

Campari Group Case Study: Applying ISA/IEC 62443 to Operating Sites

Stefano Micci

Global IT Cyber Security Manager Governance, Risk and Compliance Campari Group

Massimiliano Latini

Technical Director H-ON a TÜV Rheinland Company

About Authors

Stefano Micci Global IT Cyber Security Manager Governance, Risk and Compliance **Campari Group**

Management Engineer with more of 10 years of experience in technology risk gained in a multinational management consulting firm and now globally focused in Cyber Security Governance, Risk and Compliance topics for Campari Group.



camparigroup.com



Campari Group



**CAMPARI
GROUP**

Massimiliano Latini Technical Director **H-ON a TÜV Rheinland Company**

Also, Cyber Security Manager at BYHON - Mechanical Engineer with more than 20 years of experience in the safety and cybersecurity of industrial automation, ISA/IEC 62443 Cybersecurity Expert certified.



h-on.it | byhon.it

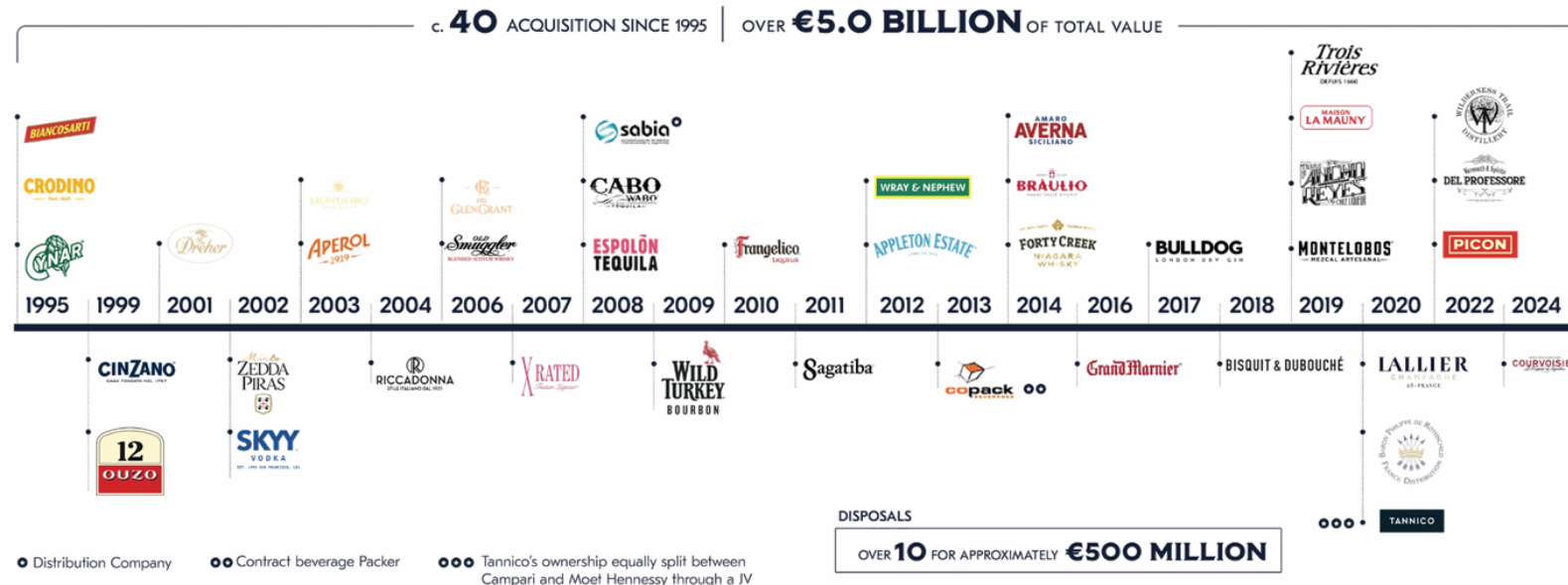


H-ON a TÜV Rheinland Company



H-ON

- **Campari Group** today is a **major player in the global branded spirits industry**, with a portfolio of over **50 premium and super premium brands**, marketed and distributed in over **190 markets around the world**, with leading positions in Europe and the Americas.
- The Group employs around **4,900 people** and has an **extensive portfolio** of premium and super premium brands, spreading across **Global, Regional and Local priorities**.
- Shares of the parent company Davide Campari - Milano N.V. are listed on the Italian Stock Exchange since 2001.
- Campari Group is today the sixth-largest player worldwide in the premium spirits industry.



