ISA France

Setting the Standard for Automation™

L'IEC 62443 (ISA-99)

CYBER-SECURITE DES AUTOMATISMES ET DES SYSTEMES DE CONTRÔLE DE PROCEDE

Sommaire

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

Tous droits réservés 2022

Un didacticiel ISA-France - Version 17.7 Janvier 2022– Tous droits réservés

Droits d'exploitation

Vous avez acquis auprès de l'association ISA-France le droit d'exploiter, en version mono-utilisateur, le didacticiel « L'IEC 62443 (ISA-99) - CYBER-SECURITE DES AUTOMATISMES ET DES SYSTEMES DE CONTRÔLE DE PROCEDE » dont ISA-France détient les droits patrimoniaux. 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 ISA-France V17.4 (mai 2021) ».
- 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'ISA-France.

Responsabilités

- ISA-France apporte tout le soin possible à la préparation des informations délivrées dans les contenus qu'elle produit. 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

Tous droits réservés ISA-France et hauet.com 2021

L’auteur

Jean-Pierre HAUET, ancien Chief Technology Officer d’ALSTOM, Associate Partner de KB Intelligence, Président d’ISA-France, voting member du Comité ISA99

Tous droits réservés ISA-France et hauet.com 2021

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 spécifique de l'Internet des objets
- Proposer quelques annexes pour approfondissement éventuel

Tous droits réservés ISA-France et hauet.com 2021

Sommaire du document (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 cybersécuritaire : où trouver des informations ?

Partie 2 : l'IEC 62443 (ISA-99)

- La notion de programme de sécurité (CSMP ou SP) - L'utilité d'un référentiel
- Le comité de standardisation ISA99
- L'approche générale de l'IEC 62443

Tous droits réservés ISA-France et hauet.com 2021

Sommaire du document (2)

Partie 2 : L'IEC 62443 (ISA-99) (suite)

- 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
  - IEC 62443-4-2 : Technical security requirements for IACS components
  - IEC 62443-2-1 (ed 2) : Security program requirements for IACS asset owners
  - IEC 62443-2-2 (new)- Security protection ratings
- Evaluation et certification
  - Evaluation : des outils commencent à apparaître
  - La certification
  - IEC TR62443-1-4 : Exemples de détermination et d'analyse des zones et des conduits

Tous droits réservés ISA-France et hauet.com 2021

Sommaire du document (3)

Partie 3 : Se protéger

- Les mesures organisationnelles
- Les mesures techniques

Partie 4 : La problématique de l'Internet industriel des objets (IIoT)

- Exemples d'attaques sur l'IoT
- Comment protéger l'IoT

Conclusions

Annexes

- Annexe 1 : Rétrospective de quelques attaques
- Annexe 2 : Autres standards et réglementations
- Annexe 3 : Aperçu sur les techniques de chiffrement
- Annexe 4 : Une check-list pour se préparer la construction d'un programme de sécurité Annexe 2 : Recommandations de bon sens pour l'élaboration d'un programme de sécurité
- Annexe 5 : Liens utiles

