Setting the Standard for Automation™

Engr. Felipe Sabino Costa

Moxa ICS Expert & ISA Cybersecurity Director (District 4)

"Enhancing the Cybersecurity on Mission-critical Applications using Cognitive Technologies"

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

Presenter

Engr. Felipe Sabino Costa

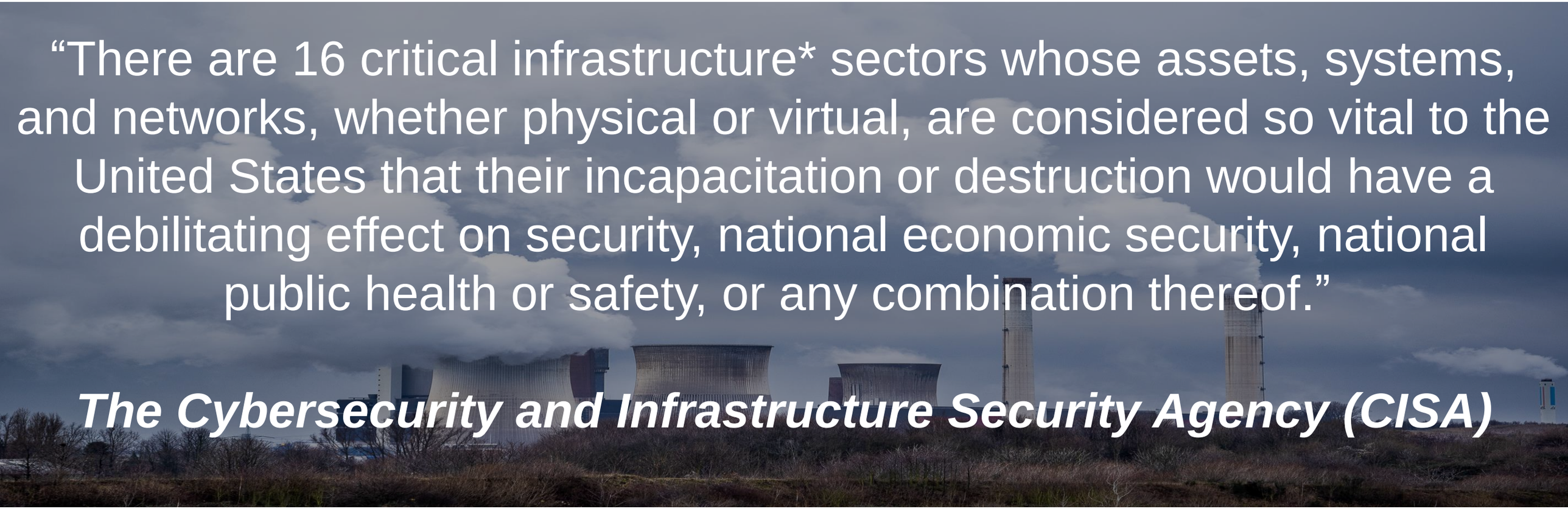
Moxa ICS Expert & ISA Cybersecurity Director (District 4)

- **+ 16 years** of Experience in Automation
- **+ 7 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
- **Post graduation in Artificial Intelligence (AI)** – In progress

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

Secure

Physical Security
Asset Inventory
Hardening
Patch Mgmt

Defend

DMZ
Anti-Malware
Access Control

Contain

Zone
Firewalls
Whitelisting

Manage

SIEM
Incident Management

Anticipate

Anomaly &
Breach detection
Threat intelligence

Industrial Cybersecurity Maturity Model

ARC ICS Cybersecurity Model

Current Challenges

Current Challenges

- How to adjust current good practices for each system singularity.
- Lack of operator knowledge to detect configurations security flaws in different parameters (protocols, authentication, communication, etc.)
- High number of configuration possibilities (over Centillion singular possibilities for a single network asset)

