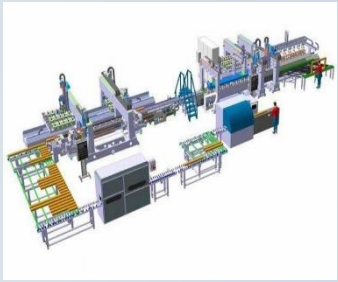
eXcelsior Safety

ISEAClub



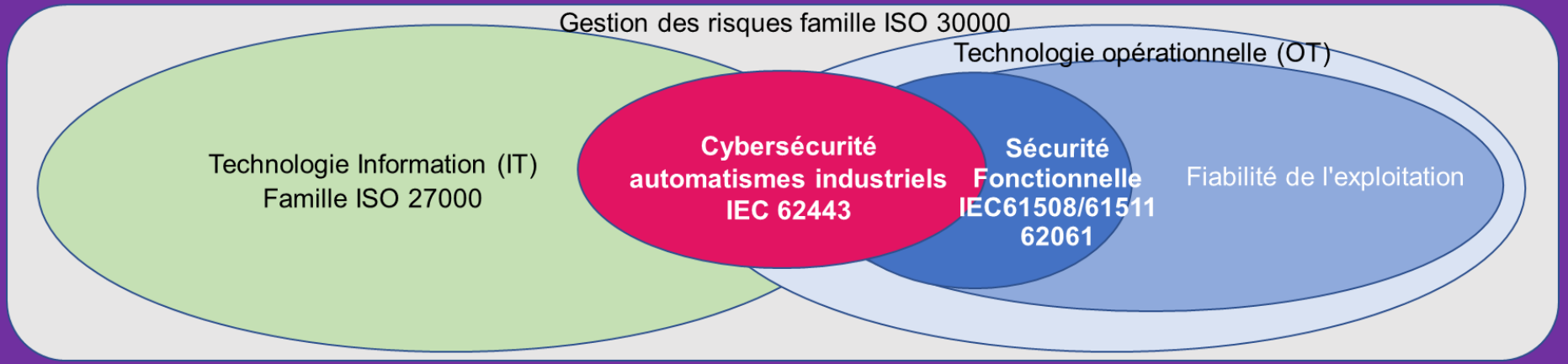
Cybersécurité, Jeu du chat et de la sourie

Pourquoi?

Sécurité intimement liée à la cybersécurité

Zone IT Bureautique & internet

Zone OT temps réel



AGENDA « success story »

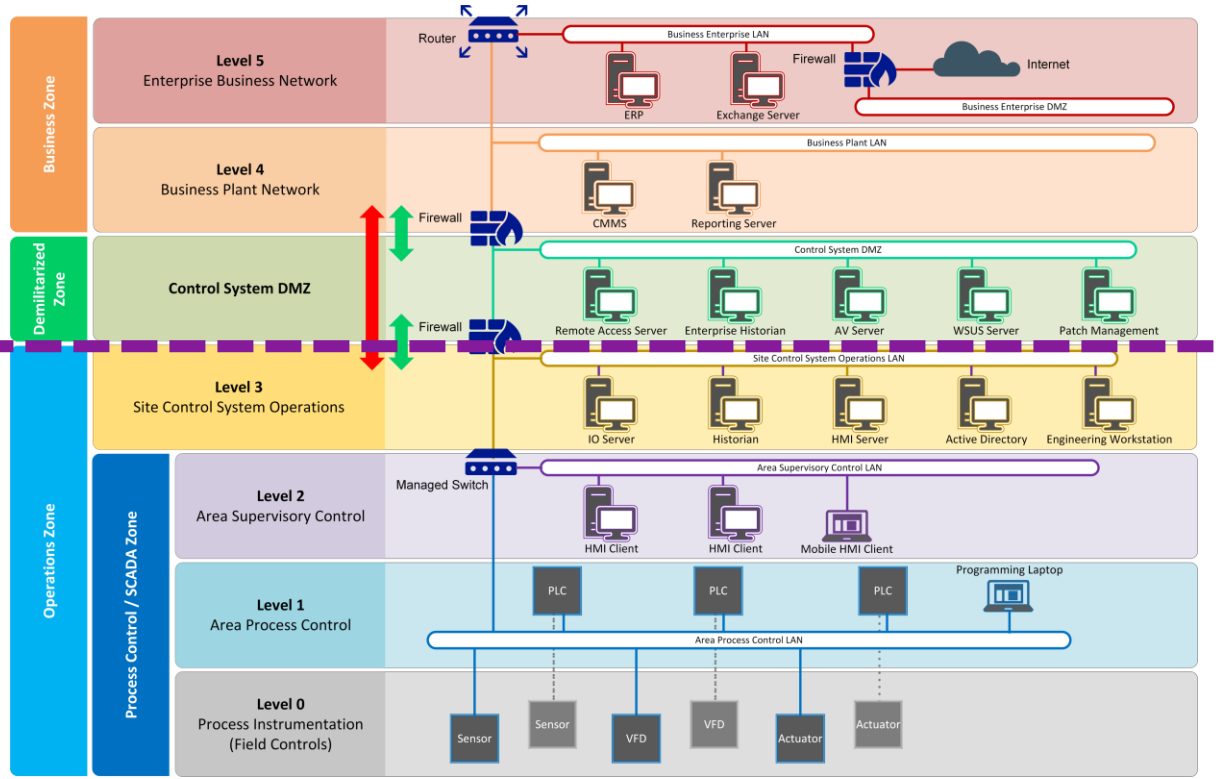
1. Le genèse FSM versus Cybersécurité
2. Audit cyber IEC62443/ANSSI
3. Etat des lieux Cartographie/inventaire/flux
4. Mise en place Big DATA pour OT/IACS

PURDUE Model

IT

OT/IACS

Safety/Security



Success story HUTCHINSON

HUTCHINSON

TotalEnergies

Success Story

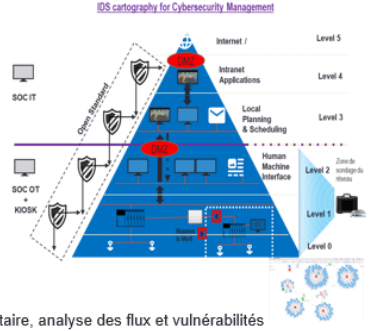
eXcelsior Safety

HUTCHINSON

Données de production dans le Cloud possibles et sécurisées

Les industriels process et manufacturiers sont confrontées à une augmentation exponentielle de la demande de données afin de répondre aux exigences normatives CSRD, énergétique décret tertiaire, excellence opérationnelle ROI/TRS et sécuritaire NIS2, IEC62443, etc. Cette demande fait de plus en plus appel à la puissance de stockage et de calcul des technologies CLOUD. Elle est aussi antinomique avec les recommandations de cybersécurité qui demande de cloisonner et limiter les flux IT/OT surtout lors qu'il s'agit de flux extérieurs voir accès distant par exemple.

Partant de ce constat, les industriels se doivent d'êtres de plus en plus vigilants sur leurs organisations, leurs procédures ainsi que sur les installations IT & OT. La première étape, réaliser un état des lieux précis, cartographique & inventaire ainsi que la gestion des flux des installations et réseaux industriels. Analyser les vulnérabilités. Vérifier la mise en place de zone démilitarisée (DMZ) avec le système IT et à différents endroits suivant les risques et les technologies utilisées telles que IoT, IIoT, réseaux sans fils par exemple.
Grâce à toutes les technologies disponibles sur le marché, des solutions adaptées peuvent être mises en place suivant les niveaux de sécurité nécessaire et localisation dans l'architecture du modèle PURDUE. (recommandations IEC62443/ANSSI)



Service de cartographie/inventaire, analyse des flux et vulnérabilités

Objectifs du client:
- Cartographie détaillée complète, réseaux/flux, inventaire des actifs, analyse des vulnérabilités.
- Gestion de la qualité de la production en temps réel grâce à la technologie cloud.
- Centralisation des données dans le cloud sans risques pour l'usine et respect conformité de la politique du groupe de l'entreprise.
- Tableaux de bord de la production en temps réel au niveau Corporate et au niveau local.
- Solution rentable, facile à utiliser et à mettre en œuvre.

Active member ISEAClub

Contacts : 07 62 96 16 34
contact@excelsiorsafety.fr

Success Story

eXcelsior Safety

HUTCHINSON

Données de production dans le Cloud possibles et sécurisées

Challenges:
- Livraison rapide.
- Coffret local collecte de données SAFE pour exporter les données de production OT en temps réel dans le CLOUD (AIR-GAPPED).
- Collecte des données OT sous différents formats.
- Possibilité de traitement local des données et/ou de règles avant l'exportation des données vers le CLOUD (Magic Software FactoryEye).
- Gestion de la base de données et affinage des données dans le CLOUD (Magic Software FactoryEye).
- Permettre l'utilisation et support par une équipe délocalisée de DATA scientistes.
- Facile à utiliser et à mettre en œuvre.
- Autonomie du client.

Bénéfices/Résultats du client:
- Solution d'exportation de données et de réseaux 100% sécurisé.
- Délai de livraison de 3 mois, solution Low code/No code.
- Prise en main immédiate par les data scientistes.
- Mesure de la qualité du produit en temps réel.
- 25% de gain de temps de production.

