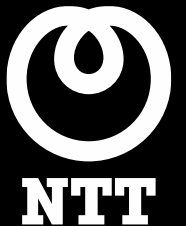


ICS Cyber Security

Water production and distribution

Mezri SAHTOUT
Practice Leader OT/IoT Security



By bringing
together the NTT
family, we are
**better positioned
than ever to make
a difference**

*annual average over the next 5 years across NTT Group

NTT Group

One of the largest ICT
companies in the world by
revenue

USD 11 billion

combined revenue
as NTT Ltd.

40,000

Employees in NTT Ltd.
worldwide

**Bringing together
leading ICT
companies**

to deliver high value

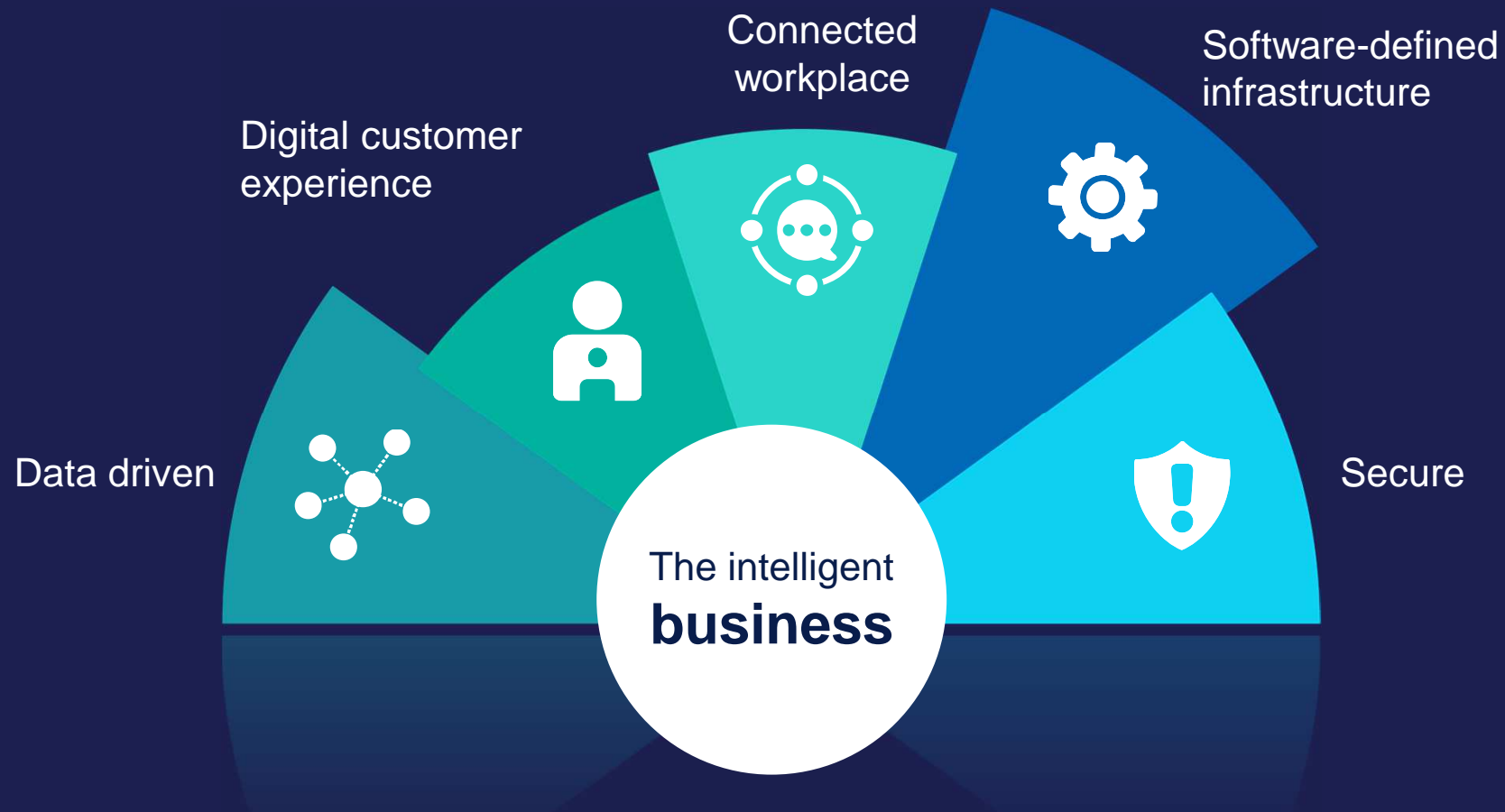
**Delivering
services in over
200 countries**

across 5 regions

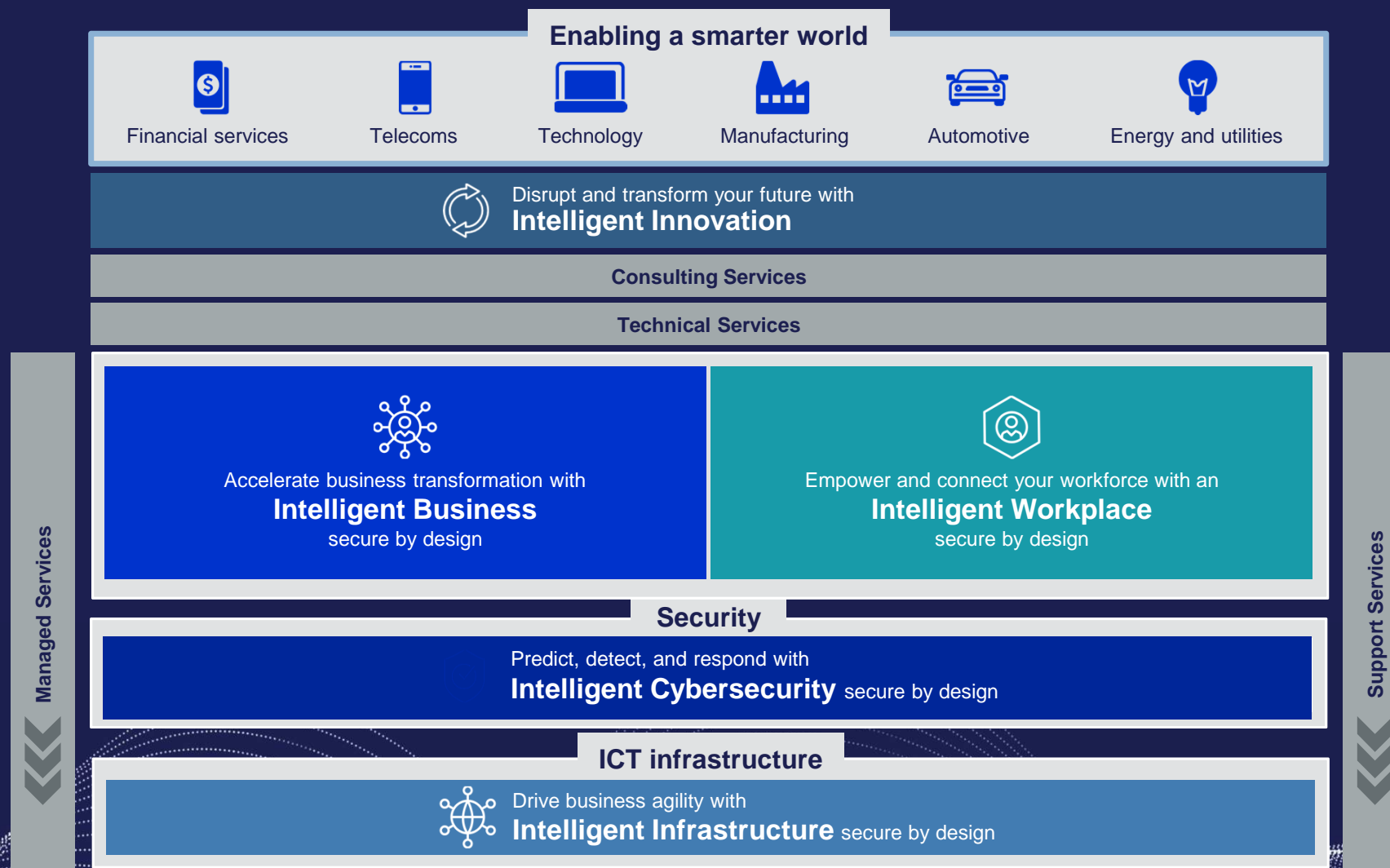
**NTT Group invests
USD 3.6 billion* in R&D
annually**

and employs 5,500 R&D
professionals

The new business model that has emerged to operate in the digital world



NTT has a unique breadth of integrated capabilities



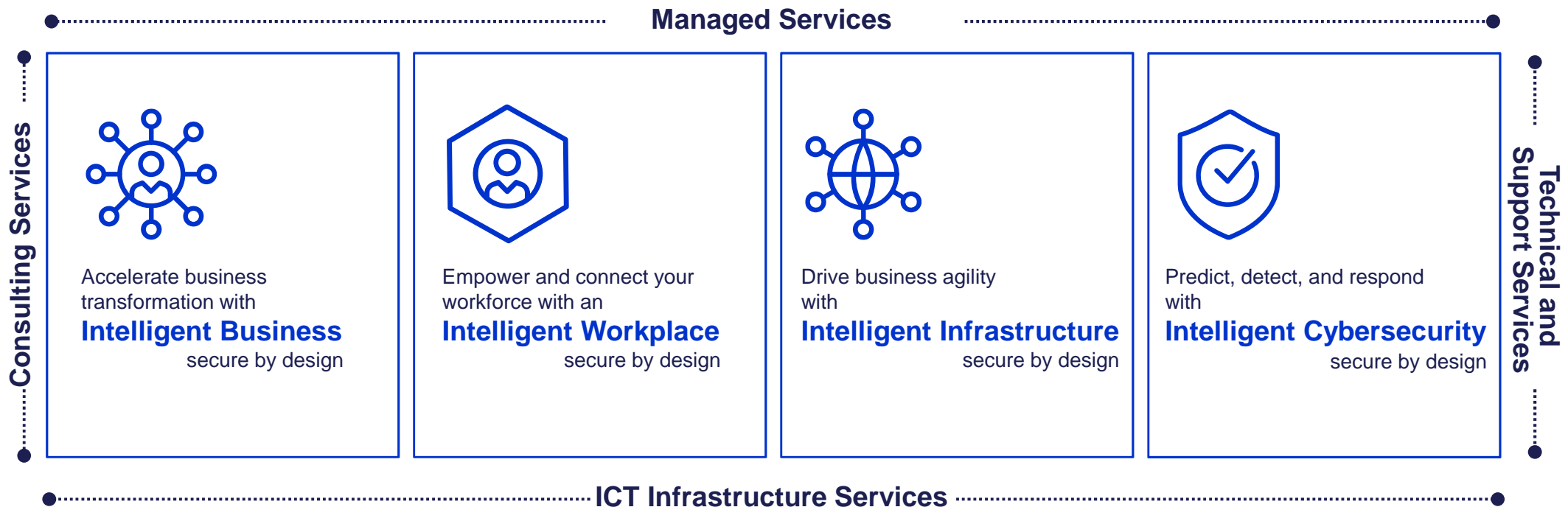
What we do



We partner with organizations **globally** to shape and achieve **outcomes** through **intelligent technology solutions**. For us, intelligent means data driven, connected, digital, and secure.