Cyber Security in Campari Group

- The Cyber Security function resides within the IT department with the below mission:



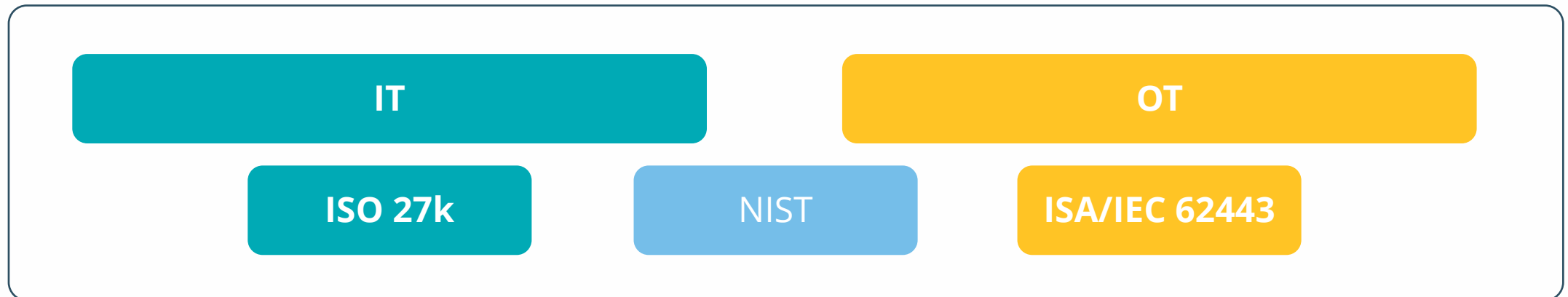
ENSURE THE SECURITY (& CONTINUITY) OF VALUE CREATION



- Key capabilities that under the responsibility of the Cyber Security function are:
 - Cyber Security Governance, Risk and Compliance
 - Cyber Security Technological Strategy & Architecture
 - Cyber Security Operation
 - Data Protection
 - Identity Protection
 - Information Technology (IT) Asset protection
 - Operational Technology (OT) protection
- The IT / OT operating model is currently under review in order to improve the management of IT & OT responsibilities among interested parties:
 - Global Supply Chain (GSC) Department & Plants
 - IT Department, involving GCS IT Business partners, IT Operation, IT Architecture and Cyber Security

References for Cyber Security activities

- Although Campari Group does not operate in a regulated sector, it takes internationally recognized standards and best practices as a reference for its Cyber Security program.



- Using these standards and best practices as a reference brings a number of benefits, including:
 - increased credibility/confidence towards third parties
 - increased benchmarking possibilities

