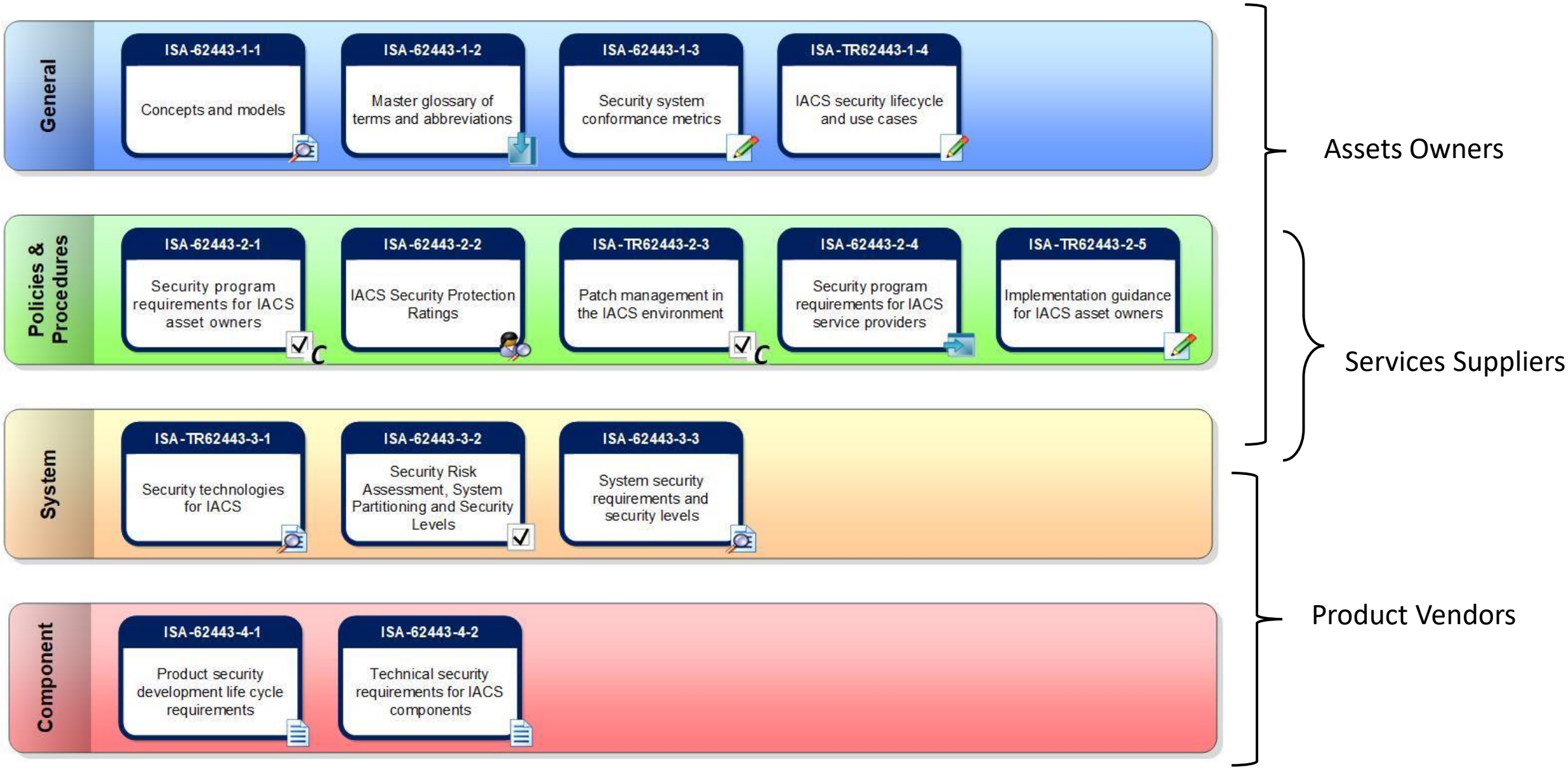
ISA-62443-3-3 Standard, lessons learn from the plant floor