Disrupt and transform your future with
Intelligent Innovation



What

we deliver

solutions that are secure by design

We'll architect and implement the required solution **across your infrastructure**, workplace, and business solutions

We can provide all this as a **Managed Service** on a global basis

We can advise you on the threats you face and the **security posture you need to adopt**



We'll give you the threat intelligence you need, secure your OT, IoT, and multicloud, and **protect you against ransomware**

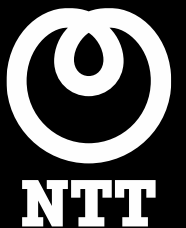


By partnering with us you overcome your skills gap and get access to the world's best security technologies, ready to go

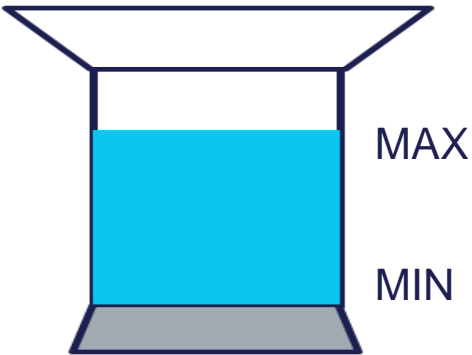
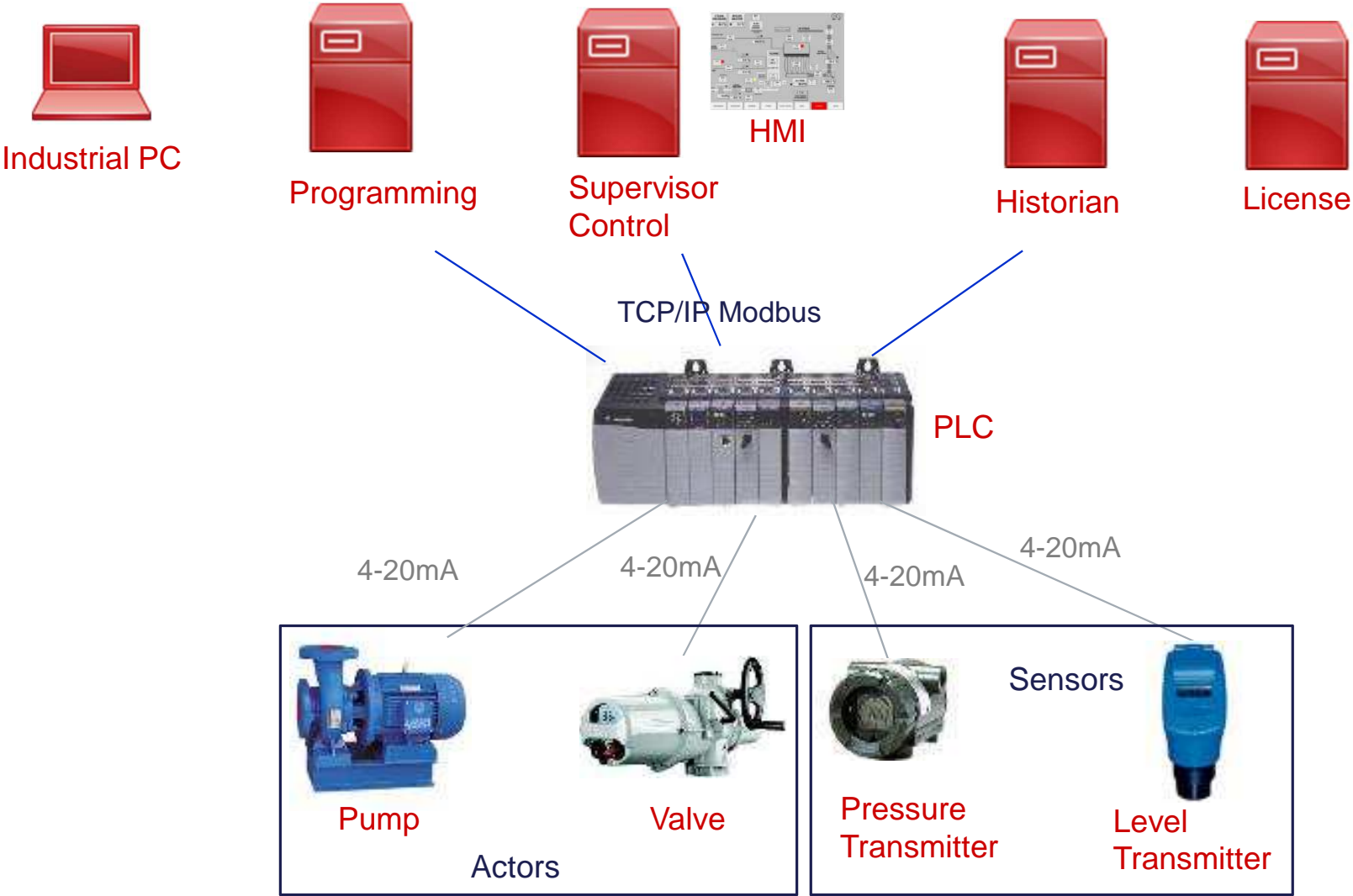


Analysts and clients think **we're one of the best**, and we're even stronger with **NTT Security** behind us

ICS Water Production and Distribution



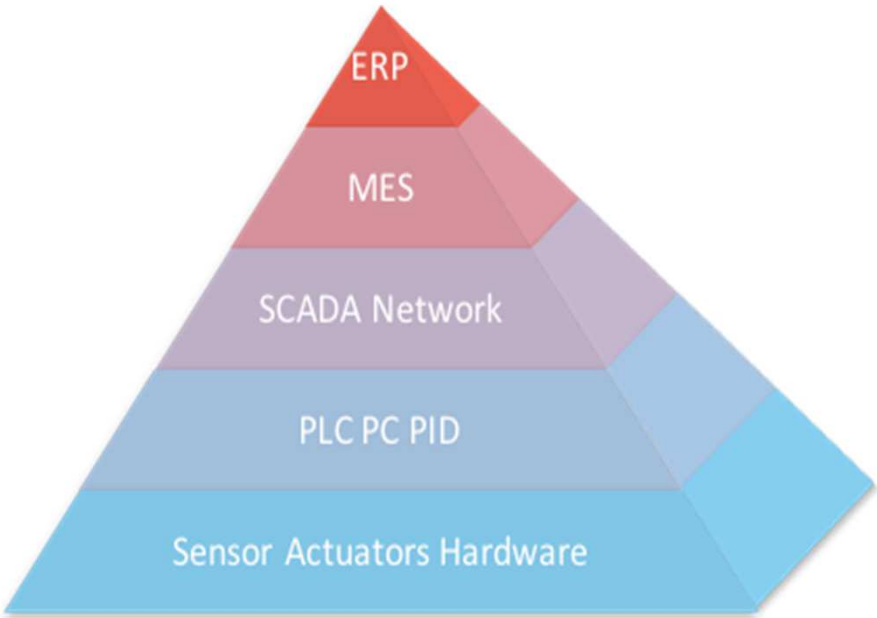
Business Process “Telegestation”



