
Terafence
IoT Cyber Security
Air-Gap technology by Terafence
Connectivity without compromising security
Leandro Roisenberg
Global Sales Manager
Distributed in Greece and Cyprus by e-Systems Ltd (www.e-systems.gr)

Control Systems Attacks are not Hypothetical

- **Types of Cyber Attacks are Growing.**
- **Explosion of Ransomware Attacks.**
- **Attacks are Aimed at the Control Systems – Direct Disruption of Service.**
- **Cyber Attacks are trickle through IT environments – IT & OT are connected**

A Wake-Up Call for a Proactive Approach

Facilities & Utilities - Cybersecurity Challenges

- **Traditional OT systems are Air-Gapped from IT networks.**
- **Current Air-Gap solutions are exceptionally ridged and force customers to adopt their process to the solution (limited) capabilities.**
- **Industry 4.0 suggests major efficiency improvements to OT environments by uploading OT data to the cloud for AI analysis.**
- **OT/IT interconnectivity is dangerous to both sides, Air-Gap MUST be maintained.**
- **Any connectivity of OT networks to Internet based services is considered a Cyber Threat and should be avoided unless totally secured.**

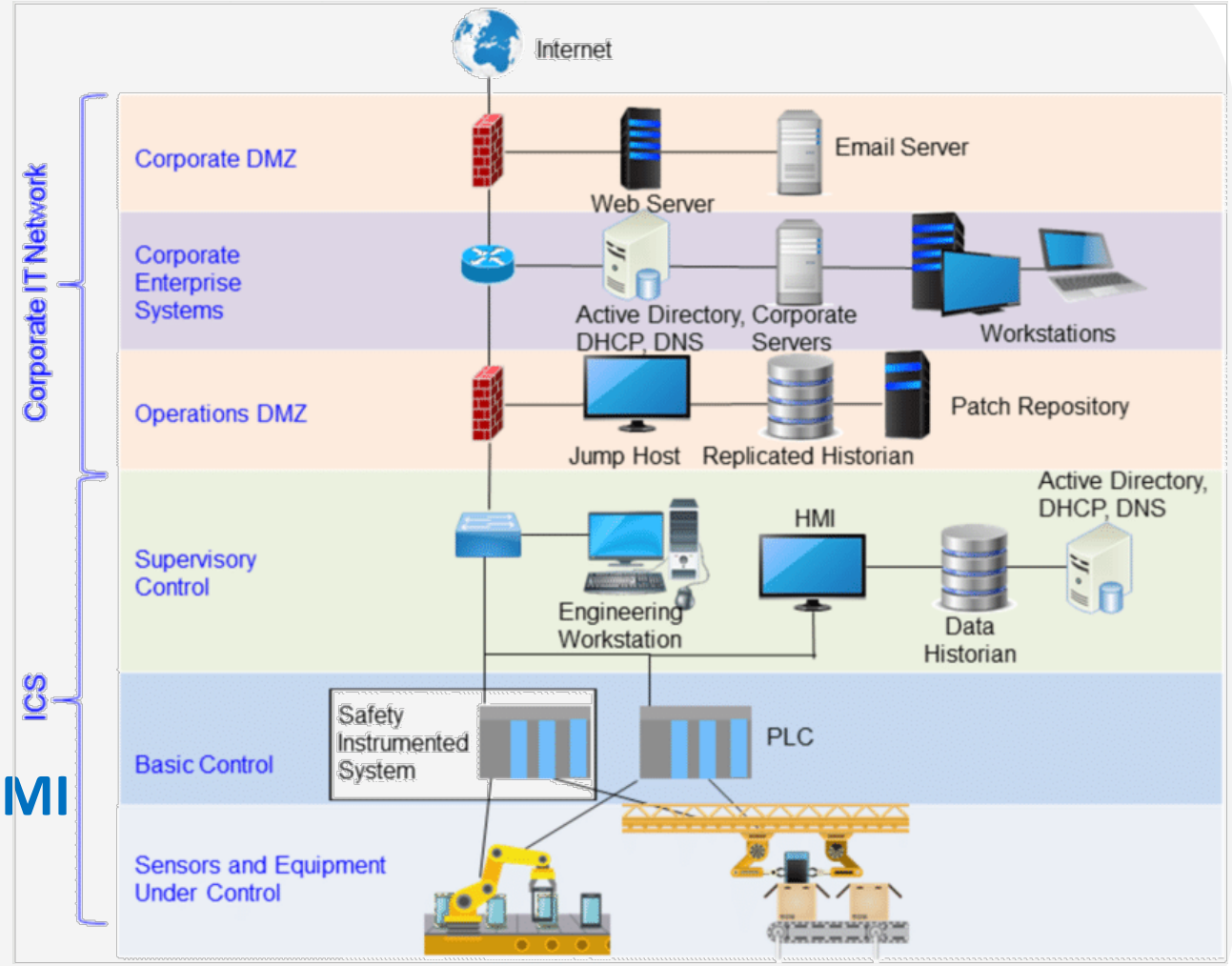
Terafence
IoT Cyber Security

