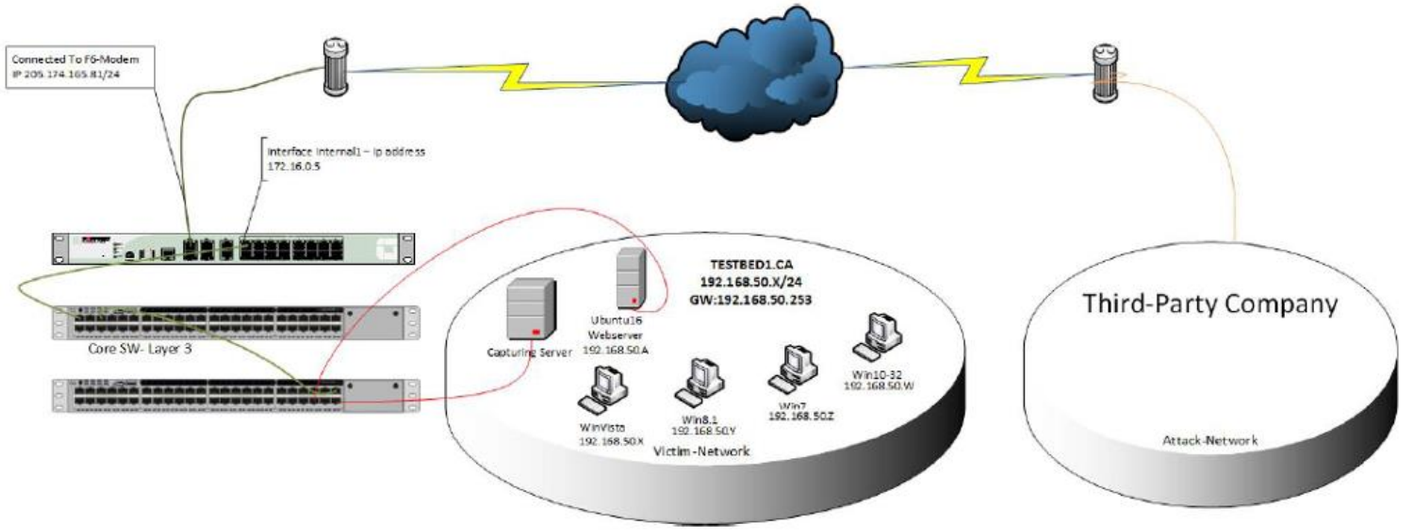


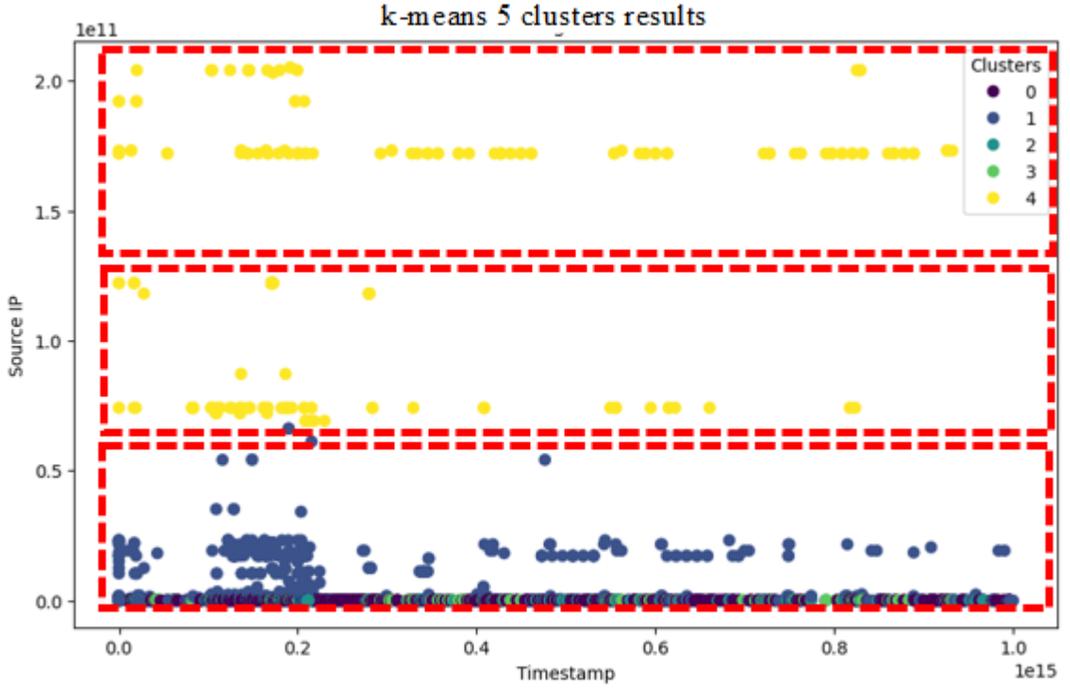
Figure 2: Testbed Architecture

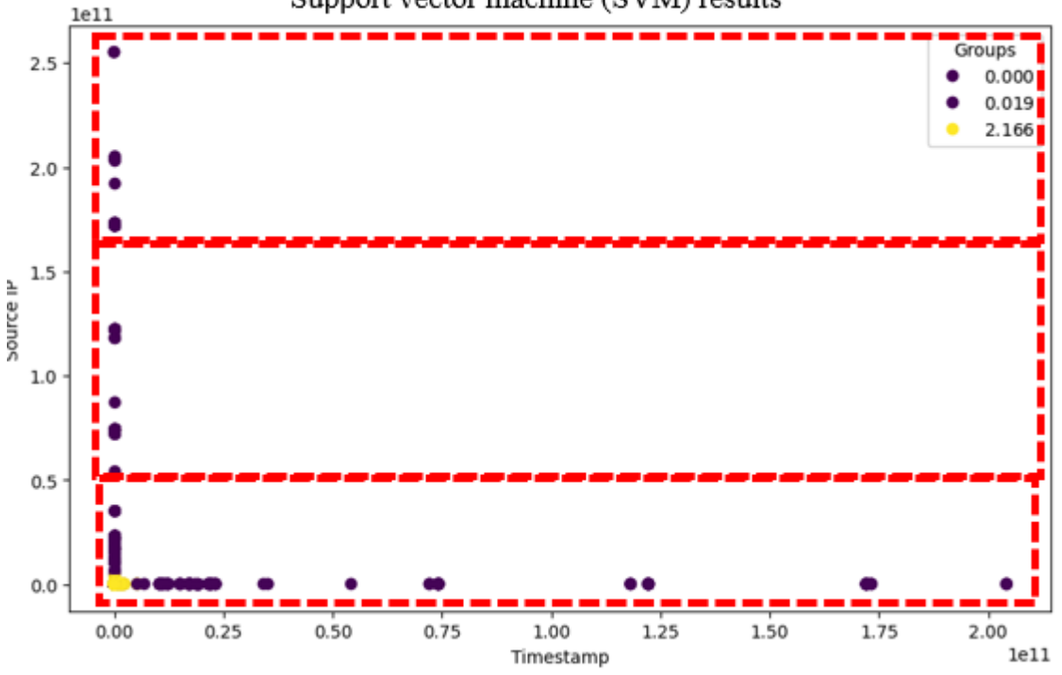
* I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy", IEEE 53rd International Carnahan Conference on Security Technology, Chennai, India, 2019

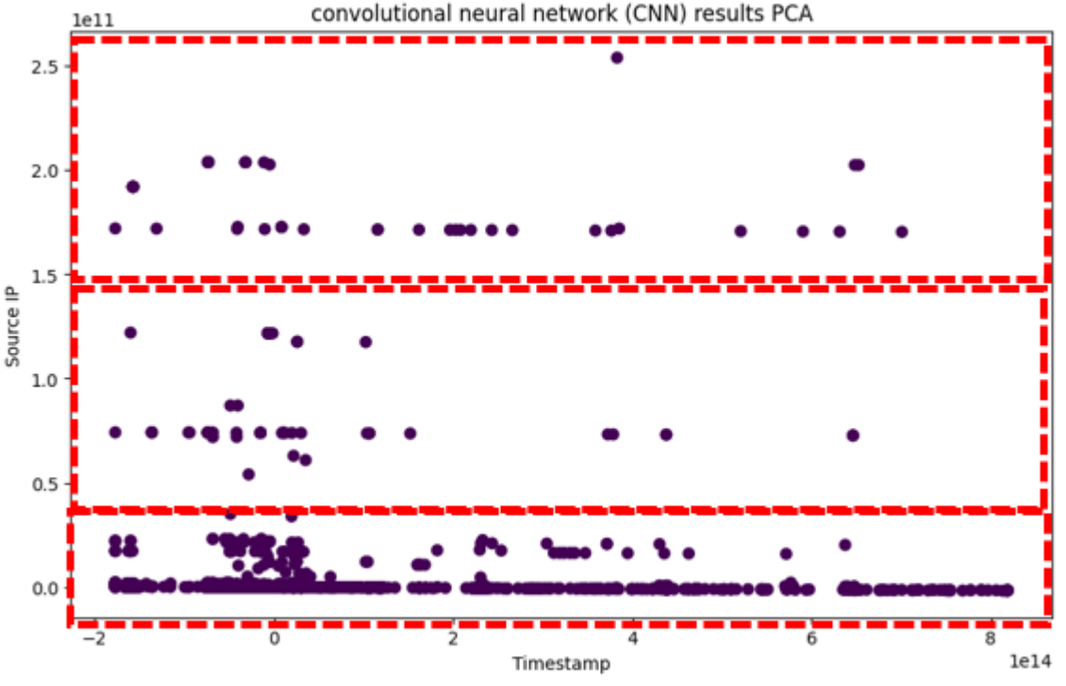
** (elimination of special characters from the ip addressing scheme, unnecessary additional spacing and columns)

Results

Algorithm	Processing time of dataset (min.)
K-means	0.35
SVM	22.10
CNN	75.2


k-means 5 clusters results
1e11
Clusters
0
1
2
3
4
Source IP
Timestamp
1e15


Support vector machine (SVM) results
1e11
Groups
0.000
0.019
2.166
Source IP
Timestamp
1e11


convolutional neural network (CNN) results PCA
1e11
Source IP
Timestamp
1e14

Conclusions

1. This paper compared 3 different types of algorithms:
   - unsupervised learning with k-means clustering,
   - supervised learning with Support vector machine (SVM) and
   - neural networks with convolutional neural network (CNN).
2. Similar results were found proposing logical groupings of assets based on predefine features,
   - 'Source IP', 'Source Port',
   - 'Destination IP',
   - 'Destination Port', 'Protocol' and
   - 'Timestamp'
3. Support vector machine (SVM)
   - presented the most promising result having the second-best processing time of 22.10 min.
4. As future developments
   - Test the same algorithms with ICS specific dataset

Felipe Sabino Costa, MSc, MBA
Industrial Cybersecurity Expert (ICS) /
International ICS Speaker and technical articl...

Felipe Sabino Costa
Felipe.costa@moxa.com
multsoma@outlook.com

https://www.linkedin.com/in/felipecybersecurity/

Let's keep in touch