Cybersecurity for autonomous systems

Vulnerabilities and threats

11.03.2019

TRICONEX
BATTERY
POWER MODULE MODEL 8311

POWER
1
REMOTE
RUN
PROGRAM
STOP
LOCAL
TRICONEX
24VDC
5A 1Φ 47-63Hz 3 WIRE/5A 3 WIRE
PASS
FAIL
PASS
FAULT
ACTIVE
MAINT1
MAINT2

Agenda

1. Systems overview

2. Vulnerabilites

3. Incidents and trends

4. Future threats?

5. Mitigation?

Industrial Automation and Control System (IACS)

Process control systems

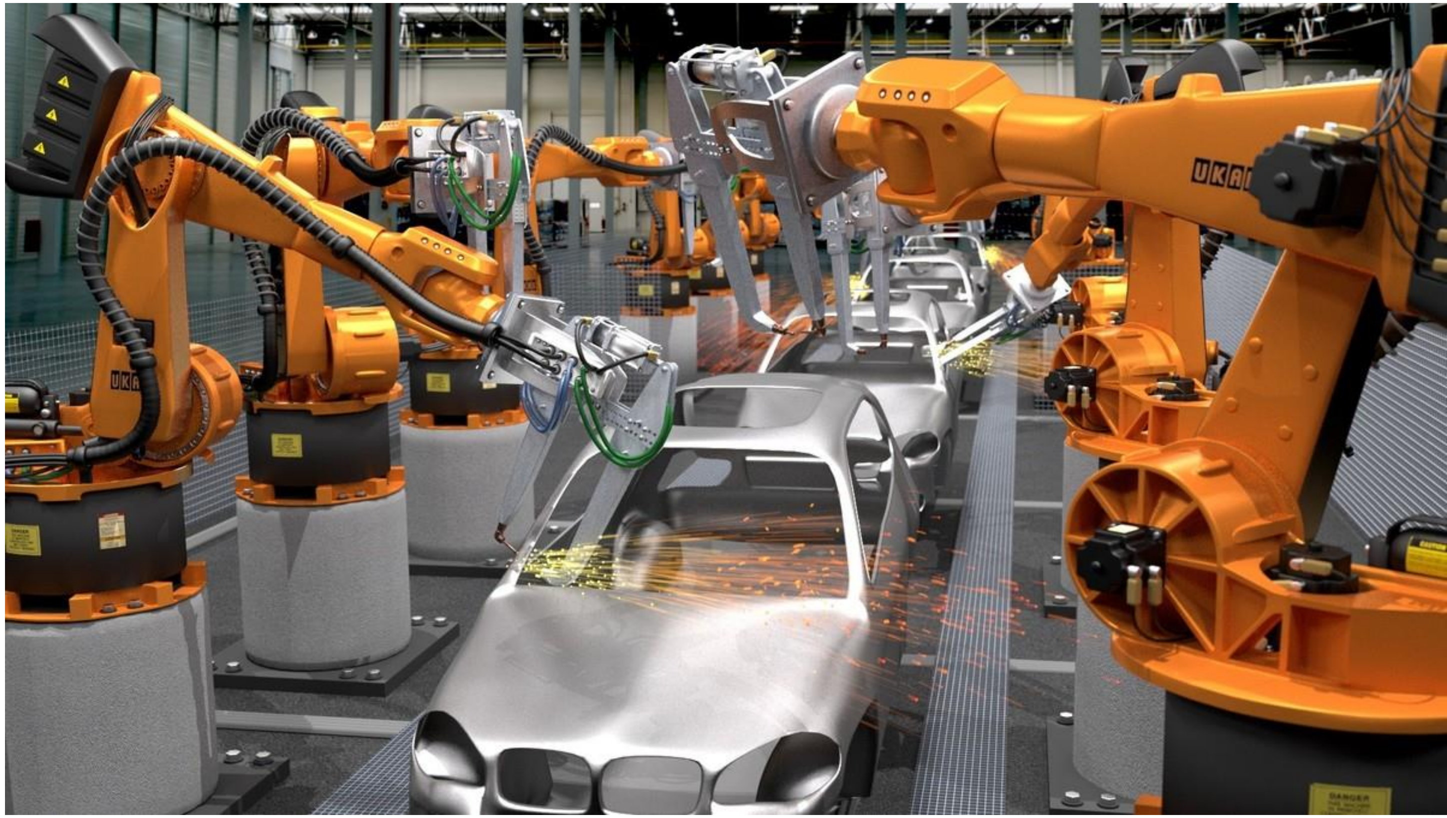
Safety instrumented systems

Dynamic positioning

IACS

Manufacturing