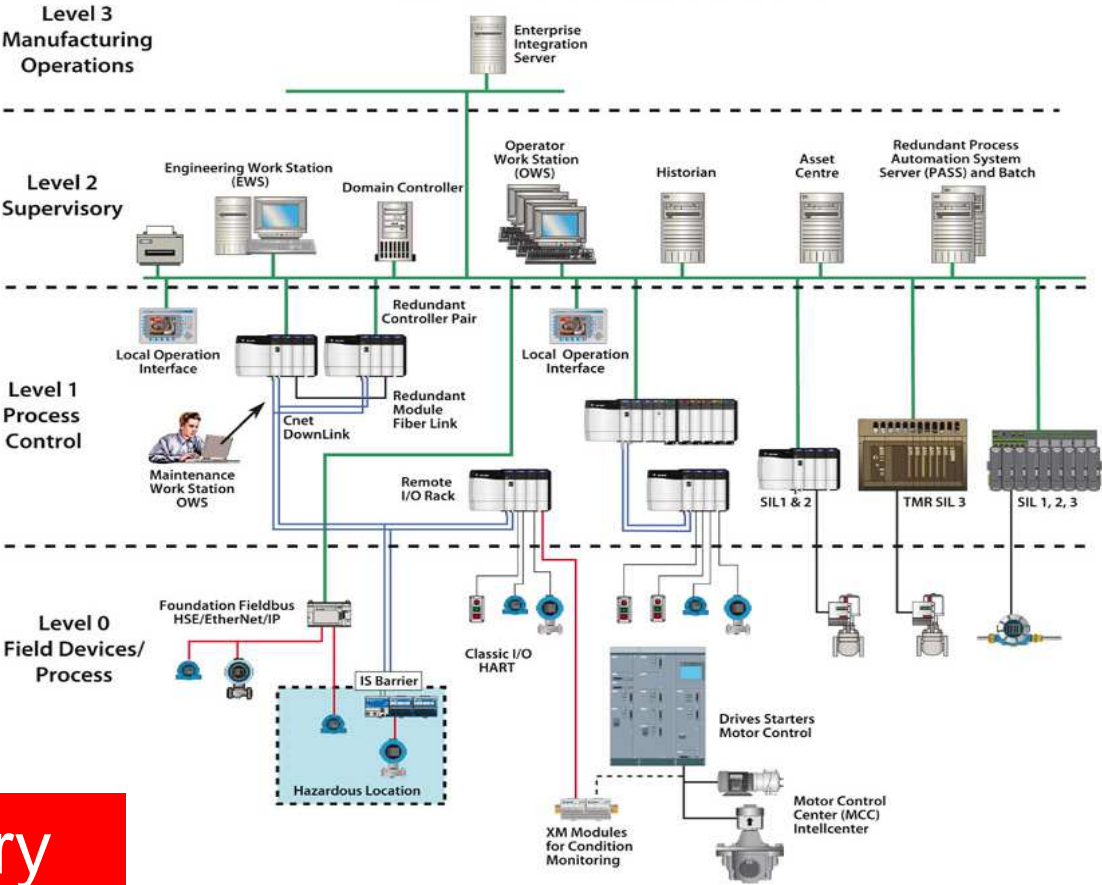
ICS Architecture : Purdue Model



Level 4/5 – Enterprise Zone

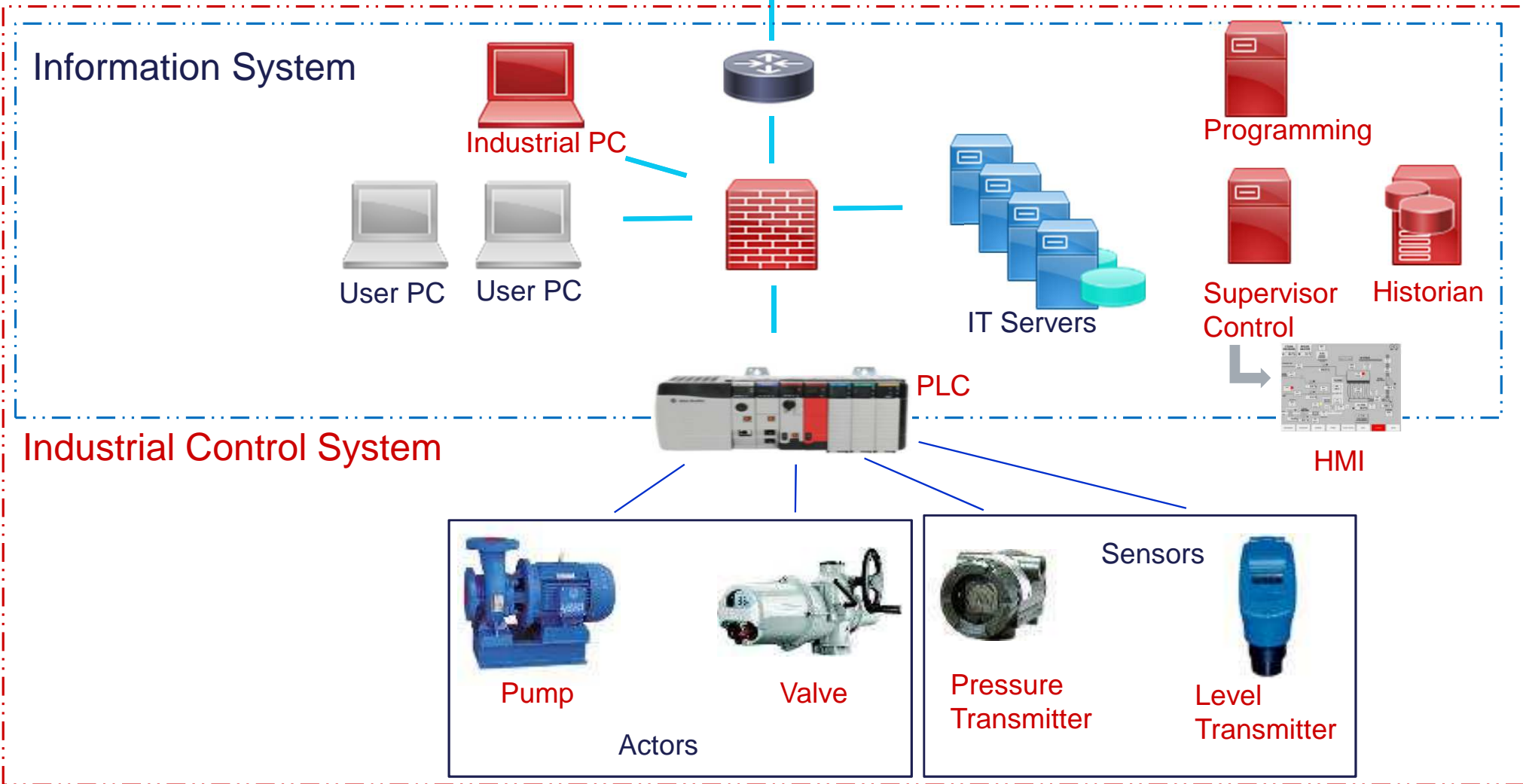


In theory



ICS Architecture : The reality !
Example 1 – Water industry

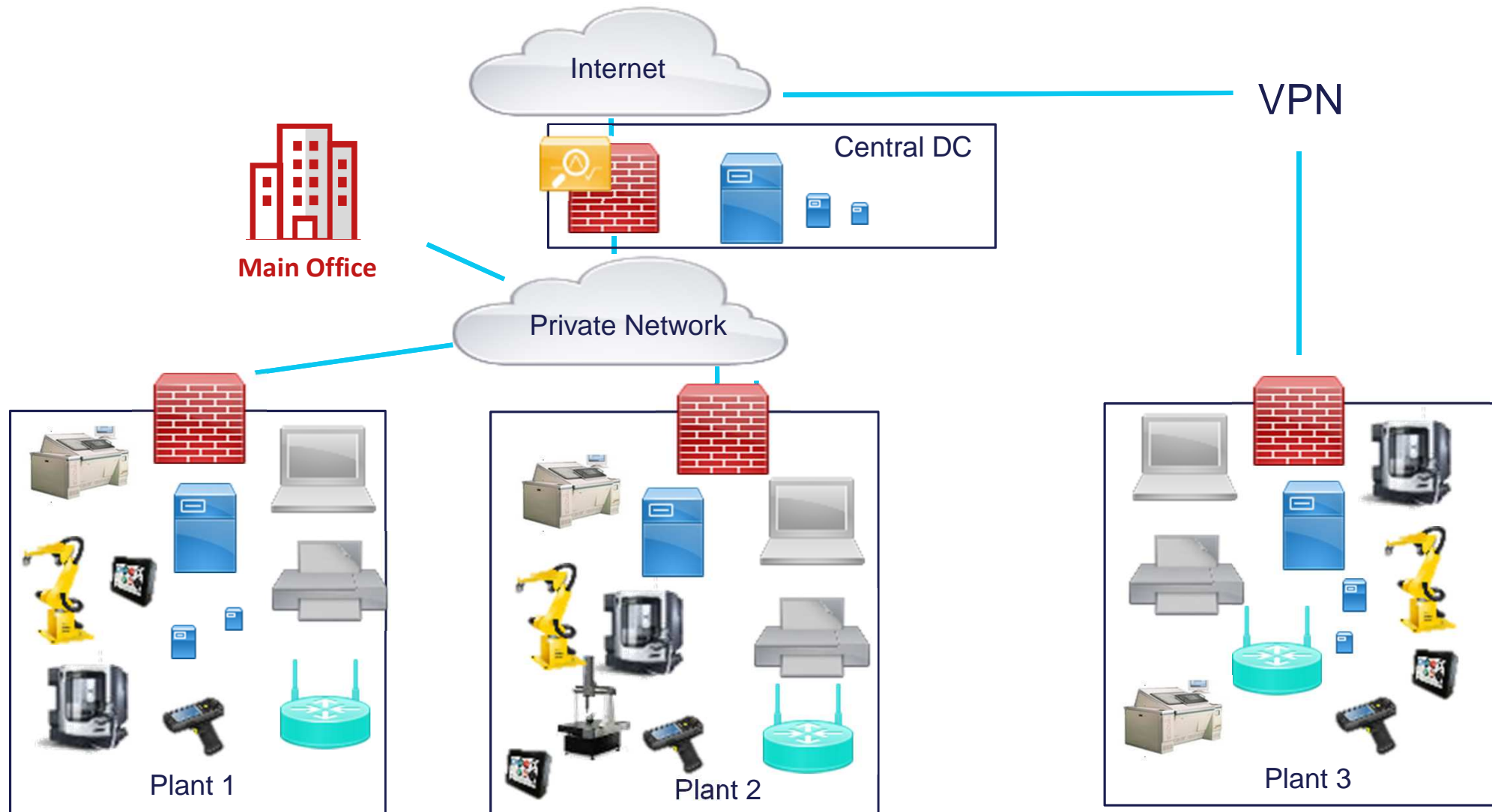
Public IP



IT
VS
OT

ICS Architecture : The reality !