Tous droits réservés ISA-France et hauet.com 2021

ISA France

Setting the Standard for Automation™

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

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

Tous droits réservés 2022

Un didacticiel ISA-France - Version 17.7 Janvier 2022– Tous droits réservés

ISA France

Setting the Standard for Automation™

Concepts généraux

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

Tous droits réservés 2022

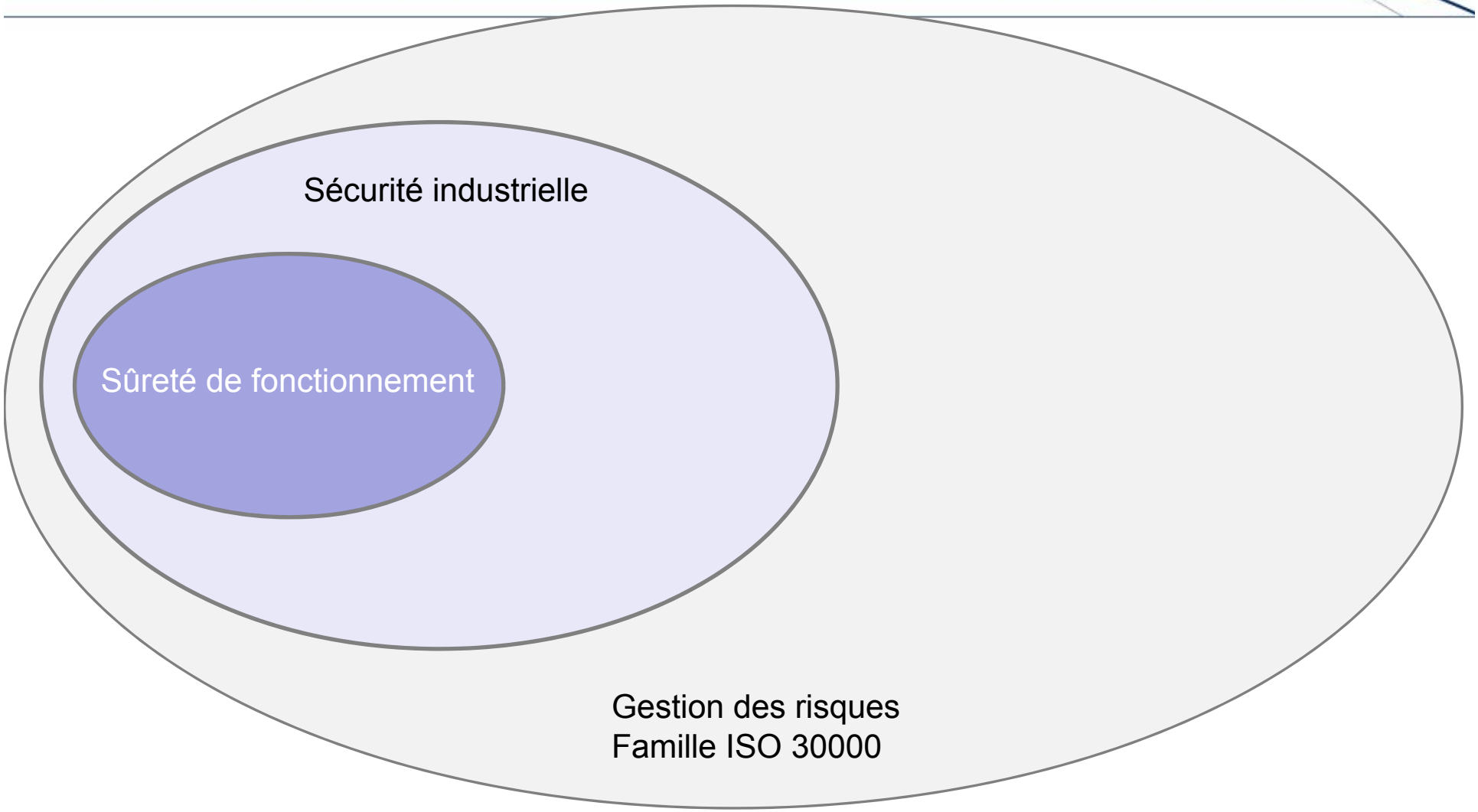
Un didacticiel ISA-France - Version 17.7 Janvier 2022 – Tous droits réservés

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 problématique 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 générale 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 « sûreté de fonctionnement » résulte de la combinaison de deux facteurs essentiels :
  - La disponibilité, elle-même fonction de la fiabilité (λ) et de la maintenabilité (μ)
  - La sécurité, correspondant à la protection contre les risques engendrés par l'activité considérée