Production lines



IACS

Power & Energy

IACS

Nuclear power plants

Converging names

SAS, SIS, ICS, IACS, SCADA, DCS, IIoT, ++

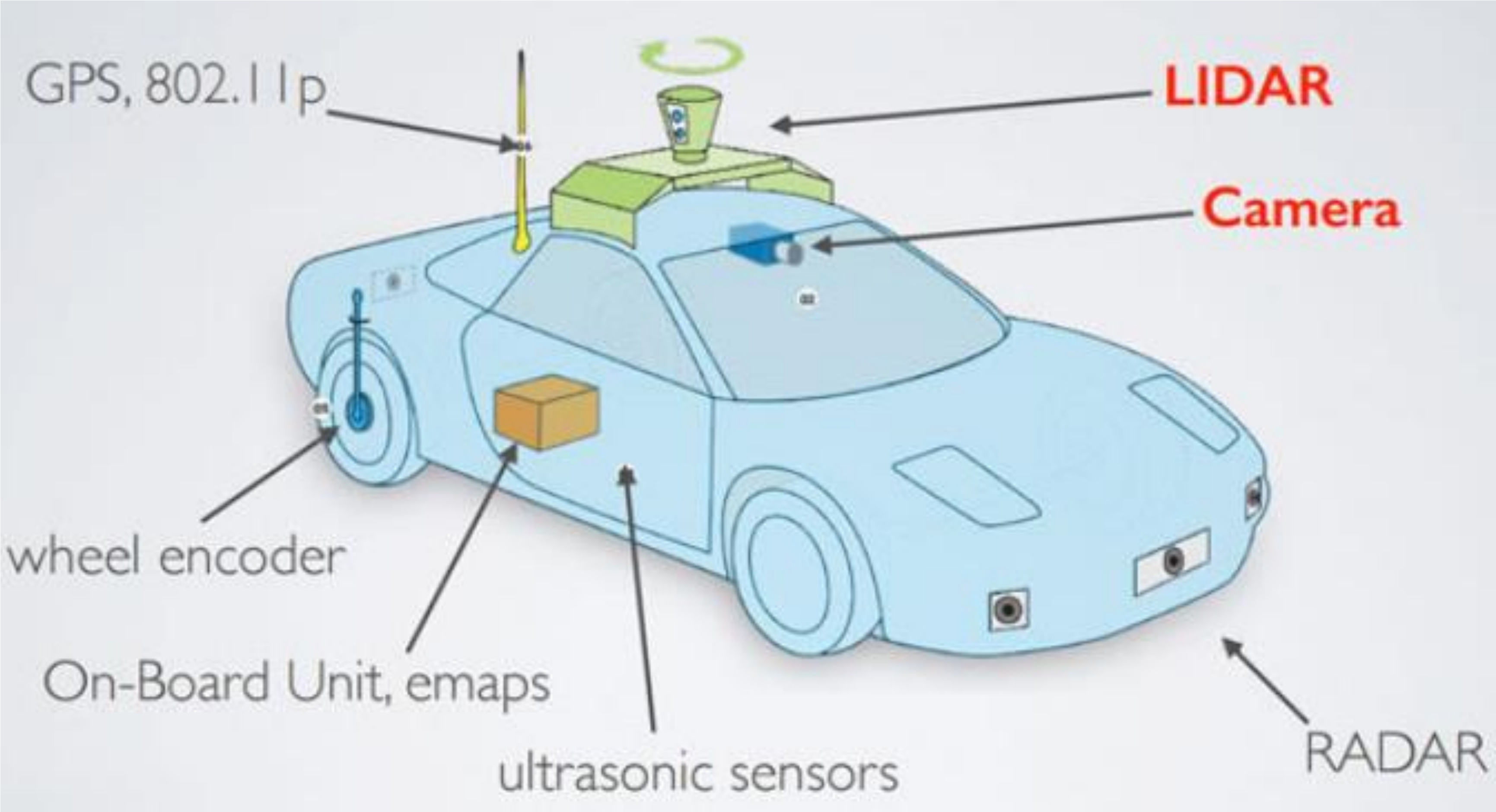
SAS = Safety and Automation System

SIS = Safety Instrumented Systems

ICS = Industrial Control Systems

IACS = Industrial Automation and Control Systems

Autonomous system



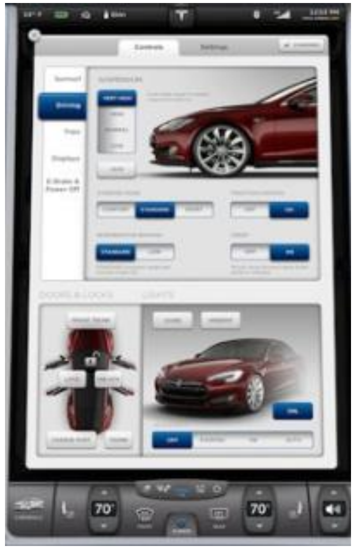
IACS

Simple IACS lab

The controller

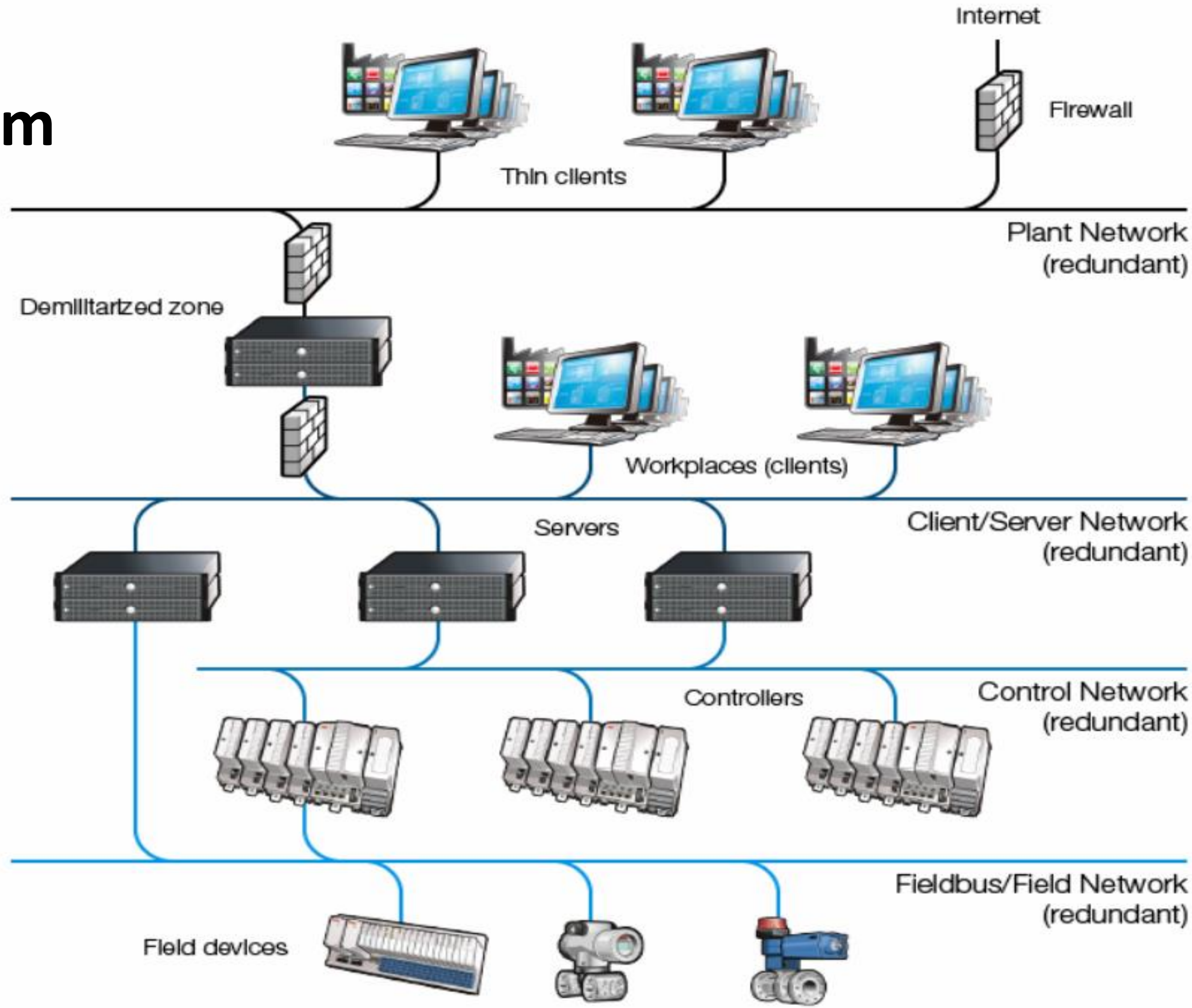
HMI

Human Machine
Interface



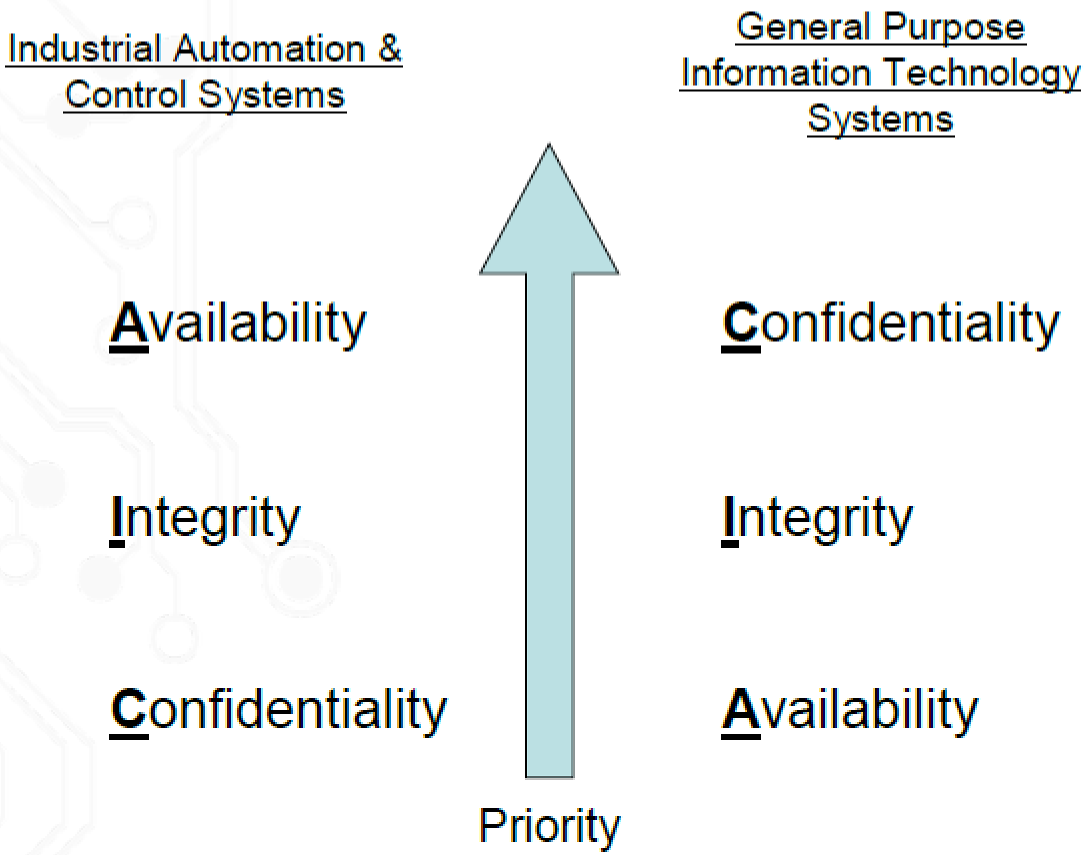