Presenter: Gilles Loridon, Cyberium CEO

Cyberium

- 29 experience of working in IT/OT systems development and OT Cyber Security.
- IEC/ISA 62443 certified.
- Pioneered implementation IEC/ISA 62443 CSMS in Middle East.
- SME in Nuclear Safety relative to AIA & LOLA, NRC 5.71.
- Regular speaker in ISA & Nuclear Security conferences

Part I – Refresher on ISA-62443-3-3


General
ISA-62443-1-1
Concepts and models
ISA-62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
Security system conformance metrics
ISA-TR62443-1-4
IACS security lifecycle and use cases
Policies & Procedures
ISA-62443-2-1
Security program requirements for IACS asset owners
ISA-62443-2-2
IACS Security Protection Ratings
ISA-TR62443-2-3
Patch management in the IACS environment
ISA-62443-2-4
Security program requirements for IACS service providers
ISA-TR62443-2-5
Implementation guidance for IACS asset owners
System
ISA-TR62443-3-1
Security technologies for IACS
ISA-62443-3-2
Security Risk Assessment, System Partitioning and Security Levels
ISA-62443-3-3
System security requirements and security levels
Component
ISA-62443-4-1
Product security development life cycle requirements
ISA-62443-4-2
Technical security requirements for IACS components
Assets Owners
Services Suppliers
Product Vendors

ISA-62443-3-3

Systems

- **TR62443-3-1 is a Technical Report** describing security technologies for ICS (under revision)
- **62443-3-2** provides specific guidance on methodology to perform Cyber Security Risk Assessment for ICS (Brand new).
- **62443-3-3** provides the list of controls for each of the 7 Foundational Requirements (FR) according to Security Level, SL (Published in 2013 under revision).

Impact Factor

- **Confidentiality:** impact of disclosure of confidential information
- **Integrity:** impact of unauthorized modification/destruction of information
- **Availability:** impact of system's availability
- **Identification and Authentication (IAC):** the Business Consequences of failure to authenticate users (humans, processes or devices)
- **Use Control (UC):** the Business Consequences of failure to enforce policies which restrict use to those authenticated users with sufficient privileges
- **Timely Response to Event (TRE):** the Business Consequences of failure to respond promptly to Information Security violations
- **Restricted Data Flow (RDF):** the Business Consequences of unnecessary data causing restrictions to necessary data flow

Foundational Requirements & Security Vector

7 Foundational Requirements	Example Security Vector: SL-x=(3,3,3,1,2,1,3)
FR 1 – Identification and authentication control	3
FR 2 – Use control	3
FR 3 – System integrity	3
FR 4 – Data confidentiality	1
FR 5 – Restricted data flow	2
FR 6 – Timely response to events	1
FR 7 – Resource availability	3