Next Generation Air-Gap Approach

Segmentation
Between IT and OT –
Current solutions fall short

Closing the gap between HMI / SCADA, ICS / OT and Cloud / AI platform adoption

Provide Service visibility across separate systems and isolated HMI / SCADA, ICS / OT environments

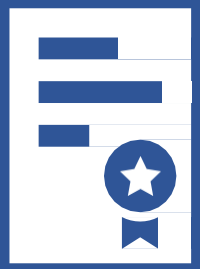


Terafence's SDFC (Smart Data Flow Controller) - a4Gate/TFG

Connectivity

Security

Compliance



a4Gate/TFG are Vendor neutral

and offers unhackable ultimate protection to all critical IT / OT / IoT Infrastructures


Energy


Transportation


Mining


Healthcare


...and MORE

Digitalization changes everything and requires additional security

- Industry 4.0 = digitalization
- Vertical integration of production systems
- Horizontal integration of the value chain
- Through-engineering or continuous engineering

30 billion connected IoT / IIoT devices estimated by 2030*

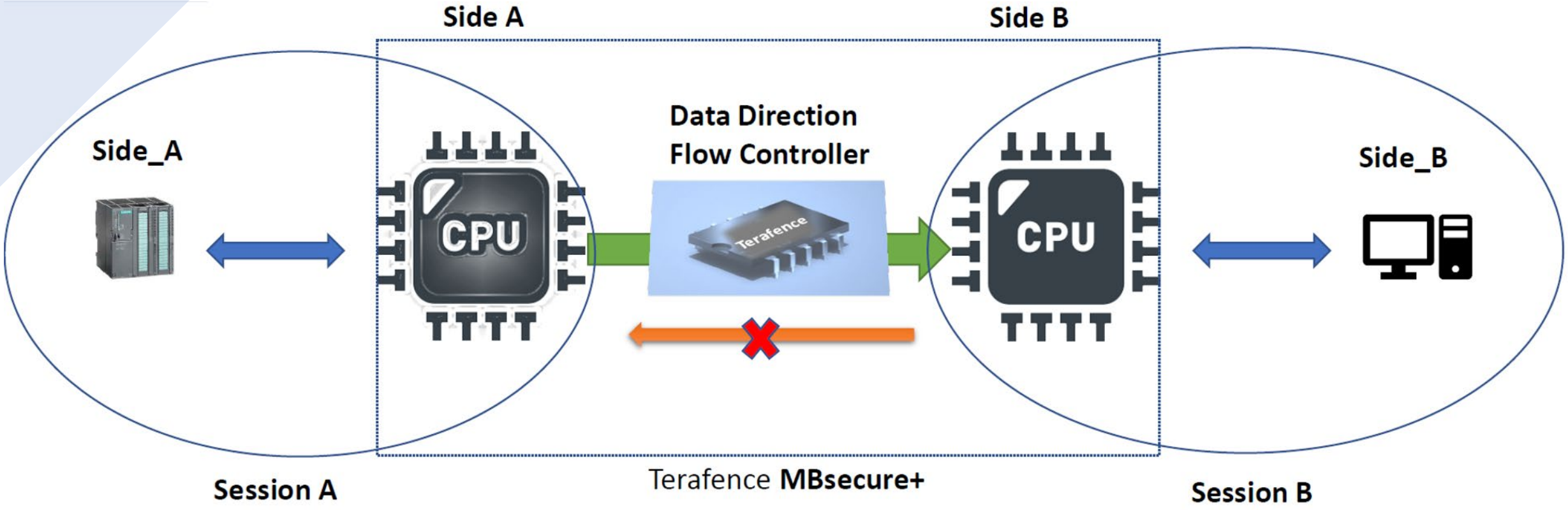
- Increased connectivity requirements
- Highly heterogeneous networks
- Widespread wireless, remote, and continuous connections
- Real-time demand and response
- By www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Security investments as an opportunity to generate additional value