Challenges when it comes to our production facilities



SEVERAL PLANTS
ACQUIRED OVER THE
YEARS WITH
HETEROGENEOUS
TECHNOLOGIES



LEGACY PLANT
TECHNOLOGY



LIMITED VISIBILITY OF
ASSETS TO BE SECURED



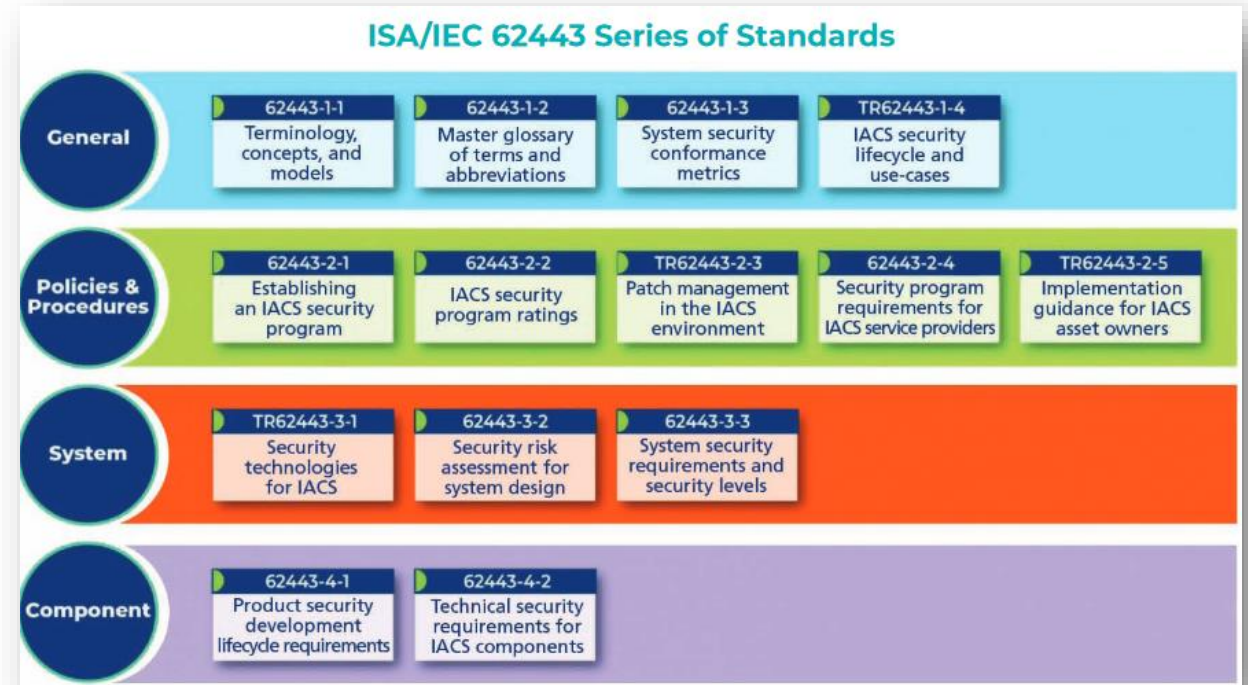
SKILLS SHORTAGE

How they reflect on Cyber Security

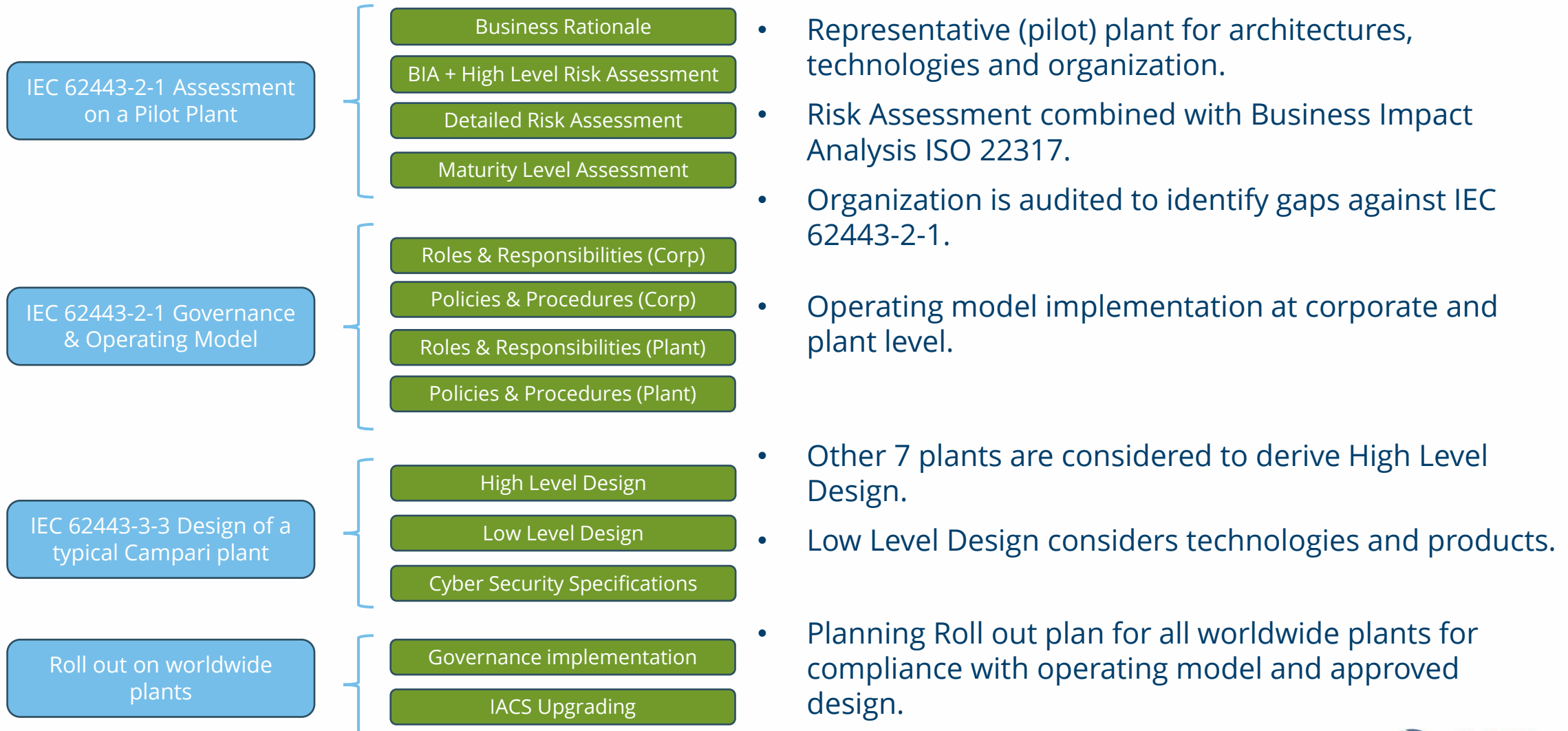
1. Priority is to ensure businesses integration
2. Great reliance on vendors support
3. Grey areas when it comes on interventions in the technologies used in plants
4. Need to cope with production facilities priorities

Why ISA/IEC 62443 for OT

- Worldwide recognized standard for OT Security.
- Somehow referred by critical infrastructure regulations.
- A complete set covering all actors, governance, security and requirements for different device types.