Security Level

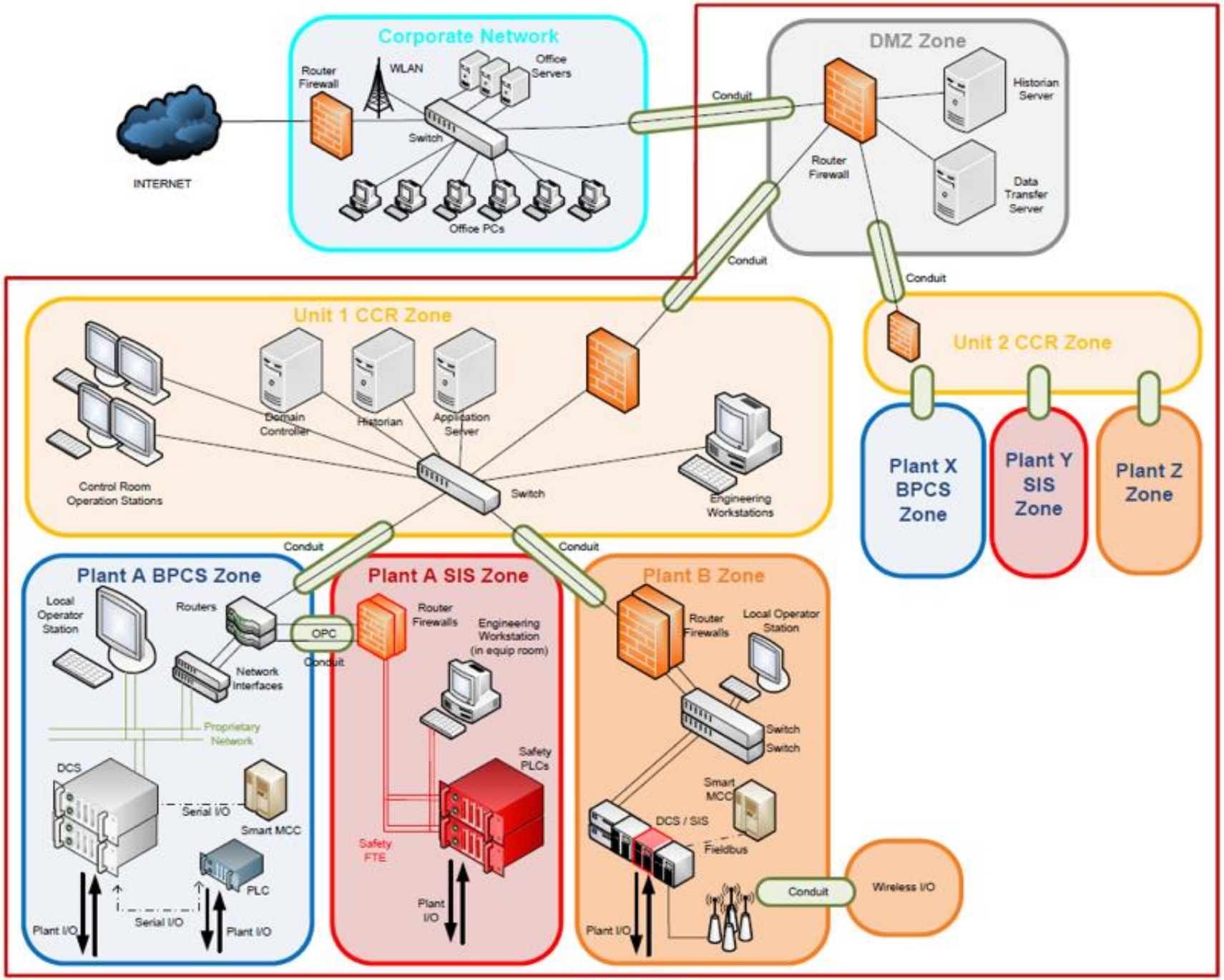
The Zone or conduit defines the SL Target SL-T, controls can achieve a certain SL, Capability SL-C, and after implementation of controls the SL Achieved SL-A, can be same or lower.

The targeted security level is determined by a threat and impact analysis

SL1	Protection against casual or coincidental violation
SL2	Protection against intentional violation using simple means, low resources, generic skills, low motivation
SL3	Protection against intentional violation using sophisticated means, moderate resources, IACS specific skills, moderate motivation
SL4	Protection against intentional violation using sophisticated means, extended resources, IACS specific skills, high motivation

ISF IRAM 2 Threat Landscape

Threat	Threat Group	Origin	LoI	TS
Nation-state	Adversarial	External	High	Very High
Organised criminal group	Adversarial	External	High	High
Power failure or fluctuation	Environmental	External	High	High
Employee (privileged)	Adversarial	Internal	Low	High
Fire (structural)	Environmental	Internal/external	Low	High
Supplier/vendor/partner	Adversarial	Internal	Low	High
Employee (privileged)	Accidental	Internal	Low	High
Pathogen	Environmental	Internal/External	High	Low
Hacking group	Adversarial	External	Moderate	Moderate
Flooding	Environmental	Internal/external	Low	Moderate
Individual hacker	Adversarial	External	Low	Moderate
Failure of environmental control systems	Environmental	Internal/External	Low	Moderate
Supplier/vendor/partner	Adversarial	External	Low	Moderate
Hardware malfunction or failure	Environmental	Internal/external	Low	Moderate
Employee (general)	Adversarial	Internal	Low	Low
Customer	Adversarial	External	Low	Low
Employee (general)	Accidental	Internal	Low	Low
Supplier/vendor/partner	Accidental	Internal	Low	Low
Damage to or loss of external communications	Environmental	External	Low	Low
Customer	Accidental	External	Low	Negligible