- Ensured plant/process availability
- Increased traceability through the entire production process
- Asset visibility and resource optimization
- Meeting critical infrastructure regulations
- Ensured system reliability and user access

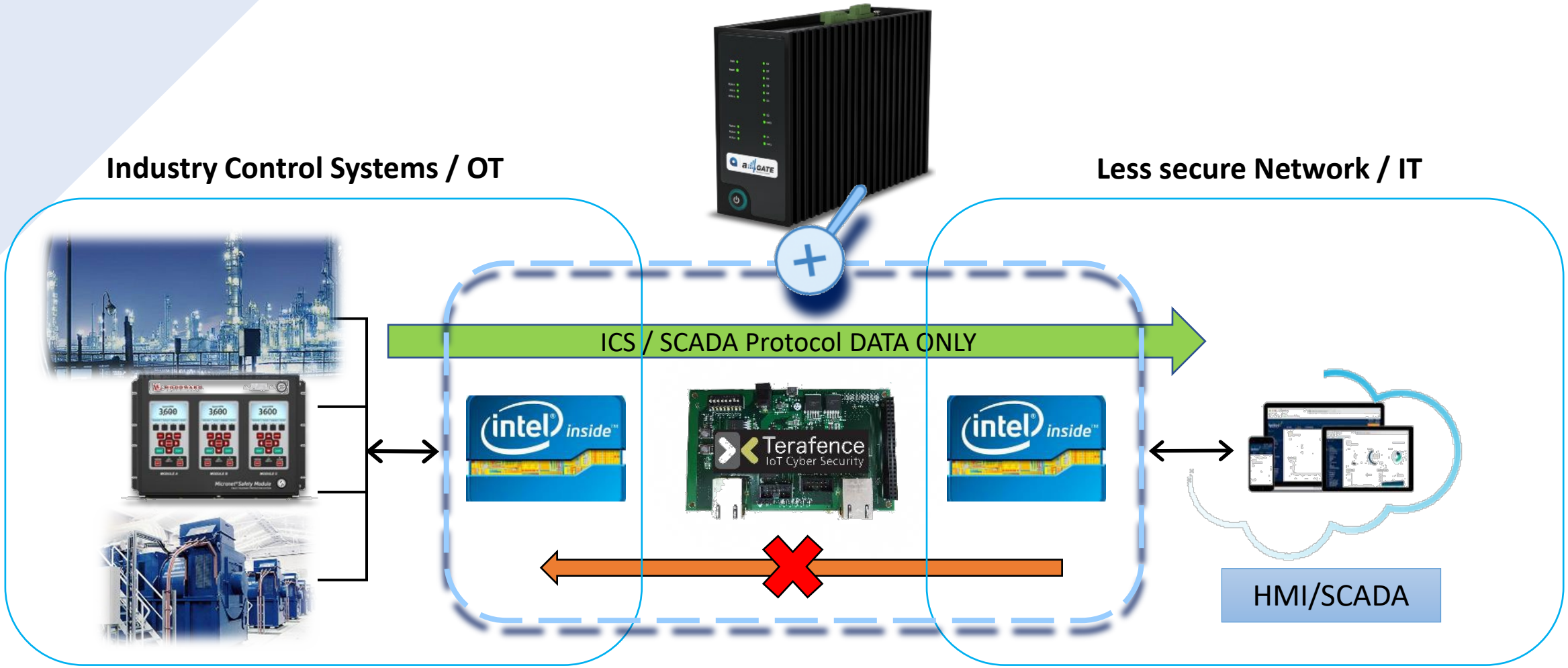
Distributed in Greece and Cyprus by e-Systems Ltd (www.e-systems.gr)

Terafence Cyber-Security
Air-Gap Innovative Approach



Distributed in Greece and Cyprus by e-Systems Ltd (www.e-systems.gr)

Terafence Air-Gap Innovative Approach
OT -> IT Example



Distributed in Greece and Cyprus by e-Systems Ltd (www.e-systems.gr)

Terafence Supported Protocols Examples

Terafence
IoT Cyber Security

I can do the same with a FireWall?, right?

Wrong!

FireWall is:

- A device for controlling access
- Will allow full end-to-end TCP/IP session
- Has rules and access lists
- Uses software to control accesses
- Operate on OSI Layers 3-4
- Requires Host CPU, OS, updates…
- ***Will not actively support ICS protocols***

Terafence is:

- A device to physically block access
- Will not allow any end-to-end IP session
- No rules, no lists, no access
- Access denial by hardware "Air-Gap"
- Total block at OSI Layers 1-2
- No CPU, no MAC, no IP address
- **Actively support ICS protocols**

And of course ALL firewalls are hackable – TERAFENCE IS NOT !!!