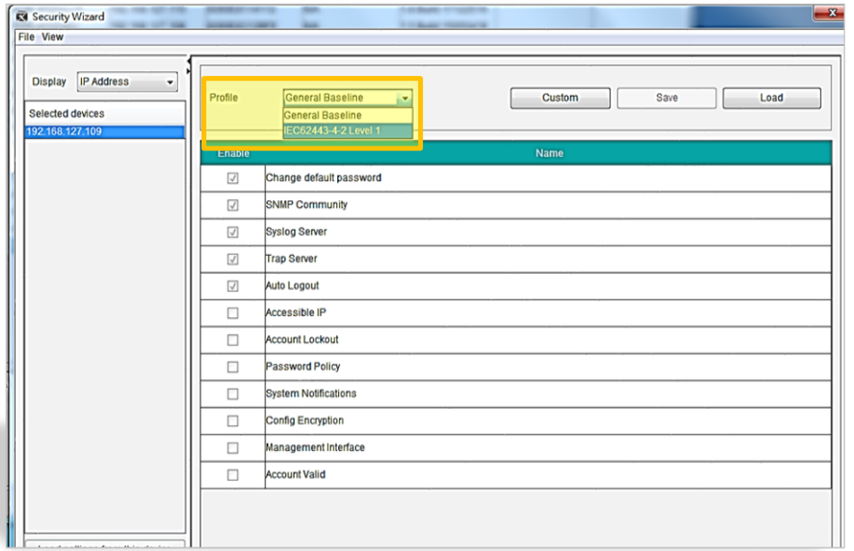
Static Model

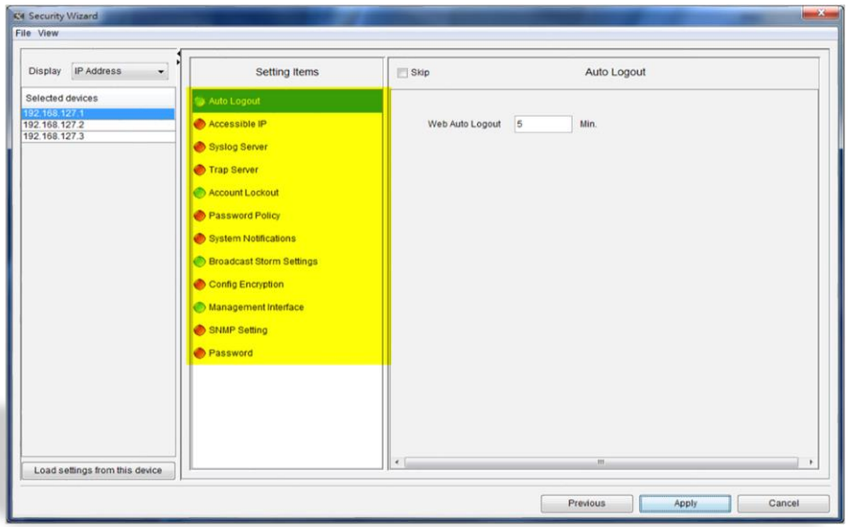
(Current available solution)

Static Model
RPA (robotic process automation)

Characteristics:

- Establishment of a consistent configuration using good practices (e.g. ISO 27000, NIST, CIS, IEC-62443)
- Demands an intense upfront development
- Minimizes some potential vulnerabilities, compared to current manual checks
- May not address some communication system specifics
- Unable to adapt ICS changes and different types of threats dynamically



