Automation Hub

La transformation digitale des systèmes industriels

L'IEC 62443

La CYBERSECURITE DES AUTOMATISMES ET DES SYSTEMES DE CONTRÔLE DE PROCEDE

Janvier 2025

Un didacticiel Automation Hub

Droits d’exploitation

Vous avez acquis auprès de l’association Automation-Hub le droit d’exploiter, en version mono-utilisateur, le didacticiel « L’IEC 62443 – LA CYBER-SECURITE DES AUTOMATISMES ET DES SYSTEMES DE CONTRÔLE DE PROCEDE » dont Automation Hub détient un droit de commercialisation, de diffusion et d’exploitation. Ceci implique le respect des conditions qui suivent

Droits d’utilisation et de reproduction

- Vous pouvez utiliser librement le didacticiel pour vos besoins dans le cadre de vos fonctions dans votre entreprise.
- La modification, la reproduction et/ou la diffusion via Internet ou le Web, intranet, extranet ou toute autre forme numérique ou imprimée, de tout ou partie du contenu téléchargé sont interdites. Vous avez cependant la possibilité de reproduire des extraits de ce contenu, dans le cadre des travaux ou des activités de votre entreprise auxquels ils sont utiles, à la condition qu’ils soient limités et que l’origine de ces reproductions partielles soit mentionnée de façon lisible sous la forme : « Source : Didacticiel Automation Hub V2025-1».
- Ces dispositions s’appliquent également aux figures, illustrations, logos ou images. Tout extrait destiné à être utilisé dans des publicités, des communiqués de presse ou du matériel de formation ou de promotion nécessite un accord préalable écrit d’Automation Hub.

Responsabilités

- Automation Hub et l’auteur apportent tout le soin possible à la préparation des informations délivrées dans les contenus qu’elle produit ou qu’elle diffuse. Cependant elle ne peut, être tenue pour responsable d’aucune perte ou frais qui pourrait résulter d'imprécisions, d'inexactitudes, d'erreurs ou de possibles omissions, ni des résultats obtenus par l'utilisation et la pratique des informations délivrées

L’auteur

Jean-Pierre HAUET, ancien Chief Technology Officer d’ALSTOM, Associate Partner de KB Intelligence, Président d’Automation Hub, voting member du Comité ISA99, www.hauet.com

Objectifs du didacticiel

- Rappeler l'enjeu de la cybersécurité des systèmes de contrôle et la nature des attaques survenues au cours des dernières années
- Expliquer la démarche préconisée par l'ISA-99 devenue IEC 62443 afin de permettre aux responsables de construire un système de gestion de la cybersécurité leurs systèmes ou de leurs installations
- Présenter la terminologie et le contenu des principaux documents normatifs de l'IEC 62443 afin de faciliter leur accès aux futurs utilisateurs
- Préconiser des pratiques de défense de nature à accroître le niveau de cybersécurité des installations, sans prétendre faire une analyse exhaustive des techniques de sécurité
- Aborder la problématique propre à l'Internet des objets
- Proposer quelques annexes pour approfondissement éventuel

Sommaire du didacticiel (1)

Introduction : La cybersécurité, une nouvelle composante de la sécurité industrielle

- Concepts généraux
- Quelques définitions
- Cybersécurité et sécurité fonctionnelle
- Cybersécurité industrielle et cybersécurité des systèmes d'information
  - Pourquoi les IACS sont-ils devenus vulnérables ?
  - Les solutions de l'informatique classique ne sont pas suffisantes

Partie 1 : Comprendre la menace

- Comprendre les attaques pour savoir y faire face
- La veille en cybersécurité : où trouver des informations ?

Partie 2 : l'IEC 62443

- **La notion de programme de sécurité (SP) – Les référentiels**
- **Les comités de standardisation IEC et ISA**
- **L'approche générale de l'IEC 62443**
- **IEC 62443 : plan documentaire et principaux documents**
- **IEC 62443 : les textes clés**
  - IEC 62443-1-1 : modèles et concepts
  - IEC 62443-2-4 : Security program requirements for IACS service providers
  - IEC 62443-3-2 : Security risk assessment for system design
  - IEC 62443-3-3 : System security requirements and security levels
  - IEC 62443-4-1 : Product security development life-cycle requirements

Sommaire du didacticiel (2)

Partie 2 : l'IEC 62443 (suite)

- IEC 62443 : les textes clés (suite)
  - IEC 62443-4-2 : Technical security requirements for IACS components
  - IEC 62443-2-1 (2024) : Security program requirements for IACS asset owners
  - IEC 62443-2-2 (draft)- Security Program Rating
  - IEC 62443 et ISO/IEC 27001/2
- La législation européenne (NIS 2)
- Evaluation et certification IEC 62443
  - Evaluation : des outils commencent à apparaître
  - Les certifications ISA Secure et IECEE
- **La certification européenne**
  - Le Cyber Security Act
  - Le Cyber Resilience Act (CRA)
- **Exemples de détermination et d'analyse des zones et des conduits**

Partie 3 : se protéger

- **Les mesures organisationnelles**
- **Les mesures techniques**

Partie 4 : Incidences de l'Internet industriel des objets et des nouvelles architectures de systèmes d'automatisme

- **Trois évolutions majeures**
- **Comment se protéger : quatre principes**

Conclusions

Annexes

- Annexe 1 : Rétrospective de quelques attaques
- Annexe 2 : Standards et réglementations
- Annexe 3 : Aperçu sur les techniques de chiffrement
- Annexe 4 : Exemples d'attaques sur l'IoT
- Annexe 5 : Une check-list pour se préparer la construction d'un programme de sécurité

Introduction : la cybersécurité, une nouvelle composante de la sécurité industrielle

Concepts généraux

- La cybersécurité des systèmes d'automatisme et de contrôle industriel (IACS, selon l'acronyme de l'IEC 62443) est une discipline à part entière
- Elle interfère avec deux disciplines dont elle hérite de nombreux principes :
  - la sûreté de fonctionnement et la sécurité fonctionnelle
  - la sécurité des systèmes d'information
- Il est essentiel de bien comprendre les similitudes et les différences qui l'unissent avec et qui la différencient de ces deux disciplines

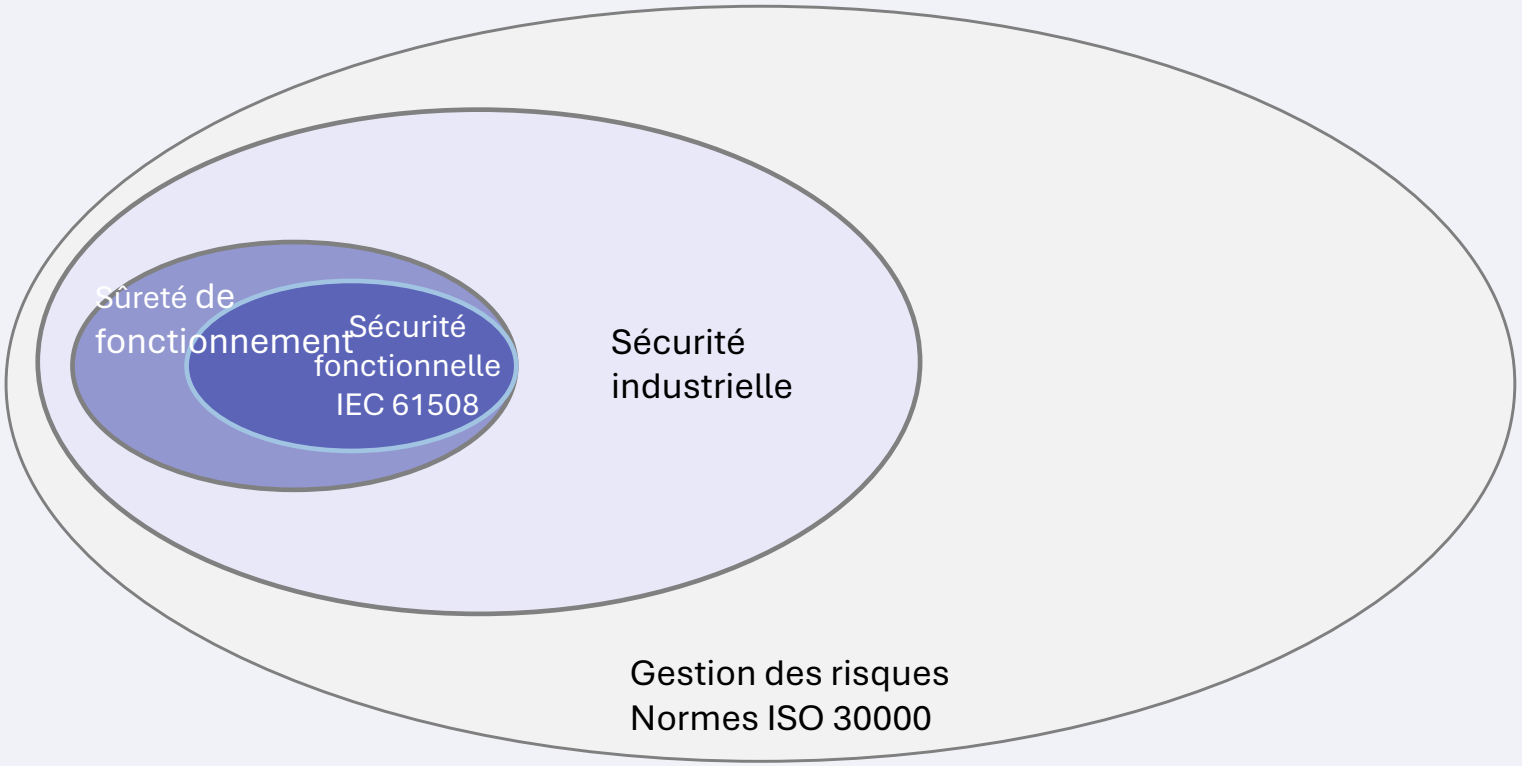
La sûreté de fonctionnement : une préoccupation ancienne