Example 2 - Manufacturing

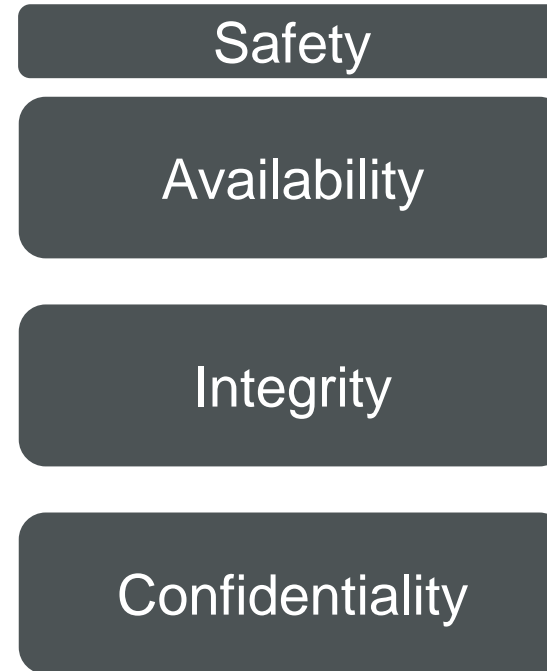


IT vs OT



IT

OT

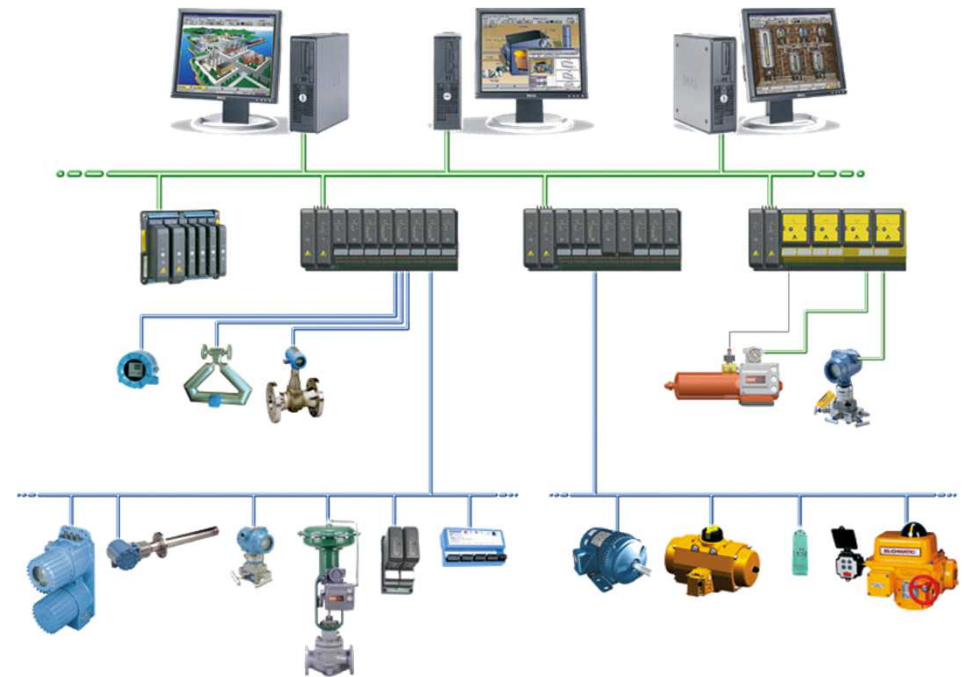


IT vs OT



How do you use
cybersecurity to
secure the
physical world?

How do you secure
system that *don't*
run IPv4 or Windows
or Linux or have a
display?



How do you secure a system that was
designed 10 years ago, *not to be*
patched or upgraded?

Attackers



Nation States



Insiders



Terrorists



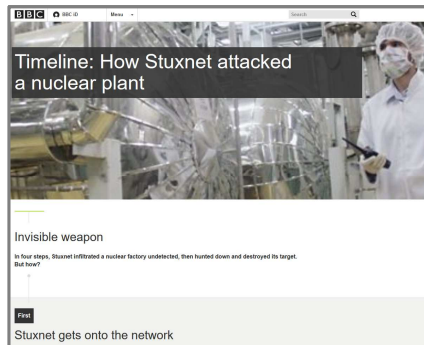
Hacktivists



Cyber Criminals



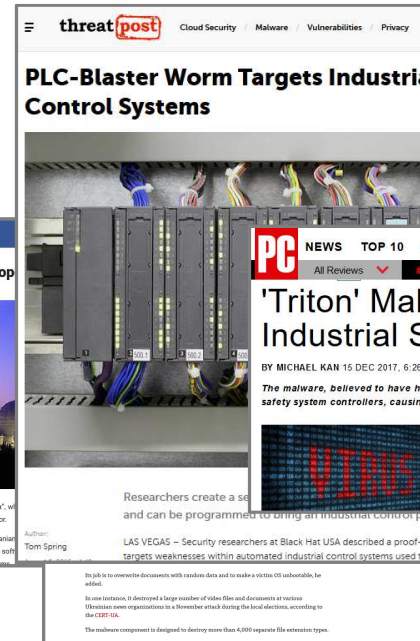
ICS Malware Timeline



Stuxnet



**Havex/Dragonfly/
Energetic Bear**



BlackEnergy 2



BlackEnergy 3

PLC-Blaster

**Crash Override/
Industroyer**

**Triton/Trisis/
HatMan**



Cyber Attacks Cost



The Register
Rising the hand that feeds IT

Security

NotPetya ransomware attack cost us \$300m – shipping giant Maersk

IT crippled so badly firm relied on WhatsApp

By

FOOD PROCESSING

The Information Source for Food and Beverage Manufacturers

MENU

Home / Articles / 2017 / Malware May Have Cost Mondelez \$100 Million

Malware May Have Cost Mondelez \$100 Million

A June 27 ransomware attack crippled the top food company, especially business units.

Nov 06, 2017

Print Email

A June 27 global malware incident may have impacted Mondelez International's \$100 million.

In its third quarter financial report, released Oct. 30, the global snack company reported a computer outage across its global operations. "Given the timing of this significant global attack, despite our best efforts, we experienced disruption in our ability to ship and invoice during the last four days of our second quarter where we have permanently lost some of that revenue due to holiday fees. We expect we will be able to recognize the majority of these delayed shipments in our third quarter."

At the time of the ransomware attack, Mondelez reported a computer outage across its global operations. "Given the timing of this significant global attack, despite our best efforts, we experienced disruption in our ability to ship and invoice during the last four days of our second quarter where we have permanently lost some of that revenue due to holiday fees. We expect we will be able to recognize the majority of these delayed shipments in our third quarter."

Back to the third quarter report: "The malware affected a significant portion of the distribution and financial networks... the company executed business continuity and containment plans to contain the impact and minimize the damages and restore its systems environment."

The cyber attack has been called alternately a variant of Petya, a known ransomware that Kaspersky Lab dubbed ExPetr. Reports say the bug locks a computer and then demands a \$300 ransom to be paid in Bitcoins.

TechRepublic

SECURITY

NotPetya ransomware outbreak cost \$300M per quarter

The massive ransomware bill faced by Merck and other enterprises like Maersk and FedEx.

ZDNet

NotPetya cyber attack on TNT Express cost FedEx \$300m

Falling victim to global ransomware attack 'posed significant operational challenges', the company says in its latest financial report.

By Danny Palmer | September 20, 2017 -- 16:12 GMT (02:12 AEST) | Topic: Security

Norsk Hydro ransomware incident losses reach \$40 million after one week

Norsk Hydro up and running with the exception of one business unit where 'operations remain almost at a standstill'

By Catalin Cimpanu for Zero Day | March 28, 2019 -- 21:43 GMT (14:33 GMT) | Topic: Security

Voici HPE Primera.
Un stockage 100% disponible, repensé.

Voici HPE Primera.
Un stockage 100% disponible, repensé.

MORE FROM CATALIN CIMPANU

- Security: Linux to get kernel 'lockdown' feature
- Open Source: Pi-hole drops support for ad blockers used by browser-based ads

BUSINESS INSIDER

TECH | FINANCE | POLITICS | STRATEGY | LIFE | ALL

Ukraine power company says hit by second cyber attack Thursday

Reuters Jun. 30, 2017, 3:05 AM 4/3

KIEV (Reuters) - Ukrainian state power distributor Ukrenergo was hit by another cyber attack on Thursday which used a computer virus different from one that hit Ukraine on Tuesday, said Ukrenergo's acting head said.

The second attack did not affect Ukraine's power network, Vsevolod Kovalchuk told a news briefing on Friday.

"The virus was slightly different, of a different nature, similar to WannaCry," he said. "The effect from it was insignificant, as some computers remained offline."

Dispatcher shows diagram of power lines inside control room of Ukraine's National power company Ukrenergo in Kiev

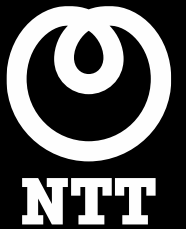
Thomson Reuters

ICS Vulnerabilities



Theme	Details
Policy & Procedure	<ul style="list-style-type: none">• No formal ICS security training and awareness program• Lack of access control policy• Lack of authentication policy• Inadequate incident detection and response plan and procedures
Architecture and Design	<ul style="list-style-type: none">• No visibility• No Security Perimeters defined• No segregation between IT and OT
Threat Detection	<ul style="list-style-type: none">• Intrusion and detection / prevention not installed
Maintenance	<ul style="list-style-type: none">• Poor remote access controls• Lack of OS and Application

IEC 62443



Compliance for OT Networks



	Information System	General-Purpose Control System		Petroleum/ Chemical Plant	Electrical Power System	Smart Grid	Railway System	
Organisation	ISO/IEC 27001 (ISMS)	NIST Cyber Security Framework	IEC 62443		IAEA Nuclear Security Recommendations Rev.5	NERC CIP	NISTIR 7628	ISO/IEC 62278 (RAMS)
System			ISASecure Certification (SSA)	WIB Certification		IEC 61850		IEC 62280
Device/ Component			Achilles Certification (EDSA)			IEEE 1686		
Specific Technologies (encryption, etc)		ISO/IEC 29192			IEC 62351		IEEE 2030	