Corporate Network
Router Firewall
WLAN
Office Servers
Switch
Office PCs
INTERNET
DMZ Zone
Conduit
Historian Server
Router Firewall
Data Transfer Server
Conduit
Conduit
Unit 1 CCR Zone
Domain Controller
Historian
Application Server
Control Room Operation Stations
Switch
Engineering Workstations
Unit 2 CCR Zone
Plant X BPCS Zone
Plant Y SIS Zone
Plant Z Zone
Conduit
Conduit
Plant A BPCS Zone
Local Operator Station
Routers
OPC
Network Interfaces
Proprietary Network
DCS
Serial I/O
Smart MCC
PLC
Serial I/O
Plant I/O
Plant I/O
Plant A SIS Zone
Router Firewalls
Conduit
Engineering Workstation (in equip room)
Safety PLCs
Safety FTE
Plant I/O
Plant B Zone
Router Firewalls
Local Operator Station
Switch
Switch
Smart MCC
DCS / SIS
Fieldbus
Conduit
Wireless I/O
Plant I/O
IACS Boundary

IEC62443 FR 5 – Restricted data flow

SR and RE	SL 1	SL 2	SL 3	SL 4
FR 5 – Restricted data flow				
SR5.1 - Network segmentation	X	X	X	X
SR5.1 RE 1 Physical Network segmentation		X	X	X
SR5.1 RE 2 Independence from non-control system networks			X	X
SR5.1 RE 3 Logical and physical isolation of critical networks				X
SR5.2 - Zone boundary protection	X	X	X	X
SR5.2 RE 1 Deny by default, allow by exception		X	X	X
SR5.2 RE 2 Island mode			X	X
SR5.2 RE 3 Fail close			X	X
SR5.3 - General purpose person-to-person restriction	X	X	X	X
SR5.3 RE 1 Prohibit all general purpose person-to-person communication			X	X
SR5.4 - Application partitioning	X	X	X	X