- Faire en sorte qu'un système fonctionne de façon fiable, sans générer de risques pour le personnel et pour l'entourage, est une préoccupation ancienne
- L'ensemble des mesures utilisées pour le bon fonctionnement d'un système fait partie d'une discipline appelée, en France, « **sûreté de fonctionnement** » et qui s'inscrit dans le cadre plus général de la gestion des risques industriels, incluant la protection contre le feu et les explosions, les inondations et autres événements naturels, les risques, etc.
- La sécurité fonctionnelle est un sous-ensemble de la sûreté de fonctionnement, qui a trait la sécurisation d'un procédé par des fonctions instrumentées de sécurité électriques, électroniques et électroniques programmables (E/E/PE) supportées par des systèmes intégrés de sécurité (SIS) → norme IEC 61508 et dérivées

La sécurité fonctionnelle

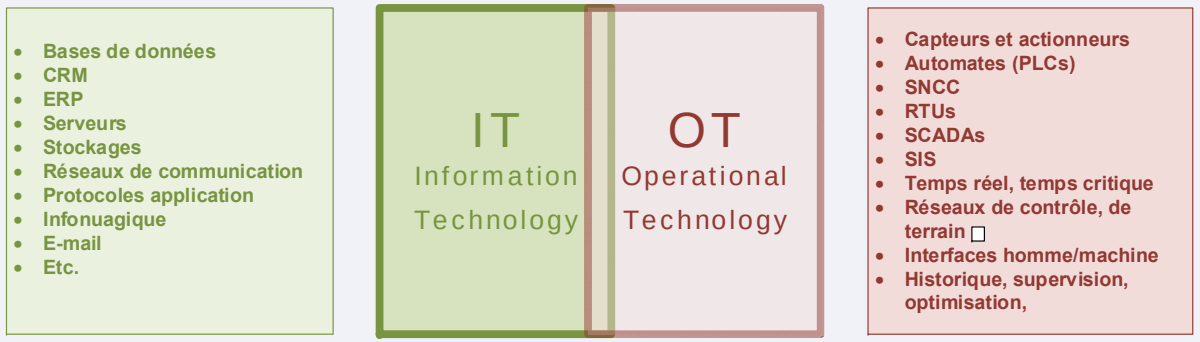
- La « **sécurité fonctionnelle** » ou « **functional safety** » a été introduite par les normes IEC 61508 et 61511 (ou ISA-84) comme sous-ensemble de la sûreté de fonctionnement
- **Définition : s***ous-ensemble de la sécurité globale, relatif aux équipements et aux systèmes de contrôle-commande associés, qui dépend du fonctionnement correct de systèmes électriques, électroniques, programmables électroniques (E/E/PE) concernés par la sécurité*
- La sécurité fonctionnelle s'intéresse aux systèmes de sécurité (systèmes comprenant une ou plusieurs dispositions dont la défaillance peut mettre en cause la sécurité des personnes et de l'environnement) et aux systèmes actifs (ex : systèmes de détection de fumées)
- Nota 1 : Les systèmes passifs ne relèvent pas de la sécurité fonctionnelle (ex : portes résistant au feu)
- Nota 2 : La sécurité fonctionnelle, telle que définie initialement par l'IEC 61508, n'incluait pas la **cybersécurité**

Sûreté de fonctionnement et sécurité fonctionnelle



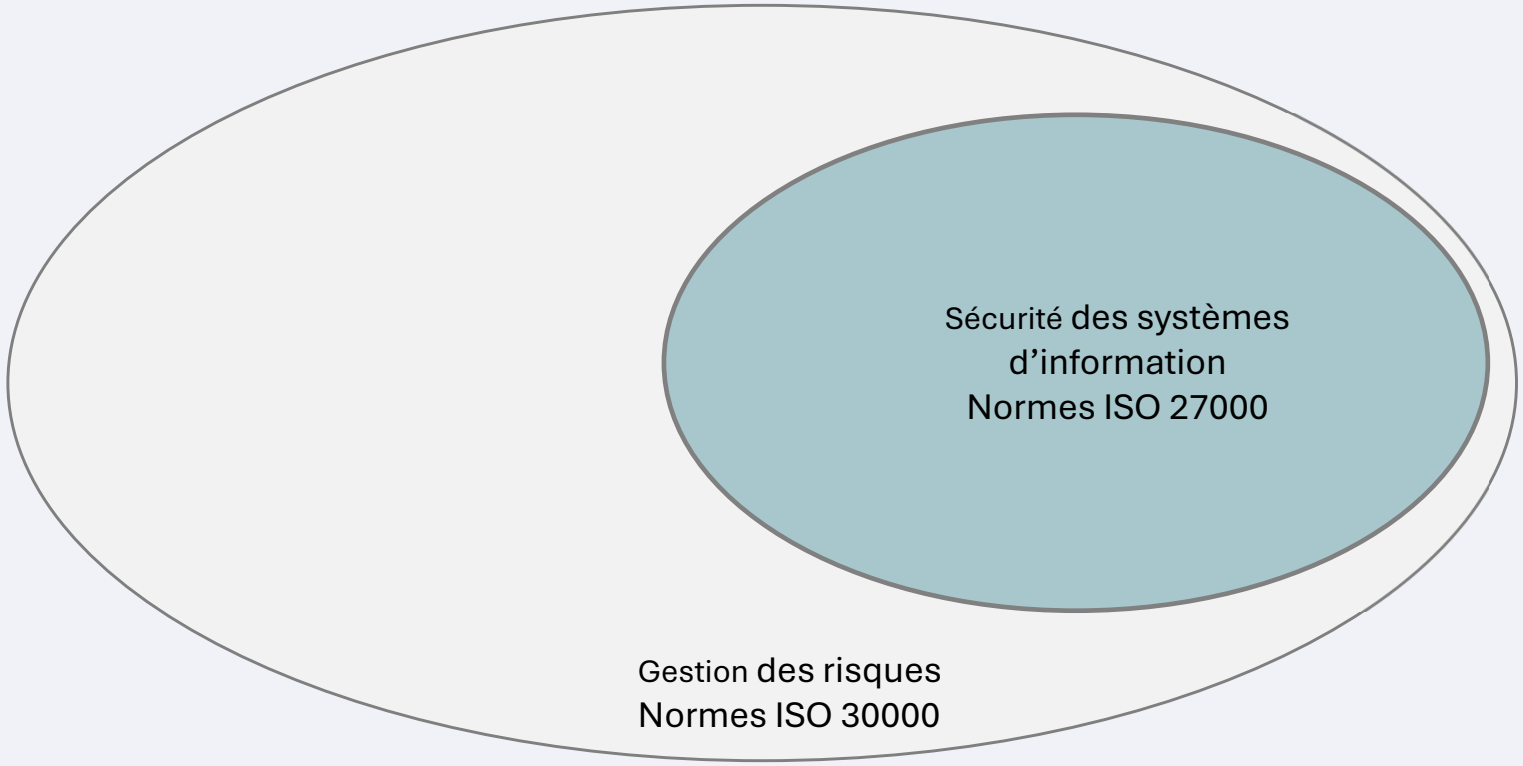
La sécurité des systèmes d'information (IT)

- La **sécurité des systèmes d'information** (systèmes IT) vise à assurer le bon fonctionnement, la confidentialité et l'intégrité des systèmes informatiques de gestion des entreprises → les normes ISO 27000 ont été conçues à cet effet