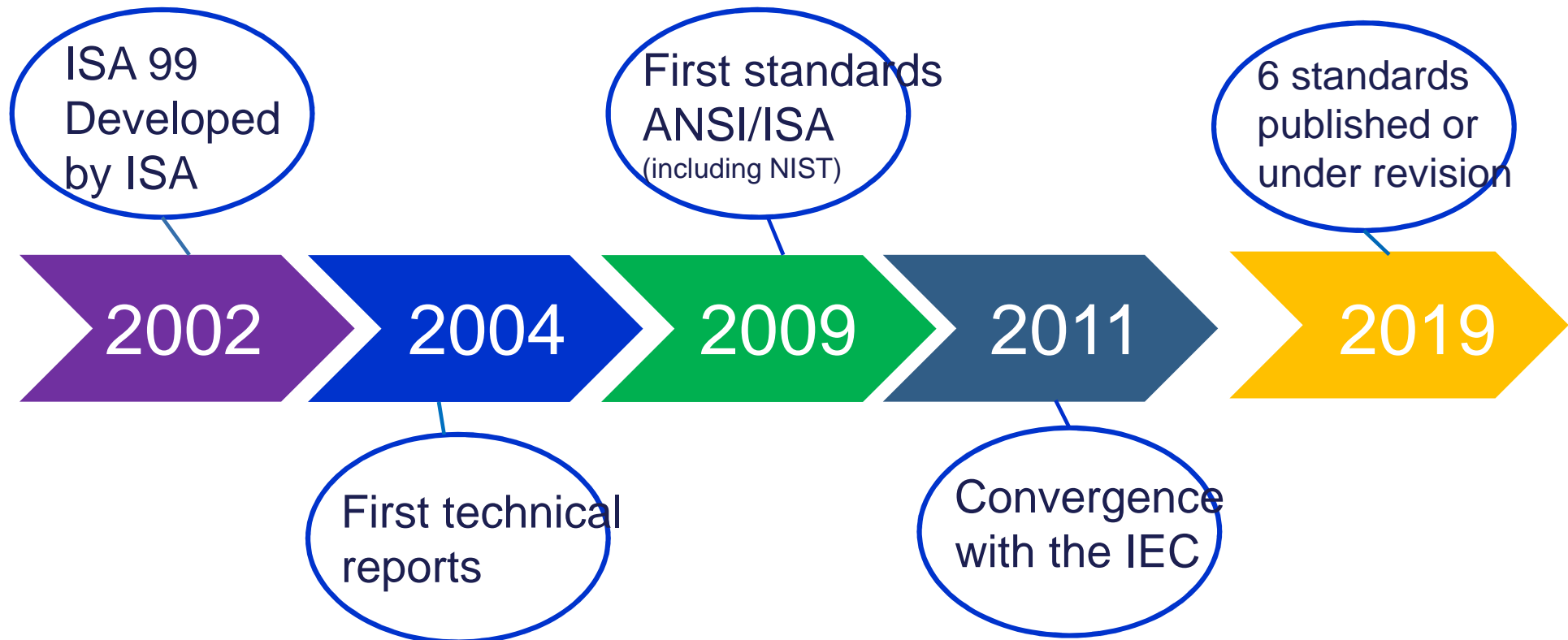
International Standard

Industry Guideline

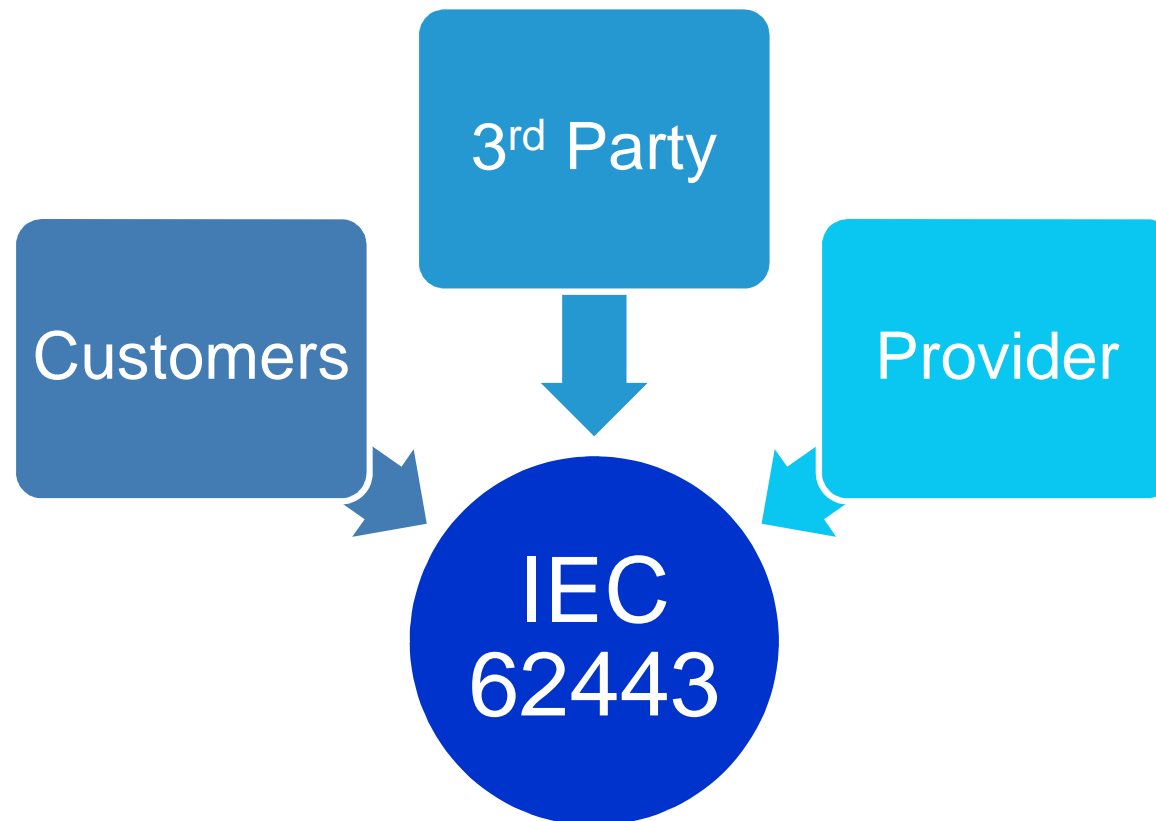
IEC 62443



- ✓ Series of standards initially developed by ISA (International Standards of Auditing), later utilized by IEC (International Electro technical Commission)
- ✓ The ISA99 standards development committee brings together industrial cyber security experts from across the globe to develop ISA standards.



Who are the stakeholders targeted?



Overview ISA/IEC 62443 Series



ISA-99 / IEC 62443 covers requirements on processes / procedures as well as functional requirements

IEC 62443 / ISA-99			
General	Policies and procedures	System	Component
1-1 Terminology, concepts and models	2-1 Establishing an IACS security program	3-1 Security technologies for IACS	4-1 Product development requirements
1-2 Master glossary of terms and abbreviations	2-2 Operating an IACS security program	3-2 Security assurance levels for zones and conduits	4-2 Technical security requirements for IACS products
1-3 System security compliance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security assurance levels	
	2-4 Certification of IACS supplier security policies and practices		
Definitions Metrics	Requirements to the security organization and processes of the plant owner and suppliers	Requirements to a secure system	Requirements to secure system components
		Functional requirements	Processes / procedures

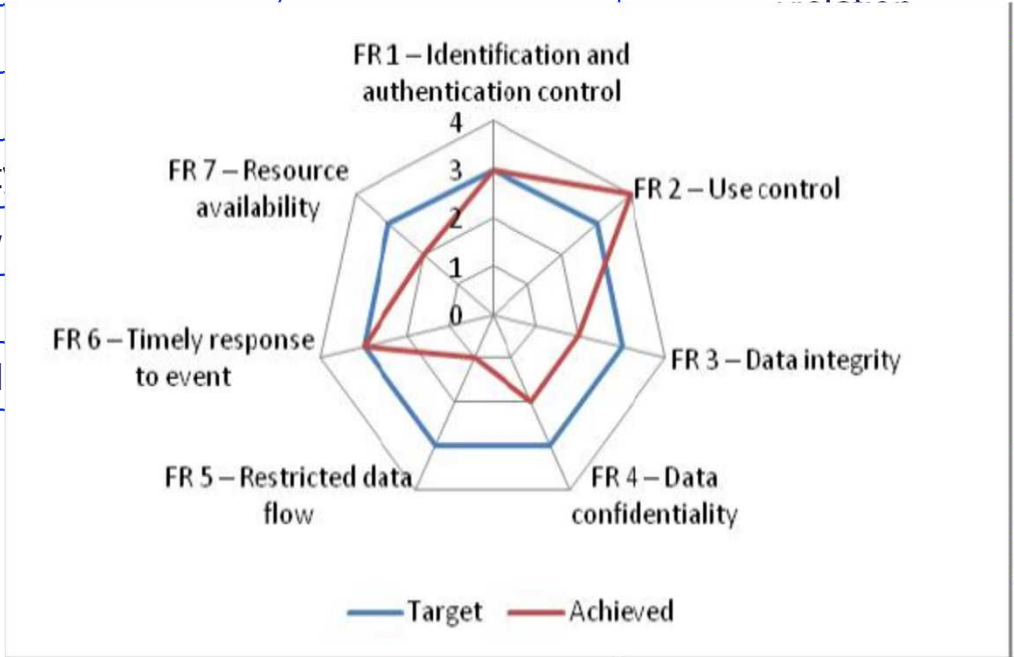
62443-3-3: System Security Requirements and Security Levels



Foundational Requirements		
FR1	AC	Identification, Authentication and Access Control
FR2	UC	Use Control
FR3	DI	Data Integrity
FR4	DC	Data Confidentiality
FR5	RDF	Restrict Data Flow
FR6	TRE	Time Response to
FR7	RA	Resource Availabil



Security Level	
SL-0	No specific security protection necessary
SL-1	Protection against casual or coincidental violation
	Protection against international violation means with low resources, and low motivation
	Protection against international violation means with moderate CS specific skills and vation
	Protection against international violation means with extended CS specific skills and high

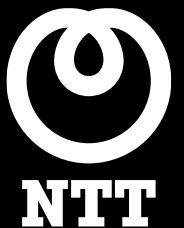


ISA/IEC 62443-3-2: Security Risk Assessment, System Partitioning and Security Levels



- 1 Identify System Under Consideration (SuC)
- 2 High-Level Cyber Security Risk Assessment
- 3 Partition the SuC in zone
- 4 Detailed Risk Assessment by zone
- 5 Define security measures