Vulnerabilites

System


Internet
Firewall
Thin clients
Plant Network
(redundant)
Demilitarized zone
Workplaces (clients)
Client/Server Network
(redundant)
Servers
Controllers
Control Network
(redundant)
Fieldbus/Field Network
(redundant)
Field devices

Priorities

Operational Technology (OT)



Industrial Automation & Control Systems

Availability

Integrity

Confidentiality

General Purpose Information Technology Systems

Confidentiality

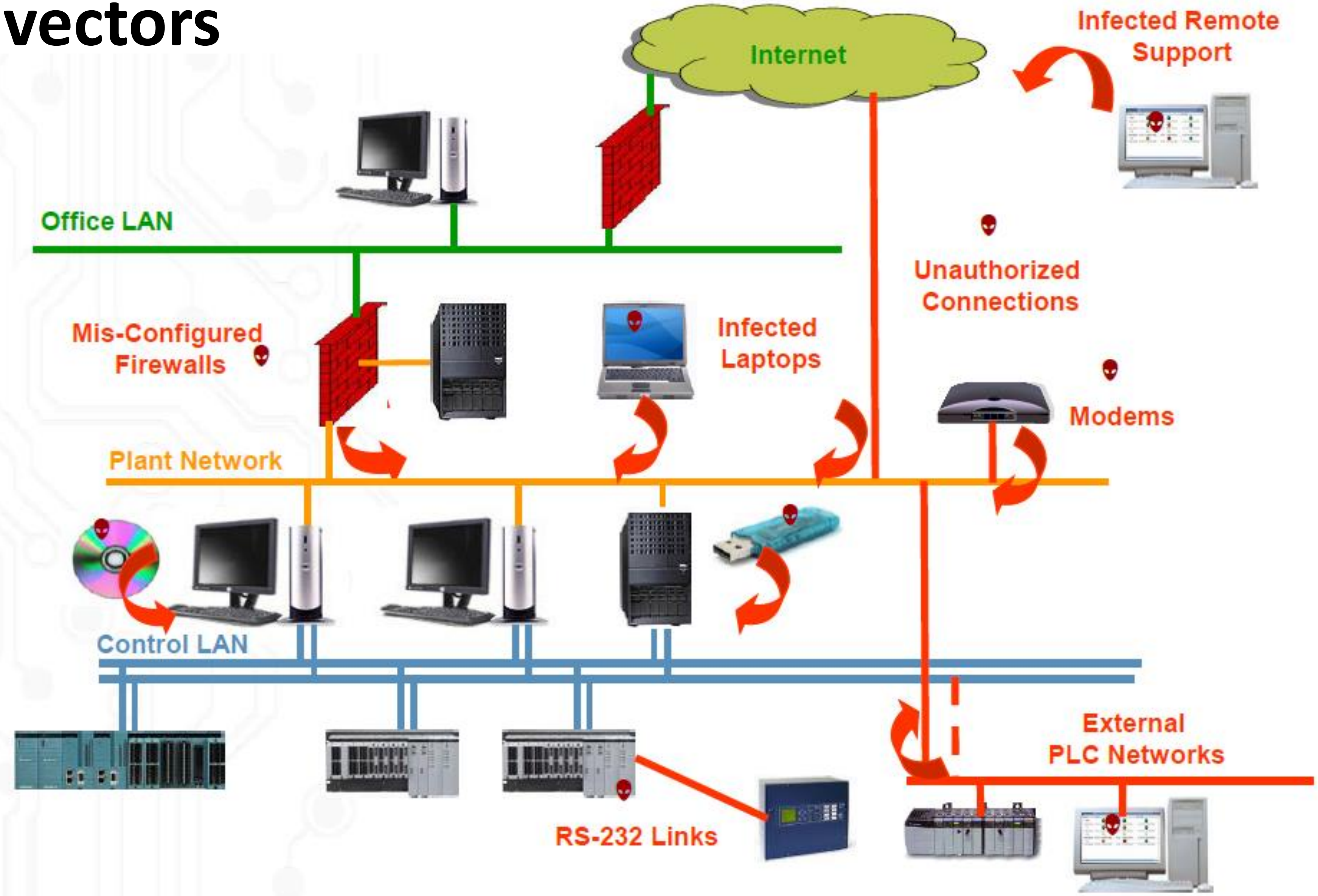
Integrity

Availability

Priority

Information Technology (IT)