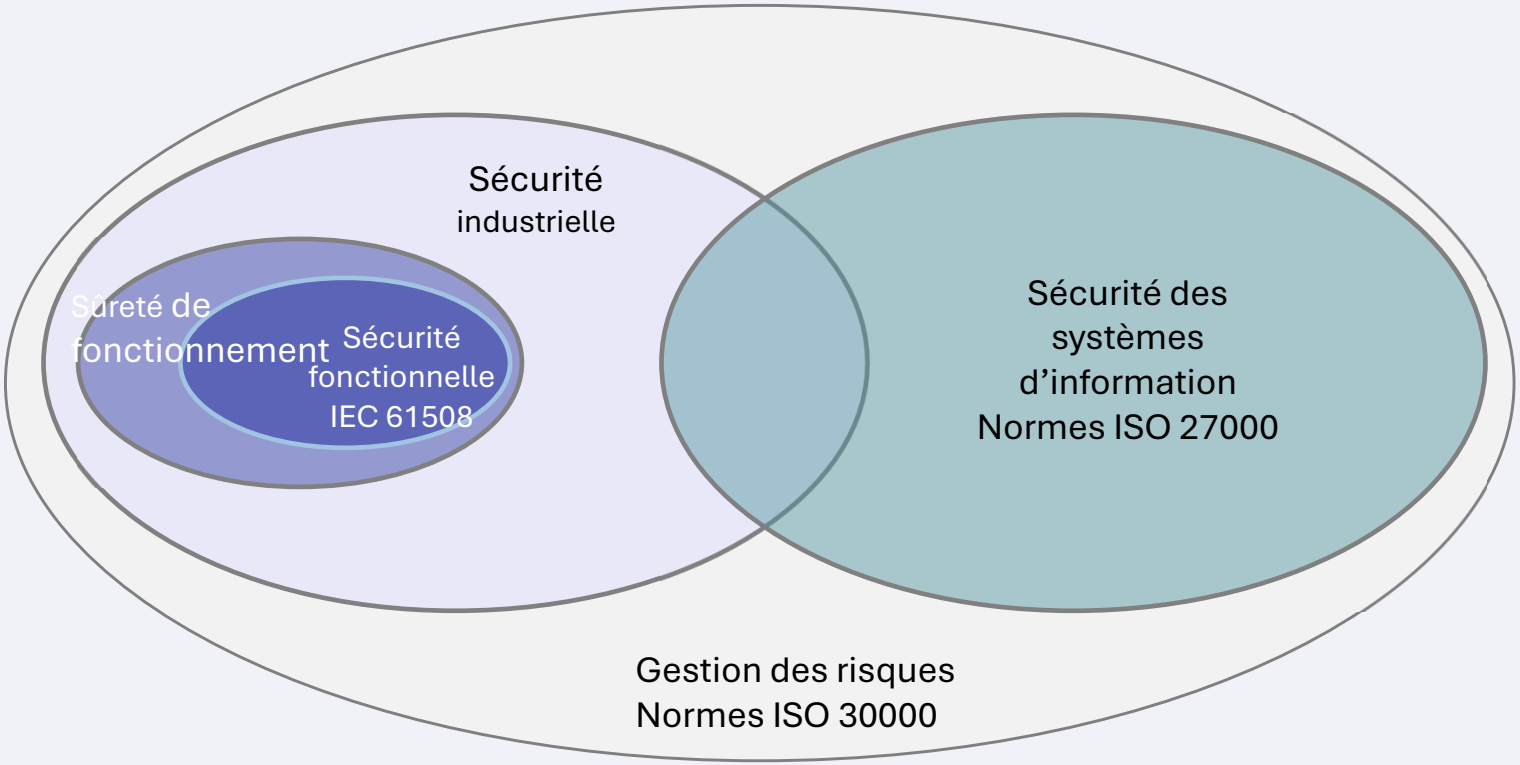


- Les **Operational Technologies (OT)** désignent l'ensemble des techniques servant à provoquer, détecter, faciliter, contrôler le changement d'une entité physique grâce à des équipements et systèmes d'automatisme et de contrôle.

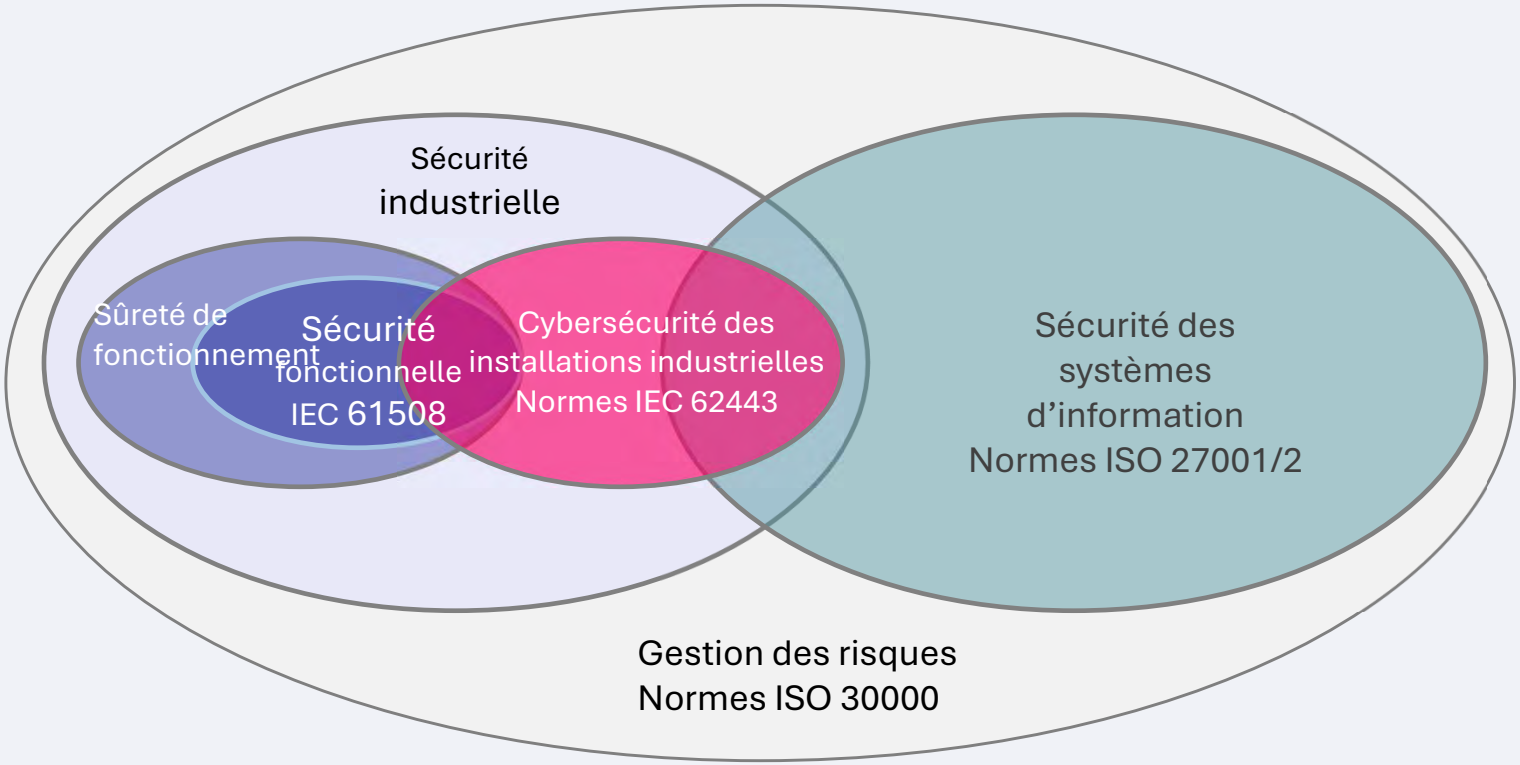
La sécurité des systèmes d’information



L’interpénétration des périmètres



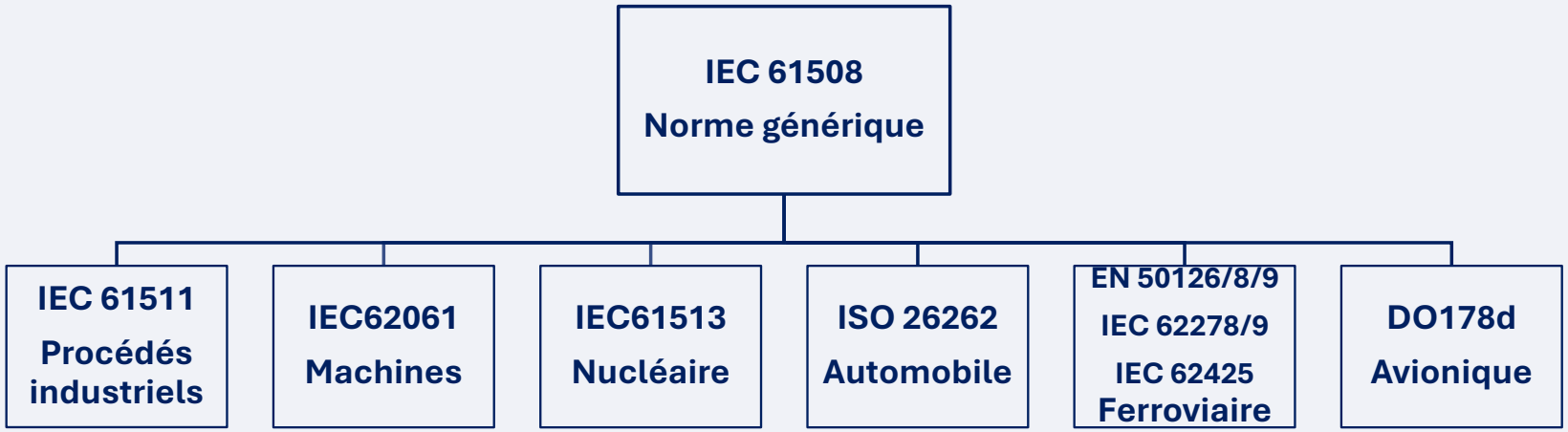
La cybersécurité s’appuie sur les deux piliers préexistants