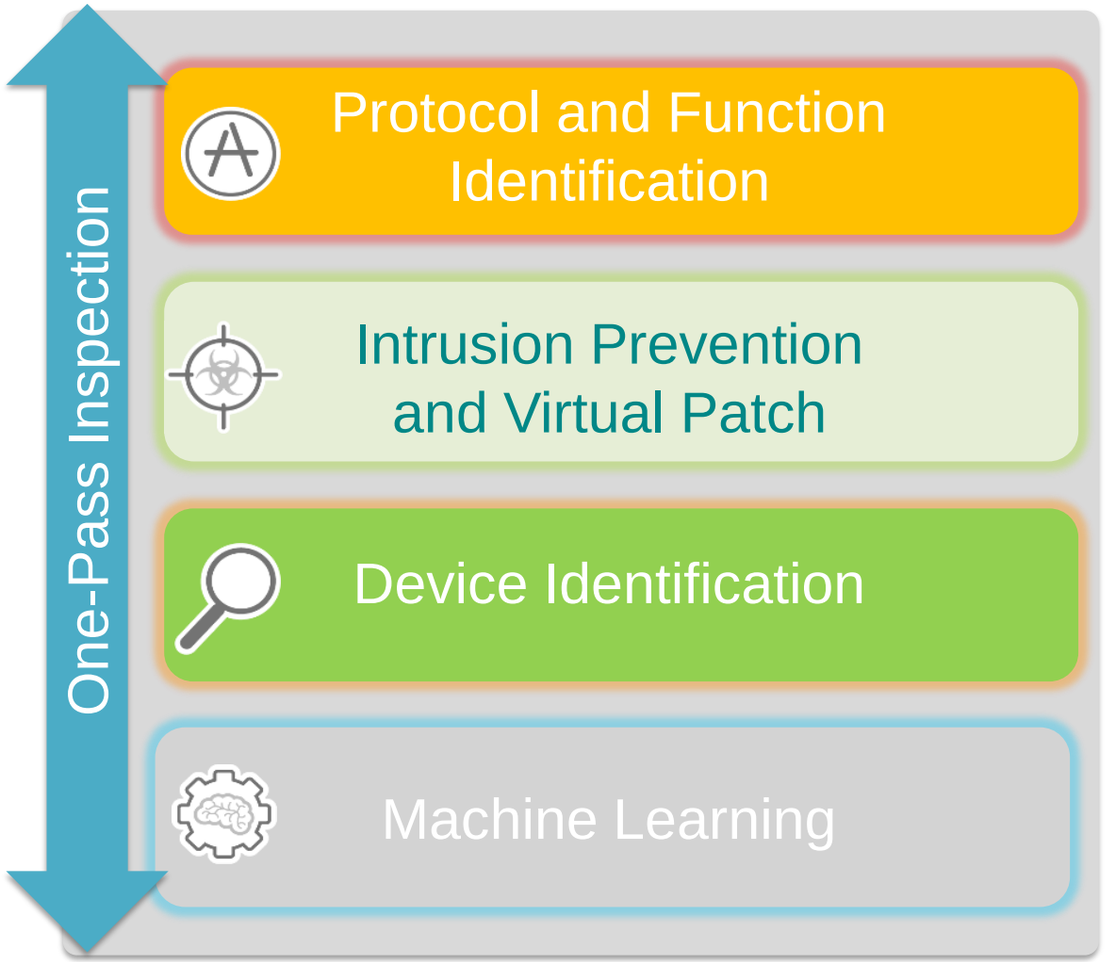


Cognitive System Applied to Cybersecurity

Common Application Areas

- Malware detection
- Trigger anomalous network behavior
- Cybersecurity events triage

Reference Application



Intrusion Detection Systems (IDS)

Output

```
[**] [122:1:0] (portscan) TCP Portscan [**]
[Priority: 3]
PROTO:255 172.16.52.1 -> 172.16.52.2
[Similarity: 1]
```

```
[**] [1:1002:7] WEB-IIS cmd.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
02/28-13:34:26.5926 80.101.45.10:59494 ->
TCP 172.16.52.1:56665 -> 172.16.52.2:80
[Similarity: 1]
```

```
[**] [1:1002:7] WEB-IIS cmd.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
TCP 172.16.52.1:36329 -> 172.16.52.2:80
[Similarity: 1]
```

```
[**] [1:1444:3] TFTP Get [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
UDP 172.16.52.2:1039 -> 172.16.52.1:69
[Similarity: 1]
```

```
[**] [1:1002:7] WEB-IIS cmd.exe access [**]
[Classification: Web Application Attack] [Priority: 1]
TCP 172.16.52.1:46661 -> 172.16.52.2:80
[Similarity: 1]
```

