allentis

Cyberium

Standard ISA-62443

# Retour d'expérience d'implémentation

# AGENDA

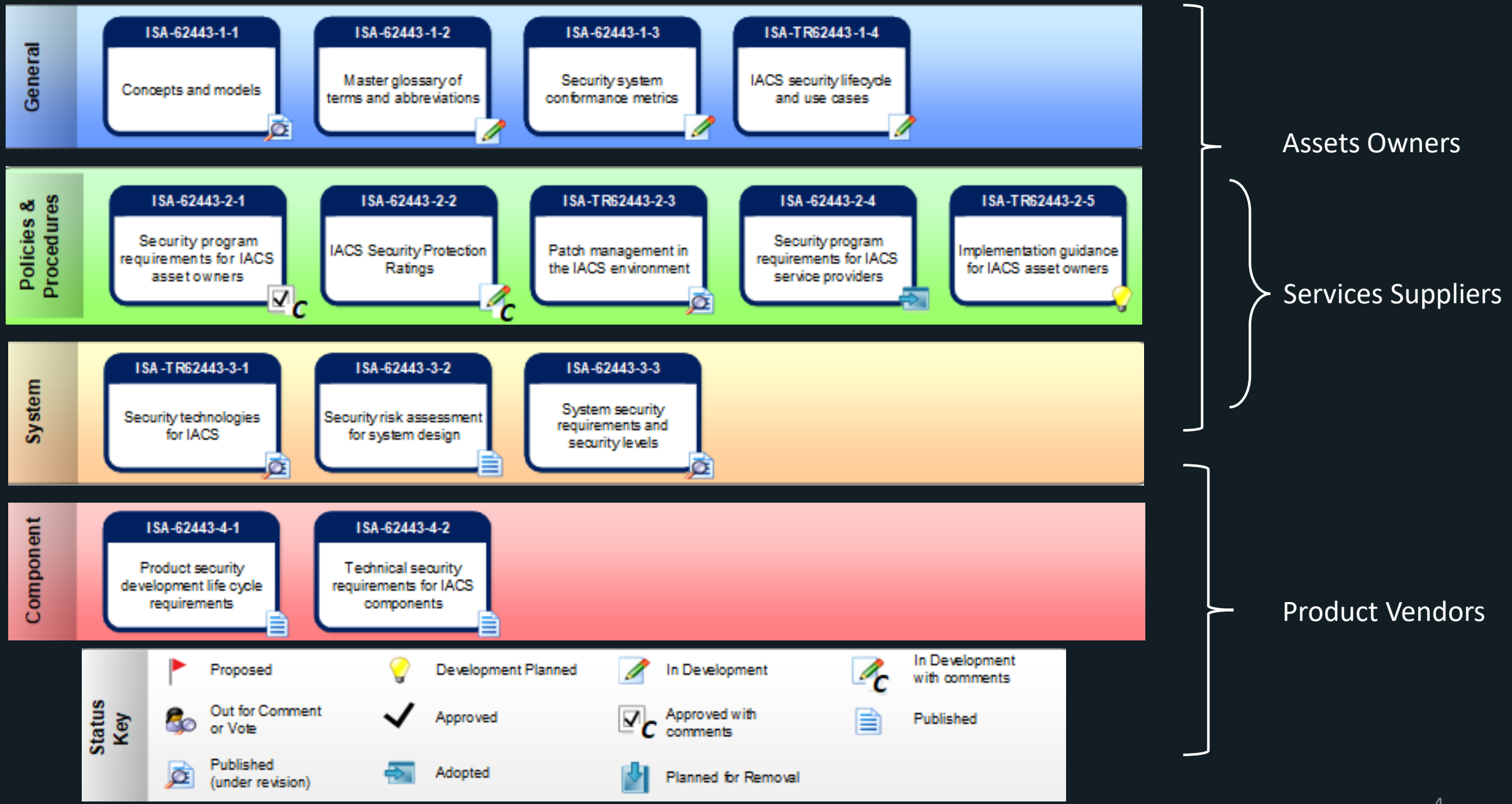
**Partie 1** — Introduction à ISA-62443

**Partie 2** — Comment utiliser ISA-62443 en tant qu'opérateur d'une unité de production « critique » ?

**Partie 3** — Comment utiliser le standard pour développer un cahier des charges : exemple sur FR-5 Restricted Data Flow