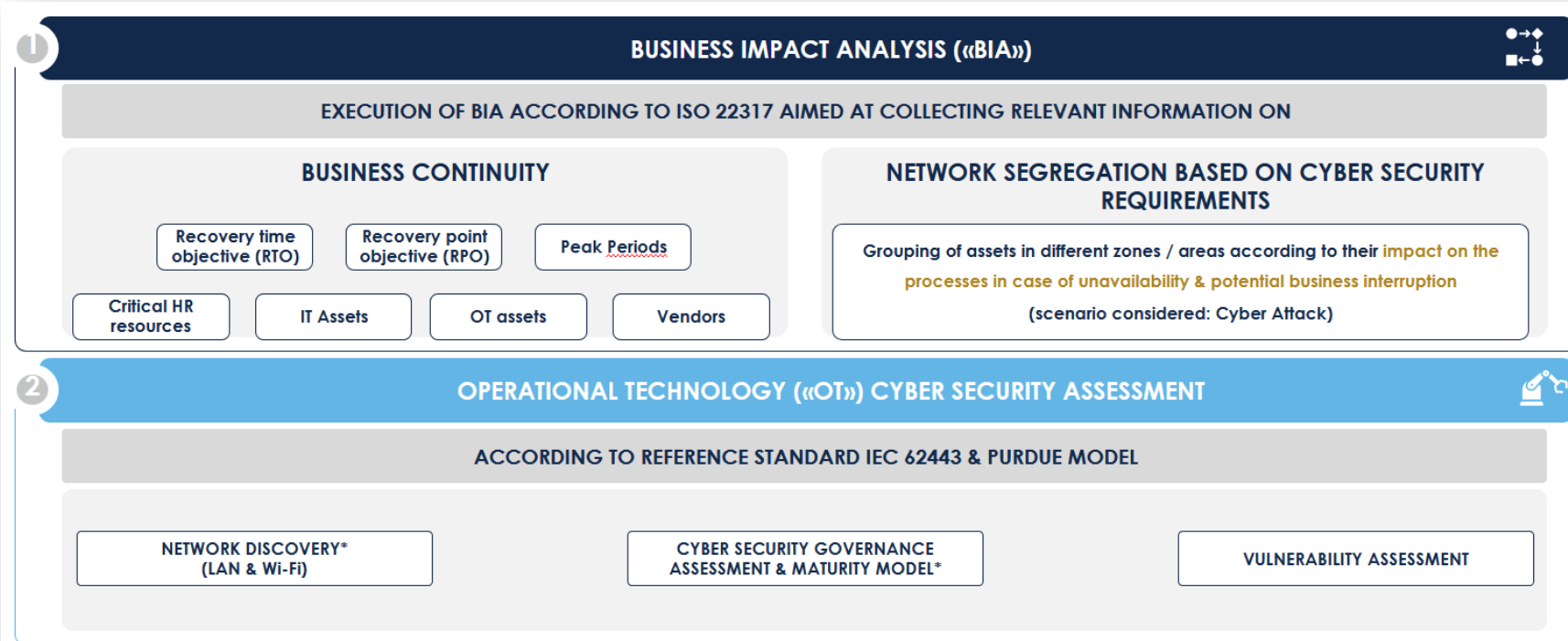
The ISA/IEC 62443 based process



ISA/IEC 62443-3-2 Risk Assessment

Combined method for:

- **Business Impact Analysis** (ISO 22317) and
- **Cyber Security Risk Assessment** (IEC 62443-3-2)



Risk Assessment Method: BR

IMPACT SCALES FOCUS TYPES	SEVERITY				
	1 NEGLECTIBLE	2 MARGINAL	3 RELEVANT	4 VERY RELEVANT	5 CRITICAL
IMPACT LEVEL FOR RTO IDENTIFICATION					
Economic-Financial	Impact < X mlj	Impact between X - Y mlj	Impact between Y - K mlj	Impact between K - Z mlj	Impact > Z mlj
Reputational	<ul style="list-style-type: none"> - Minor local complaint - No change in stakeholders' trust - No impact on reputation 	<ul style="list-style-type: none"> - Local complaint/trade magazine - Minimal change in stakeholders' trust - Impact on reputation less than a month 	<ul style="list-style-type: none"> - Local to national media coverage - Trust diminished - Impact on reputation between 1 & 3 months 	<ul style="list-style-type: none"> - National to international media coverage - Trust never fully recoverable - Serious and lasting impact on reputation 	<ul style="list-style-type: none"> - International Media coverage - Complete loss of trust - Irrecoverable reputation
Compliance	Consequences of ... < X mlj	Consequences of ... between X - Y mlj	Consequences of ... between Y - K mlj	Consequences of ... between K - Z mlj	Consequences of ... > Z mlj
Operational	Operational damage to business processes with deviation in production or service that would result in more than A hours of disruption	Operational damage to business processes with with deviation in production or service that would result in more than B hours of disruption	Operational damage to business processes with with deviation in production or service that would result in more than C hours of disruption	Operational damage to business processes with with deviation in production or service that would result in more than D hours of disruption	Operational damage to business processes with with deviation in production or service that would result in more than E days of disruption
SECURITY LEVEL 15 DAYS IMPACT	0	0	1	2	3

Risk Assessment Method: HLRA

- **HLRA** (inside BIA) assesses operational process vs impact scales after different downtime periods
- **RTO** is derived when impact becomes *Relevant* for any of the impact categories.
- This determines **criticality** of each system and a **ranking** between them in line with IEC 62443-3-2.