Attack vectors



Source: Critical Facilities Summit 2017

Incidents and trends

Major incidents

- **2008:** Conficker – Windows worm, infected 9-15 million PCs all over the world
- **2010**: Stuxnet – Targeted virus against Iran, caused mechanical breakdown of over 1000 sentrifuges for enrichment of uranium.
- **2012**: Shamoon – Virus against Saudi Aramco - 35.000 PCs got their disks deleted.

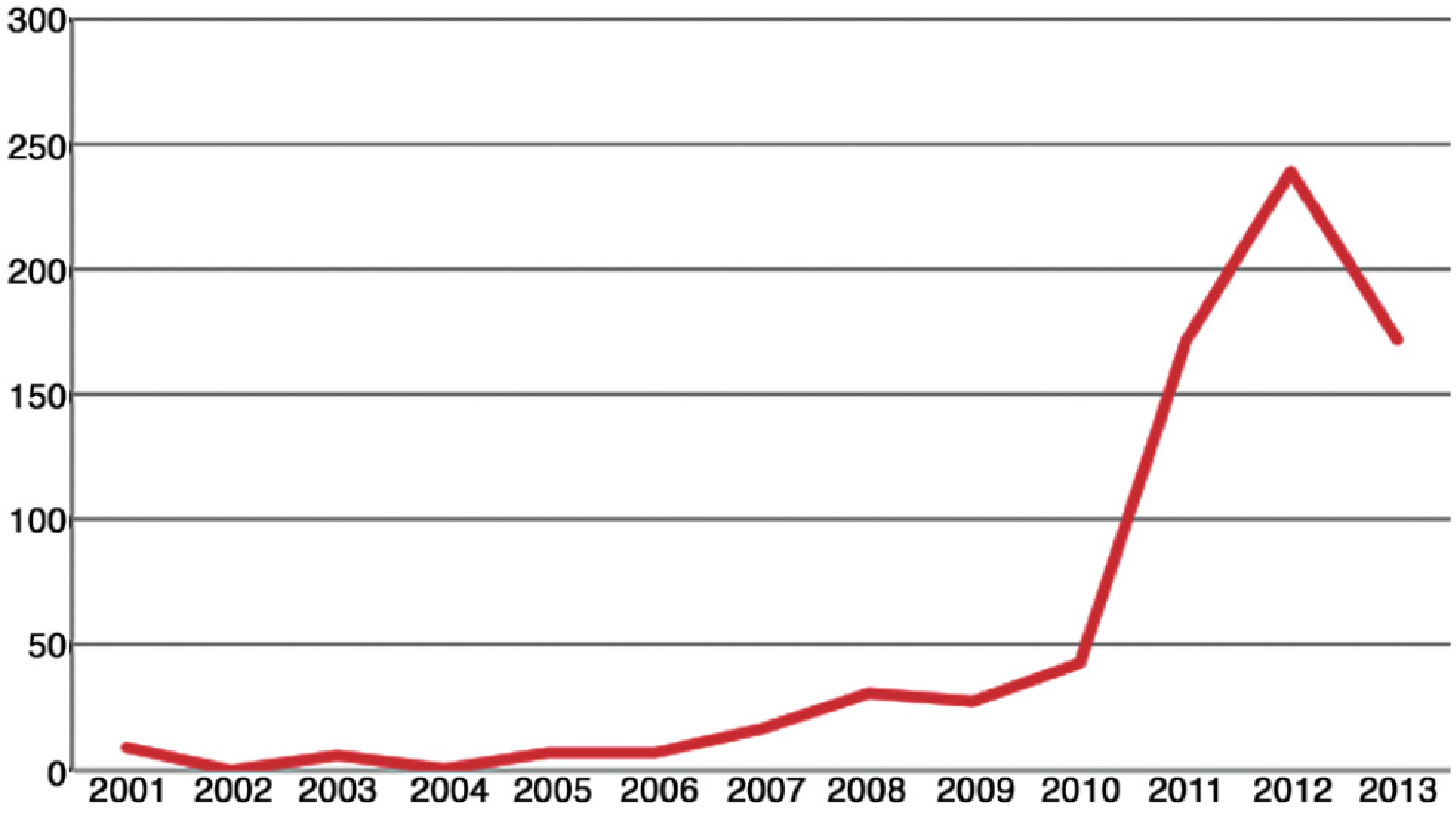
…

…

- **2017**: WannaCry – 230.000 PCs in over 150 countries hit by ransomware.
- **2017**: NotPetya – New wave of ransomware. Maersk – lost 300 million USD.
- **2017**: Triton – Emergency shutdown system in i Saudi Arabia was hacked. Target: physical destruction.
- **2018** Xenotime – The group behind Triton develops more capabilities through increased amount of knowledge sharing in security forums.