# Partie 1

# Introduction à ISA-62443


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 for system design
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
Status Key
Proposed
Development Planned
In Development
In Development with comments
Out for Comment or Vote
Approved
Approved with comments
Published
Published (under revision)
Adopted
Planned for Removal
Assets Owners
Services Suppliers
Product Vendors

# Facteurs d'Impact

**Confidentiality:** l'incidence de la divulgation de renseignements confidentiels

**Integrity:** impact de la modification/destruction non autorisée de l'information

**Availability:** impact de la disponibilité du système

**Identification and Authentication (IAC):** les conséquences de l'absence d'authentification des utilisateurs (humains, processus ou appareils)

**Use Control (UC):** les conséquences de l'échec de l'application des stratégies qui limitent l'utilisation aux utilisateurs authentifiés disposant de privilèges suffisants

**Timely Response to Event (TRE):** les conséquences de l'incapacité à réagir rapidement aux violations de la sécurité de l'information

**Restricted Data Flow (RDF):** les conséquences de données inutiles entraînant des restrictions au flux de données nécessaire

# Security Level

La zone ou le conduit définit le SL cible (Target) SL-T, les contrôles peuvent atteindre une certaine capacité SL, Capacité SL-C, et après la mise en œuvre des contrôles le SL Atteint, SL-A, peut être identique ou inférieur.

**Le niveau de sécurité ciblé est déterminé par une analyse de menace et d'impact**

| | |
|---|---|
| **SL1** | **Protection contre les violations occasionnelles ou fortuites** |
| **SL2** | **Protection contre la violation intentionnelle par des moyens simples, faibles ressources, compétences génériques, faible motivation** |
| **SL3** | **Protection contre les violations intentionnelles à l'aide de moyens sophistiqués, de ressources modérées, de compétences spécifiques au ICS et d'une motivation modérée** |
| **SL4** | **Protection contre les violations intentionnelles à l'aide de moyens sophistiqués, de ressources étendues, de compétences spécifiques au ICS, d'une motivation élevée** |

# 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** |

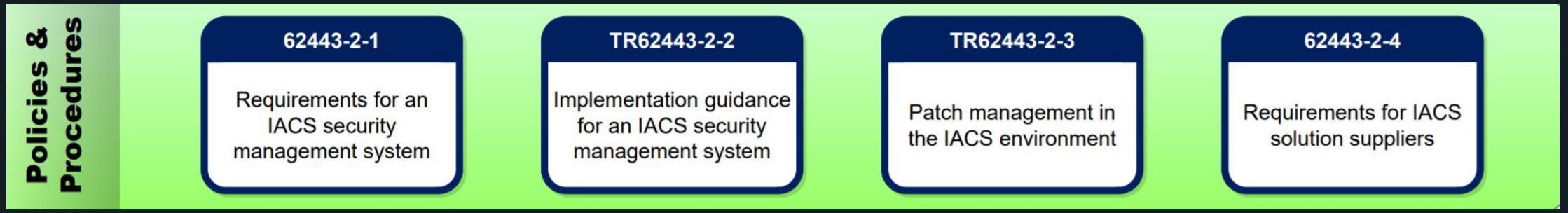
# Partie 2

# Comment utiliser ISA-62443 ?

# ISA-62443-3-2: Cyber Security Management System

**Policies & Procedures**

- **62443-2-1** description de la  CSMS, ce qui est requis pour définir et implementer un système performant pour manager la cyber sécurité industrielle (Published Under revision)
- **62443-2-2** provides specific guidance on required policies & procedures to operate an effective IACS cyber security management system for asset owners ( Draft form).
- **TR62443-2-3** technical report provides guidance on the specific subject of patch management for IACS for asset owners. (Published 2015)
- **62443-2-4** specifies requirements for suppliers of IACS. The principal audience include suppliers of control systems solutions. (Published 2018)