Tous droits réservés ISA-France et hauet.com 2021

La sûreté de fonctionnement, composante de la sécurité industrielle



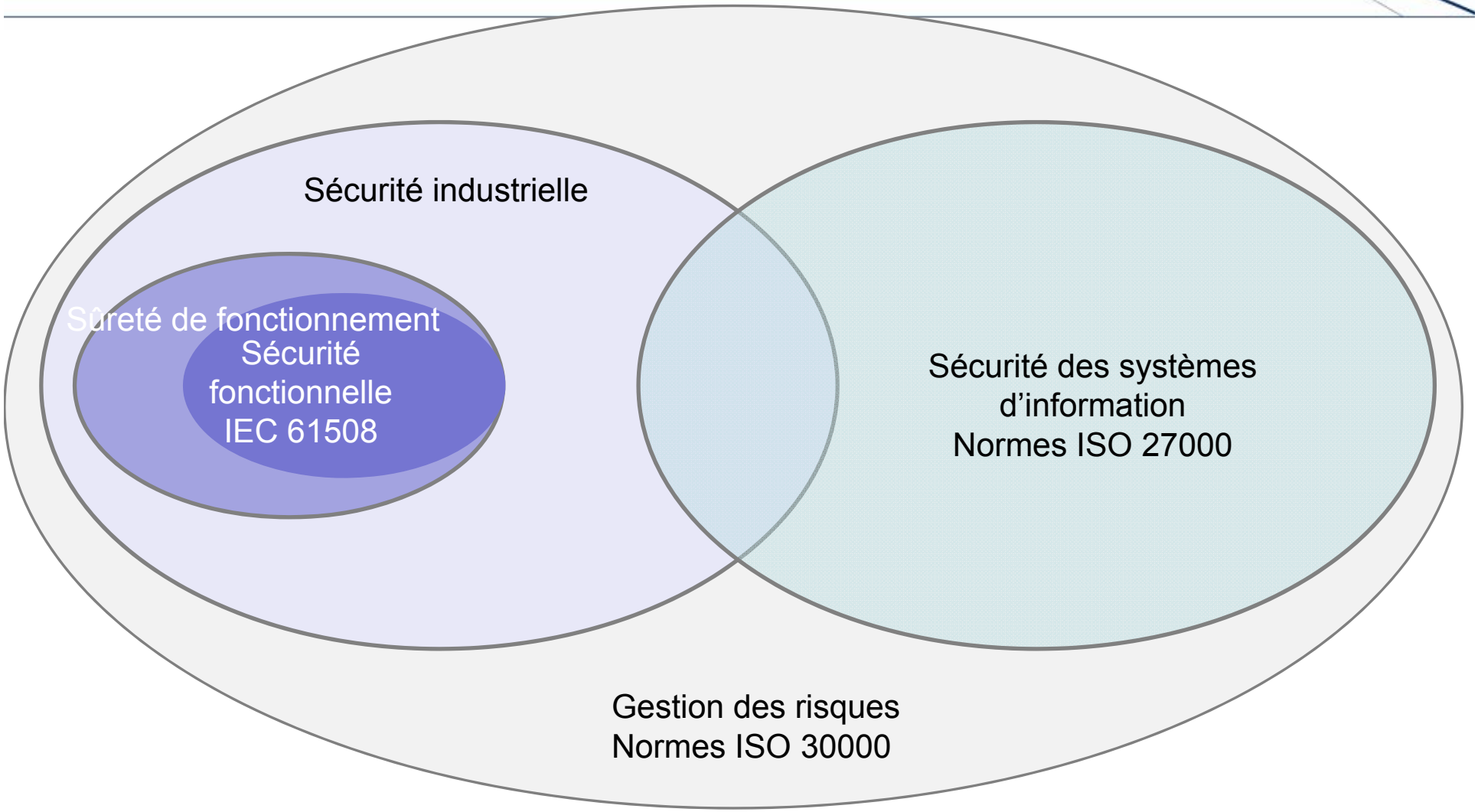
Tous droits réservés ISA-France et hauet.com 2021

Sécurité fonctionnelle et sécurité de systèmes d'information

- Plus récemment (années 1960 à 80), sont apparues deux notions nouvelles et, au départ, distinctes :
  - La **sécurité fonctionnelle**, 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 des systèmes d'information** (systèmes IT), visant à assurer le bon fonctionnement, la confidentialité et l'intégrité des systèmes informatiques de gestion des entreprises → normes ISO 27000
- La protection des systèmes informatiques industriels, la cybersécurité industrielle, était, jusqu'à une date récente, absente de ces deux préoccupations car les systèmes de contrôle industriel étaient considérés comme des ensembles isolés du monde extérieur et donc protégés