Secure Water Production and Distribution



NTT's Approach

Based on IEC
62443-3-2

SuC identification

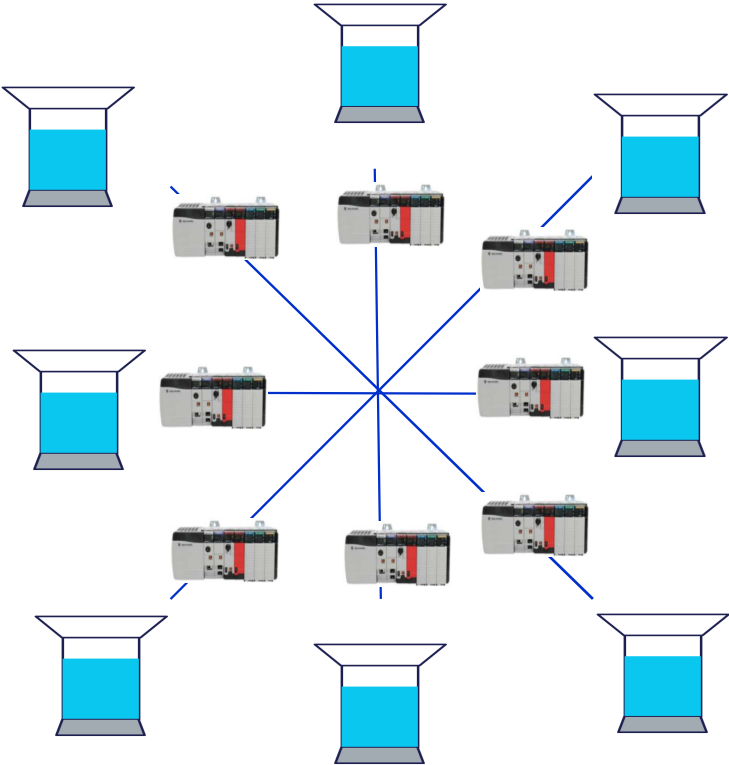
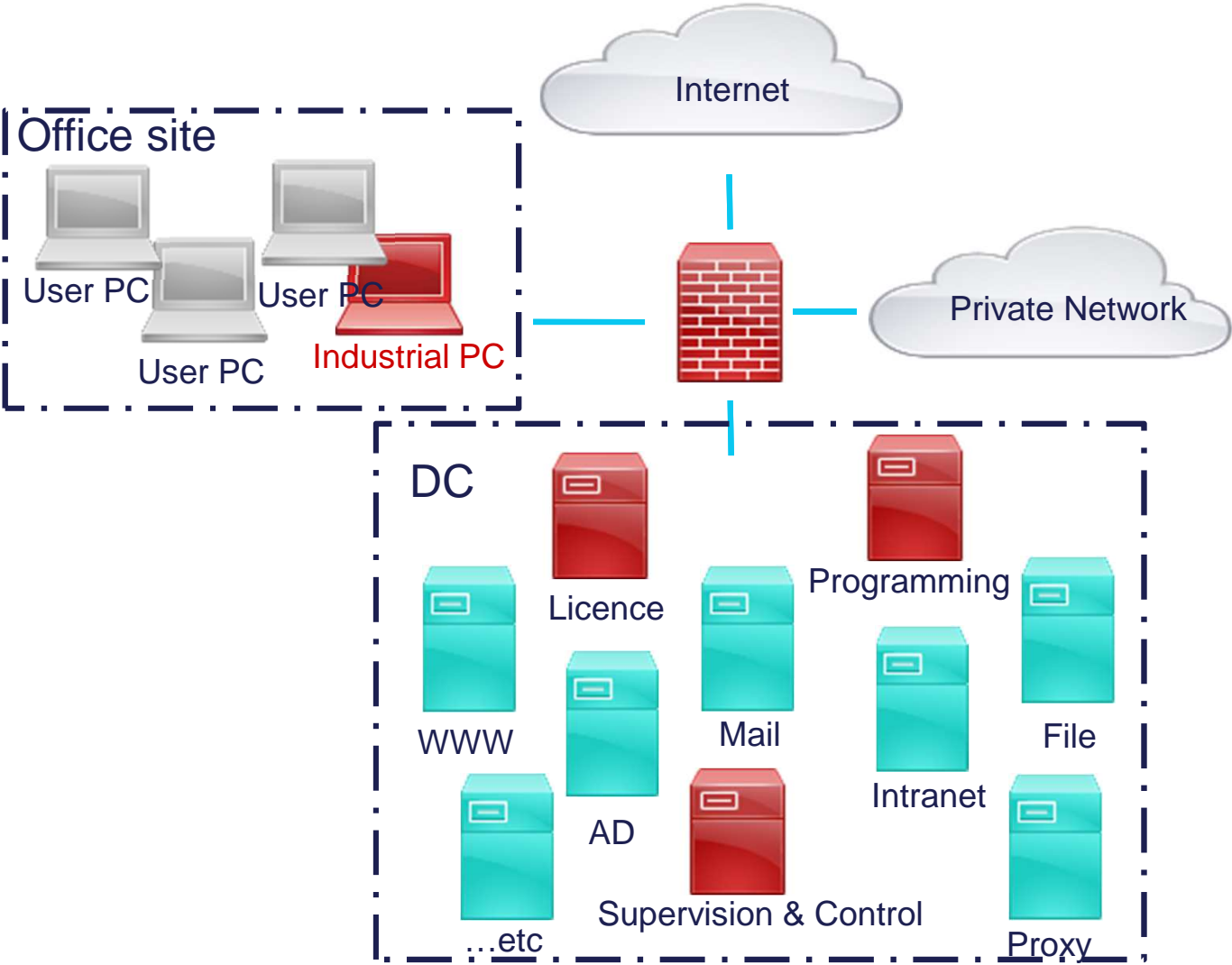
High level Risk
Assessment

Suc Partitionning

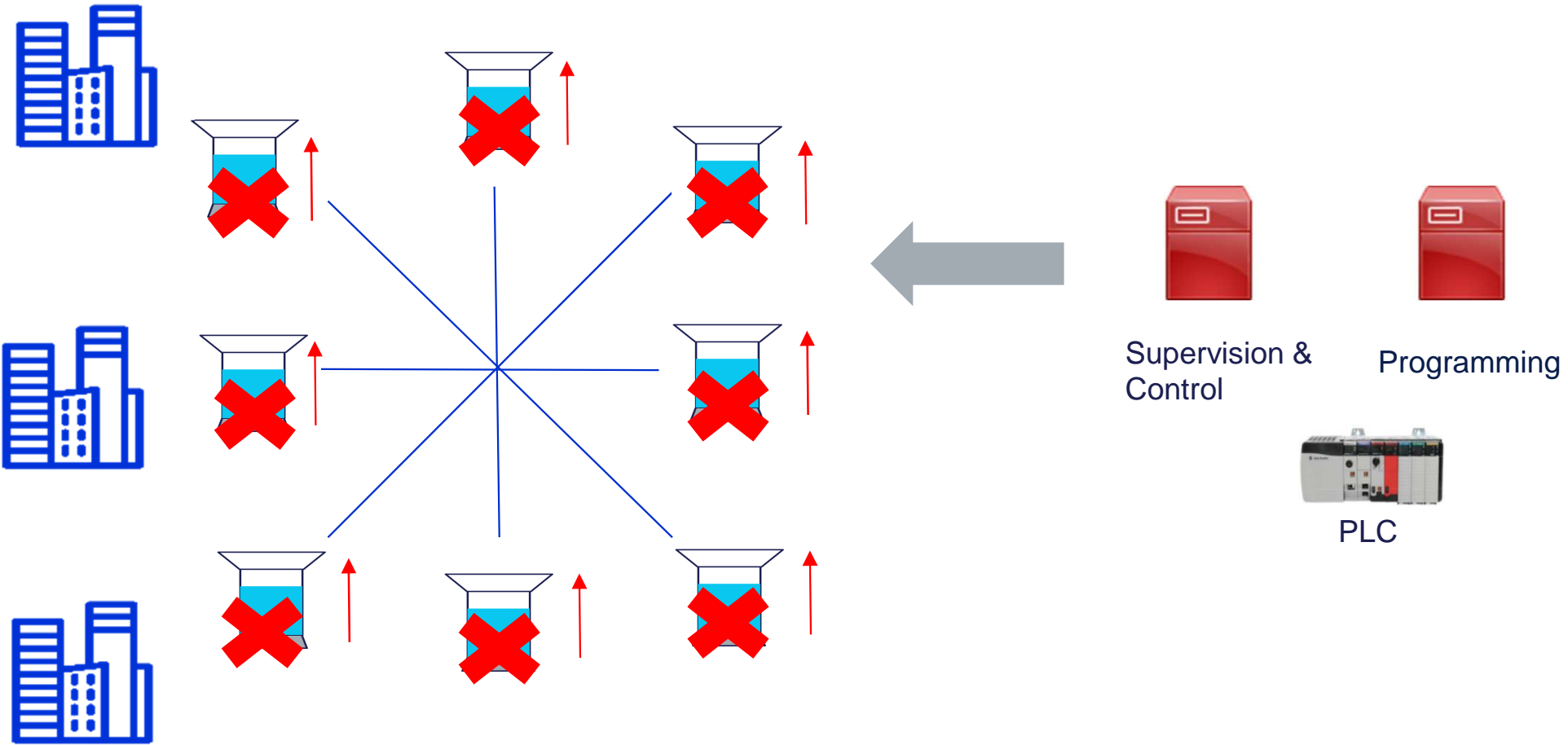
**Security
Measures**

Detailed Risk Assessment

STEP 1 : Identify system under consideration (SuC)