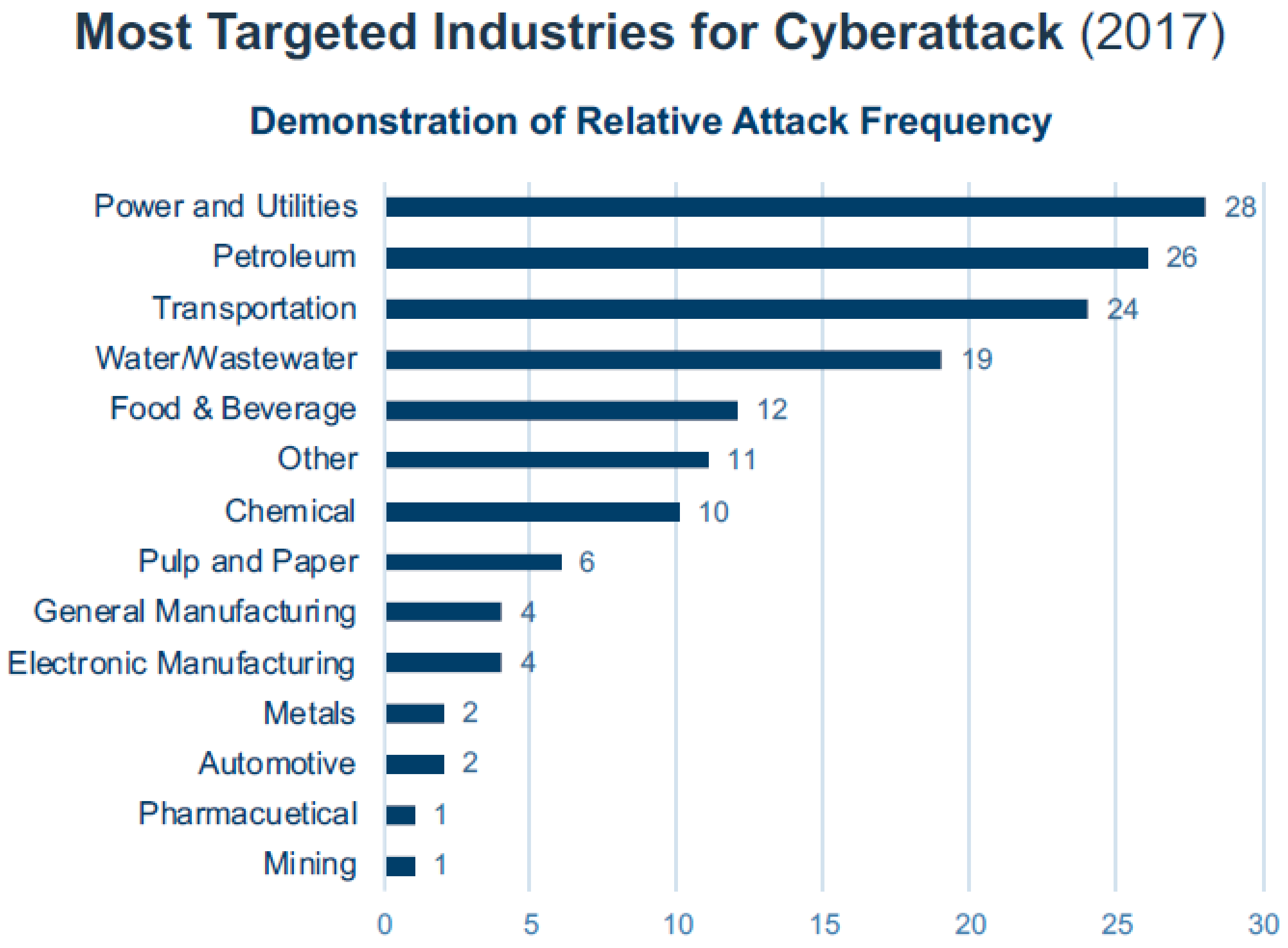
Threats – trends

Reported incidents:



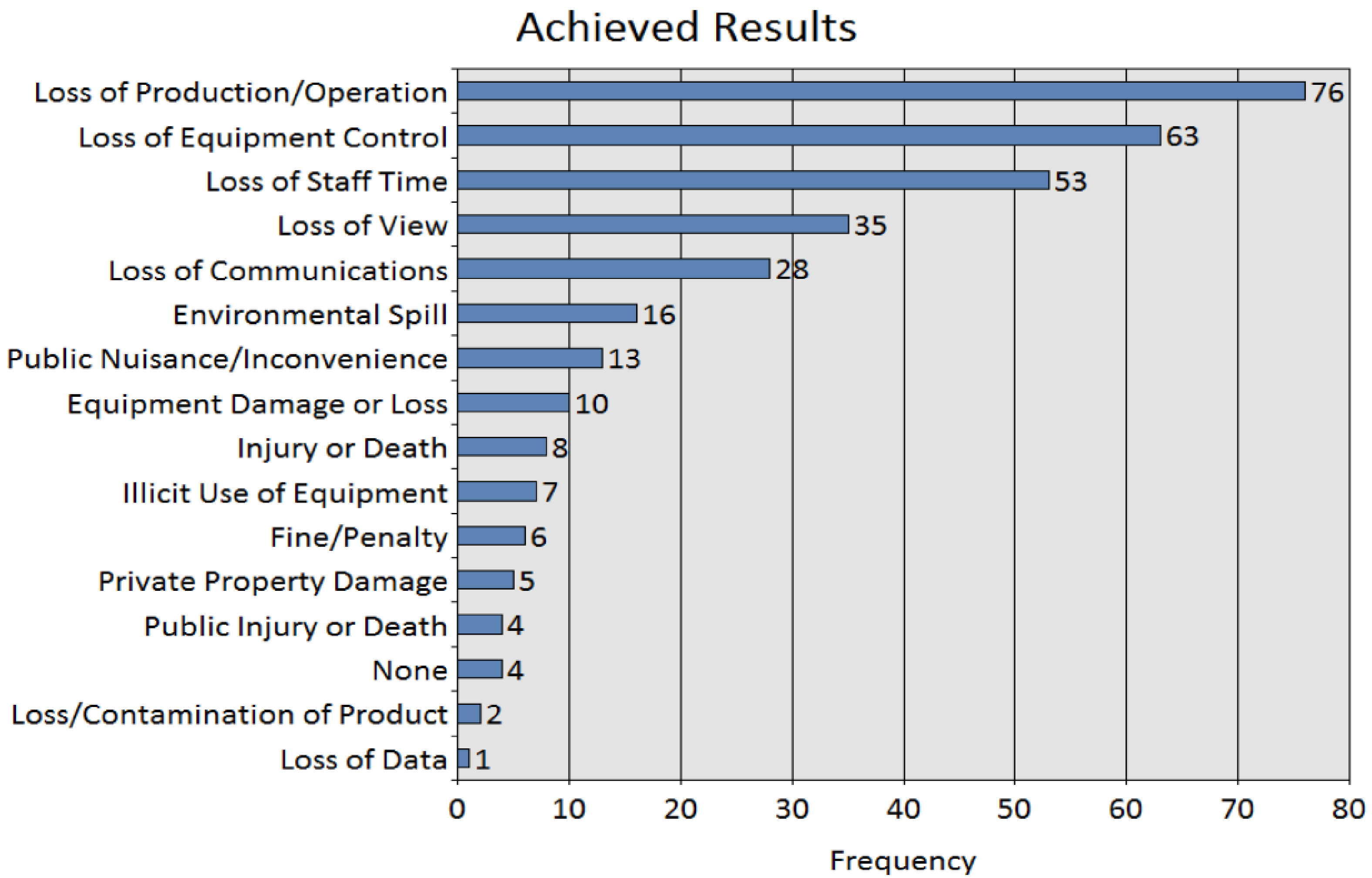
Source: RISI Online Incident Database

Threats – trends



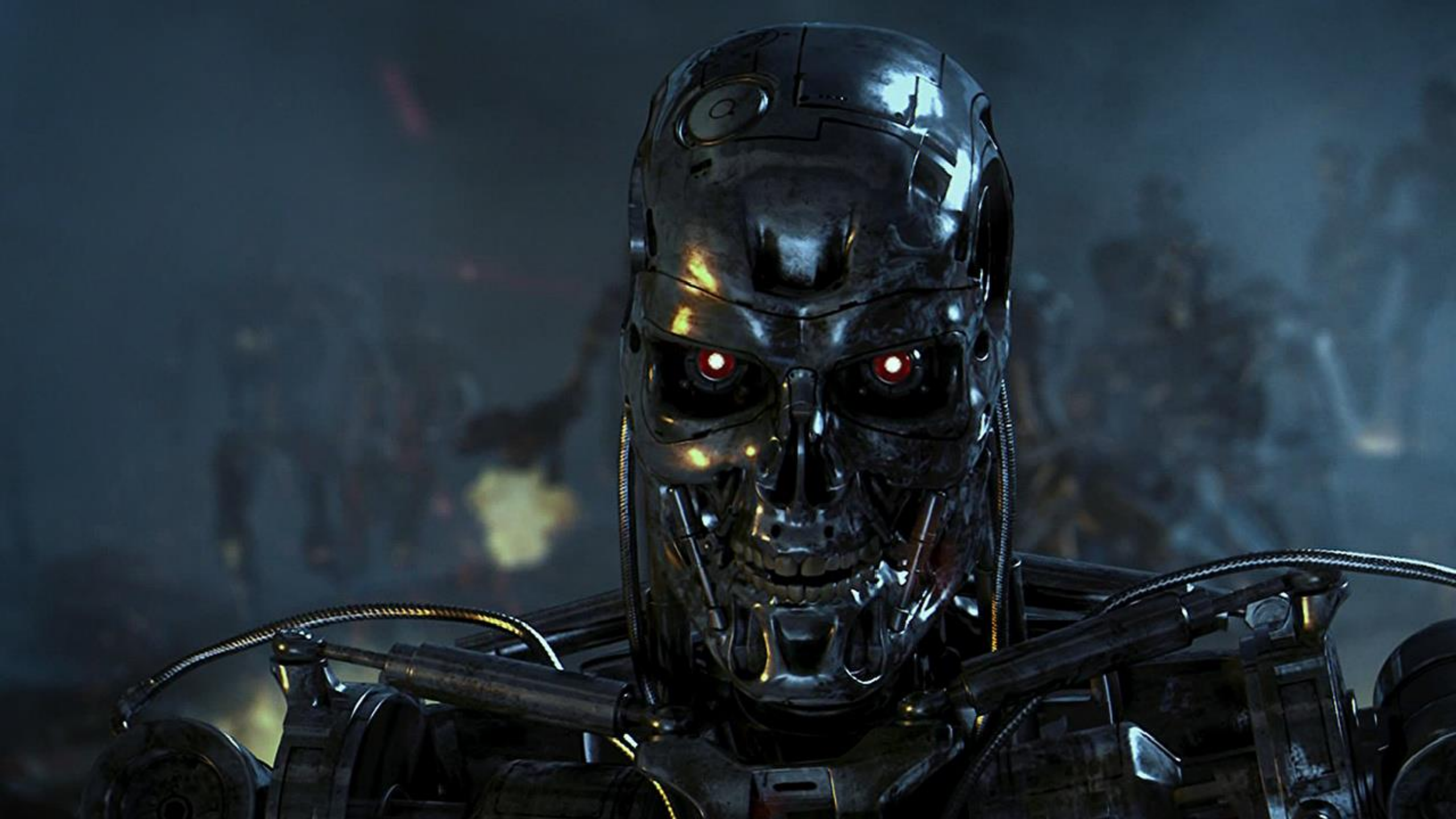
Source: IBM Institute for Business Value

Threats – trends



Source: RISI Online Incident Database

Future threats?



Future threats

What do we need to be aware of in the coming years?

Threats increase

Incidents in 2017 and Xenotime in 2018 is a good illustration.

Digitalization, remote operations, more inter-connectedness with more functionality and more autonomity:

Increasing complexity, more vulnerabilities in code and configuration.

Future threats

Security experts (white-hats, pentesters, hackers etc) constantly develop new tools and methods, and share diligently between themselves:

- Evasion and stealth-methods
- Databases of weaknesses and exploits (Shodan, Exploit-db, virustotal)
- Bypass of antivirus, SMS-authenthication, phishing
- Fileless attacks
- Living-off-the-land
- Hardware hacking
- Command & Control (C2) over DNS, MySql, Https, etc
- Worms for PLCs due to more functionality in PLCs

Mitigation?