Cybersécurité et sécurité fonctionnelle

La démarche de l'IEC 61508

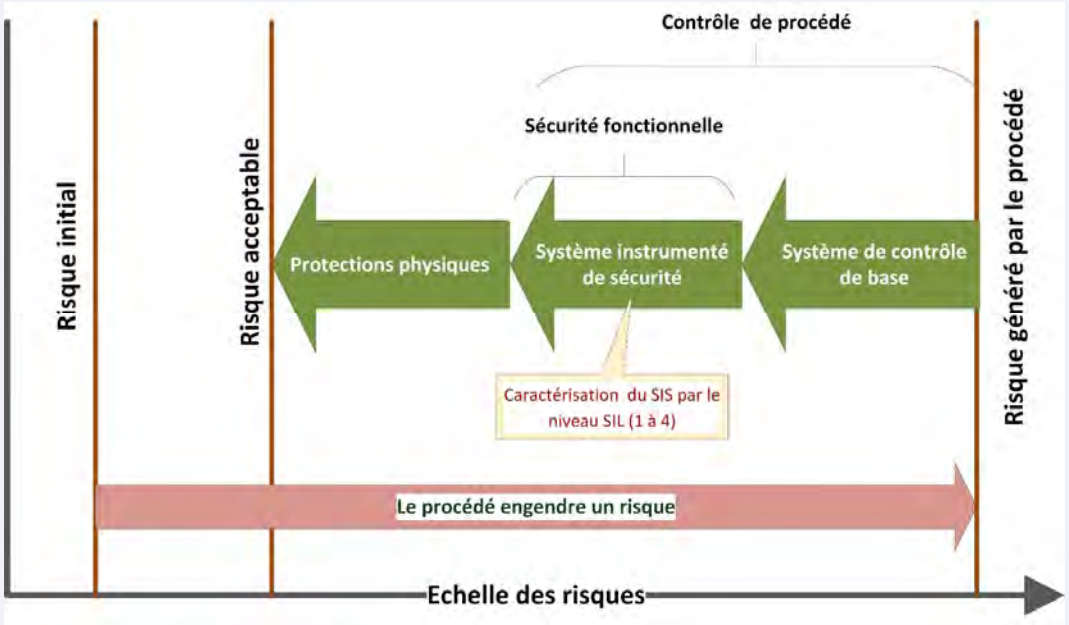
Principales normes de sécurité fonctionnelle



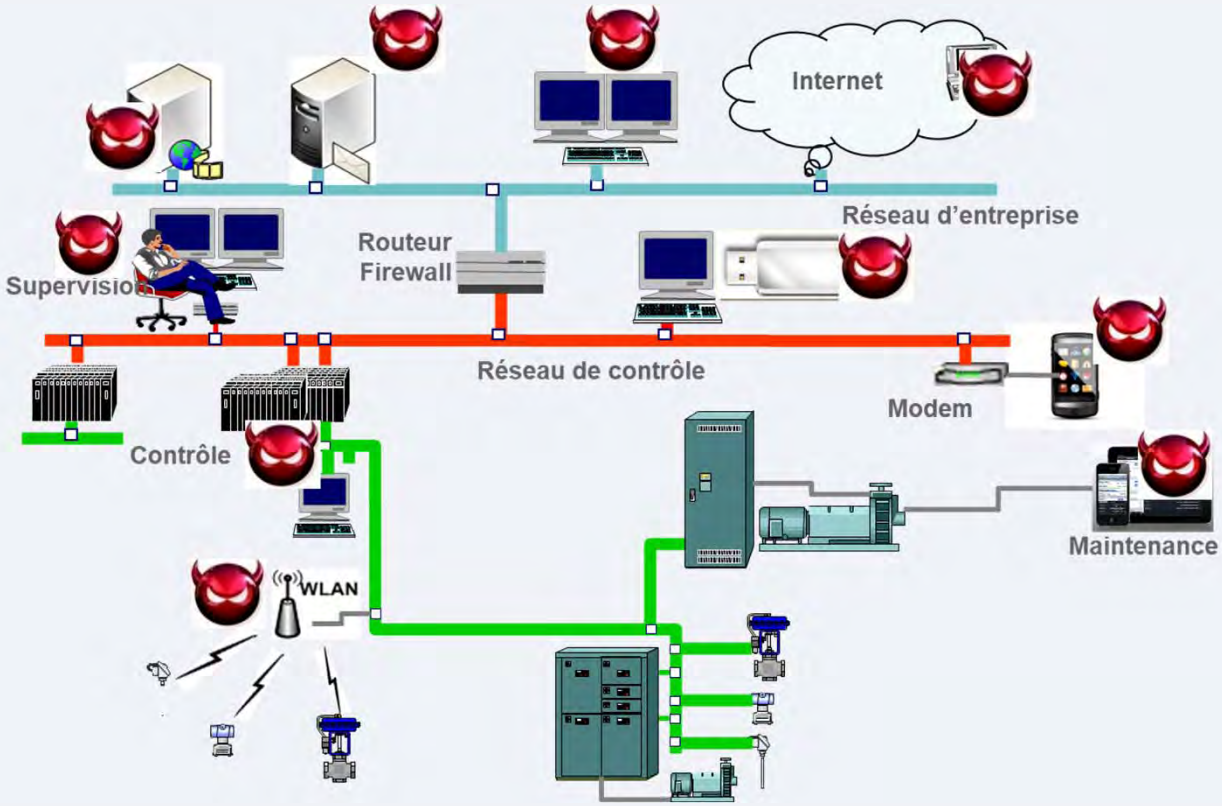
Normes sectorielles

Les systèmes instrumentés de sécurité

- Les systèmes instrumentés de sécurité (SIS) (Safety instrumented systems) sont un moyen de se rapprocher du niveau de risque tolérable en remplissant certaines fonctions de sécurité. Ils permettent de mettre en sécurité un système dès qu'un risque est détecté



Les IACS offrent de nombreux points d'entrée



De fortes différences entre les mondes OT et IT

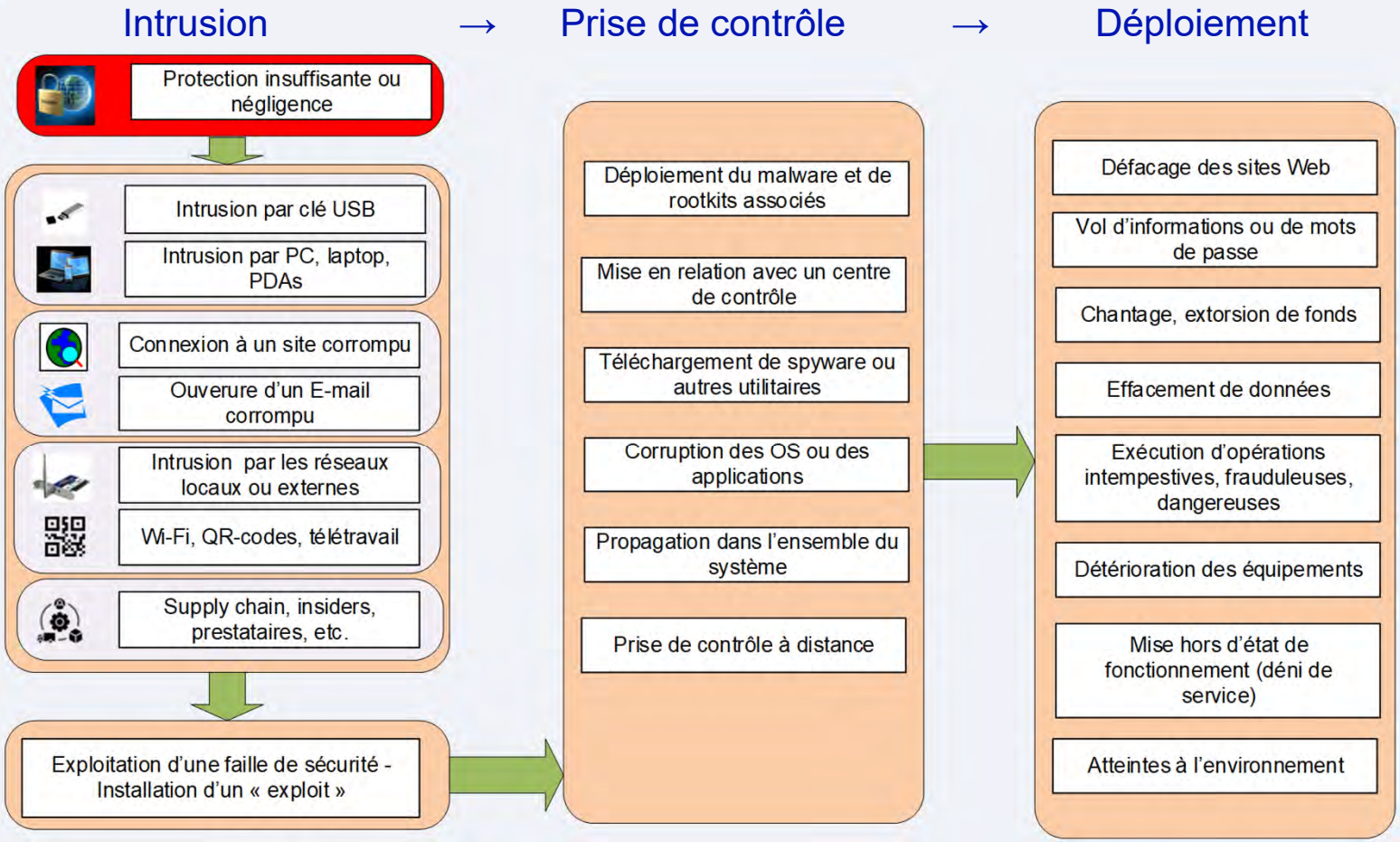
	IT	Systèmes de contrôle industriel
Temps de réponse	Impact limité des contraintes du procédé	Doit être adapté à la dynamique du procédé : s, ms….
Disponibilité	Admise occasionnellement	Interruptions généralement intolérables
Confidentialité des données	Essentielle	Généralement moins importante
Intégrité (données, configurations, logiciel…)	Critique	Critique
Durée de vie technologique	3 – 5 ans	20+ ans
Mises à jour et modifications	Régulières et souvent périodiques	Mons fréquentes – Plus difficiles Généralement ponctuelles
Anti-virus	Usuels	Peuvent générer des effets secondaires : aspects temps réel, disponibilité…
Conscience des enjeux de cybersécurité	Bonne	Assez faible mais en voie d'amélioration
Conscience des enjeux de sécurité fonctionnelle	Faible	Bonne (SIS, niveaux SIL…)
Granularité des analyses de risques	Grossière	Fine (au niveau de la boucle de contrôle)