Active member ISEAClub

Contacts : 07 62 96 16 34
contact@excelsiorsafety.fr

La genèse

Sécurité fonctionnelle IEC61508/61511
Intimement liée avec
Cybersécurité OT IEC 62443

Protection de l’entreprise

Sécurité intimement liée à la cybersécurité

Safety

Sécurité

Security

Cybersécurité

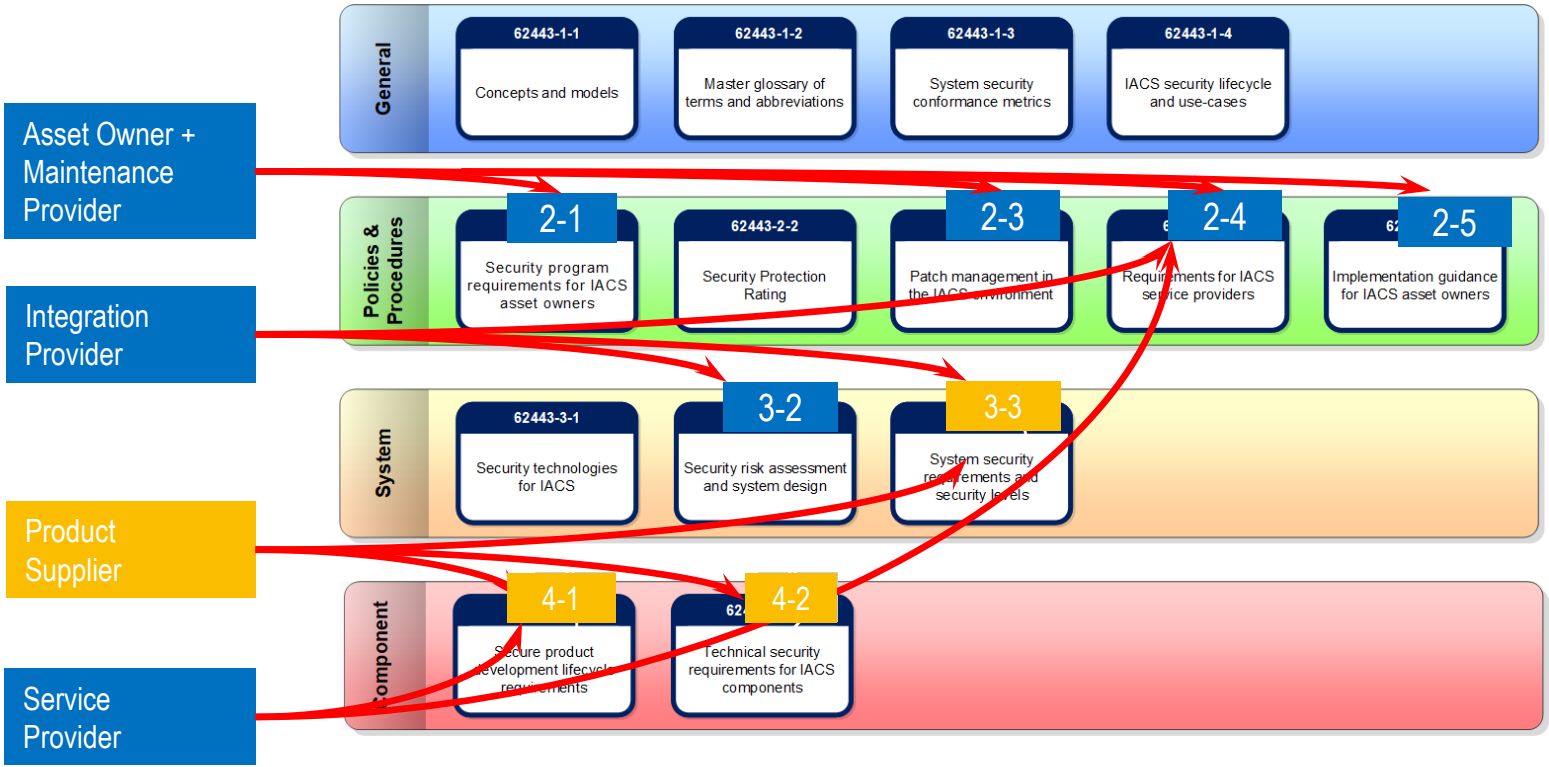
Safe = Protégé

Les Bons Mots

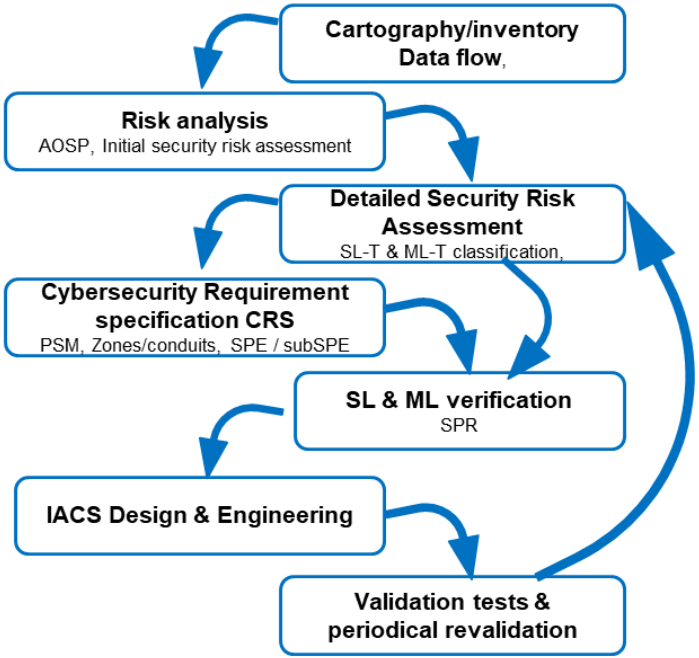
UK	France		
UK	Industrie	Nucléaire & médical	Unité mesure
Control	Contrôle	Contrôle	TF/TP
Availiability	Sureté/disponibilité	Disponibilité	%
Safety	Sécurité	Sureté	SIL
Security	Cybersécurité	Cybersécurité	SL/ML

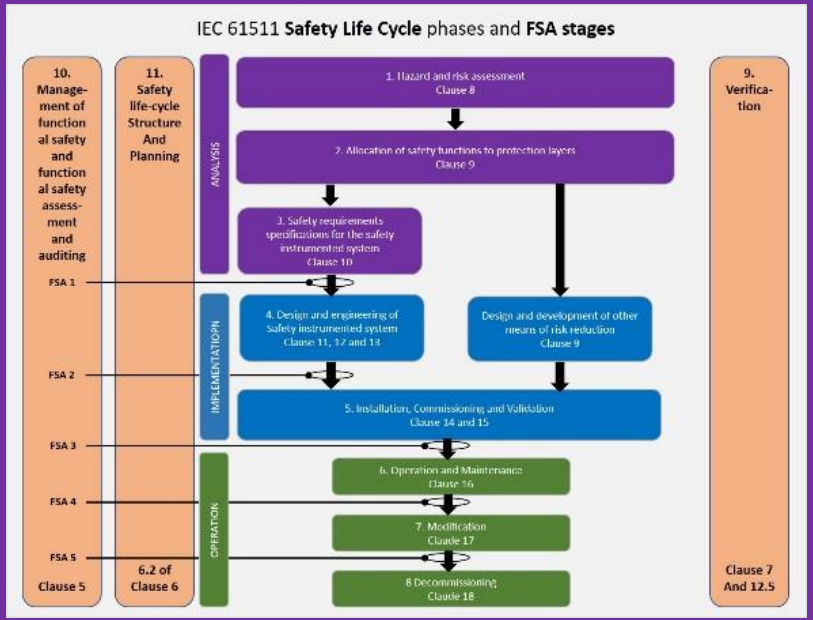
- **Définition de la Cybersécurité** : "Le risque est l'expression de la probabilité qu'une menace définie exploite une vulnérabilité spécifique d'un SNCC ou d'un SIS cible ou d'une combinaison de cibles, provoquant une Conséquence et un impact connexe".

IEC 62443 OT/IACS (EX ISA99)



Cyber OT « Versus » Sécurité Fonctionnelle





Risk Assessment

Node	1	Node Description	Natural Gas System Metering and Heater
Drawing Numbers:	[P&ID references Redacted]		

HAZOP Ref#	Parameter	Guide Word	Cause	Consequence	Safe Guards (Procedures etc..)	Mitigated Risk			Actions		Team Members
						Severity	Likelihood	Risk Ranking	ID	Description	
1	Flow	No/less	Manual valves at LNG regasification unit closed in error.	Potential loss of service of natural gas to the complex. No flow through the heaters, potential to exceed the design temperature since no gas flowing through the heaters , potential for loss of mechanical integrity, LoC leading to fire and explosion.	1. Operating procedures 2. Low pressure alarm via PAL-0001 3. Duty supply for power plant unit XXX 4. High temperature alarm via TAH-0001 5. Metering skids are two operating and one standby (manual change over) 6. High high temperature via TZAHH-	4	3	ALARP			
2	Flow	No/less	Spurious closure of ZV-0001	1. Potential to exceed the design pressure of piping upstream, potential for loss of mechanical integrity, LoC, fire and explosion 2. Potential loss of service of natural gas to the complex. No flow through the heaters, potential to exceed the design temperature since no gas flowing through the heaters , potential for loss of mechanical integrity, LoC leading to fire and explosion.	Consequence 1: 1. High pressure alarm via PAH-0001 2. Duty supply for power plant unit XXX 3. High temperature alarm via TAH-0001 4. High high temperature via TZAHH-0002 tripping EJ-001A/B. Consequence 2: 1. High pressure alarm via PAH-0001 2. Pressure relief provided via PSV-0003A/B 3. High high pressure trip via PZAHH-0002 acting on UZV-0001	4	3	ALARP			
3	Flow	No/less	PV-0005 fails closed due to PIC-0005 control failure	No forward flow to Fuel gas system unit 500, no adverse consequences in this node							
4	Flow	More	Pressure control failure via PIC-0005 leading to PV-0005 opening	Potential for overpressurisation of unit 500. Refer to unit 500 for consequences							
5	Flow	Wrong	Bleed valves opened in error	Potential for loss of gas containment, potential for fire and explosion	1. Operating procedures 2. Bleed valves are all flanged off	4	3	ALARP			

HazOp WS Node - Example | Cyber Risk Assessme WS - Exampl

stem: COMPANY IT System

	Consequence	Safe Guards (Procedures etc..)	Mitigated Risk			Actions		Team Members
			Severity	Likelihood	Risk Ranking	ID	Description	
	Access to non public customer information and account information. Loss of customer trust and damage to reputation. Potential fines from ICO.	1. Customer data not stored or sent to external systems. 2. Data at rest is encrypted. 3. Anti-virus and spyw are monitoring.	4	3	ALARP			
	Inability to access information. Potential for delays.	1. Backup servers. 2. Server monitoring.	2	2	Acceptabl			
	Access to non public customer information and account information. Loss of customer trust and damage to reputation. Potential fines from ICO.	1. TFA required by all employees. 2. Training to staff on leaving laptops / desktops unattended whilst logged in. 3. Procedures to ensure that employees do not leave desktops /	4	3	ALARP			
	Unauthorised access giving access to confidential information. Potential for client data to get compromised. Loss of customer trust and damage to reputation. Potential for delays. Potential fines from ICO.	1. Passwords are required to be changed every 6 months. 2. TFA required by all employees. 3. Training to all staff on Phising attacks.	3	2	ALARP			
	Damage to computer. Potential loss of data. Potential for client data to get compromised. Loss of customer trust and damage to reputation. Potential for delays. Potential fines from ICO.	1. Work desktop / laptops are not to be used for personal use. 2. Anti-virus and spyw are monitoring. 3. Employee training.	3	3	ALARP			
6	Not a credible threat due to all USB ports being disabled by the IT system prior to a laptop being given to the employee.							
7					#N/A			
8					#N/A			
9					#N/A			
10					#N/A			
11					#N/A			
12					#N/A			
13					#N/A			

Desktop / Laptop | USB with virus injected.