			(SUB) PROCESS CRITICALITY																																						
SUBPROCESS NAME	SUBPROCESS DESCRIPTION	SUBPROCESS DEPENDENCIES	LEVEL OF IMPACT IN CASE OF BUSINESS INTERRUPTION OF THE SUBPROCESS																								RTO - RECOVERY TIME OBJECTIVE	RPO - RECOVERY POINT OBJECTIVE													
			[E.G. CYBER ATTACK CAUSING A PRODUCTION STOPPAGE OF 15 DAYS]																																						
			ECONOMIC-FINANCIAL								COMPLIANCE						OPERATIONAL						REPUTATIONAL																		
			0 Days	0.5 Days	1 Days	2 Days	3 Days	4 Days	5 Days	10 Days	15 Days	>15 Days	0 Days	0.5 Days	1 Days	2 Days	3 Days	4 Days	5 Days	10 Days	15 Days	>15 Days	0 Days	0.5 Days	1 Days	2 Days			3 Days	4 Days	5 Days	10 Days	15 Days	>15 Days							
Process 1	Subprocess description	IN: What is needed to be operative before this OUT: Which process will this impact later	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	Marginal	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Negligible	Marginal	Relevant	Very relevant	Very relevant	Critical	Critical	Critical	Critical	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	1 Days	1 Days
Process 2	Subprocess description	IN: What is needed to be operative before this OUT: Which process will this impact later	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	Marginal	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Negligible	Marginal	Relevant	Very relevant	Very relevant	Critical	Critical	Critical	Critical	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	1 Days	1 Days

Risk Assessment Method: HLRA

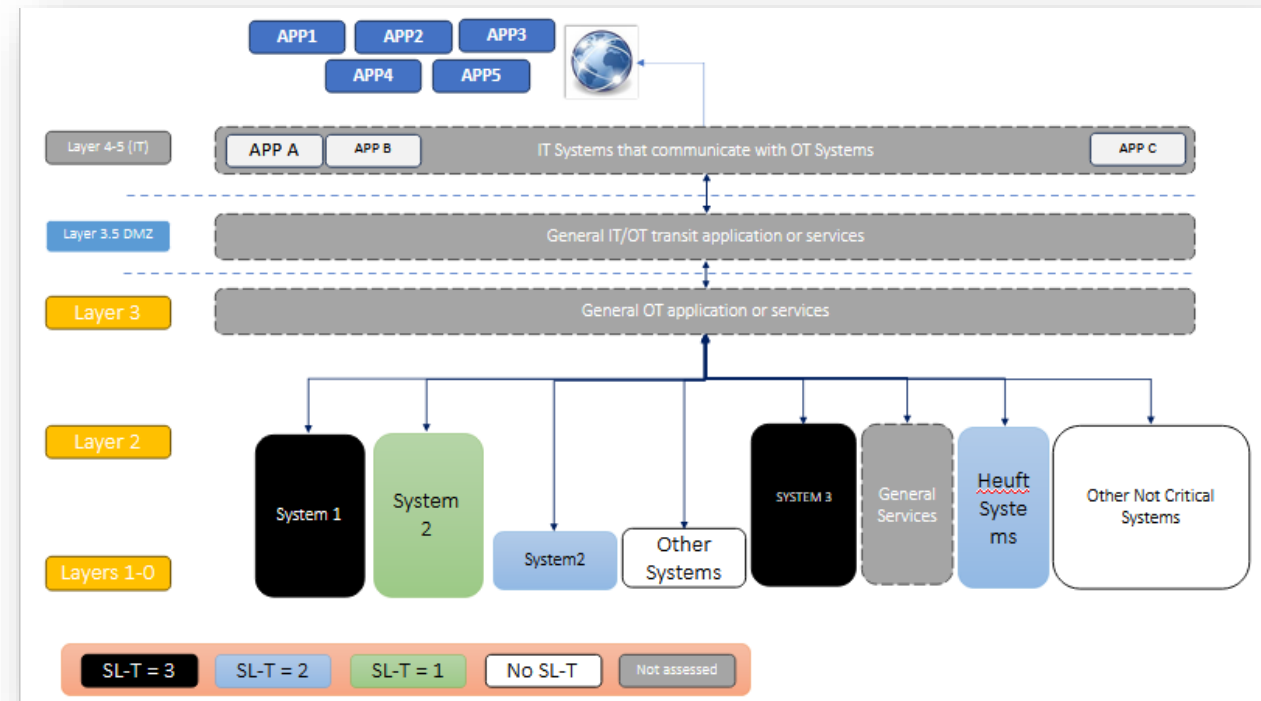
Second step allows to determine:

- **SL-T** for the whole system required for the assessed process.
- Relevant **Assets** that composes the process and related SL-T for each → to be used for **Z&C**
- **Business Continuity Plan** related information → **Asset Priorities**.