Partie 1 : Comprendre la menace

Comprendre la menace pour savoir y faire face

- Les trois séquences des attaques
- Les modes d'intrusion
- Zoom sur les rançongiciels
- L'évolution des attaques et les tendances récentes
- Les groupes criminels (APT)

La schématique des principales attaques reste fondée sur trois séquences

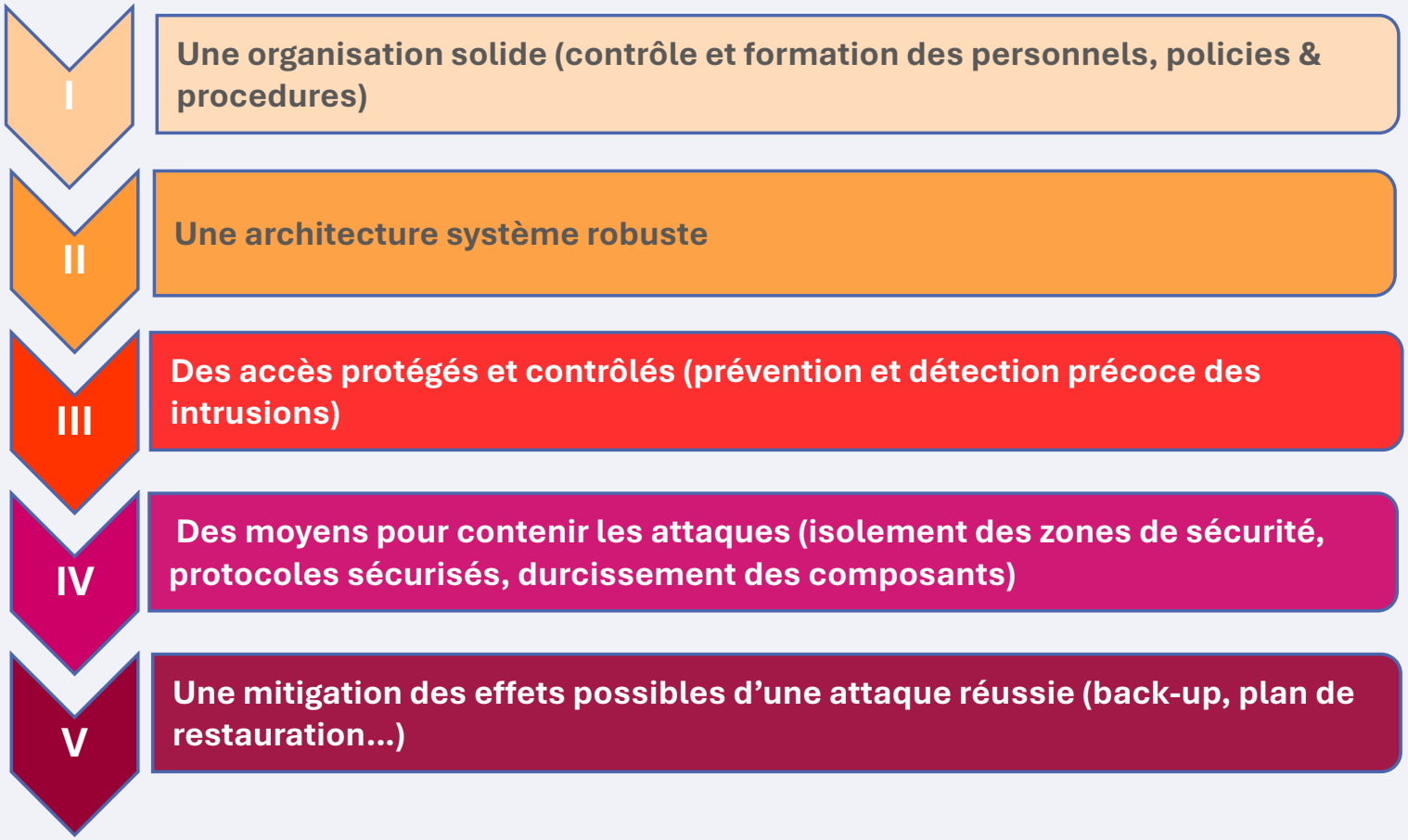


Partie 2 : l'IEC 62443

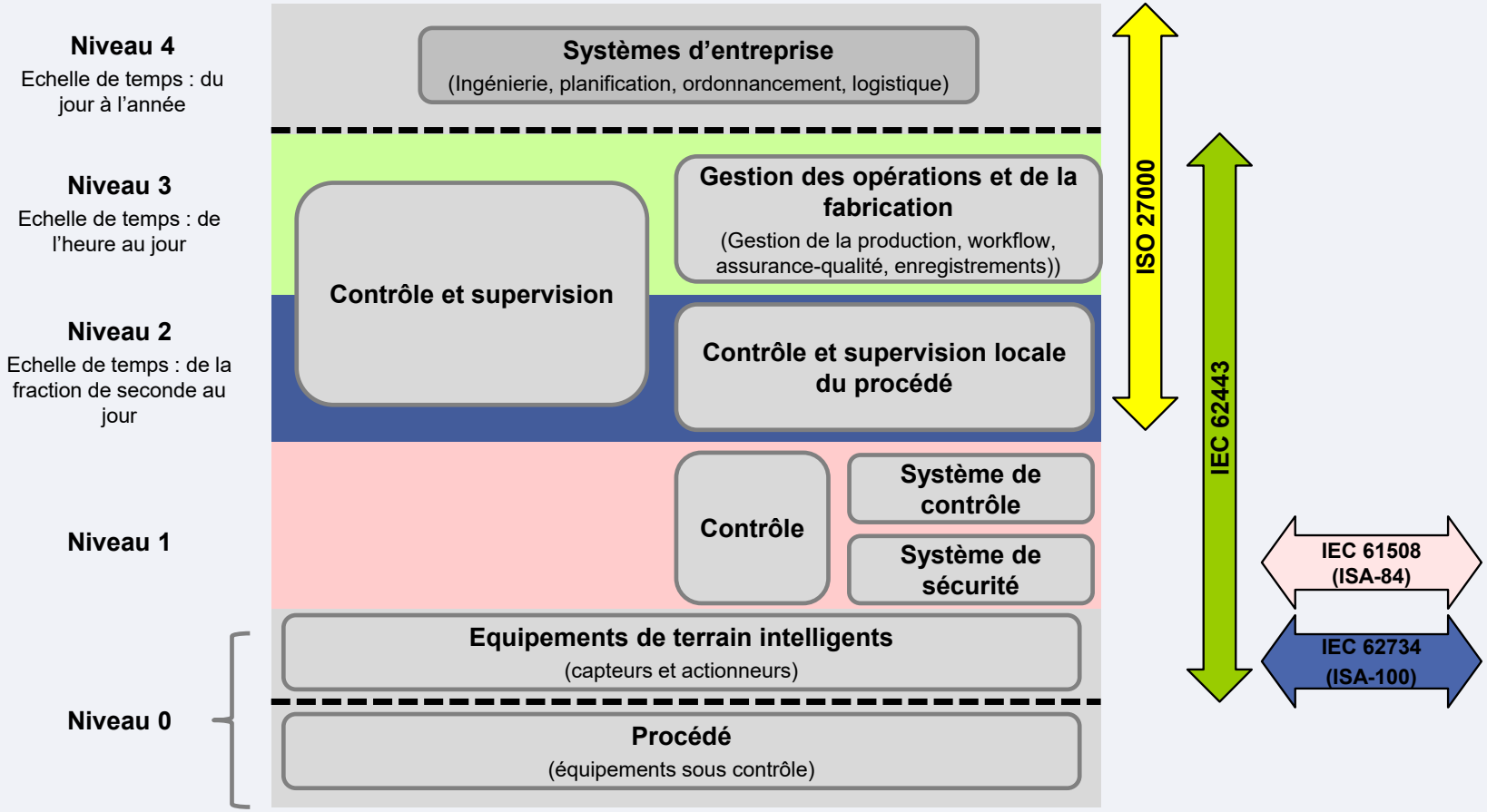
La notion de programme de sécurité – Les référentiels

- Notion de sécurité programme
- Les référentiels
  - Normatifs, indicatifs, réglementaires, d'entreprises
  - Nationaux, internationaux
  - Génériques, spécifiques