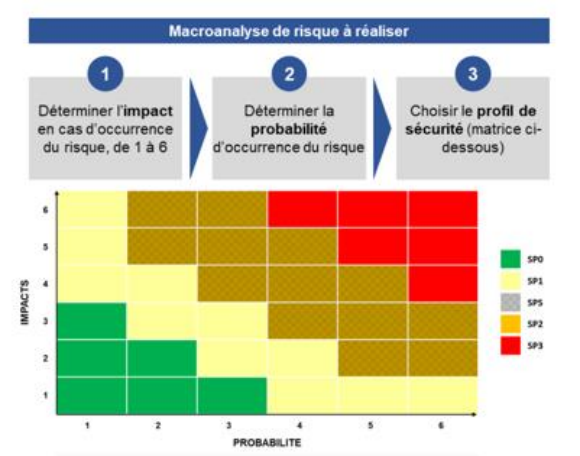
HazOp WS Node - Example | Cyber Risk Assessme WS - Exampl

Évaluation de Risque

SAFETY/SIL
matrice d'évaluation de réduction de risque industriel

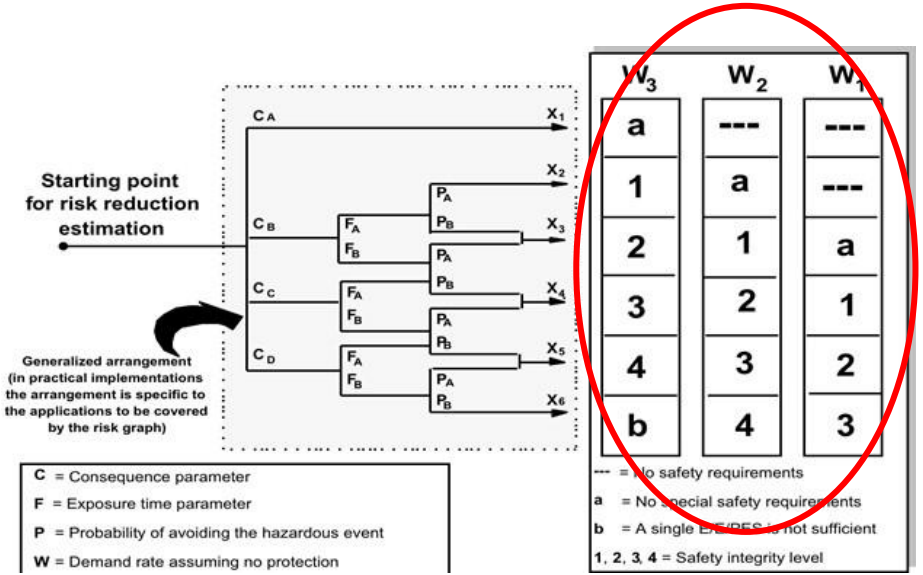
severity		Frequency of the hazardous Event					
		1 per 100000 yrs	1 per 10000 yrs	1 per 1000 years	1 per 100 years	1 per 10 years	1 per year
Catastrophic	> 1 death	III	II	II	I	I	I
Critical	1 death or Serious	III	III	II	II	I	I
Major	Major injury	IV	III	III	II	II	I
Minor	Minor Injury	IV	IV	III	III	II	II

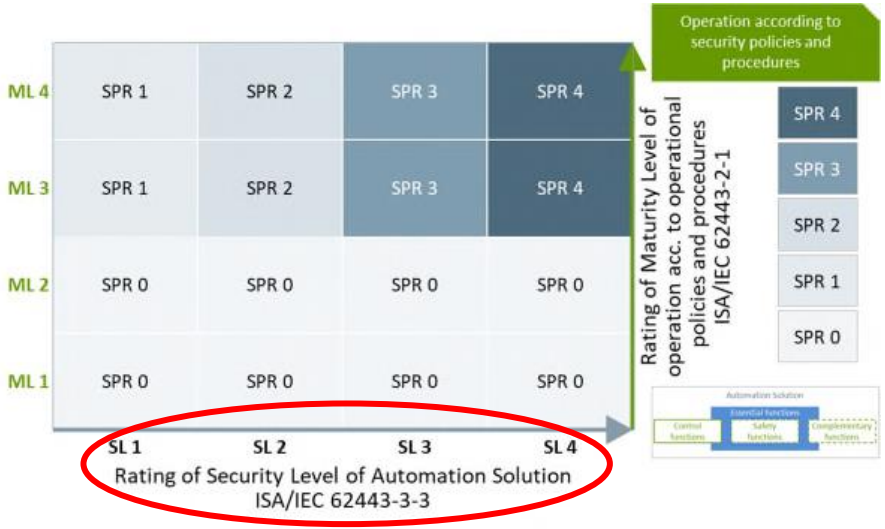
CYBER/SL/ML
Exemple matrice évaluation de risque