Tous droits réservés ISA-France et hauet.com 2021

L'interpénétration des périmètres



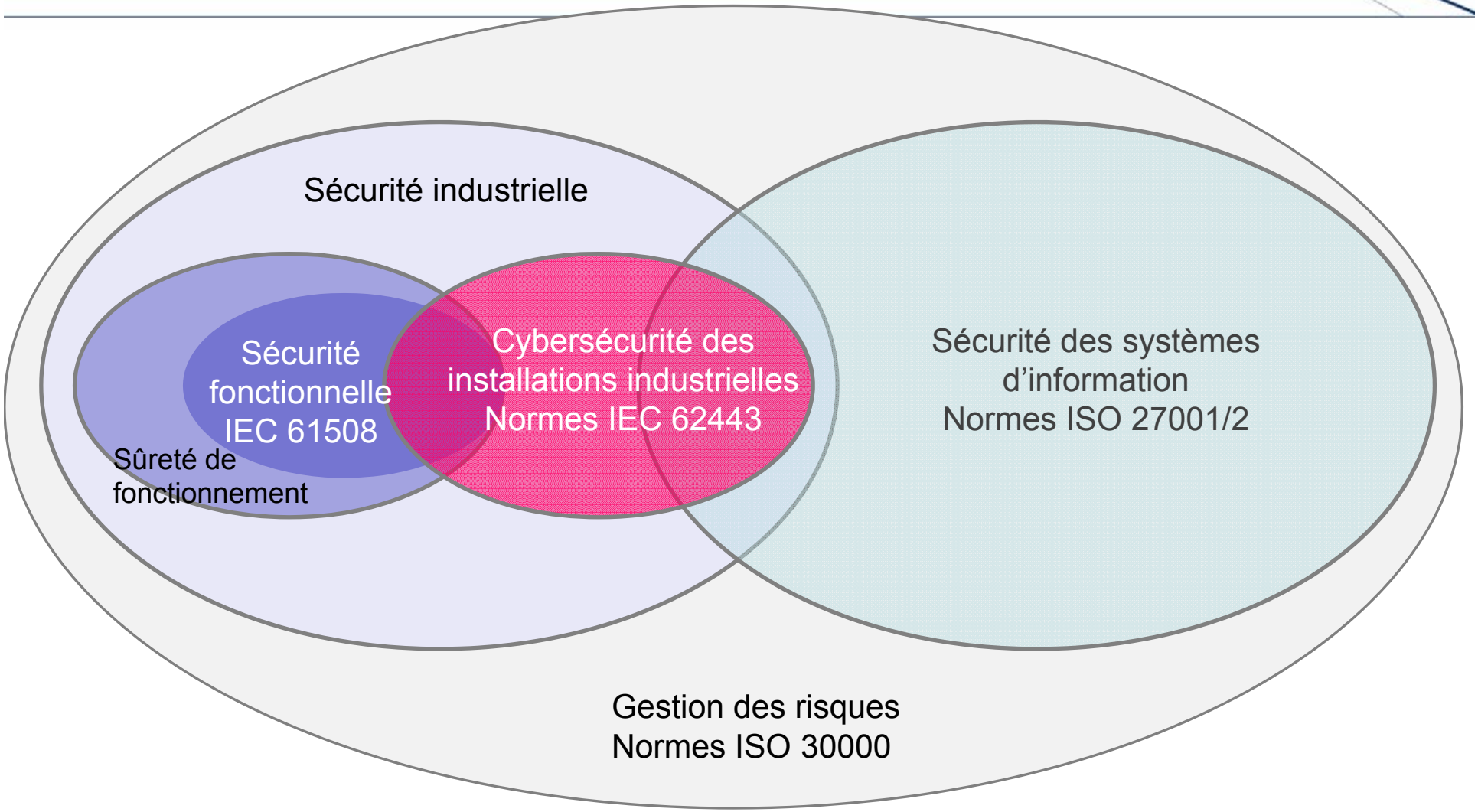
Tous droits réservés ISA-France et hauet.com 2021

Apparition de la cybersécurité industrielle

- La préoccupation de la cybersécurité des système de contrôle industriel (IACS : Industrial Automation Control System) est apparue au début des années 2000, notamment après l'attentat du 11 septembre 2001
- Les systèmes de contrôle étaient jusqu'alors considérés comme des installations professionnelles où les défaillances étaient l'exception ; peu d'installations étaient sécurisées.
- Mais si des terroristes étaient arrivés à se former au pilotage d'avions sophistiqués, il leur était a priori possible de s'initier au fonctionnement des systèmes contrôlant des **infrastructures stratégiques** : alimentation en eau, centrales et réseaux électriques, moyens de transport et autres installations sensibles
- Le syndrome du 11 septembre et des tests réalisés ont convaincu de la nécessité de se protéger contre le cyber-terrorisme, l'espionnage ou la simplement la malveillance : une nouvelle discipline est née qui donnera lieu à l'ISA-99 devenue IEC 62443