STEP 2 : High Level Risk Assessment



STEP 2 : High Level Risk Assessment

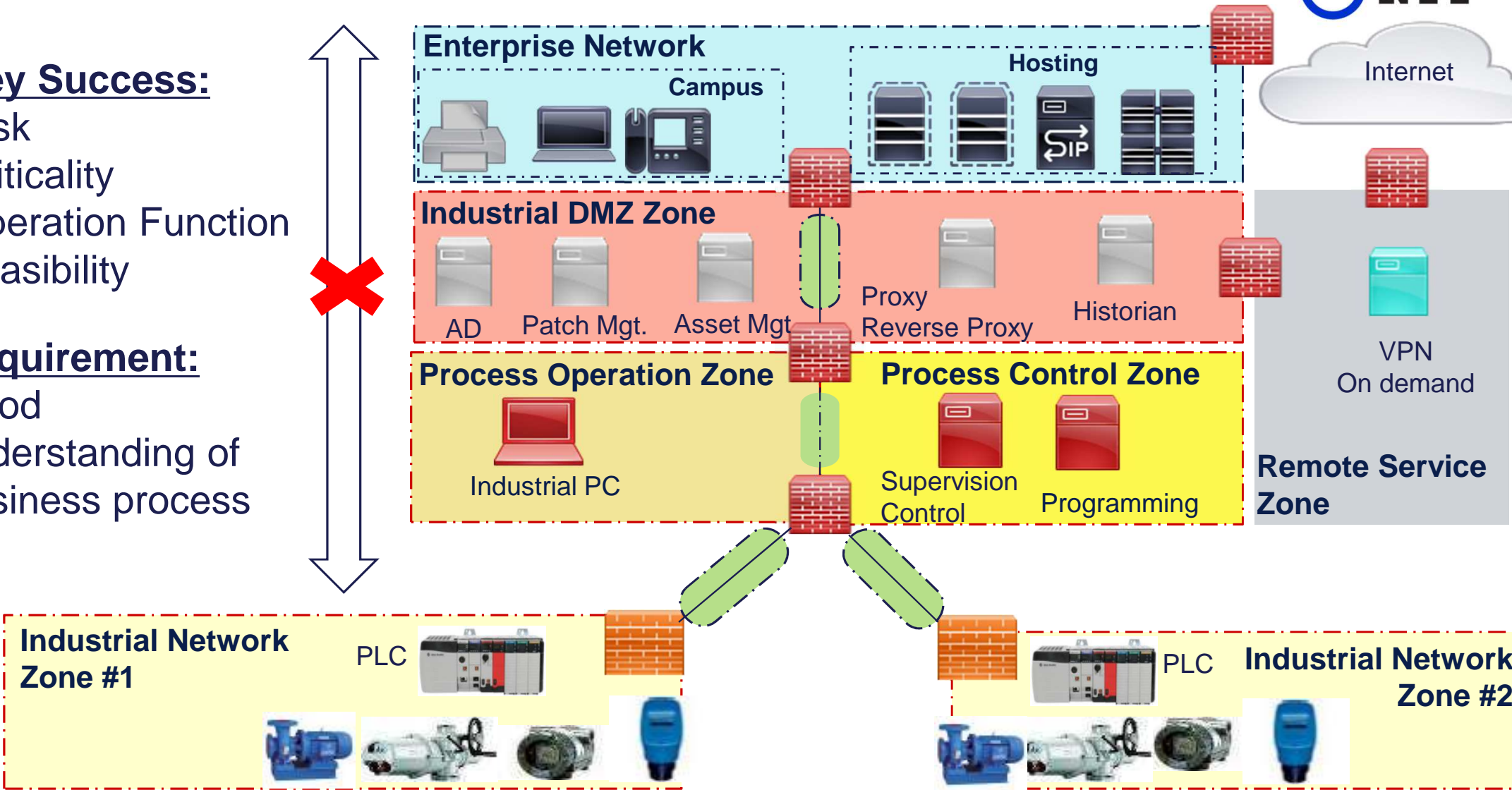
Measuring the impact of a risk scenario on the company

	Impacts subscale				
Impact Rating	Reputation	Operational	Legal	Financial	Human
0 Minor	Impact on the organisation reputation can be scaled from an isolated criticism by the mass media to a permanent deterioration of its image	Operational impact can be scaled based on the number of sites impacted , the production interruption duration .	The legal impact is scaled according to the severity of the legal consequences : from isolated prosecutions to various convictions/penalties	The financial impact is estimated on a scale based on percentages of the Company annual revenue	The human impact is estimated on a scale based on percentages of people harmed by the event
1 Low					
2 Moderate					
3 Severe					
4 Critical					

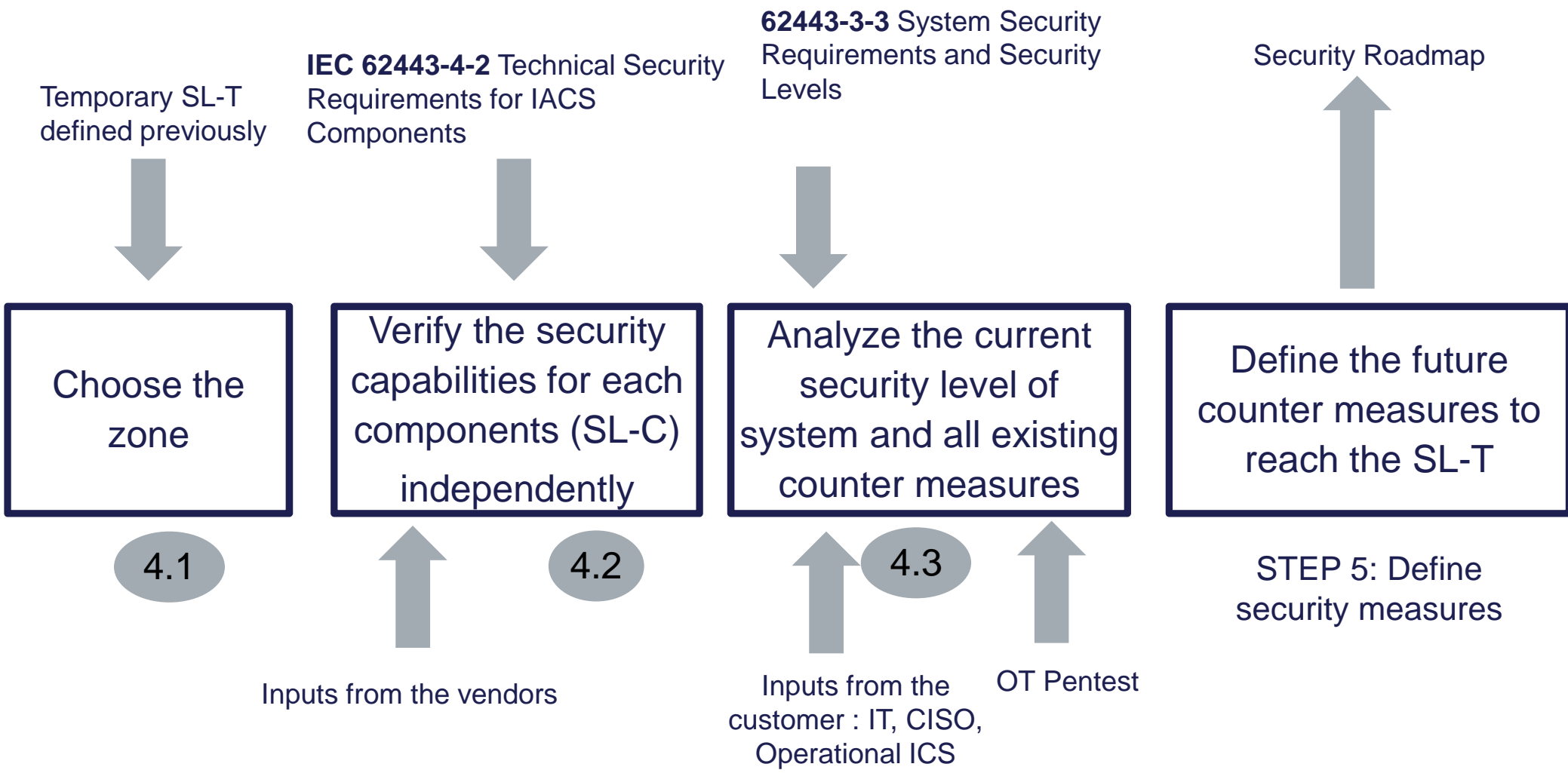
STEP 3: Partition the SuC in zone concept

Key Success:
Risk
Criticality
Operation Function
Feasibility

Requirement:
Good
understanding of
business process



STEP 4: Detailed Risk Assessment by zone



STEP 4: Detailed Risk Assessment by zone

Example



Step 4.1: Verify the security capabilities of each component before installation



- Interview with the vendors
- Analyze Technical document

IEC 62443-4-2 Technical Security Requirements for IACS Components

Step 4.2: Analyze the security level of the current system and all current counter measures