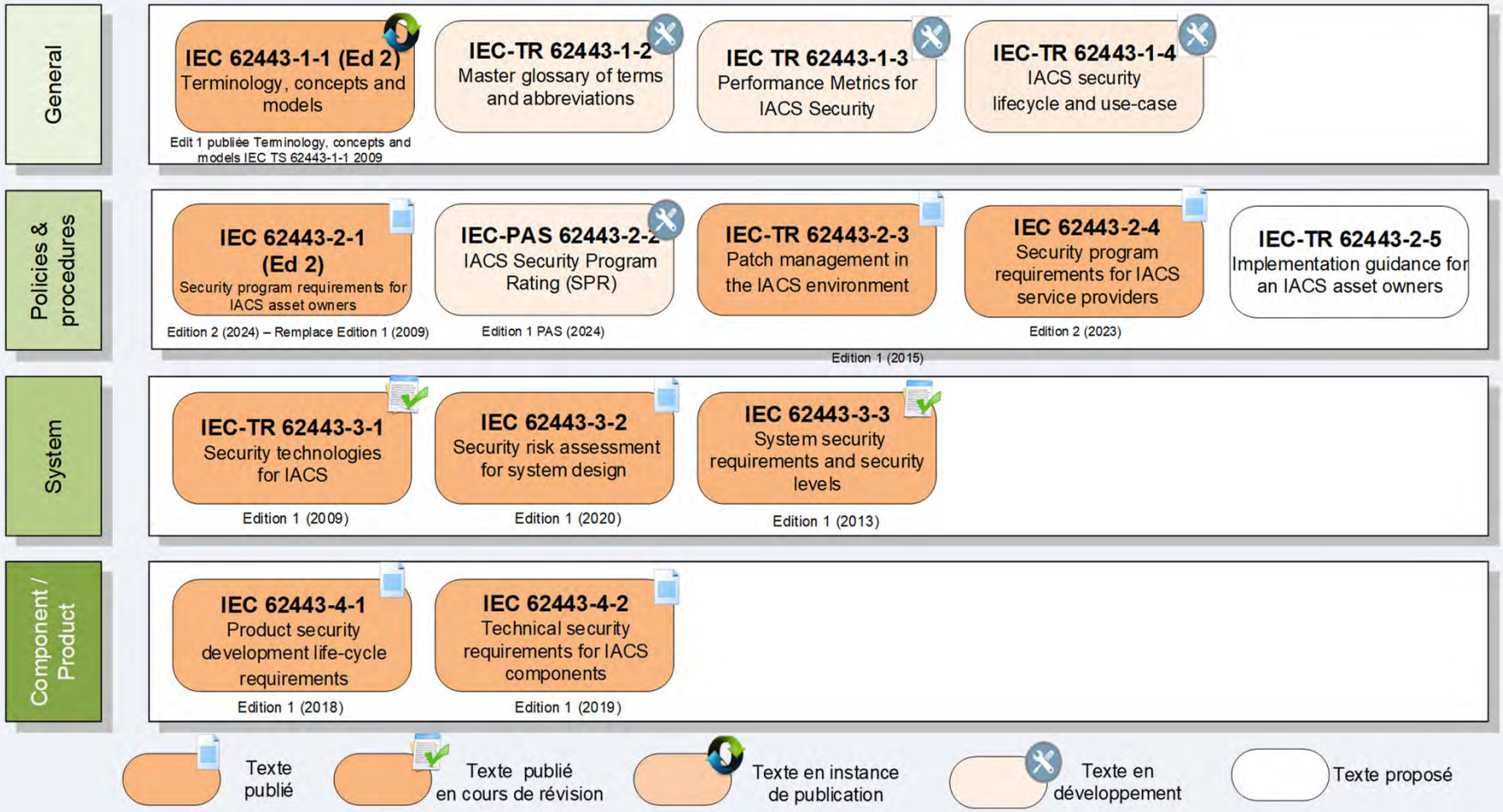
Un système de protection demande une approche méthodique



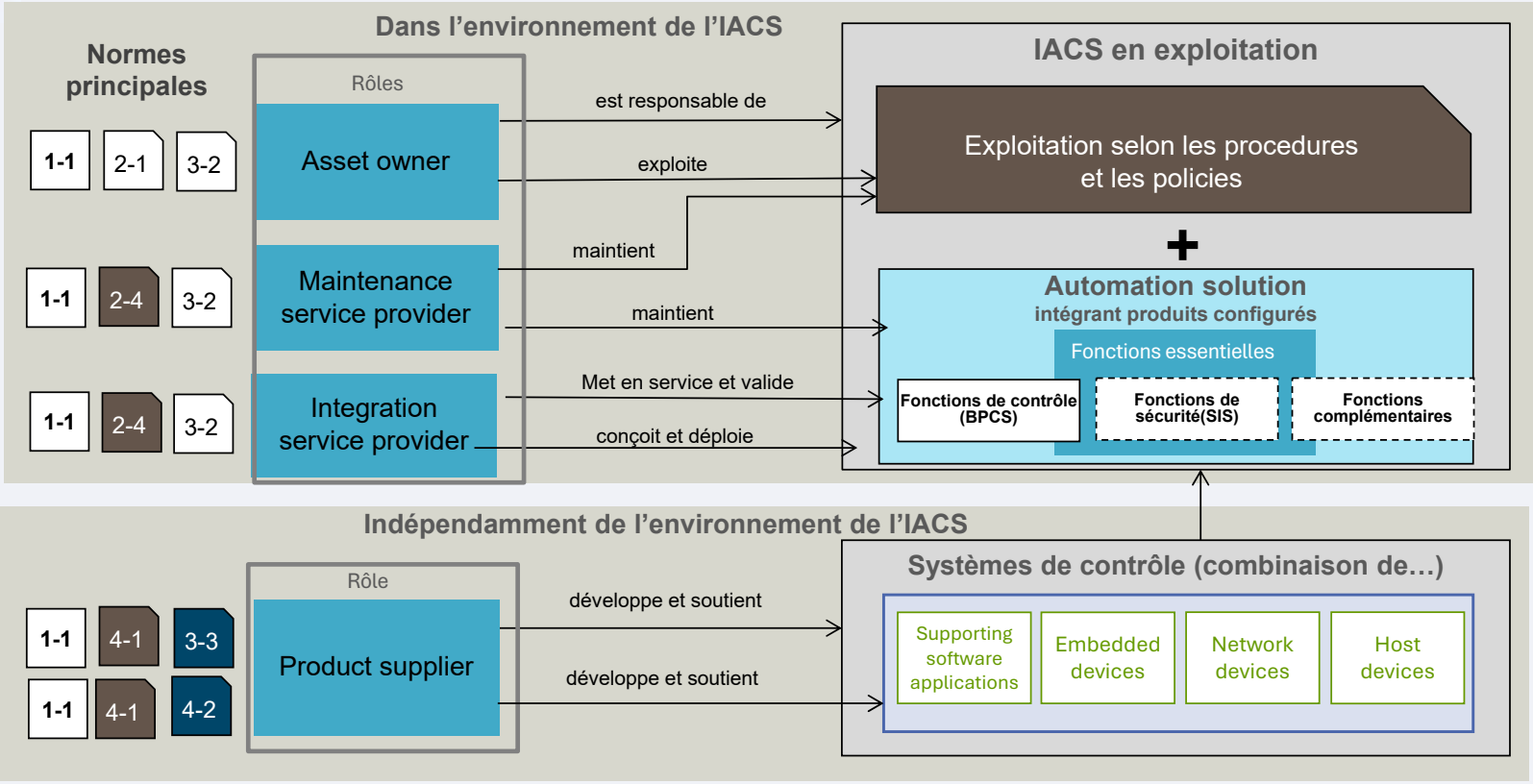
Positionnement du standard IEC 62443 vis-à-vis des principales normes de sécurité



Structure documentaire IEC 62443 (au 1er janvier 2025)



Rôles, responsabilités et standards



Exigences sur les process (organisationnelles)

Exigences sur les capacités techniques

Exigences générales

Déterminer les SL-T : approche qualitative

- Le niveau de risque non mitigé permet de déterminer le niveau de sécurité objectif (SL-T) à assigner à chacune des zones et conduits
- Risques non mitigés → SL- T
- Les SL-T sont une expression du degré de protection à implémenter dans chaque zone pour ramener le risque initial à un niveau acceptable

		Criticité des conséquences			
		Pas d'impact	Mineure	Majeure	Très sévère
Probabilité	Haute	Risque moyen	Risque élevé	Risque très élevé	Risque très élevé
	Moyenne	Risque moyen	Risque élevé	Risque très élevé	Risque très élevé
	Faible	Risque faible	Risque moyen	Risque moyen	Risque élevé
	Très faible	Risque faible	Risque faible	Risque moyen	Risque élevé

Informatif

Attention : Dans le choix des SL-T, tenir compte du coût des contre-mesures (itération nécessaire)

Niveau de risque et SL correspondant		Criticité des conséquences			
		Pas d'impact	Mineure	Majeure	Très sévère
Probabilité	Haute	SL-T 2	SL-T 3	SL -T 4	SL -T 4
	Moyenne	SL-T 2	SL-T 3	SL -T 4	SL -T 4
	Faible	SL-T 1	SL-T 2	SL-T 2	SL-T 3
	Très faible	SL-T 1	SL-T 1	SL-T 2	SL-T 3