Technology Comparison

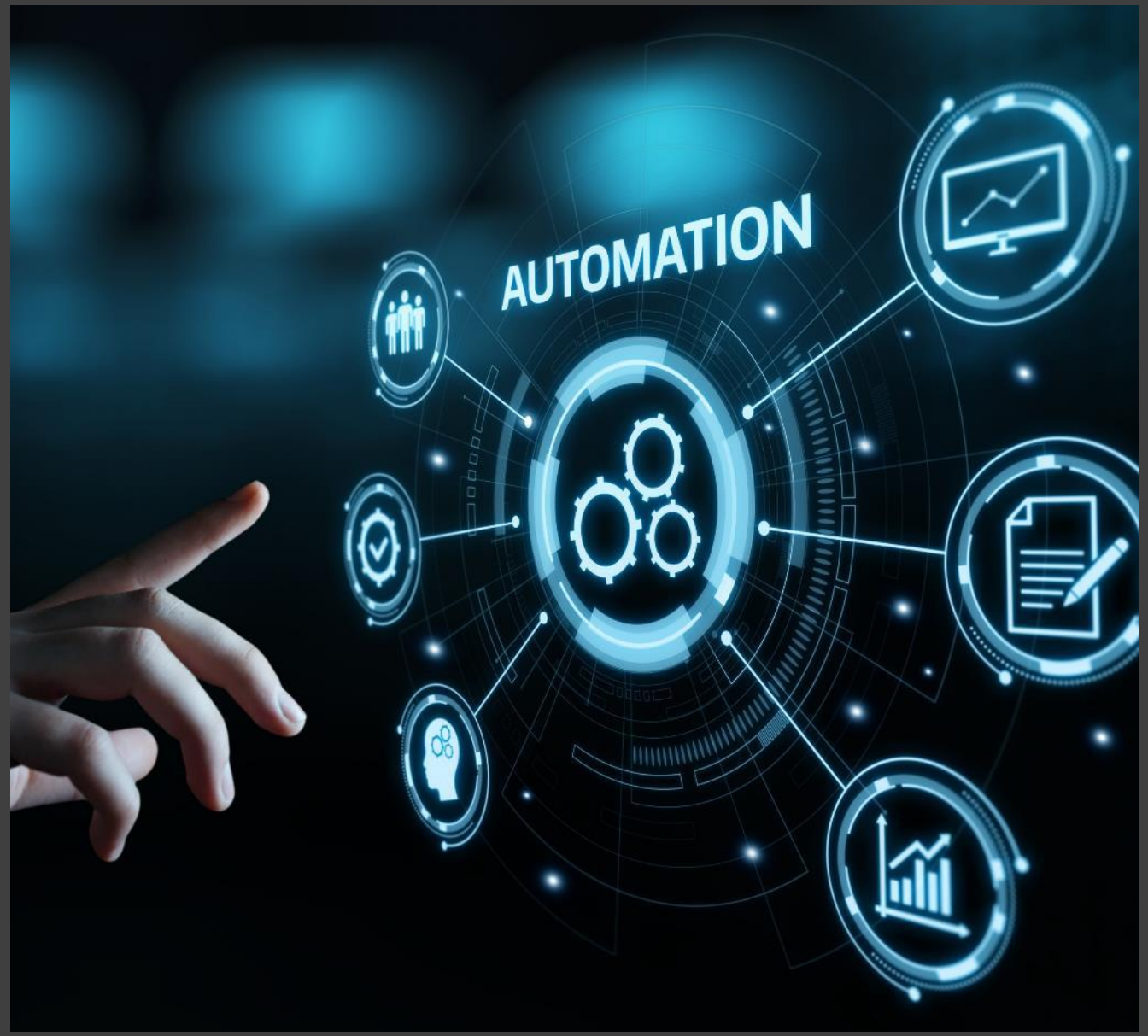
SR and RE	Firewalls	Two way gateway	Hardware DataDiode
FR 5 – Restricted data flow			
SR5.1 - Network segmentation	Yes	Yes	Yes
SR5.1 RE 1 Physical Network segmentation	No	Debatable	Yes
SR5.1 RE 2 Independence from non-control system networks	Maybe	Maybe	Yes
SR5.1 RE 3 Logical and physical isolation of critical networks	No	Debatable	Yes
SR5.2 - Zone boundary protection	Yes	Yes	Yes
SR5.2 RE 1 Deny by default, allow by exception	Maybe	Yes	Yes
SR5.2 RE 2 Island mode	?	?	Yes
SR5.2 RE 3 Fail close	Maybe	Yes	Yes
SR5.3 - General purpose person-to-person restriction	Possible	Possible	Yes
SR5.3 RE 1 Prohibit all general purpose person-to-person communication	Possible	Possible	Yes
SR5.4 - Application partitioning	Possible with exception	Possible with exception	Yes

Some Industrial protocols are extremely difficult to secure with a F/W, ie, OPC DA

Firewall & protection

- A National Oil Company: USD 313 million profit in 2019
- 26/12/19, after a merry Christmas, employees (expats) discover that all PCs have been hacked by ransomware
- The hackers penetrated the network through the vulnerabilities of the firewall VPN (no kidding...)
- During Christmas they cracked admin passwords and encrypted all PCs.

Not only the firewalls didn’t protect the network but they facilitate the attack!!!!!