Terafence
IoT Cyber Security

“**Terafence TFG** obtained the Security Level Assessment **IEC62443-4-2, SL2"**

"The solution does not expose any service, and it can be considered as immune to direct attacks; beyond this first protection level, **there is a physical protection level ensured by the Datadiode card**.”

All tests were performed by a team composed of a Siemens CPIN and Cisco CCNA certified Network and security specialist, an EC Council Certified Ethical Hacker and under the supervision of an ISA / IEC 62443 Cybersecurity Fundamentals Specialist.

SSE

C|EH

IMPENETRABLE SHIELD
FOR IoT DEVICES

Terafence Differentiation

- Unique FPGA Implementation
- Military grade Air-Gap solution
- Revolutionary technology
- Low Cost & Small Form Factor
- Full Data Flow Control & Monitoring
- Total OT Operational Integrity

Terafence
IoT Cyber Security

USE CASES

Distributed in Greece and Cyprus by e-Systems Ltd (www.e-systems.gr)

Safety critical interlocking systems

Data mining and secure internet connectivity for predictive maintenance

Industry 4.0 Pharma

IMA Sustain Ability

IMA GROUP

Robotics smart-machines

Secure Back Channel

IMA Digital Center

Data analytics for predictive maintenance and secured channel for synchronization

Distributed in Greece and Cyprus by e-Systems Ltd (www.e-systems.gr)

Third-party Industrial assets

Connectivity for environment monitoring Apps

Power Plant Emission

CEMS – Continuous Environment Monitoring System (Siemens)

SIEMENS energy

0 0 1 0 1 1

Cloud-based monitoring App

Real time data analytics for the Ministry of Environment

Distributed in Greece and Cyprus by e-Systems Ltd (www.e-systems.gr)

Third-party Industrial assets - **Industrial control Systems**
Chemical processes

Ammonia Production Plant

Haifa

SCADA – PLC's

Modbus

ABB Control Center

Remote monitoring & Predictive Maintenance

ABB

Distributed in Greece and Cyprus by e-Systems Ltd (www.e-systems.gr)

Industrial control Systems

Water plant

Treatment and Distribution plant

Jordan Valley Water Association

SCADA – PLC's SYSLOG

Cyber Israel
National Cyber Directorate

National Ministry of Energy SOC

Remote monitoring & emergency respond

Distributed in Greece and Cyprus by e-Systems Ltd (www.e-systems.gr)