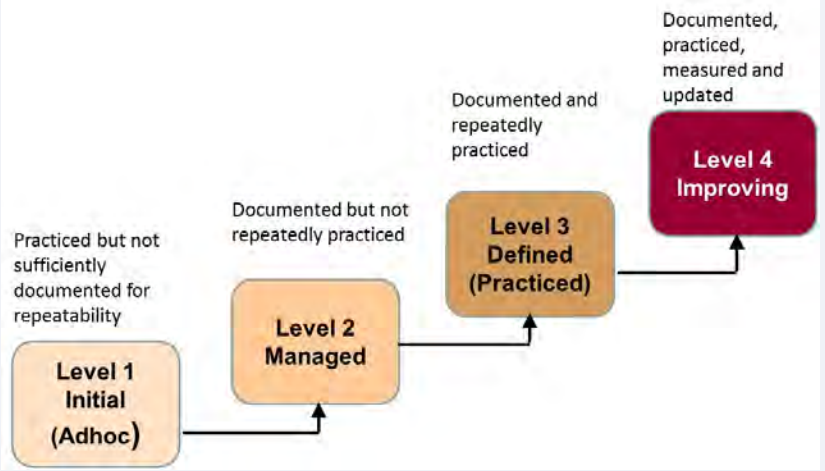
Rappel : maturity levels et security levels

- **Security level :** caractérise la capacité technique d'un composant ou d'un système (ou par extension d'une Automation Solution) à permettre d'atteindre un niveau de sécurité donné au niveau d'un IACS en opération

  Les Security Levels sont évalués selon l'IEC 62443-3-3 (systèmes) et - 4-2 (composants)

- **Maturity level** : caractérise la maîtrise d'une pratique de cybersécurité, dans un domaine donné, par les intervenants sur une installation donnée (concept introduit dans 62443-1-1 et utilisé dans 62443-2-4, -2-1 et -4-1)

Pas de SL (SL-0)	•Protection inférieure au niveau 1
SL-1	•Protection contre des violations usuelles ou de pure coïncidence
SL-2	•Protection contre des violations intentionnelles utilisant des ressources simples
SL-3	•Protection contre des violations intentionnelles utilisant des moyens sophistiqués
SL-4	•Protection contre des violations intentionnelles utilisant des ressources très étendues



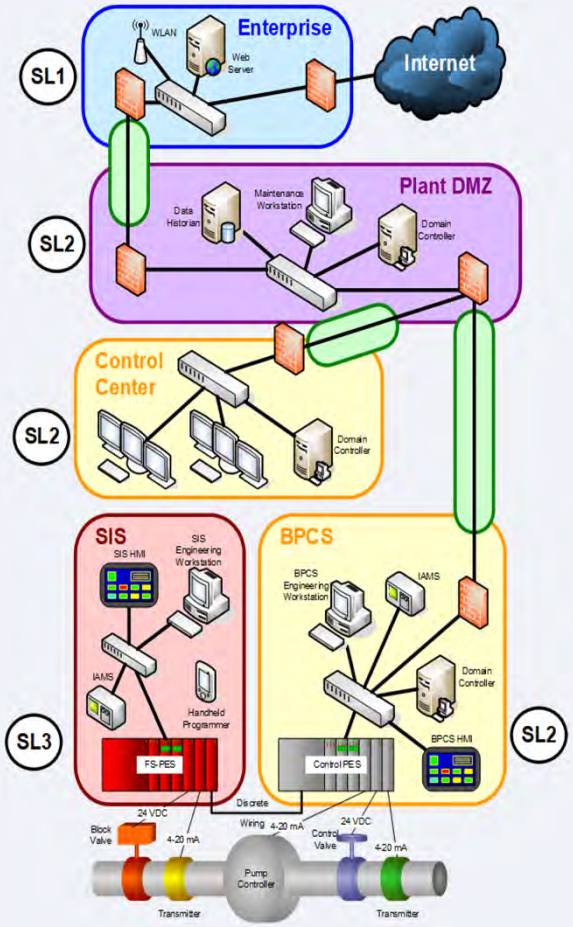
Nota : définitions résumées

Ce que l'IEC 62443 permet de certifier

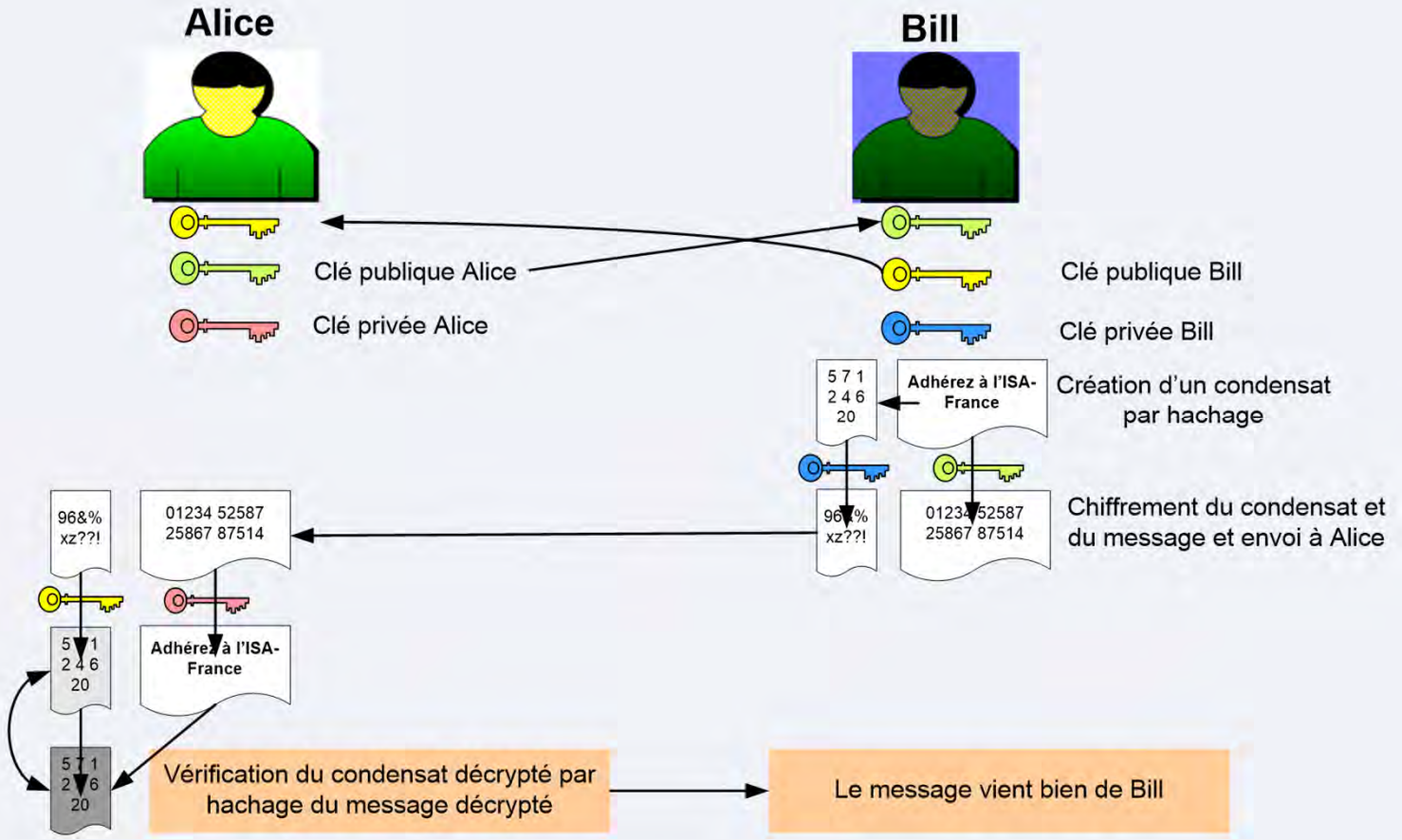
Standard	Objet de la certification
62443-2-4	Fournisseurs de service d'intégration et de maintenance
62443-3-3	Systèmes de contrôle (en tant que « produits »)
62443-4-2	Composants (contrôleurs : automates, RTUs…, stations de travail, composant réseaux, logiciels d'application)
62443-4-1	Fournisseurs de produits (procédures de développement)
En développement	
62443-2-1 et 62443-2-2	Certification du niveau de sécurité atteint par une installation en exploitation

Analyse de l’architecture 1 : air gappée

Foundational requirements	Analyse
IAC (identification et contrôle d’accès)	Les zones BPCS et SIS disposeront de contrôles d’accès et de système d’identification distincts. Les mots de passe ou jetons utilisés devront être distincts. Le système de contrôle d’accès de la zone SIS ne doit laisser passer que les personnels autorisés et dûment formés au système.
UC Contrôle des droits d’utilisation	Les protocoles de contrôle d’accès des zones BPCS et SIS seront distincts. Les autorisations d’intervention sur le SIS doivent être limitées au personnel habilité et formé à cet effet.
SI Intégrité du système (données, traitements…)	Le SIS étant « air gappé » les atteintes à l’intégrité du système impliquent un accès physique. Des contre-mesures physiques peuvent réduire le risque d’accès non autorisé. Des signaux corrompus en provenance du BPCS via la liaison câblée ne doivent pas perturber le SIS si celui-ci a été correctement mis en œuvre.
DC Confidentialité des données	L’accès aux données du SIS nécessite un accès physique au contrôleur ou à son réseau, à l’exception des liaisons câblées entre le SIS et le contrôleur du BPCS. Des contremesures d’accès physique peuvent réduire le risque de perte de la confidentialité des informations.
RF -Segmentation du système – Restriction des flux de données	Le SIS est dans une zone physiquement segmentée des autres zones. La frontière de la zone et les échanges de données sont strictement contrôlés. Les accès à partir de media mobiles doivent être rigoureusement contrôlés.
TRE Temps de réponse aux événements	Le temps de réponse à des violations de la sécurité est largement dépendant du contrôle physique des accès. Le réseau du SIS doit être surveillé afin de pouvoir analyser, au moins a posteriori, les causes éventuelles de fonctionnements anormaux qui pourraient être détectés et liés, par exemple, à des insuffisances dans le management des media portables.
RA Resource availability	En l’absence de connexion à Internet, une attaque en déni de service est hautement improbable, sauf connexion organisée de façon délibérée supposant une intrusion. Des ruptures de communication peuvent cependant survenir comme dans tout autre système.