Snort (Syslog)

Dynamic Model

(Proposed Model)

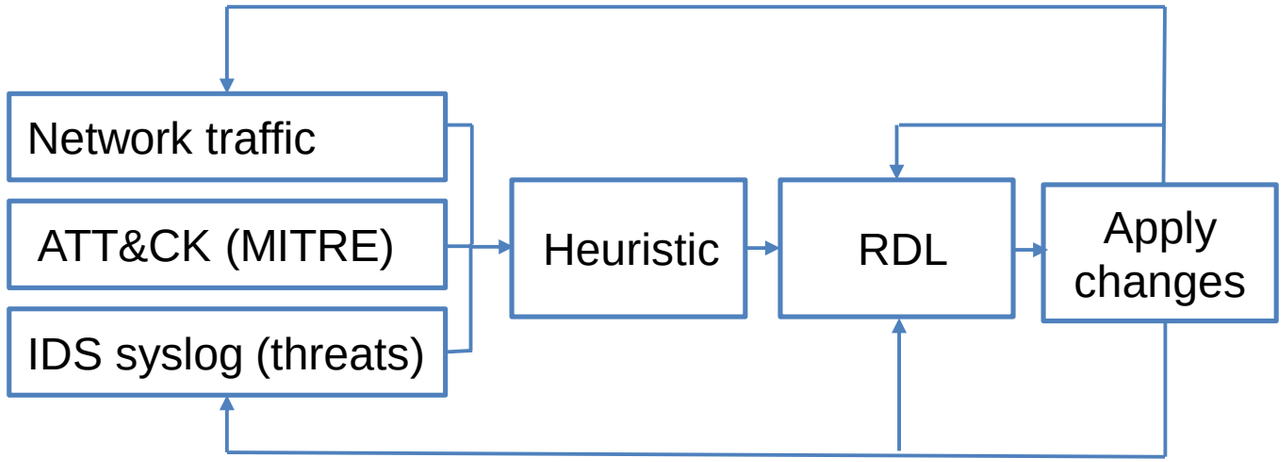
Common ICS Vulnerabilities

Proposed Enhancement

Poor Code Quality	Network Design
Vulnerable Web Services	Network Component Configurations
Poor Network Protocol Implementations	Information Disclosure
Poor Patch Management	Least User Privileges Violation
Weak Authentication	

Source: The Cybersecurity and Infrastructure Security Agency (CISA) "210W-07 ICS Cybersecurity Vulnerabilities"

Dynamic Model
DRL (Deep Reinforcement Learning)



Description	Role
Network traffic	Attacks and health system (baseline) indicators
ATT&CK (MITRE)	Solid attack framework to map different attack techniques
IDS syslog (threats)	Usually uses (ML) can provide specific attack flags
Heuristic	It will combine the specific technique and current alarms to suggest the most likely classes of configurations to RDL compute
RDL	Deep Reinforcement Learning the algorithm that will generate the insights (Lack of public and private datasets)
Apply changes	SNMP (API) The protocol that will effectively perform the changes
	Deploy suggested changes in the network assets

Why Deep Reinforcement Learning?

- Lack of historical data, empirical data from operators.
- Difficult to train the algorithm due the lack of public or private relevant data sets
- Complex to replicate the specific system (Proof of Concept)
- High number of configuration possibilities

Dynamic / Static models Comparison

Static Model (Current)	Dynamic Model (Proposed)
Limited to the general good practices recommendation	Not limited to good practices recommendation
Customizations limited to the operator knowledge	Discover potential improvements
Demands an intense upfront development	Reduced development to heuristics creation only
May not address some communication system specifics	Insights generation based on specific traffic behavior and error/ attack logs
Unable to adapt ICS changes and different types of threats dynamically	Able to adapt devices and threats which might change dynamically

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