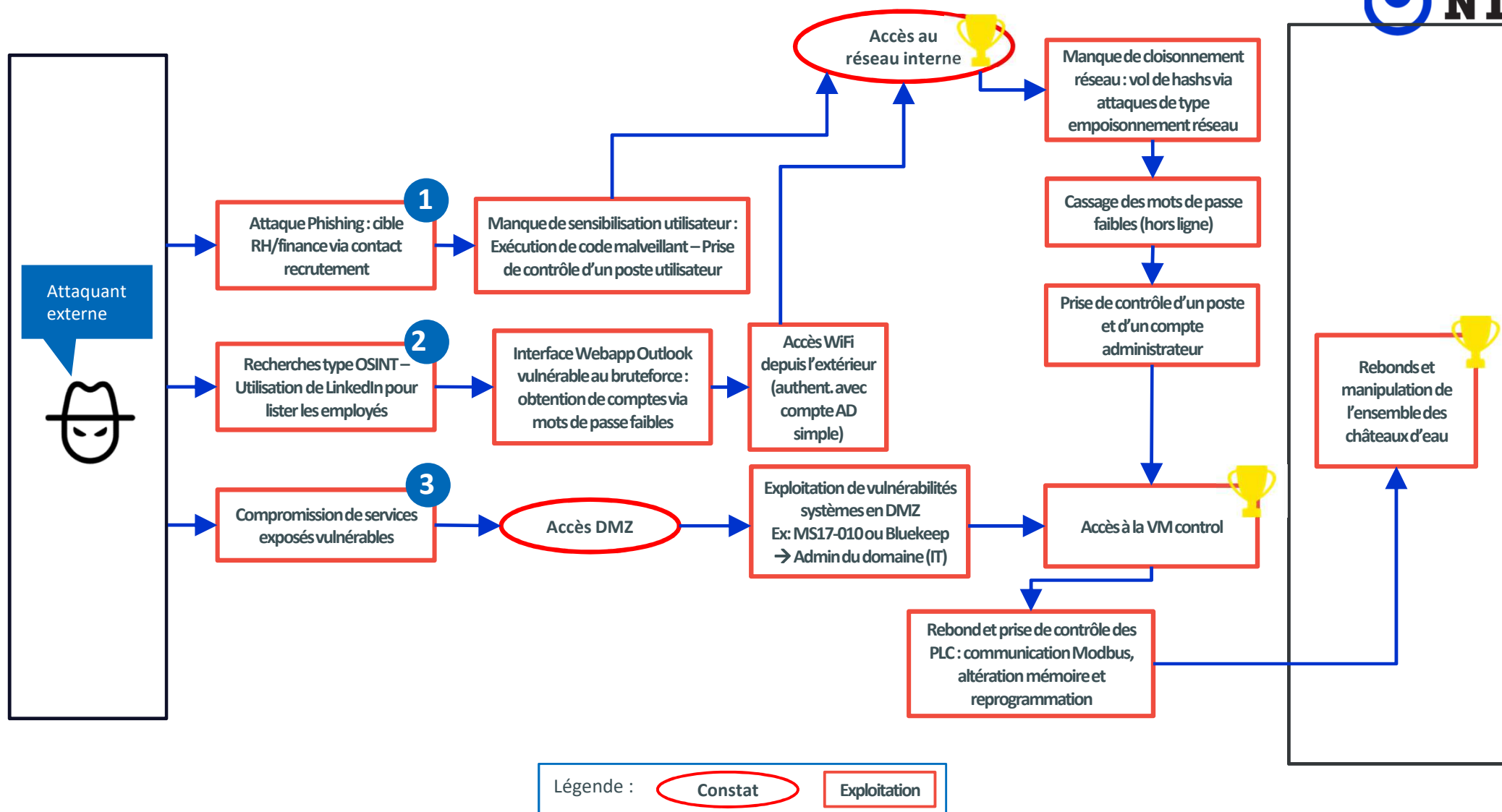
- OT Pentest
- Interview with the integrator
- Interview IT Team

62443-3-3 System Security Requirements and Security Levels

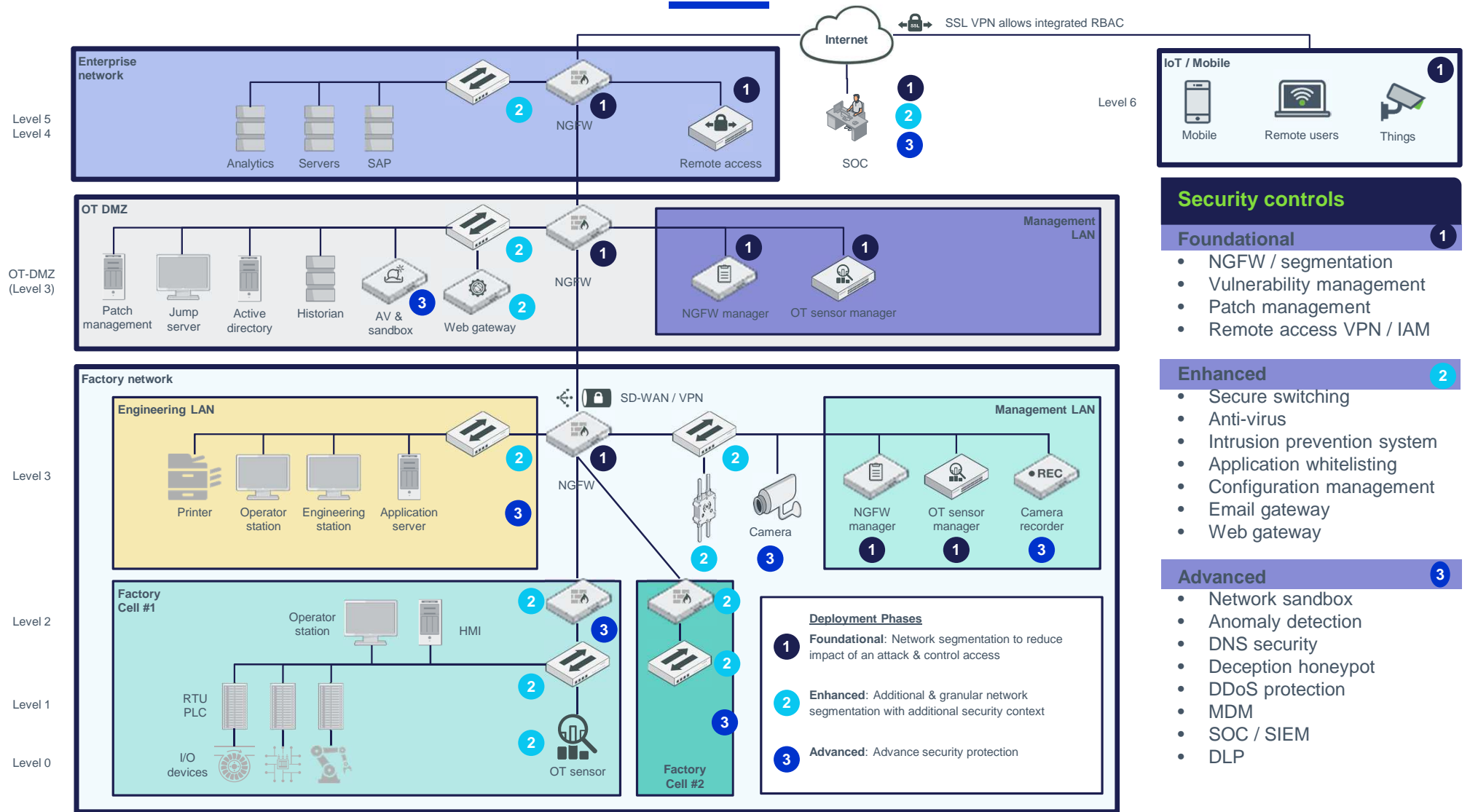
Step 4.3: Identify all vulnerabilities and the target security level

Define all counter measure to reach the target security level and correct all vulnerabilities

STEP 4.2: Attack scenarios during OT Pentest



STEP 5: Define security measures



STEP 5: Define security measures (not exhaustive)

Technical Measures

OT/IT Segregation
OT Segmentation

Visibility
OT Threat Detection

Identity and Access
Management

SOC

Organizational Measures

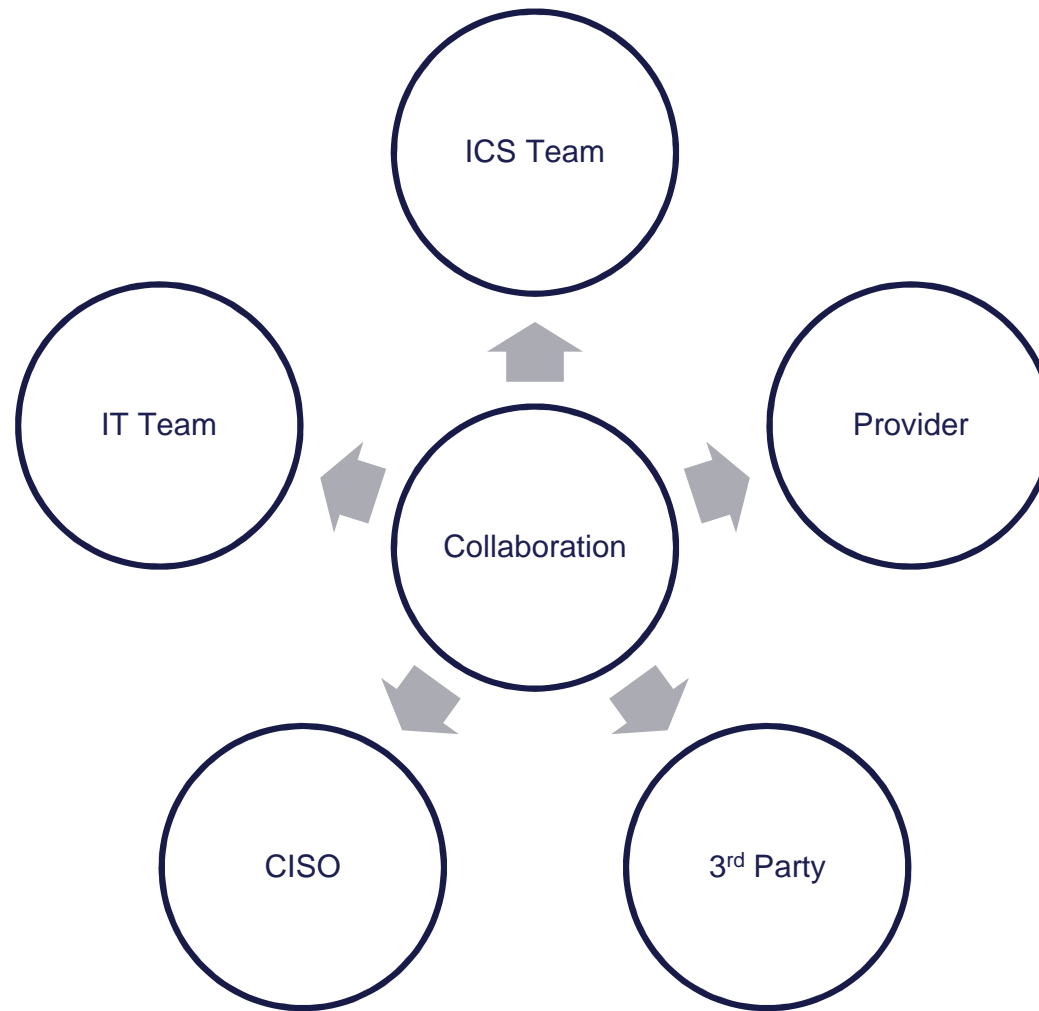
Business Description
(Operation process,
Criticality..)

Asset Management

Policies and
Procedures

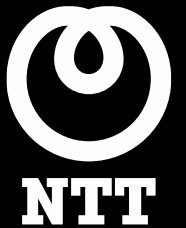
Risk Management

Success Key for ICS Security



Thank you!

Mezri SAHTOUT
Practice Leader OT/IoT Security



Q&A