SIL/Omega10 versus SL

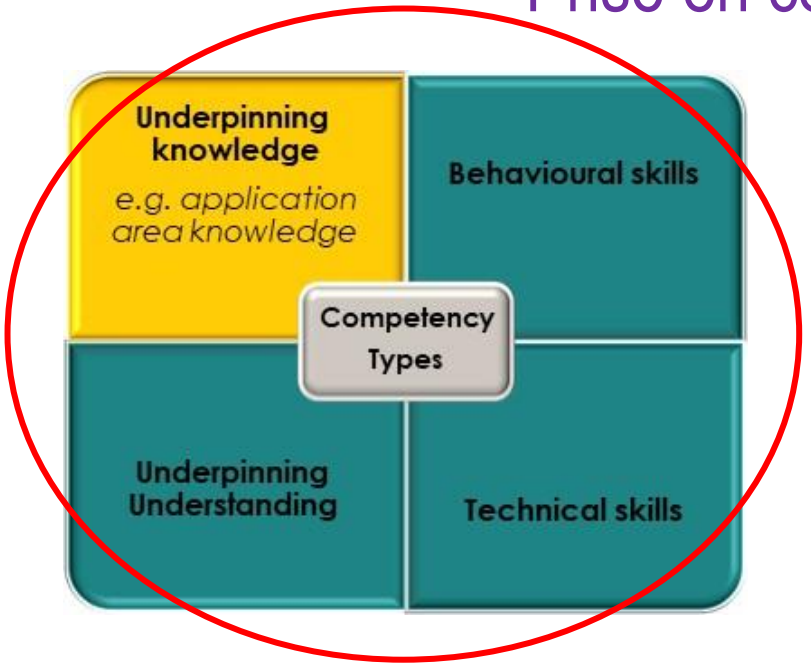
Barrières techniques

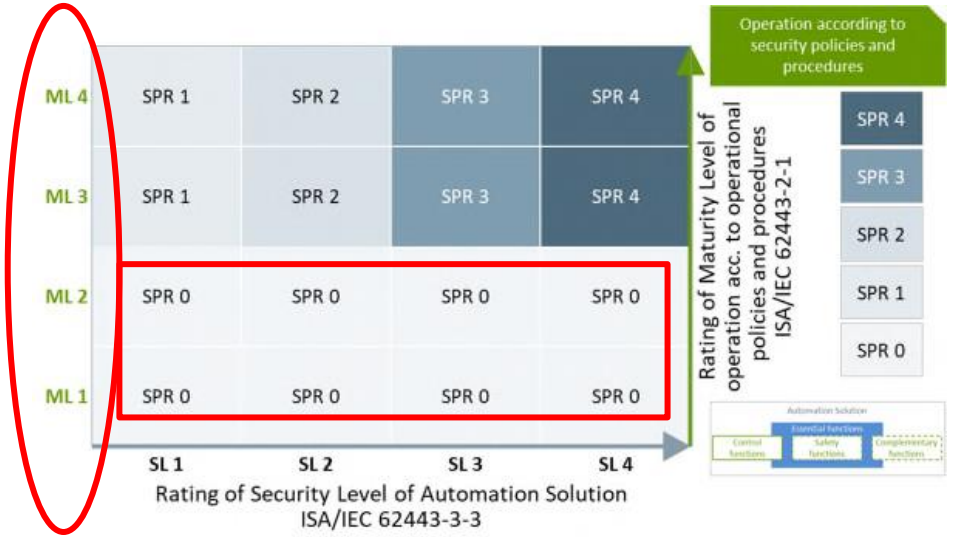




SIL/Omega20 versus ML

Prise en compte facteur Humain

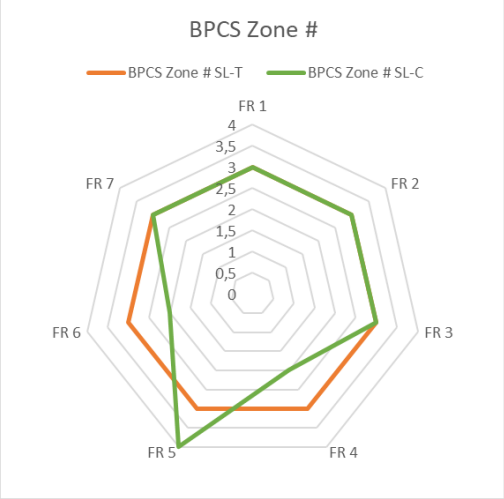


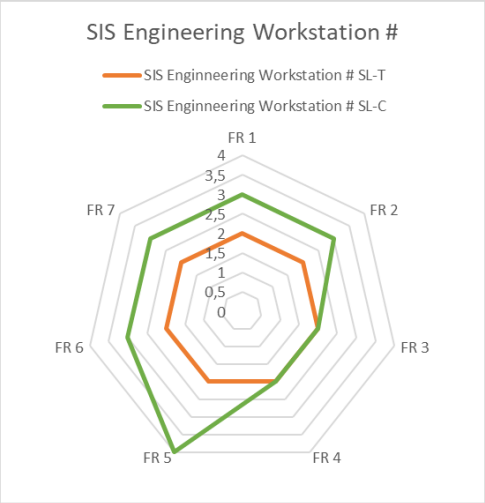


Outils Audit & Management IEC 62443 Performance/Organisationnel

Audit 62443-3-3 Performances Techniques

Domain #	SL-#	FR 1	FR 2	FR 3	FR 4	FR 5	FR 6	FR 7
BPCS Zone #	SL-T	3	3	3	3	3	3	3
BPCS Zone #	SL-A	4	2	3	1	4	3	2
BPCS Zone #	SL-C	3	3	3	2	4	2	3
SIS Enginneering Workstation #	SL-T	2	2	2	2	2	2	2
SIS Enginneering Workstation #	SL-A	4	2	3	1	4	3	2
SIS Enginneering Workstation #	SL-C	3	3	2	2	4	3	3



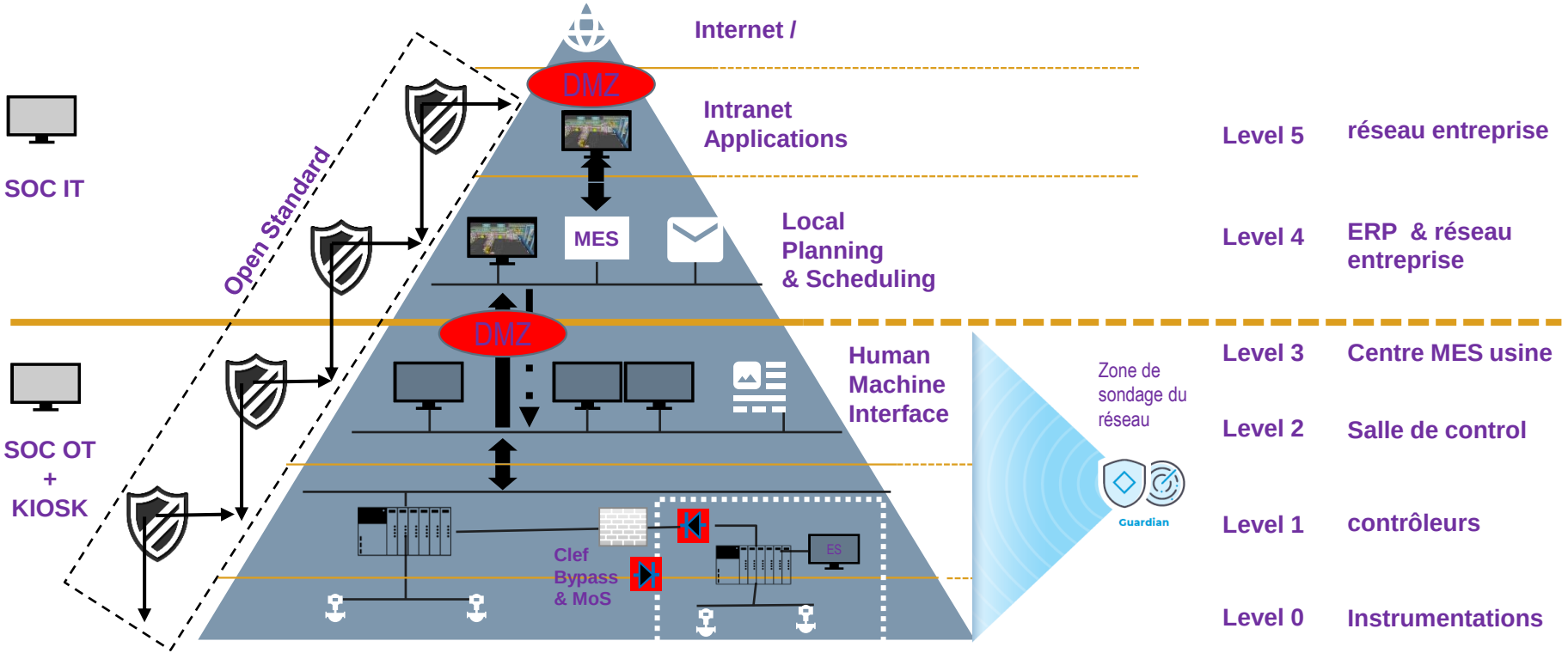


Audit 62443-2-1 Organisationnel (89 points)

	Reference / Requirement	Description	Status		Reference	STATUS	SL1	SL2	SL3	SL4	ML1	ML2	ML3	ML4	Target	Max Scoring	current Scoring
62443-2-1	**6 SPE 1**	**Organizational security measures**					1	2	3	4	1	2	3	4			
62443-2-1	6.2 ORG 1	Security related organizatrion and policies						X				X			2	36	50%
62443-2-1	6.2.1 ORG 1.1	Information Security Management System (ISMS)	Fully Implemented	ISO 27001	04.1+04.2+04.3+05.1+05.2+06.1.1+06.2+07.1+07.4+07.5.1+07.5.2+07.5.3+08.1+10.1+A5.1.1+A6.1.3+A6.1.4+A6.1.5+A7.1.2+A7.2.3+A8.1.4+A11.2.6+A12.1.1+A13.1.2+A13.2.2+A14.2.7+A15.1.2+A16.1.6+A18.1.1+A18.1.2+A18.2.1+A18.2.2	ADD VALUE		X				X					6
62443-2-1	6.2.2 ORG 1.2	Background checks	Partially Implemented	ISO 27001	A7.1.1	No ADD		X				X					4
62443-2-1	6.2.3 ORG 1.3	Security roles and responsibilities	Partially Implemented	ISO 27001	05.1+07.2+ 05.3+A6.1.1+A7.2.1+A11.2.9	ADD VALUE		X				X					4
62443-2-1	6.2.4 ORG 1.4	Security Awareness Training	NA	ISO 27001	07.3+A7.2.2	No ADD											
62443-2-1	6.2.5 ORG 1.5	Security responsibilities training	Not Implemented	ISO 27001	07.2+A7.2.2	No ADD		X				X					2
62443-2-1	6.2.6 ORG 1.6	Supply chain security	Not Implemented	ISO 27001	A15.1.3+A15.2.1+A15.2.2	No ADD		X				X					2
62443-2-1	6.3 ORG 2	Security assessment and reviews					X				X				1	24	88%
62443-2-1	6.3.1 ORG 2.1	Security risk mitigation	Fully Implemented	ISO 27001	06.1.1+06.1.2+06.1.3+07.5.2+07.5.3+08.2+08.3+A6.1.1+A6.1.2+A6.1.3	ADD VALUE	X				X						5
62443-2-1	6.3.2 ORG 2.2	Processes for discovery of security anomalies	Fully Implemented	ISO 27001	10,1	ADD VALUE	X				X						6
62443-2-1	6.3.3 ORG 2.3	Secure development and support	Fully Implemented	ISO 27001	A6.1.5+A14.1.1+A14.2.1+A14.2.5+A14.2.6+A14.2.8	No ADD	X				X						6
62443-2-1	6.3.4 ORG 2.4	SP reviews	Fully Implemented	ISO 27001	10.2+09.1+09.2+09.3+04.4+05.1+06.2+A5.1.2+A18.2.1+A18.2.2+A18.2.3	ADD VALUE	X				X						4

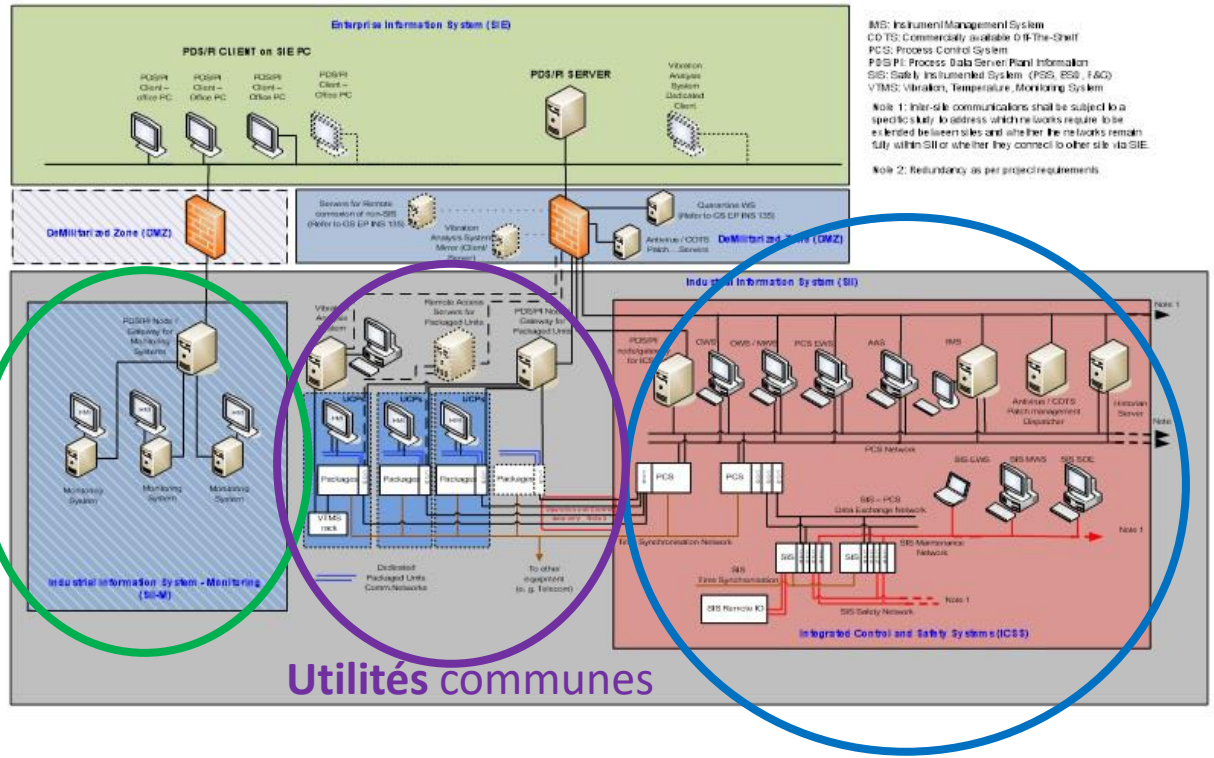
Cartographie / Inventaire
Flux versus Risk