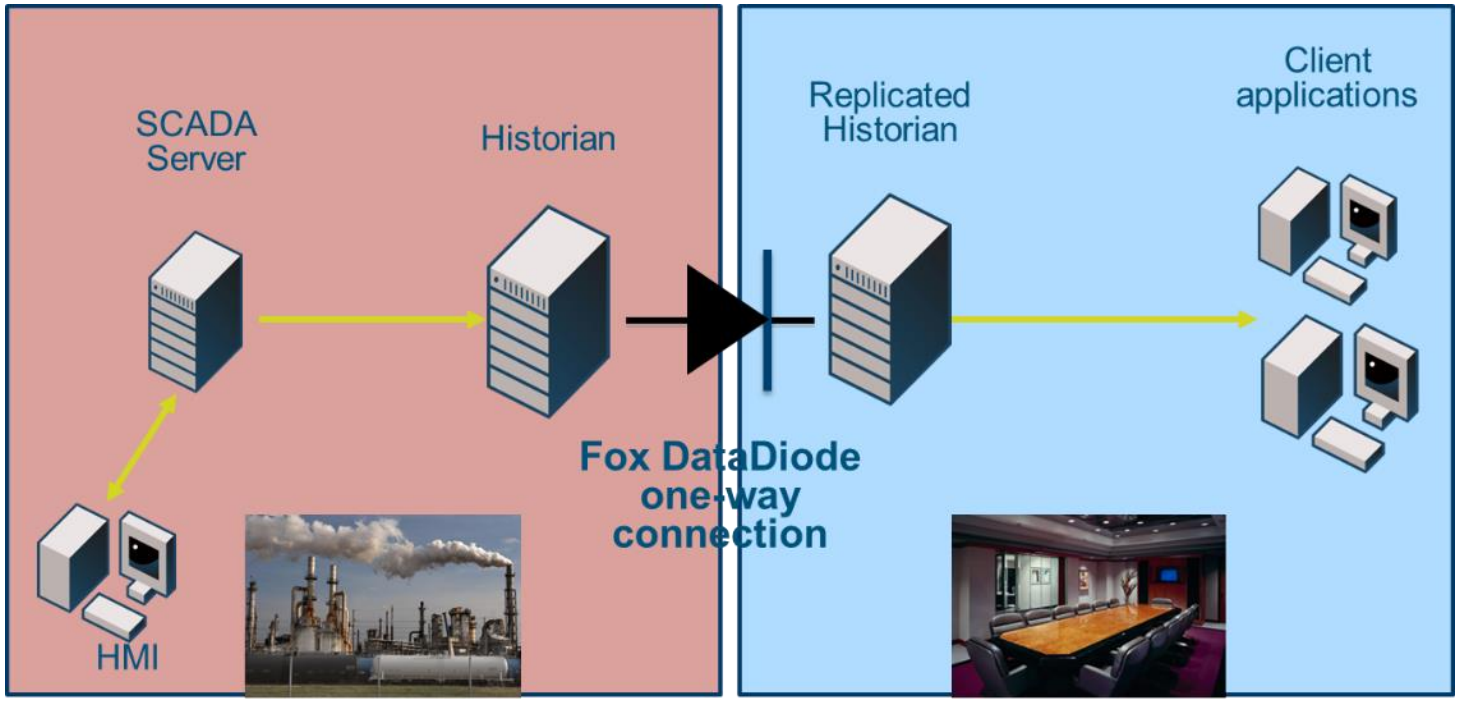
Part II – Case studies

Honeywell PHD Historian replication

Case Study 1

PHD Historian replication setup

- Existing Honeywell PHD server with millions of data points in back log.
- Master PHD server connected to Slave PHD server with 1 Gbps network connection
- OT Engineers familiar with the historian protocols
- Factory Acceptance Test: few thousands data points replicated from OT to IT through FTP file transfer. FAT passed with flying colours.