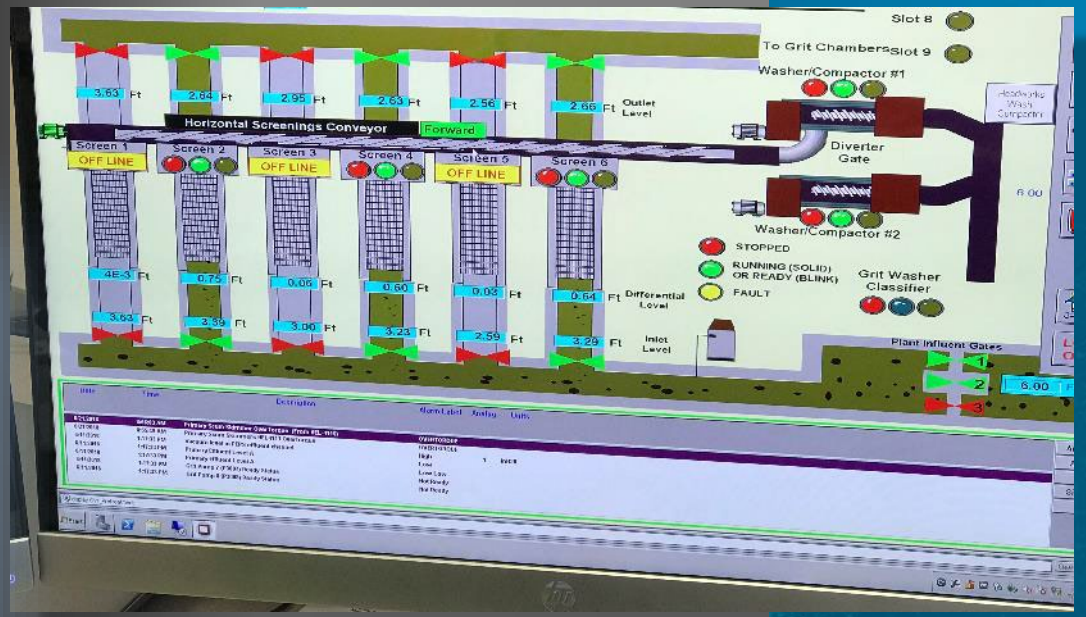
Building management system

Defense facilities

Israel Drefense Force

SCADA – PLC's

Modbus



Local HMI

Unidirectional Monitoring and Reporting

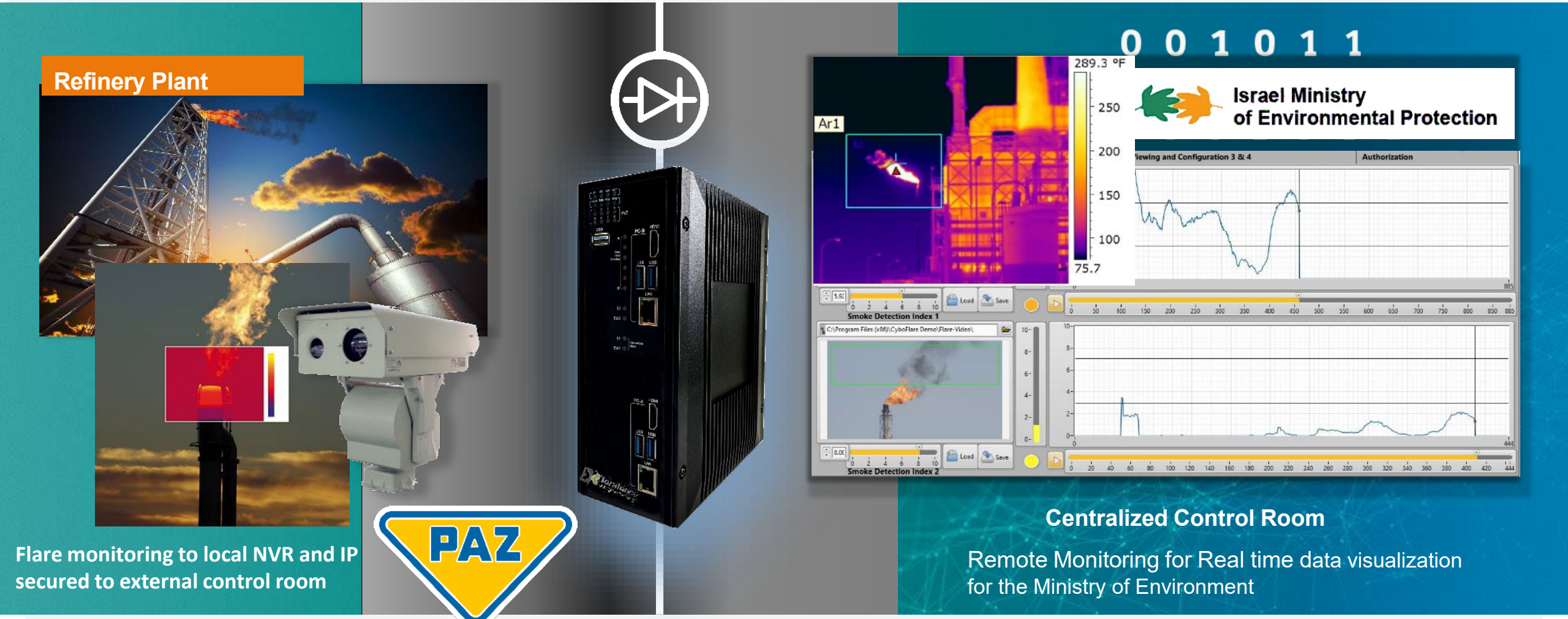
Distributed in Greece and Cyprus by e-Systems Ltd (www.e-systems.gr)

CCTV’s security
Defense facilities

Distributed in Greece and Cyprus by e-Systems Ltd (www.e-systems.gr)

Third-party Industrial assets – Refinery

Secured Connectivity for environment flare CCTV monitoring



Flare monitoring to local NVR and IP secured to external control room

Centralized Control Room

Remote Monitoring for Real time data visualization for the Ministry of Environment

Distributed in Greece and Cyprus by e-Systems Ltd (www.e-systems.gr)

Secure File-Transfer

Secured Connectivity for National Elections

Distributed in Greece and Cyprus by e-Systems Ltd (www.e-systems.gr)

Thank You!

For more information, free demo, and PoC,

And for a free invitation to a further-information event,
today at 18:00 at Yacht Club of Greece, followed by a reception

Come and visit us at the booth of

e-Systems