Frameworks for building cybersecure systems

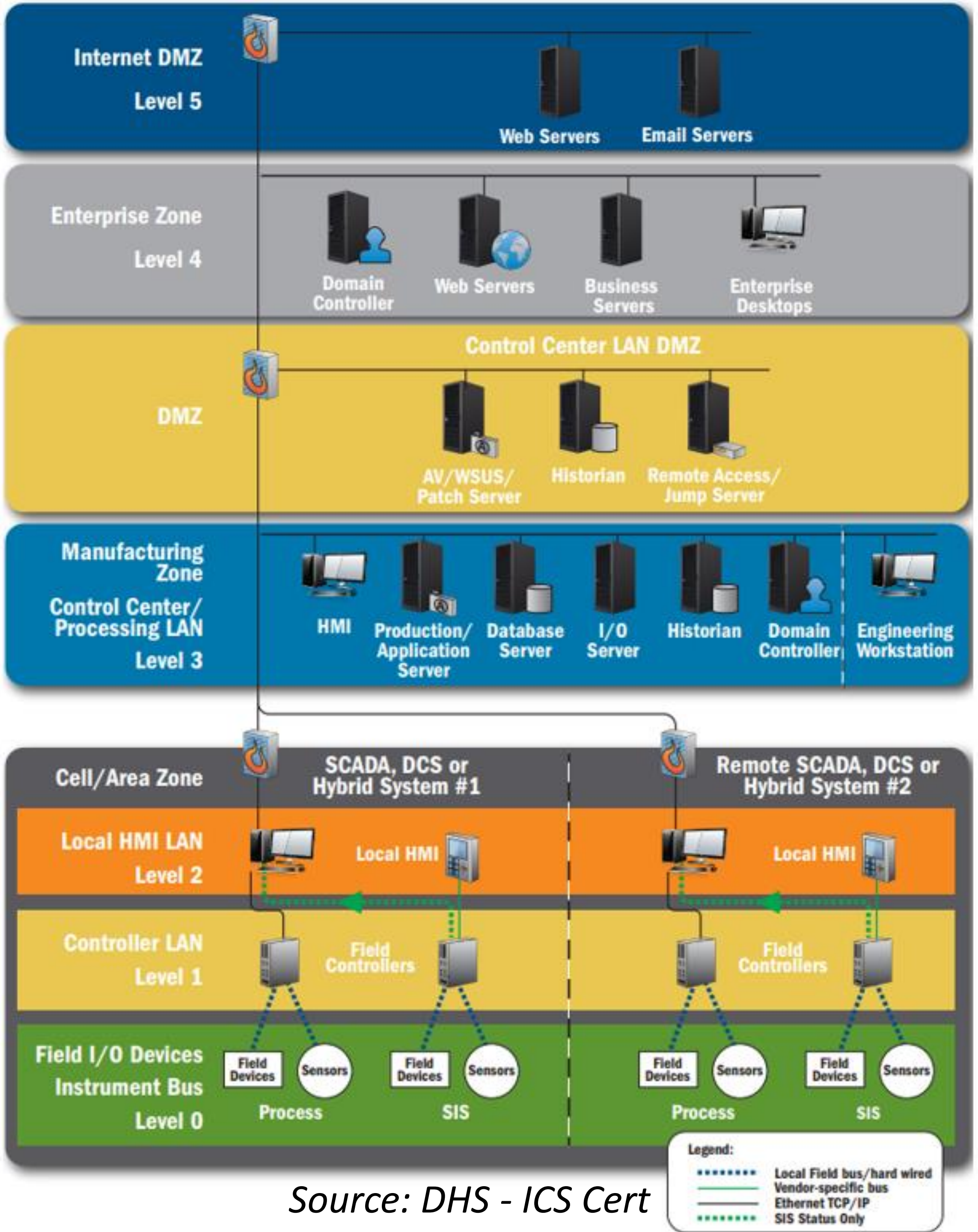
IEC 62443

NIST CSF

CIS CSC

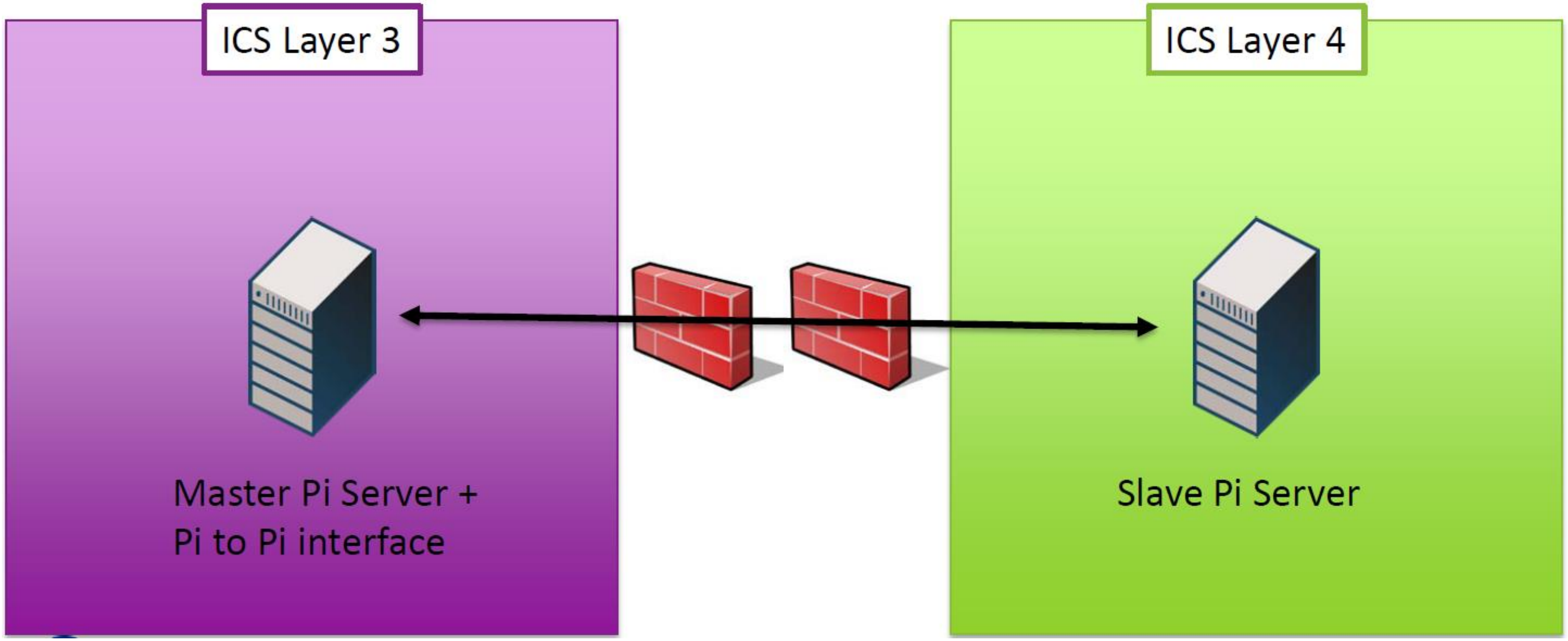
Some recommended actions

- Zone/conduit-model. Segregation
- Continously monitor and assess weaknesses and status of security boundaries and -functions.
- Continously patch known vulnerabilities once they get published or detected.
- Extra solid border protection between IT and OT, in DMZ (Zone 3.5). Whitelisting, EDR, MFA.
- Understand the threats and vulnerabilites
- Assume breach, go threathunting