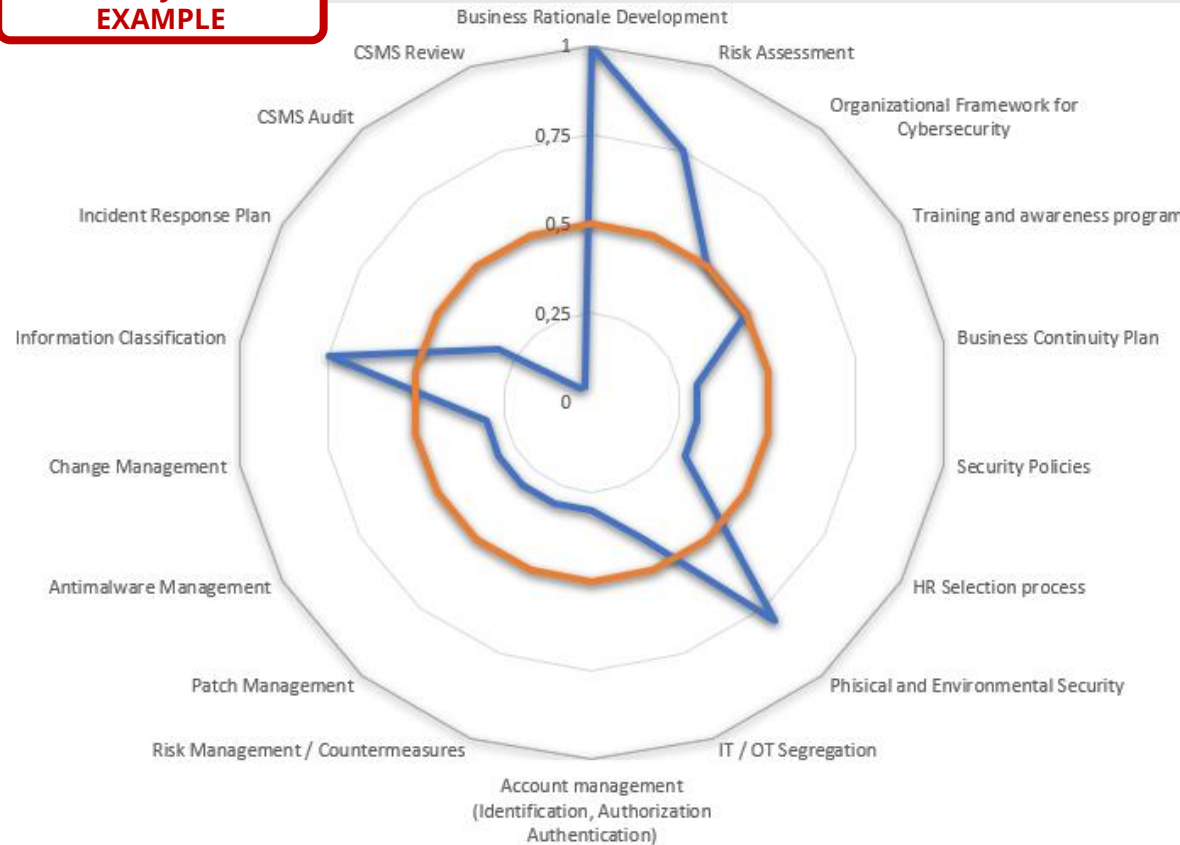
IEC 62443 - CYBER SECURITY ANALYSIS (do not consider purely IT systems)											
SUBPROCESS NAME	TECHNOLOGY	TECHNOLOGY STACK TYPE	TYPE	CRITICALITY OF THE ASSET FOR THE PROPER PROCESS EXECUTION	ZONE SECURITY LEVEL TARGET	MANUAL WORKAROUND AVAILABLE?	WORKAROUND SUSTAINABILITY	RRT (Real Recovery Time)	RESULTING TIME (REAL TIME OF PROCESS UNAVAILABILITY FOLLOWING SYSTEM DOWNTIME)	REAL LEVEL OF IMPACT AS PER IEC 62443	ASSET SECURITY LEVEL TARGET
Process 1	OT Asset 1	OT	SCADA	Critical	3	No	N/A	10 Days	10 Days	Critical	3
Process 1	OT Asset 2	OT	SCADA	Critical	3	Yes	D + 3	1 Days	0 Days	Negligible	0
Process 1	OT Asset 3	IT	App / Web-app	Relevant	1	Yes	D + 5	3 Days	0 Days	Negligible	0
Process 2	OT Asset 1	OT	SCADA	Critical	3	No	N/A	10 Days	10 Days	Critical	3
Process 2	OT Asset 4	OT	PLCs	Critical	3	No	N/A	2 Days	2 Days	Relevant	1
Process 2	OT Asset 5	OT	PLCs	Critical	3	No	N/A	2 Days	2 Days	Relevant	1
Process 2	OT Asset 6	OT	PLCs	Critical	3	Yes	D + 15	1 Days	0 Days	Negligible	0
Process 2	OT Asset 7	OT	PLCs	Critical	3	Yes	D + 3	5 Days	2 Days	Relevant	1
Process 2	OT Asset 3	IT	App / Web-app	Relevant	1	Yes	D + 5	3 Days	0 Days	Negligible	0
Process 2	Asset A	IT	App / Web-app	Critical	3	No	N/A	N/A	N/A	N/A	
Process 2	Asset B	IT	App / Web-app	Critical	3	No	N/A	N/A	N/A	N/A	

Risk Assessment Outcomes

- **Zones & Conduits.**
- **Short terms** actions (for plant resilience, to be tailored with **Detailed Risk Assessment**):
 - ❖ OT/IT and Wifi Segregation
 - ❖ Wifi limitation (in the plant border)
 - ❖ Antimalware or Whitelisting on critical systems
 - ❖ Dedicated patching solution on critical systems
 - ❖ Disaster Recovery procedure on critical systems
- **Long terms** actions / inputs for **HLD**:
 - ❖ Network architecture and segregation based on zones
 - ❖ Antimalware concepts
 - ❖ Hardening policies by device type
 - ❖ Patching solution
 - ❖ Remote access (PMA) solution
 - ❖ Identity management solution (centralized)
 - ❖ Monitoring solution
 - ❖ Backup solution
 - ❖ Communications encryption and protection



Maturity Levels EXAMPLE



- In parallel with HLD, an **operating model** is implemented for governance through a **CSMS** IEC 62443-2-1 compliant.