Cartographie/inventaire/vulnerabilités



Gestion des zones et conduits

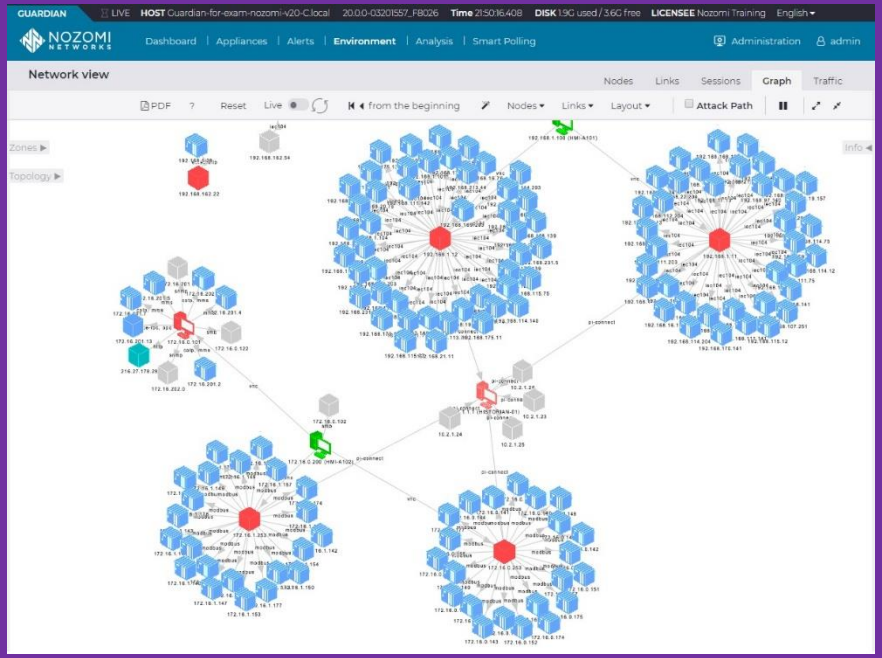
Data monitoring uniquement

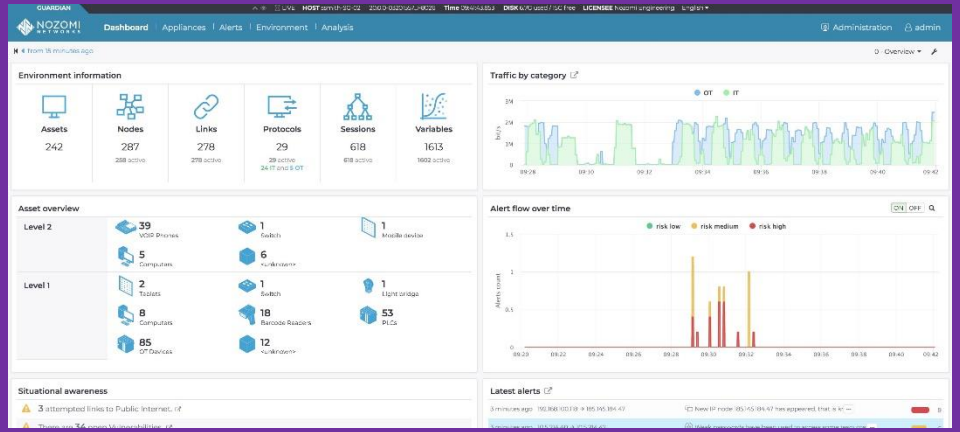


Utilités communes

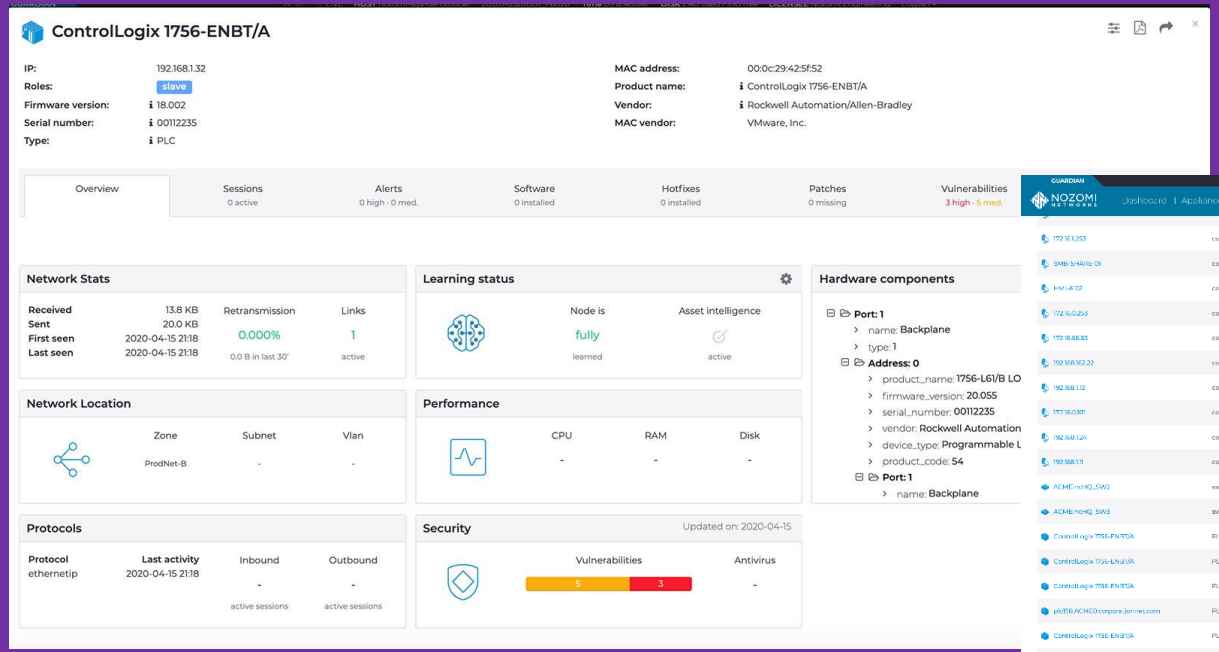
Zone production pilotage process ou machine

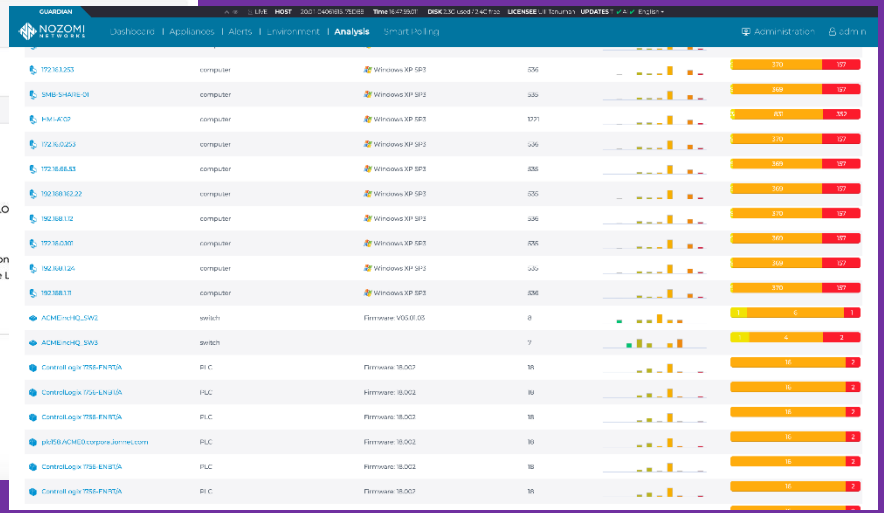
Cartographie architecture / FLUX





Inventaire


ControlLogix 1756-ENBT/A
IP: 192.168.1.32
Roles: slave
Firmware version: 18.002
Serial number: 00112235
Type: PLC
MAC address: 00:0c:29:42:5f:52
Product name: ControlLogix 1756-ENBT/A
Vendor: Rockwell Automation/Allen-Bradley
MAC vendor: VMware, Inc.
Overview
Sessions 0 active
Alerts 0 high · 0 med.
Software 0 installed
Hotfixes 0 installed
Patches 0 missing
Vulnerabilities 3 high · 5 med.
Network Stats
Received 13.8 KB
Sent 20.0 KB
First seen 2020-04-15 21:18
Last seen 2020-04-15 21:18
Retransmission 0.000%
0.0 B in last 30'
Links 1 active
Learning status
Node is fully learned
Asset intelligence active
Hardware components
Port: 1
name: Backplane
type: 1
Address: 0
product_name: 1756-L61/B LO
firmware_version: 20.055
serial_number: 00112235
vendor: Rockwell Automation
device_type: Programmable L
product_code: 54
Port: 1
name: Backplane
Network Location
Zone ProdNet-B
Subnet -
Vlan -
Performance
CPU -
RAM -
Disk -
Protocols
Protocol ethernetip
Last activity 2020-04-15 21:18
Inbound - active sessions
Outbound - active sessions
Security
Updated on: 2020-04-15
Vulnerabilities 5 3
Antivirus -


GUARDIAN
NOZOMI NETWORKS
Dashboard | Appliances | Alerts | Environment | Analysis | Smart Polling
Administration
admin

Big DATA
&
Data Lake/Cloud

Success story HUTCHINSON

HUTCHINSON®

TotalEnergies

Success Story

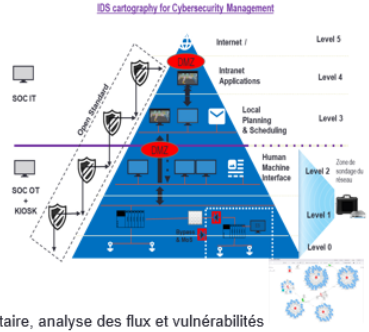
eXcelsior Safety

HUTCHINSON

Données de production dans le Cloud possibles et sécurisées

Les industriels process et manufacturiers sont confrontées à une augmentation exponentielle de la demande de données afin de répondre aux exigences normatives CSRD, énergétique décret tertiaire, excellence opérationnelle ROI/TRS et sécuritaire NIS2, IEC62443, etc. Cette demande fait de plus en plus appel à la puissance de stockage et de calcul des technologies CLOUD. Elle est aussi antinomique avec les recommandations de cybersécurité qui demande de cloisonner et limiter les flux IT/OT surtout lors qu'il s'agit de flux extérieurs voir accès distant par exemple.