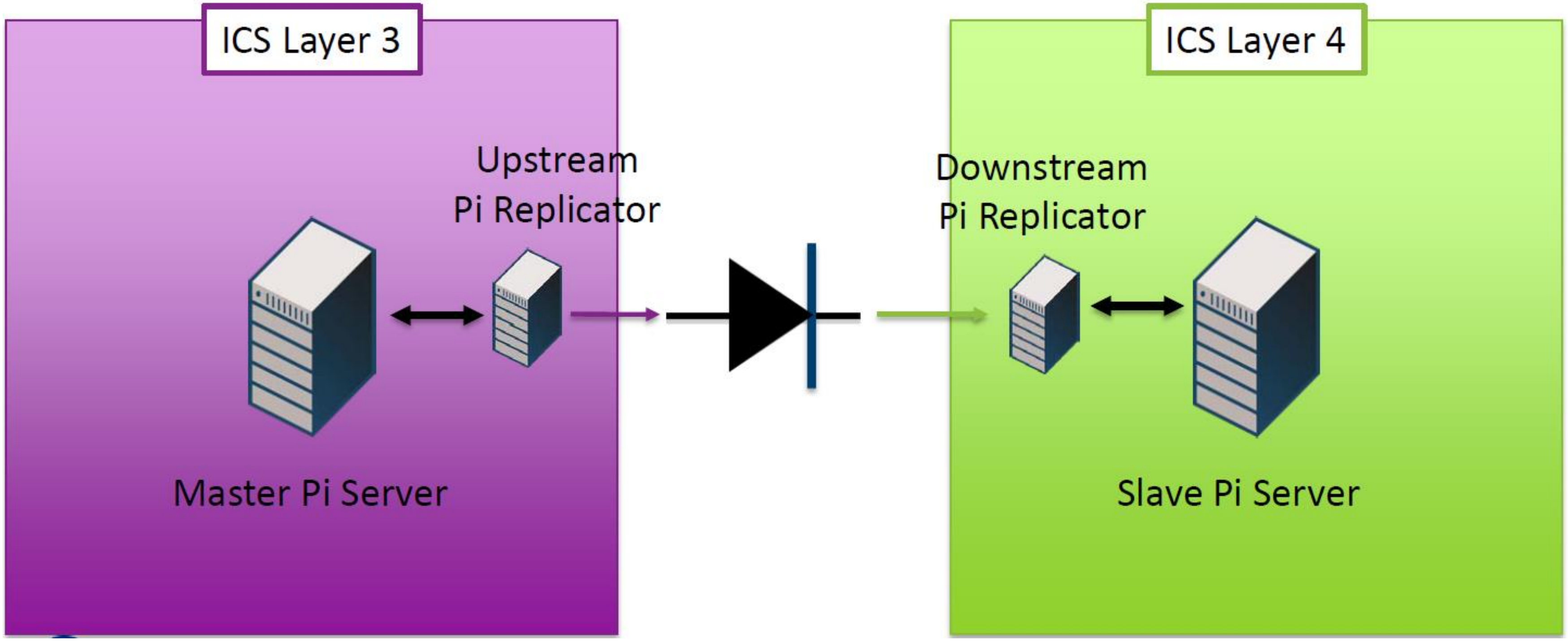
Source: DHS - ICS Cert

Move cybersecurity into the world of electronics and physics



Source: RSA Conference 2016, Abu Dhabi

Move cybersecurity into the world of electronics and physics

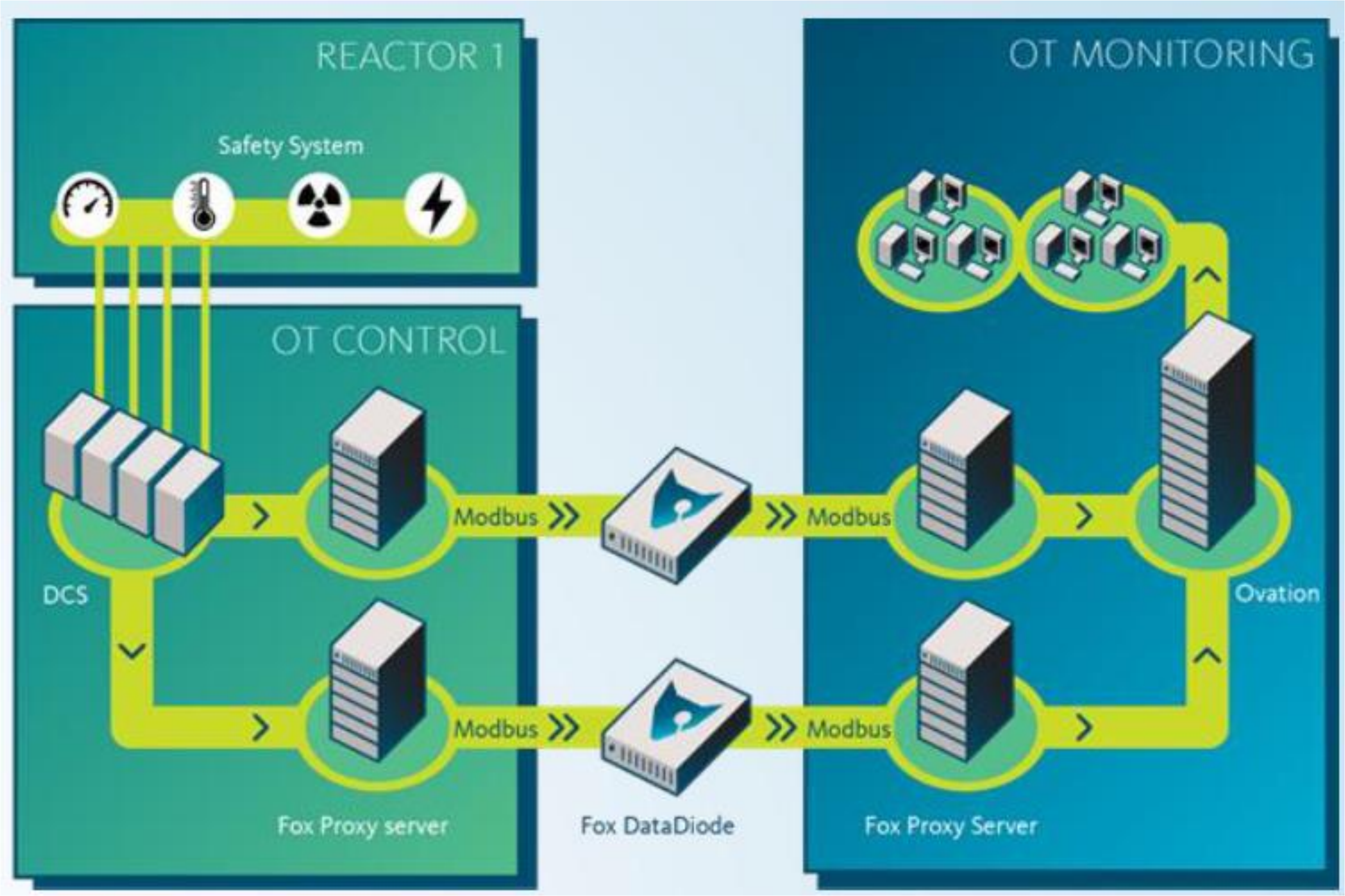


Source: RSA Conference 2016, Abu Dhabi

DataDiodes

arbit
DATADIODE
PWR
1
2
STATUS
ALARM
POWER
QC
Arbit Data Diode Pitcher Unit PU162-HD-T
PITCHER
arbit
DATADIODE
PWR
1
2
STATUS
ALARM
POWER
QC
Arbit Data Diode Catcher Unit CU162-HD-T
CATCHER

DataDiodes


REACTOR 1
Safety System
OT CONTROL
DCS
Modbus
Modbus
Fox Proxy server
Fox DataDiode
OT MONITORING
Modbus
Modbus
Ovation
Fox Proxy Server

Thank you!

sopra steria

Delivering Transformation. Together.

www.soprasteria.no