Blame the Donkey

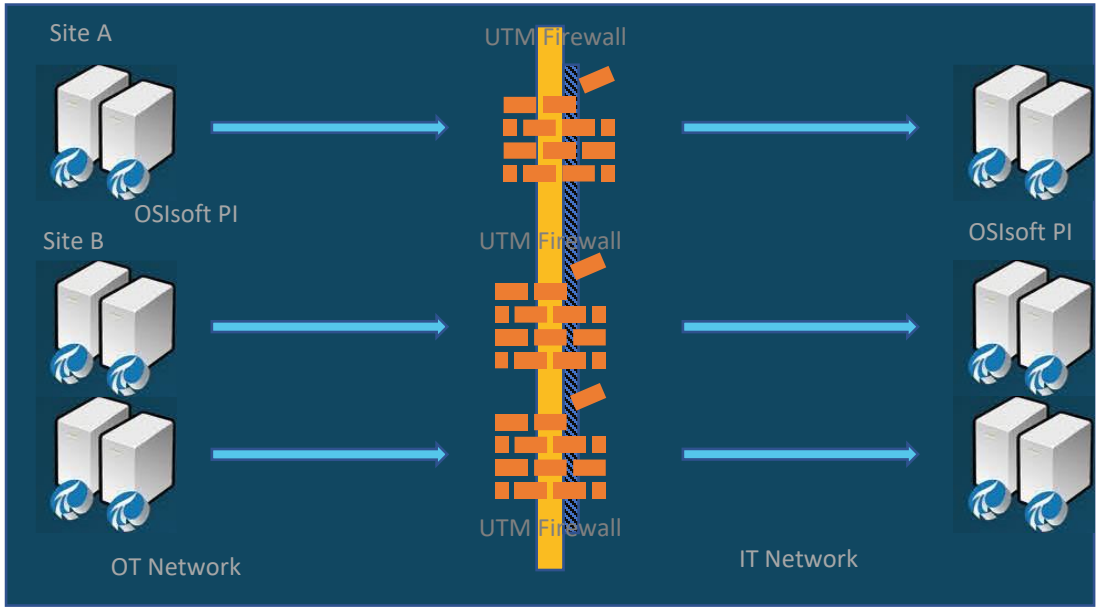
- To process the backlog the OT Engineers sent 400k files through the Data Diode to one single network share folder.
- **Surprise, surprise**: the file sharing sever crashed, I/O kernel panic.
- The OT Engineers blamed the **donkey** (=Data Diode)

OSIsoft PI to PI replication

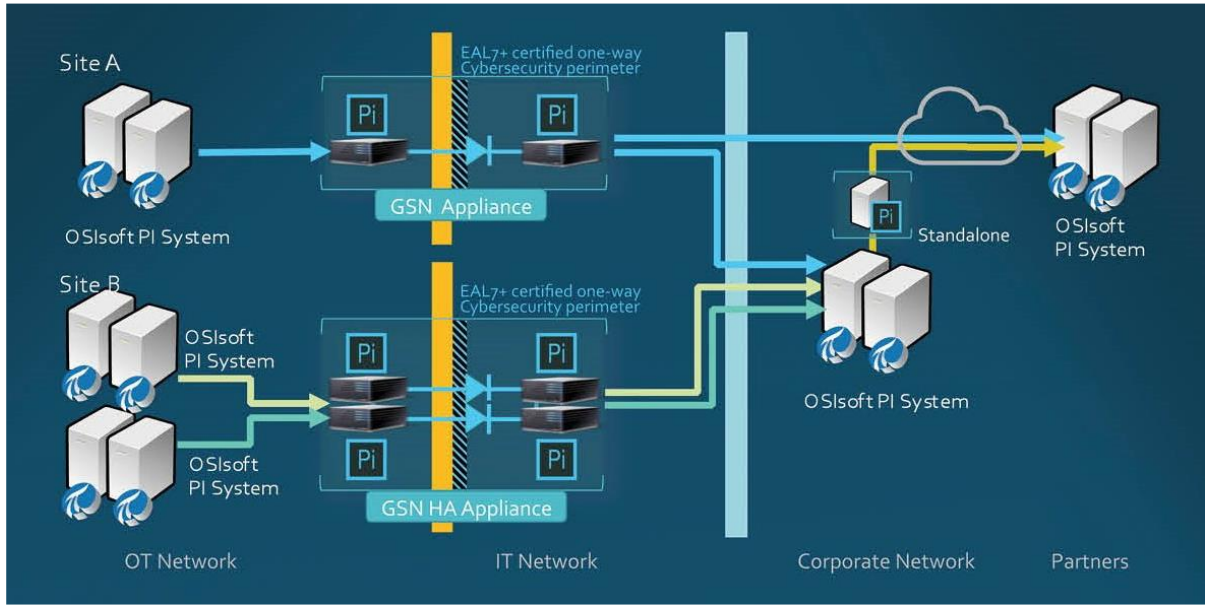
Case Study 2

Real-time HA metadata and data replication with auto backfill and auto recovery

BEFORE: complex architecture, maintenance heavy, licences cost



AFTER: less PI servers in IT, major reduction of cost and 100% protection against outsiders



The End.

Thank you

Merci