Partant de ce constat, les industriels se doivent d'êtres de plus en plus vigilants sur leurs organisations, leurs procédures ainsi que sur les installations IT & OT. La première étape, réaliser un état des lieux précis, cartographique & inventaire ainsi que la gestion des flux des installations et réseaux industriels. Analyser les vulnérabilités. Vérifier la mise en place de zone démilitarisée (DMZ) avec le système IT et à différents endroits suivant les risques et les technologies utilisées telles que IoT, IIoT, réseaux sans fils par exemple.
Grâce à toutes les technologies disponibles sur le marché, des solutions adaptées peuvent être mises en place suivant les niveaux de sécurité nécessaire et localisation dans l'architecture du modèle PURDUE. (recommandations IEC62443/ANSSI)



Service de cartographie/inventaire, analyse des flux et vulnérabilités

Objectifs du client:
- Cartographie détaillée complète, réseaux/flux, inventaire des actifs, analyse des vulnérabilités.
- Gestion de la qualité de la production en temps réel grâce à la technologie cloud.
- Centralisation des données dans le cloud sans risques pour l'usine et respect conformité de la politique du groupe de l'entreprise.
- Tableaux de bord de la production en temps réel au niveau Corporate et au niveau local.
- Solution rentable, facile à utiliser et à mettre en œuvre.

Active member ISEAClub

Contacts : 07 62 96 16 34
contact@excelsiorsafety.fr

Success Story

eXcelsior Safety

HUTCHINSON

Données de production dans le Cloud possibles et sécurisées

Challenges:
- Livraison rapide.
- Coffret local collecte de données SAFE pour exporter les données de production OT en temps réel dans le CLOUD (AIR-GAPPED).
- Collecte des données OT sous différents formats.
- Possibilité de traitement local des données et/ou de règles avant l'exportation des données vers le CLOUD (Magic Software Factory(Eye).
- Gestion de la base de données et affinage des données dans le CLOUD (Magic Software Factory(Eye).
- Permettre l'utilisation et support par une équipe délocalisée de DATA scientistes.
- Facile à utiliser et à mettre en œuvre.
- Autonomie du client.

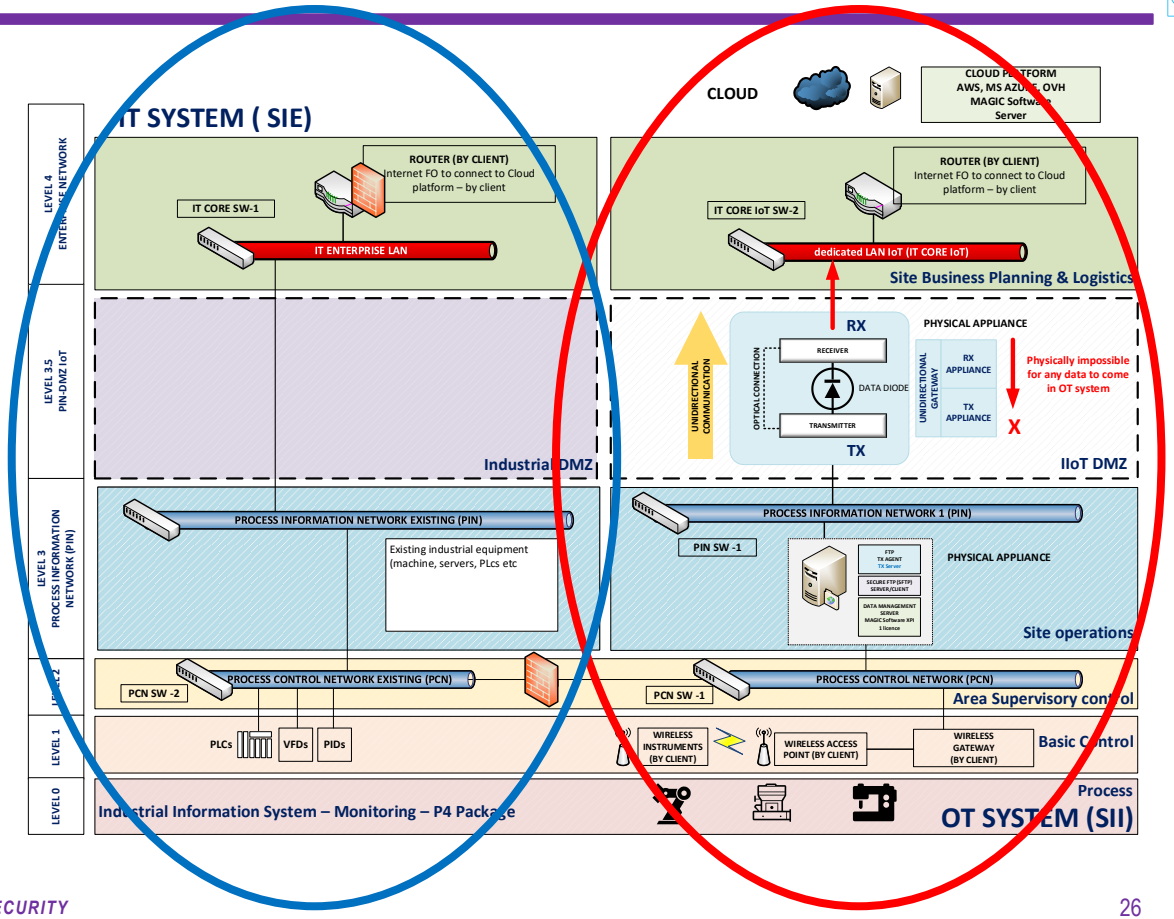
Bénéfices/Résultats du client:
- Solution d'exportation de données et de réseaux 100% sécurisé.
- Délai de livraison de 3 mois, solution Low code/No code.
- Prise en main immédiate par les data scientistes.
- Mesure de la qualité du produit en temps réel.
- 25% de gain de temps de production.