Short Term:

- ❖ Roles and responsibilities (@corporate and @plant level)
- ❖ Training
- ❖ BC and DR plan guidelines
- ❖ Change Management procedure

Long Term:

- ❖ OT Security Policies
- ❖ OT Security Procedures (IEC 62443-2-1)

ISA/IEC 62443-3-3 High Level Design (HLD)

- A **High-Level Model** is created based on 7 “typical” plants.
- This as a main reference for OT Infrastructure for all Campari plants all over the world and including:
 - ❖ General zones and conduits diagram
 - ❖ Zone and conduit properties definition
 - ❖ Network Segregation concept and main connections routes policies
- High Level Model allows to create the **High-Level Design** covering:
 - ❖ Reference Network Architecture hosting all required services and internal/external communication routes
 - ❖ Field network architectures for the different expected industrial assets and industrial protocols to be supported for different technologies and processes.
 - ❖ Security Requirements

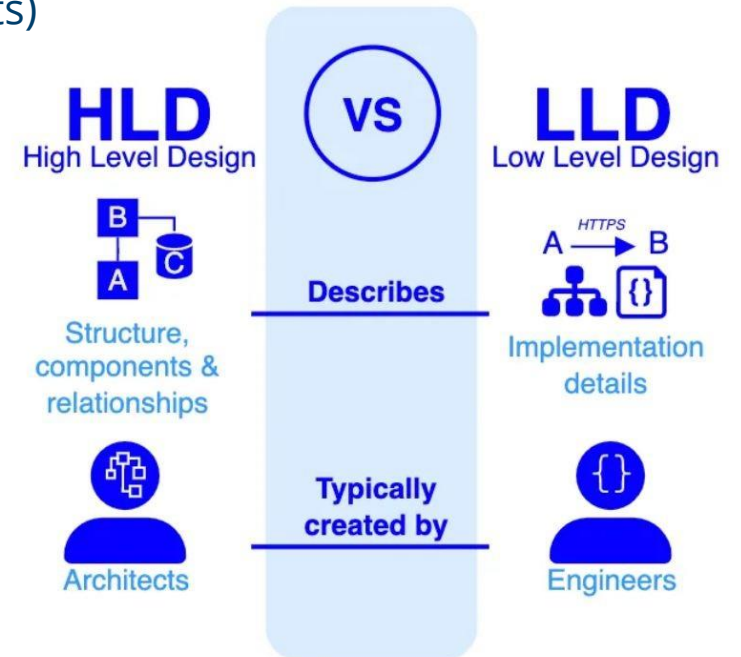
ISA/IEC 62443-3-3 Low Level Design (LLD)

With a defined **High-Level Design**, the next step leads to a more detailed **Low-Level Design** selecting the most appropriated technical solutions:

- Addressing Plan / **IP Subnetting** @corporate and @plant level
- Main **communication routes** and related technologies
- **Network technologies** (at least 2 types) at different plant levels with **criteria for device selection** (based on required performances and security requirements)