# Développer la CSMS

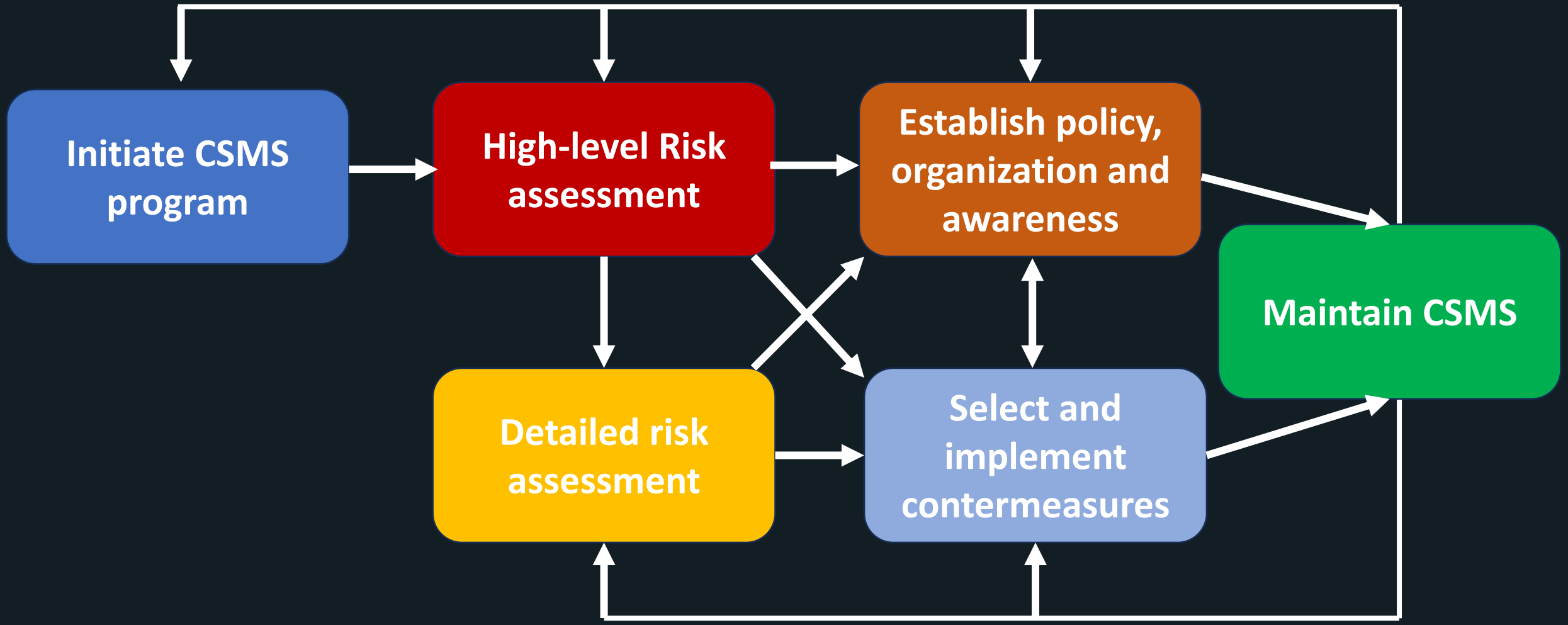



Figure - Top level activities for establishing a CSMS

# Les fondations d'une CSMS efficace

Définition des rôles & responsabilités (correspondant cyber industriels & les responsables risques industrielles)

Profil de la menace

Définition de l'échelle des impacts (finance, sûreté, santé, environnement, réglementaire & légal, réputation, opérations)

Développement de la matrice des risques alignée (mais pas trop) sur la matrice des risques de l'entreprise