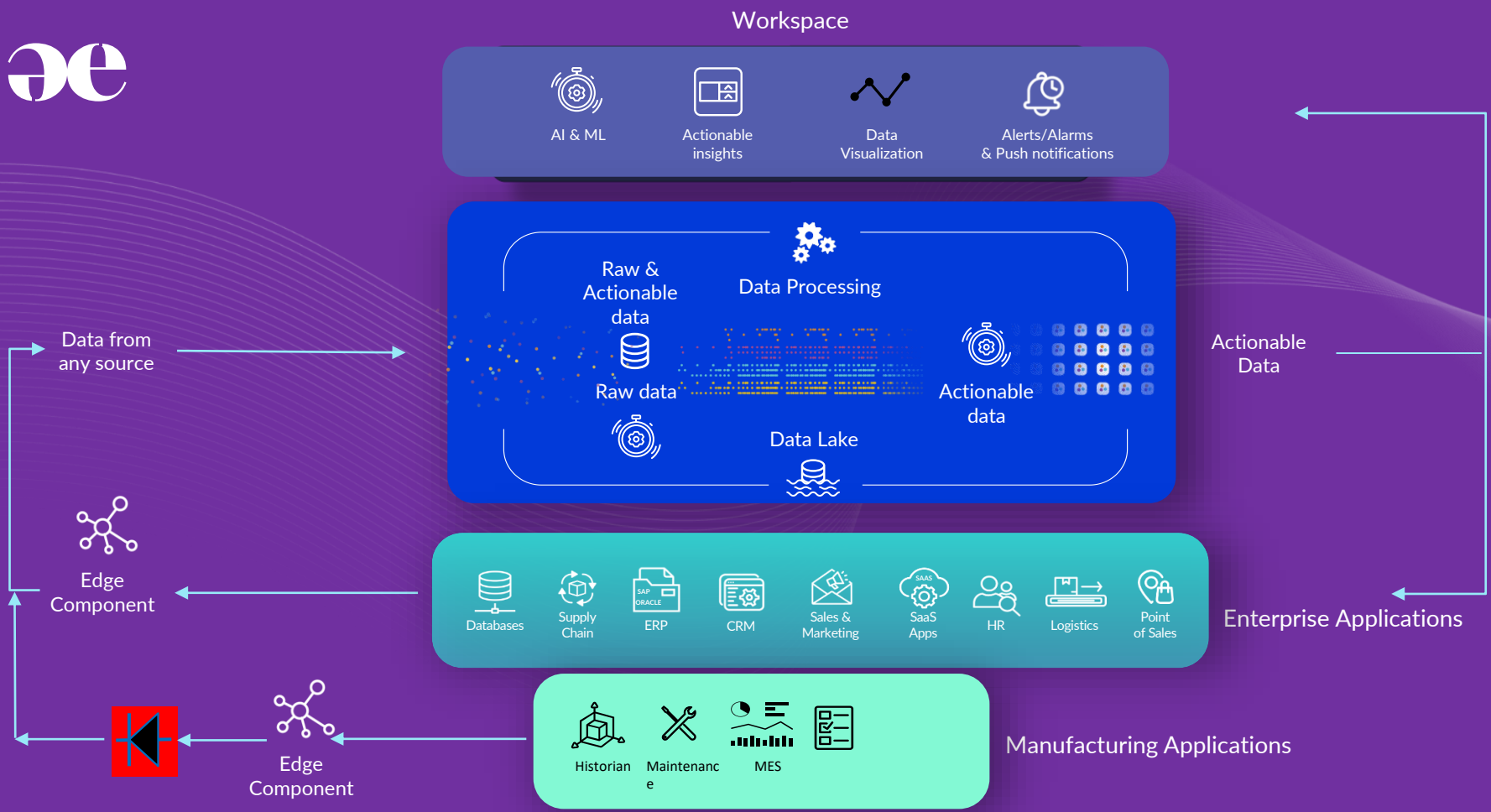
Active member ISEAClub

Contacts : 07 62 96 16 34
contact@excelsiorsafety.fr

Installation

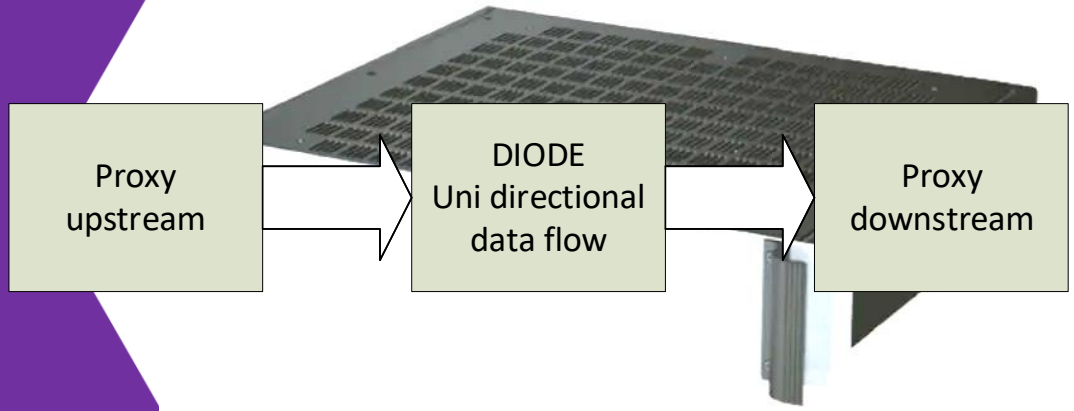
- Ségrégation ZONE et CONDUITS (process, IoT/IIoT)
- Installation serveur application BIG DATA collecteur de données en local (On premise)
- remontée des Big Datas via liaison dédiée indépendante et sécurisé vers service cloud




Workspace
AI & ML
Actionable insights
Data Visualization
Alerts/Alarms & Push notifications
Raw & Actionable data
Data Processing
Raw data
Actionable data
Data Lake
Data from any source
Actionable Data
Edge Component
Databases
Supply Chain
ERP
CRM
Sales & Marketing
SaaS Apps
HR
Logistics
Point of Sales
Enterprise Applications
Edge Component
Historian
Maintenance
MES
Manufacturing Applications

Data DIODE Intelligente 1Gb

- Proxy **Upstream** incluant :
  - outils de collecte multi Protocol et multi format base de données
  - Permettant le nettoyage des bases de données et diagnostics des flux
- API permettant le transfert des data via une diode
- Proxy **Downstream** permettant:
  - la réception control et émission des datas vers le cloud
  - Transfert de diagnostics



Air Gapped (isolation)

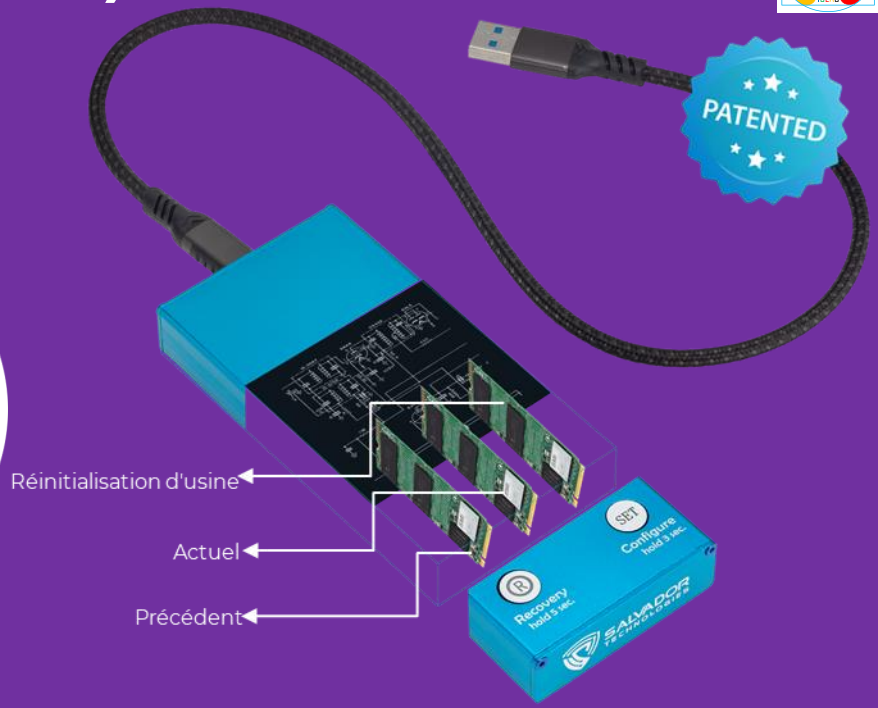
L'algorithme ne permettra aucun contrôle externe ou interne de cette fonctionnalité depuis l'ordinateur.

Cela signifie que tous les X jours, un disque différent sera accessible à l'utilisateur pour la sauvegarde des données - les autres disques sont électroniquement hors ligne.

Capacité disponible : 3 disques NVMe

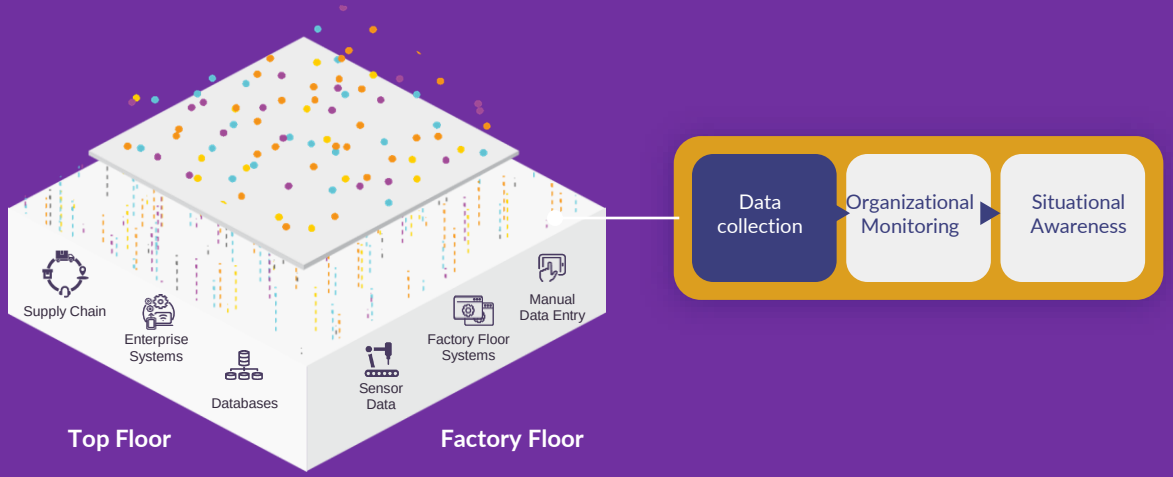
options : 512 Go / 1 To / 2 To/4 To

(PN : CRU-512 / CRU-1000 / CRU-2000 / CRU-4000)

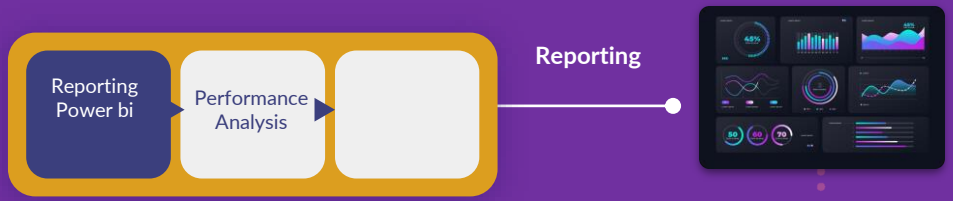


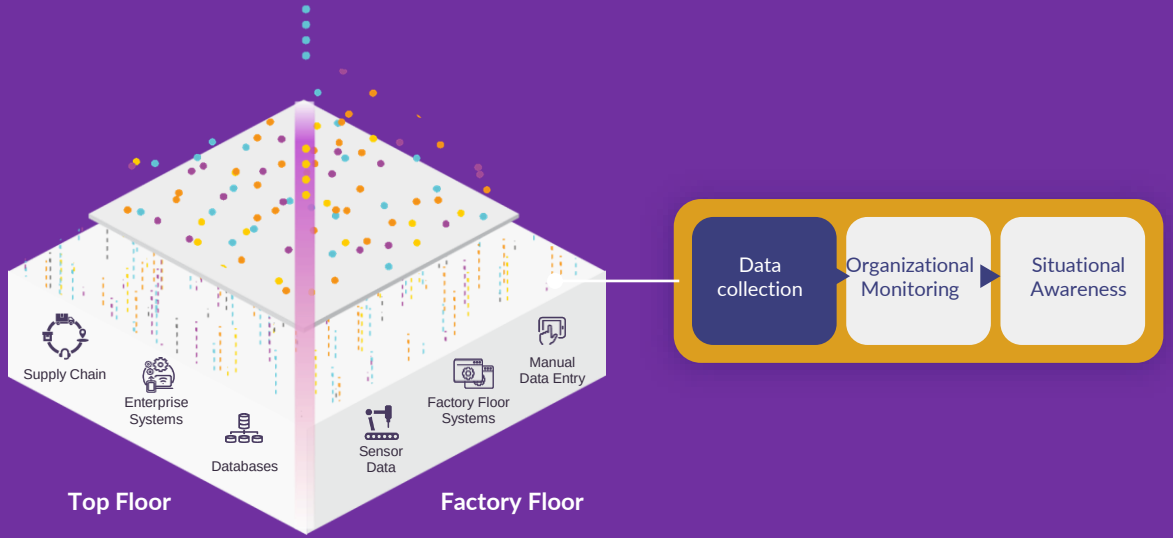
30 secondes
et vous voilà à nouveau opérationnel!