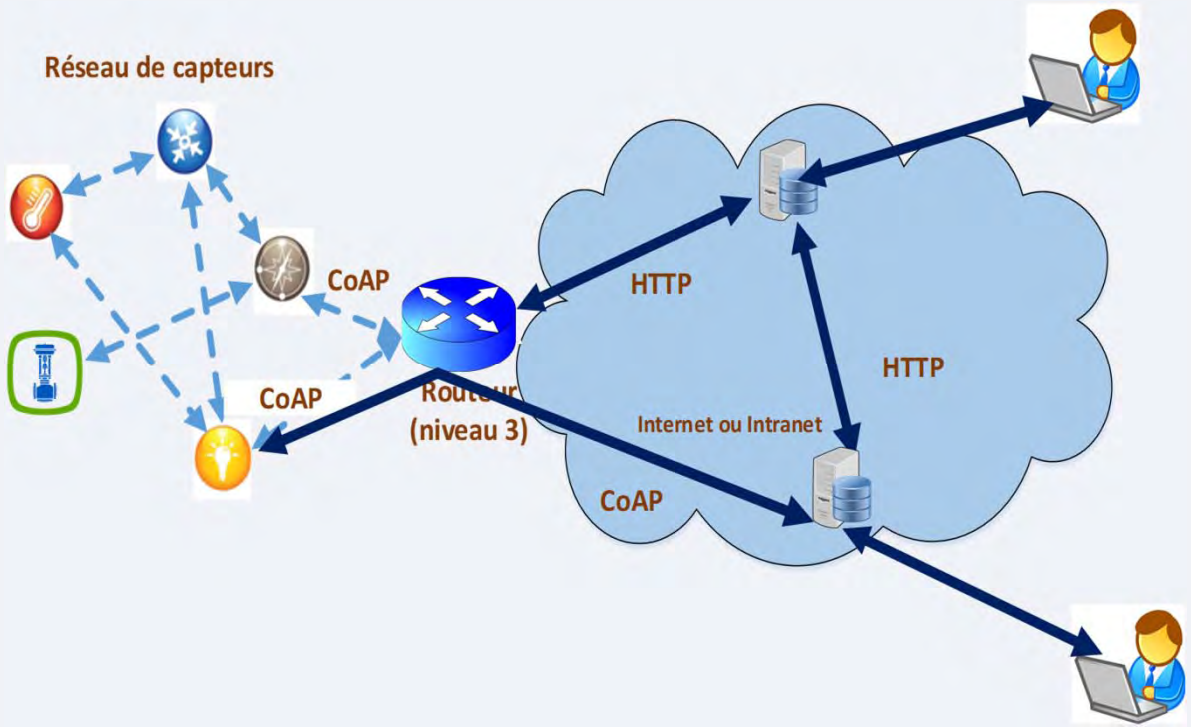


Authentification des messages par clé asymétrique



Sécuriser les éléments critiques

- La sécurisation du routeur de bordure devient primordiale, surtout s'il supporte des traitements en edge computing



Conclusions

ANNEXES

Un didacticiel Automation Hub

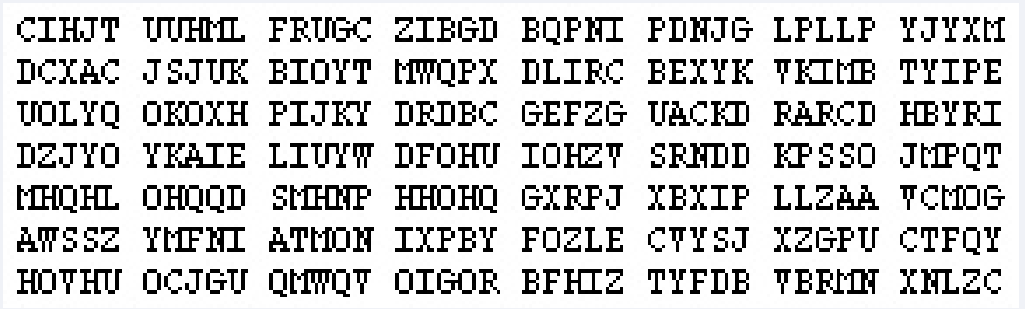
Janvier 2025

Annexe 2
Standards et réglementations

Annexe 3
Aperçu sur les techniques de chiffrement

Le chiffrement

- Le chiffrement, ou cryptage, des messages a pour objet de rendre leur compréhension quasiment impossible par ceux qui ne détiennent pas la clé du chiffrement.
- Le chiffrement consiste à appliquer une fonction F paramétrable par k à un message M, de façon que le message, une fois chiffré, **C = F(k, M)** ne puisse être déchiffré que par les personnes connaissant l'algorithme de chiffrement F et la clé k.



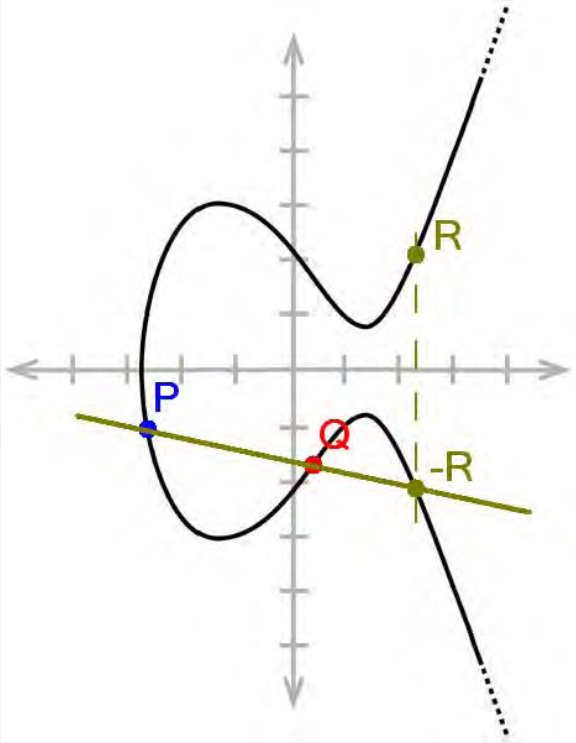
```
CIHJT UUHML FRUGC ZIBGD BQPNI PDNJG LPLLP YJYXM
DCXAC JSJUK BIOYT MWQPX DLIRC BEXYK YKIMB TYIPE
UOLYQ OKOXH PIJKY DRDBC GEFZG UACKD RARCD HBYRI
DZJYO YKAIE LIUYW DFOHU IOHZY SRNDD KPSSO JMPQT
MHQHL OHQQD SMHNP HHOHQ GXRPJ XBXIP LLZAA YCMOG
AWSSZ YMFNI ATMON IXPBY FOZLE CYYSJ XZGPU CTFQY
HOYHU OCJGU QMWQY OIGOR BFHIZ TYFDB YBRMN XNLZC
```

- Un algorithme de chiffrement F, pour pouvoir fonctionner, suppose qu'il soit possible de recalculer M à partir de C, dont qu'il existe une fonction G telle que **G (k, C) = M**
- **Selon le principe de KercKhoffs (1883), l'algorithme doit être supposé publiquement connu. Donc, ce sont les clés qui doivent rester secrètes.**

Aperçu sur le chiffrement par courbes elliptiques

- Ces méthodes utilisent les propriétés des courbes elliptiques du type $y^3 = x^3+ax+b$ sur lesquelles on peut définir une opération **P*Q = R** (symétrique de **–R**)
- Cette opération définit une loi de groupe
- Les courbes elliptiques et la loi de groupe associée peuvent être définies sur un ensemble fini **K**. La taille du corps fini K va déterminer la taille des clés
- Le chiffrement par courbes elliptiques repose sur le postulat que la résolution du problème du logarithme discret sur le groupe d'une courbe elliptique est un problème plus difficile que le problème similaire avec les entiers modulo n
- On estime qu'une clé de 200 bits (qui mesure, pour une courbe elliptique, la taille du corps fini K de cette courbe) pour les chiffres basés sur les courbes elliptiques est plus sûre qu'une clé de 1024 bits pour le RSA
- Les calculs sont plus simples qu'avec RSA et la solution qui en résulte offre une sécurité accrue.

Nota : Le problème du logarithme discret de x sur un groupe cyclique fini (par exemple les entiers modulo n), est l'inverse de l'exponentiation. Il consiste à rechercher, pour b donné, le plus petit entier k tel que $x = b^k$



Annexe 4
Exemples de scénarios d’attaque sur l’IoT

Annexe 5
Une check-list pour se préparer la construction d’un programme de sécurité

Merci de votre attention

www.automation-hub.fr

Pour tout renseignement complémentaire :
jean-pierre@automatio-hub.fr

Un didacticiel Automation Hub

Janvier 2025