Définition de la tolérance aux risques dans le cadre cyber

Définition de la formule de calcul de risque

# Résultats importants pour le cahier des charges

**Plan de remédiation (en fonction de l'état du projet industriel)**

**Définition des Zones et Conduits en fonction des SL**

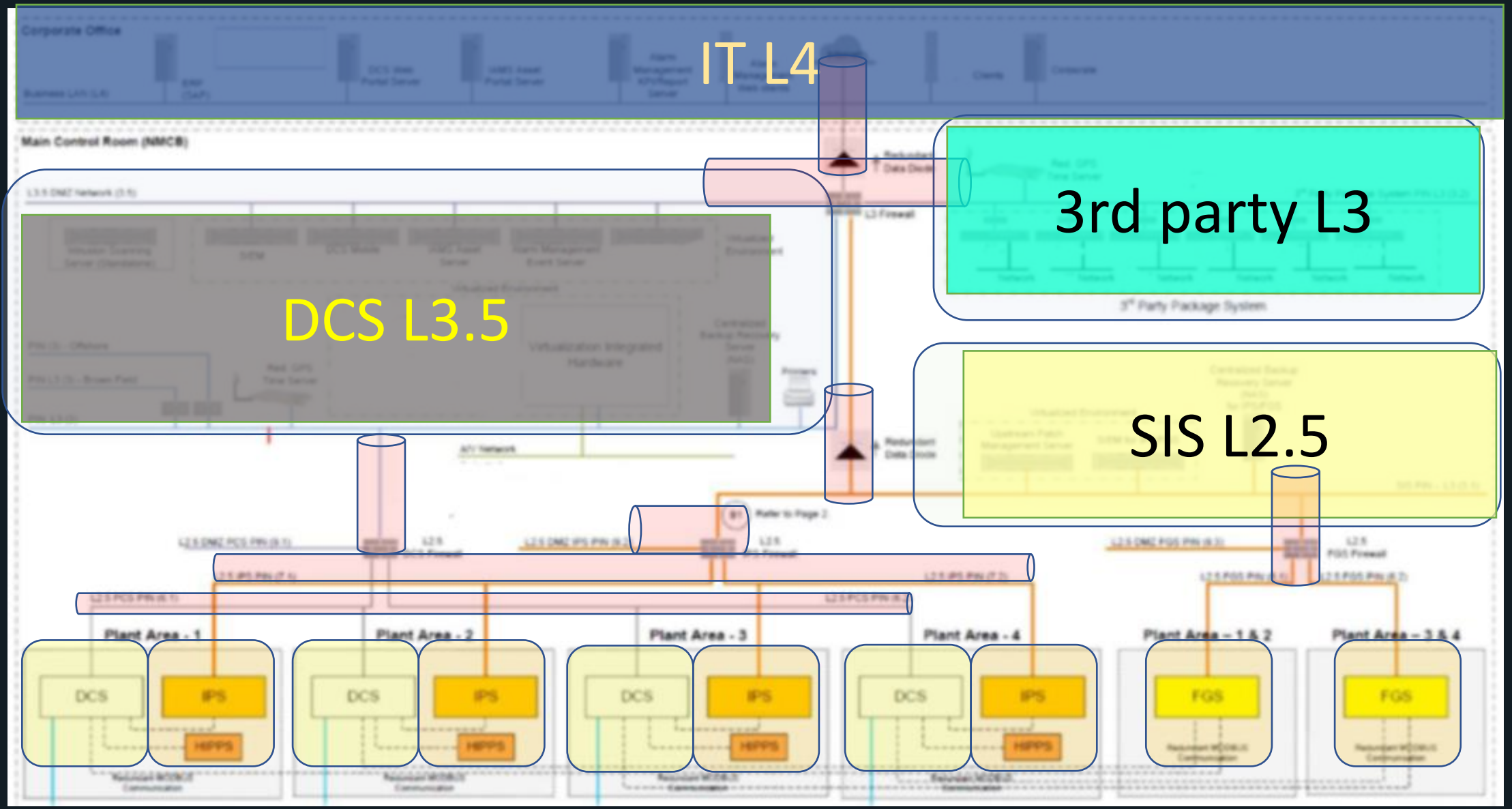
**Attention:**

**SL-T≠ SL-C ≠ SL-A**

SL-T: Target Security Level

SL-C: Capability Security Level
→ ISA-62433-3-3

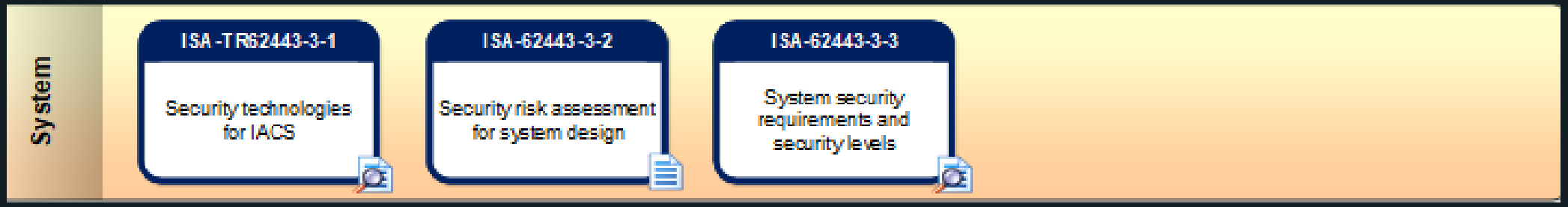
SL-A: Achieved Security Level


IT L4
3rd party L3
DCS L3.5
SIS L2.5
Plant Area - 1
Plant Area - 2
Plant Area - 3
Plant Area - 4
Plant Area – 1 & 2
Plant Area – 3 & 4
DCS
IPS
HIPPS
FGS

# Partie 3

# Cahier des charges

# ISA-62443-3: cyber sécurité des sytèmes




- **TR62443-3-1** Rapport technique décrivant les technologies de sécurité pour ICS (revision en cours)
- **62443-3-2** méthodologie pour effectuer un audit des risques de cyber sécurité pour des systèmes industriels (tout neuf).
- **62443-3-3** la liste des critères pour chaque control selon les 7 FR et selon les niveaux de sécurités SL.