Étape 1 collecte des données)

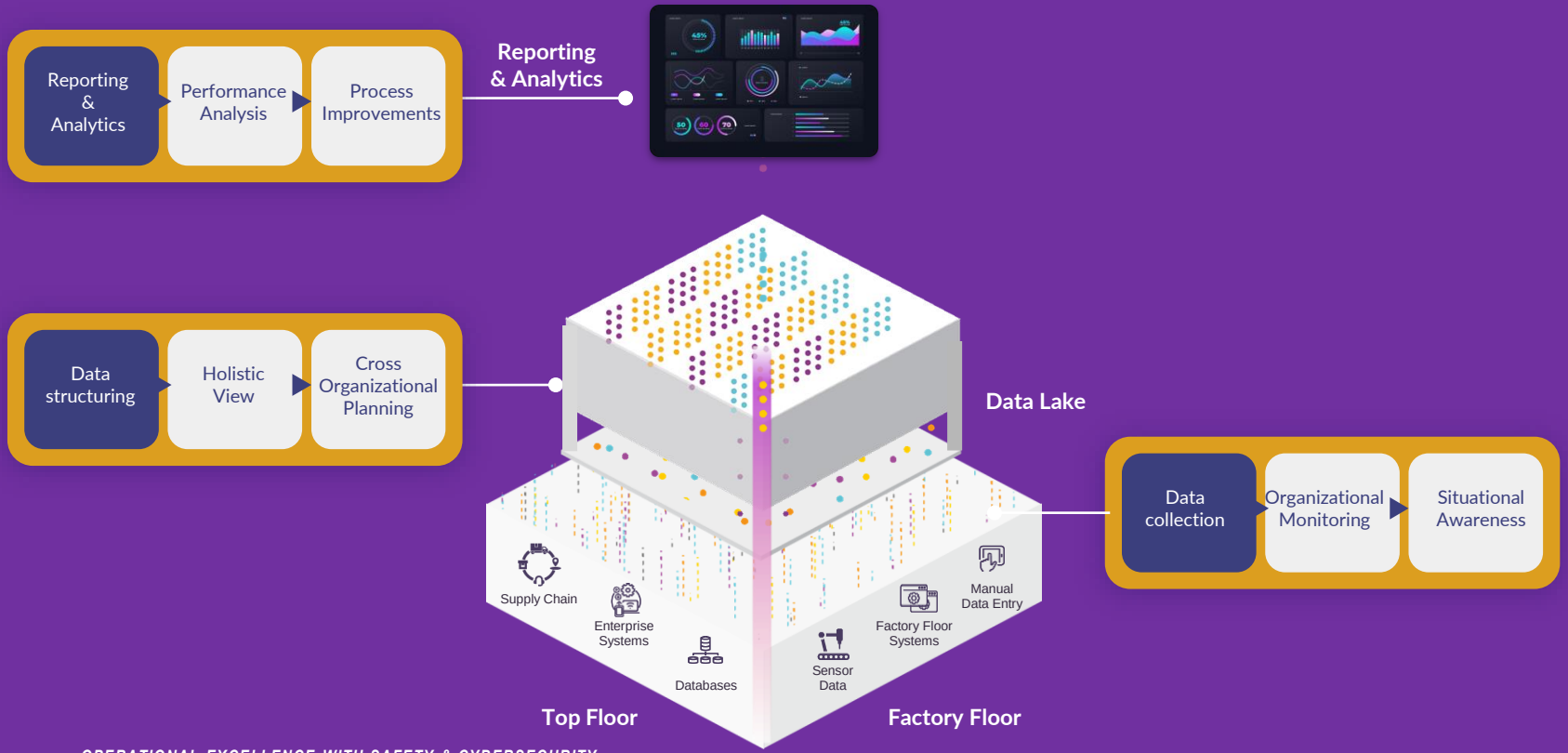


étape 2 reporting BI

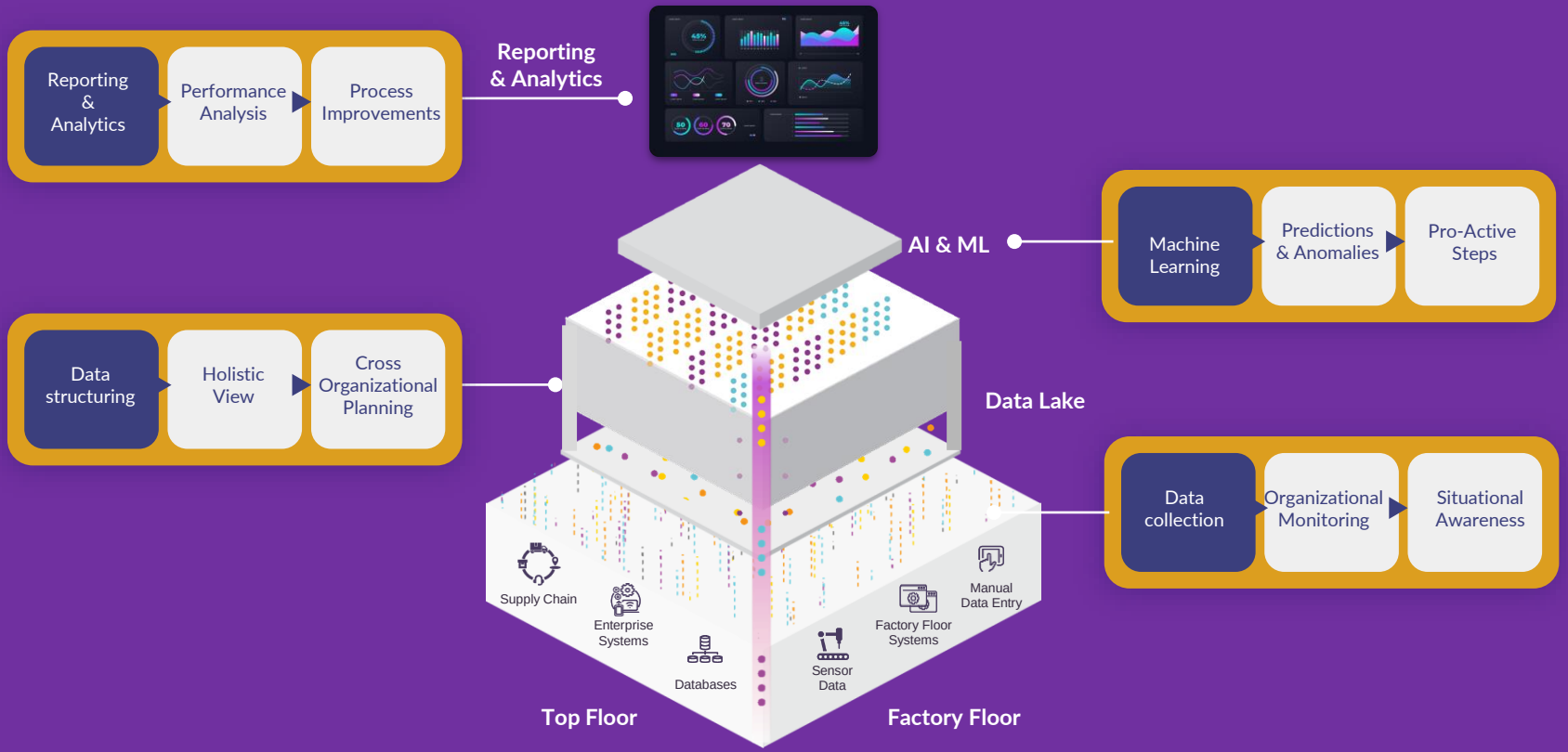




étape 3 Transformation de la donnée en information métier



étape 4 analyse des informations métier



MANUFACTURING BUSINESS INTELLIGENCE

ANALYZE & VISUALIZE

ACT & OPTIMIZE

PREDICTIVE ANALYTICS

Connect & Integrate: **Business & Manufacturing Operations**

BUSINESS OPERATIONS

SRM
- Sourcing
- Contracts
- Inbound

PLANNING
- Forecasting
- MRP Explosion
- Mfg Planning

INVENTORY MGMT
- Raw Materials
- Finished Goods
- Inbound & Outbound

SUPPLY CHAIN
- Logistics
- Warehouse Mgt
- Collaboration

HUMAN RESOURCES
- Workforce Mgmt
- Payroll/Benefits
- Performance Mgmt

FINANCE
- Cost Accounting
- Perf Tracking
- Financial Reports

CRM
- Sales
- Acct Mgmt
- Cust Sat

Connect & Integrate: **Manufacturing & Production Operations**

MANUFACTURING OPERATIONS

PLM/PDM
- MDM/BOM
- Recipe
- Lifecycle

MES
- WO instructions
- Scheduling
- Inventory

QUALITY CONTROL
- Compliance
- Worker Safety
- Corrective Action

MAINTENANCE
- Maint. WO
- Decrease MTBF
- Proactive

PROCESS CONTROL
- SCADA/HMI
- PLCS
- OPC/Historian DBs

FINISHING
- Final Assembly
- Packaging
- Shipping

Connect & Integrate: **Production Operations, IIoT, Remote Devices**

PRODUCTION OPERATIONS

CONNECT & COLLECT DATA

PREDICTIVE MAINTENANCE

AI-DRIVEN RESPONSE

Merci

E : contact@excelsiorsafety.fr
W : www.excelsiorsafety.fr
M : 0033 762 961 634