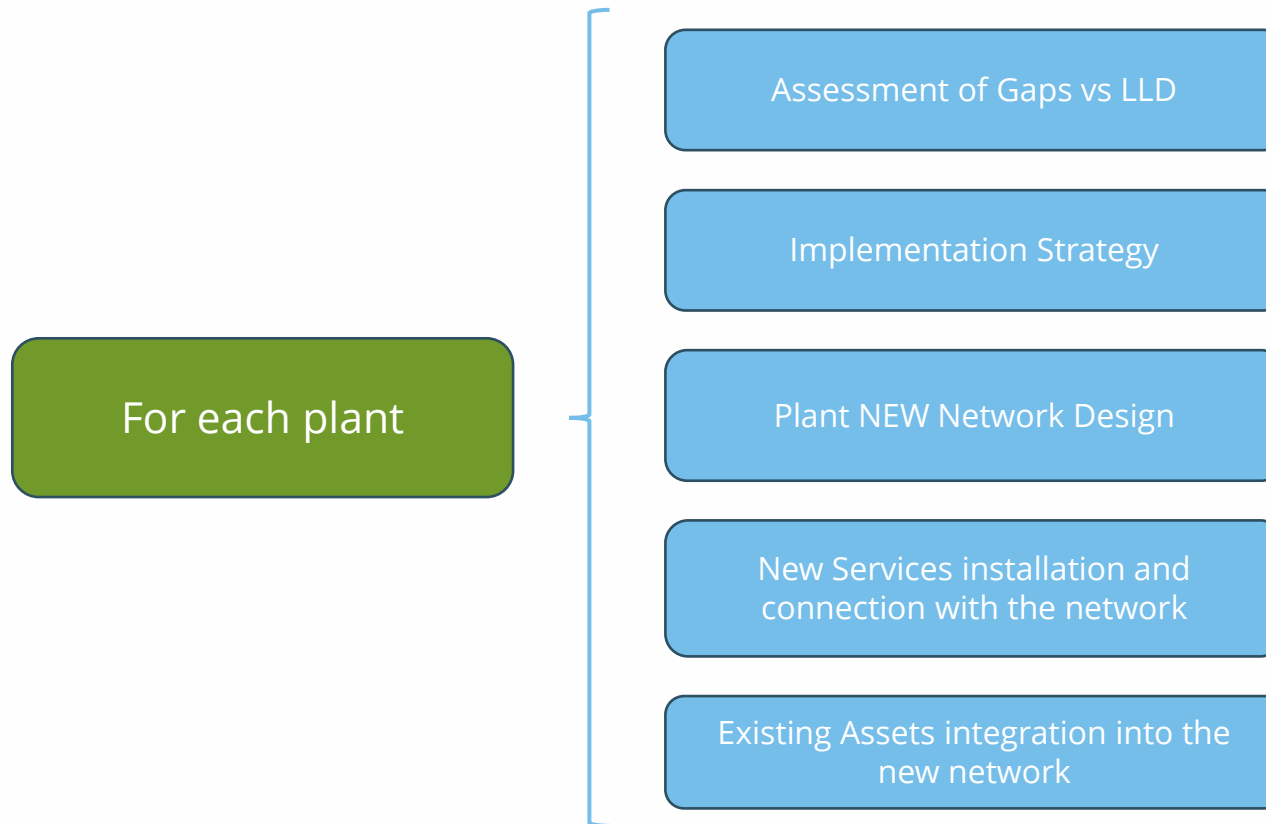
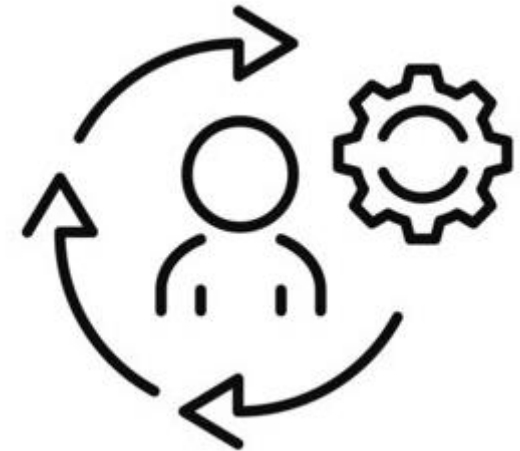
- **Technical solutions** with appropriate **selection criteria** for at least:

- ❖ Centralized Identity Management system
- ❖ Backup Systems
- ❖ Antimalware
- ❖ Remote Access Solution
- ❖ Wireless Connections
- ❖ Patch Management solutions
- ❖ IDS/IPS/Monitoring
- ❖ Logging



Plant Roll Out

The **LLD** is the reference target for all worldwide plant OT infrastructures that according to defined priorities and timing shall be aligned to it.



Conclusions

1. A pilot plant has been selected
2. An IEC 62443 risk assessment has been carried out combined with ISO 22317 methods for BC
3. Risk assessment derived either short-term and long-term measures
4. Short term measures implemented together with business continuity improvement
5. Operating model setup up based on IEC 62443-2-1CSMS
6. A High-Level Design is derived for long term measures
7. High-Level Design leads to a Low-Level Design with selection of technical solutions and design criteria
8. Design solution is rolled out on worldwide plants according to a schedule, depending on gaps

ISASecure – IEC 62443 Conformance Certification

All the ISASecure certification options:

- Component Security Assurance (CSA) - certification to ISA/IEC 62443-4-2
- IIoT Component Security Assurance (ICSA) - certification to ISA/IEC 62443-4-2
- System Security Assurance (SSA) - certification to ISA/IEC 62443-3-3
- Security Development Lifecycle Assurance (SDLA) - certification to ISA/IEC 62443-4-1
- ACS Security Assurance (ACSSA) - certification to ISA/IEC 62443-2-1, 2-4, 3-2 and 3-3



H-ON a TÜV Rheinland Company dba BYHON



Be Part of the Movement to Prioritize OT Cybersecurity

Change the Culture

Recognize cybersecurity as a fundamental workplace tenet alongside functionality, efficiency, and safety

Learn more | www.isagca.org



ISA Cybersecurity Resources

Free guidance, training, and more:

ISA Global Cybersecurity Alliance - www.isagca.org

A collaborative forum to advance OT cybersecurity and understanding of ISA/IEC 62443

ISASecure
www.isasecure.org

The world's leading conformance certification program for ISA/IEC 62443

ICS4ICS
www.ics4ics.org

Improve how cybersecurity incidents are managed with training, processes, and exercises

Get involved:

- ISA/IEC 62443 [standards](#) available from ISA (free access with ISA professional [membership!](#))
- Cybersecurity [training](#) and [certificate program](#)
- Help develop the standard – open to all at no charge – www.isa.org/ISA99