# Exemples de critères:

# 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 |

# Comparaison Technologique

| 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 |

*Certains protocoles industriels sont extrêmement difficiles à sécuriser avec un F/W, c'est-à-dire OPC DA*

# Certifications ISA disponibles ou en cours

### Component Security Assurance (CSA)

Product certification for IACS components.

### IIoT Component Security Assurance (ICSA)

Product certification for IIoT Components.

### System Security Assurance (SSA)

Process certification for IACS systems.

### Security Development Lifecycle Assurance (SDLA)

Process certification for IACS development organizations.

### IACS Security Assurance (IACSSA)

Certification for facilities operating an IACS.

allentis

## Leader Français de la chaîne complète de détection des menaces

**TAP & Agrégateurs**
pour la collecte des flux réseau

*Avec Qualification élémentaire ANSSI*

Systèmes de
**détection des menaces cyber**
& **d'analyse de performances**

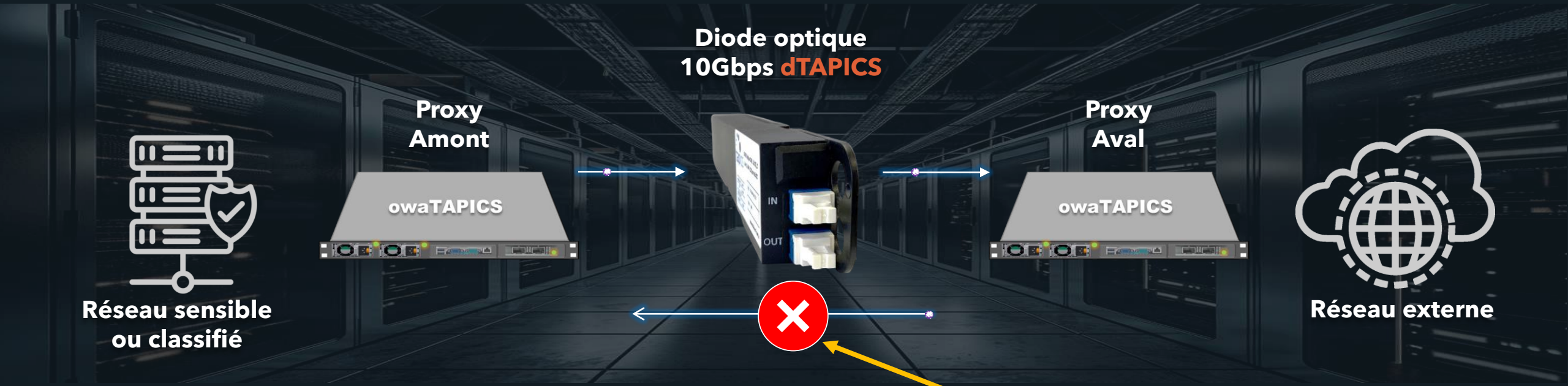
*Avec Qualification élémentaire ANSSI*

**Diodes réseau** et
**Proxys** d'isolation réseau

*Avec Qualification élémentaire ANSSI*

# Isolation des réseaux IT et OT

## ***Sanctuarisez* vos données *sensibles* et *confidentielles*,**
## *tout en préservant la compliance de vos réseaux.*




- *Transfert de fichiers, jusqu'à 100Go*
- *Transfert de données jusqu'à 10Gbps.*
- *Administrable en mode out-of-band.*
- *Configuration Haute Disponibilité.*

- *Adapté aux environnement IT et OT.*
- *Isolement physique garantie à 100%.*
- *Conformité LPM & NIS 2*

*Avec Qualification élémentaire ANSSI*

# Merci !

# Des Questions ?

allentis

Cyberium

allentis
140 Bis, rue de Rennes
75006 Paris – France
tél : +33 1 70 38 25 45
fax : +33 1 70 38 23 00
info@allentis.eu
www.allentis.eu