Tous droits réservés ISA-France et hauet.com 2021

Une nouvelle discipline



Tous droits réservés ISA-France et hauet.com 2021

Une discipline à part entière

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

Tous droits réservés ISA-France et hauet.com 2021

ISA France

Setting the Standard for Automation™

Quelques définitions

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

Tous droits réservés 2022

« Safety » et « Security »

En anglais :

- La **Safety** a trait aux mesures prises pour protéger un système de dommages inacceptables, qu'ils soient directs ou indirects (aux personnes et à l'environnement), résultent d'incidents ou d'accidents, **intentionnels ou non .** L'état qui en résulte est qualifié de « safe »..
- La **Security** a trait aux mesures prises (et à l'état qui en résulte) pour protéger un système contre des actes **intentionnés**.
- La **Cyber Security** apparait comme une rubrique de la Security. L'IEC 62443 la définit comme *« Measures taken to protect a computer or computer system against unauthorized access or attack »*

Safety = Functional safety + cyber security

Tous droits réservés ISA-France et hauet.com 2021

« Sûreté » et « Sécurité »

En français

- La **sécurité** est proche de la *Safety*. Vise l'ensemble des mesures et l'état qui en résulte pour se protéger contre les risques de toute nature : sociale, militaire, environnementale…
  - Mettre ses actifs « en sécurité » à la banque
  - Se mettre « en sécurité » en cas d'ouragan…
- Dans le domaine industriel, on parle de **sécurité industrielle**, incluant les aspects physiques, environnementaux, humains, etc.
- La **sûreté** présente des analogies avec la *Security* mais reste **un terme ambigu dont la signification dépend du contexte :**
  - Désigne souvent l'ensemble des actions visant à se prémunir contre des risques venant de l'extérieur, en particulier les attaques criminelles : sûreté de l'Etat
  - La sûreté nucléaire couvre un spectre de risques plus large
  - Dans le domaine industriel, on parle de « **sûreté de fonctionnement** » qui ne relève pas de démarches intentionnelles: « *Aptitude d'un système à accomplir les fonctions qu'on en attend, dans des conditions définies et durant un intervalle de temps donné* ».

Tous droits réservés ISA-France et hauet.com 2021

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 :** *Sous-ensemble de la sécurité globale, relatif aux équipements et aux systèmes de contrôle-commande associés, qui dépend du fonctionnement correct de systèmes électriques, électriques, 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)
- Les systèmes passifs ne relèvent pas de la sécurité fonctionnelle (ex : portes résistant au feu)
- La sécurité fonctionnelle, telle que définie initialement par l'IEC 61508, n'inclut pas la **cybersécurité**

Tous droits réservés ISA-France et hauet.com 2021

La cybersécurité des installations industrielles

- **Cybersécurité des installations industrielles** : *Sous-ensemble de la sécurité globale ayant trait à la prévention des risques associés aux intrusions dans un système d'automatisme ou de contrôle (**IACS : Industrial Automation and Control System**), liés à de possibles actions malintentionnées sur des équipements informatiques, des réseaux de communication, des logiciels ou des données*.
- La cybersécurité est une composante nouvelle de la sécurité industrielle aux côtés de la sûreté de fonctionnement et de la sécurité fonctionnelle.

Sécurité = Sécurité fonctionnelle + Cybersécurité

Tous droits réservés ISA-France et hauet.com 2021

Autres définitions utiles

Disponibilité : accessibilité des données et des équipements, en assurant leur utilisation avec des temps de réponses corrects. Dépend de la **fiabilité**, de la **maintenabilité** et de la **sécurité**.

Intégrité : assurance que les données, les traitements ou les services n'ont pas été modifiés, altérés ou détruits.

Confidentialité : protection des données contre une divulgation ou une écoute non autorisées. Elle implique deux actions complémentaires : le contrôle d'accès et le chiffrement.

Authentification : vérification de l'identité d'un utilisateur, d'un équipement ou d'une donnée.

Identification ➔ Authentification ➔ Autorisation d'accès

Non répudiation : assurance que la preuve de réception est délivrée à l'émetteur d'une information et que le receveur a reçu une preuve d'authenticité de l'émetteur de telle sorte qu'aucun d'entre eux ne peux nier la transaction.

Traçabilité : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables

Tous droits réservés ISA-France et hauet.com 2021

ISA France

Setting the Standard for Automation™

Cybersécurité et sécurité fonctionnelle

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

Tous droits réservés 2022

Un didacticiel ISA-France - Version 17.7 Janvier 2022 – Tous droits réservés