CRESITT INDUSTRIE

Centre de Ressources
Technologiques en Électronique

Cybersécurité : Focus extension IEC 62443-4-2
Recommandations et leviers
Solutions matérielles électroniques

S. ROUXEL – 26 11 2020 – v 1.0

Réf du document : DT_PPT_SR_AtelierSecurisation_v1.0_20201006

Le CRT CRESITT est soutenu par :

L'action de diffusion technologique est cofinancée par l'Union européenne.
L'Europe s'engage en région Centre-Val de Loire avec le Fonds européen de développement régional.

SOMMAIRE

- Risques Cyber
- Directive IEC 62443-4-2
- Recommandations et leviers
- Solutions matérielles

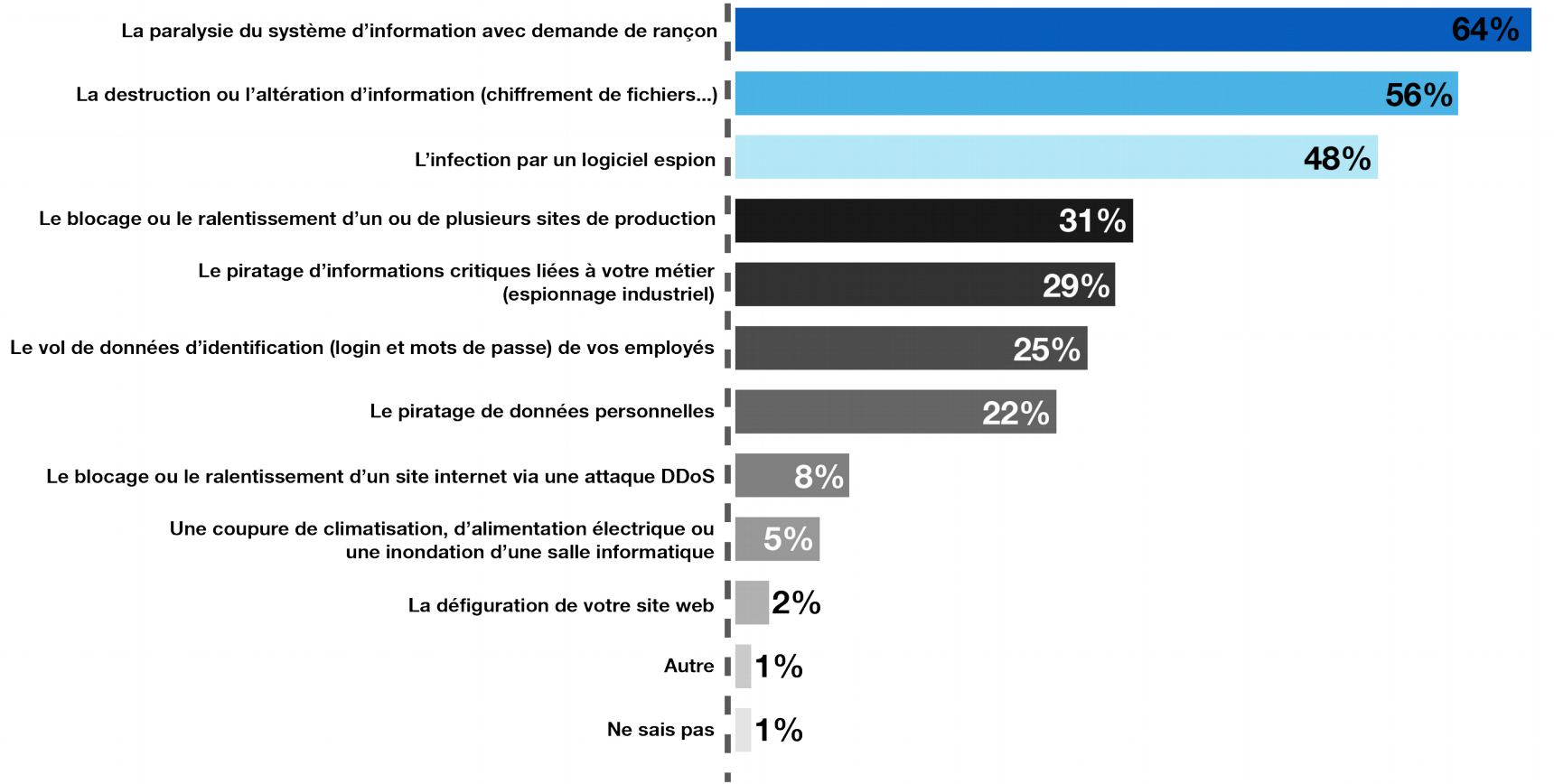
Risques Cyber

- Réalité de la menace
  - 2019 : 39 % grandes entreprises européennes victimes
  - 2020 : 67 % des entreprises françaises ont été touchées
  - Augmentation des pertes : 1,6Mds 2020 contre 1,1Mds 2019

  - Evolution des types d'attaque
    - DdoS, DoS
    - Ransomware
    - Malware (trojan, worms, virus)
    - Spambots
    - Backdoors
    - Hameçonnage
    - Destruction de données ….

src : hiscox, cyberexperts.tech, orangecyberdefense.com

Risques Cyber Redoutés

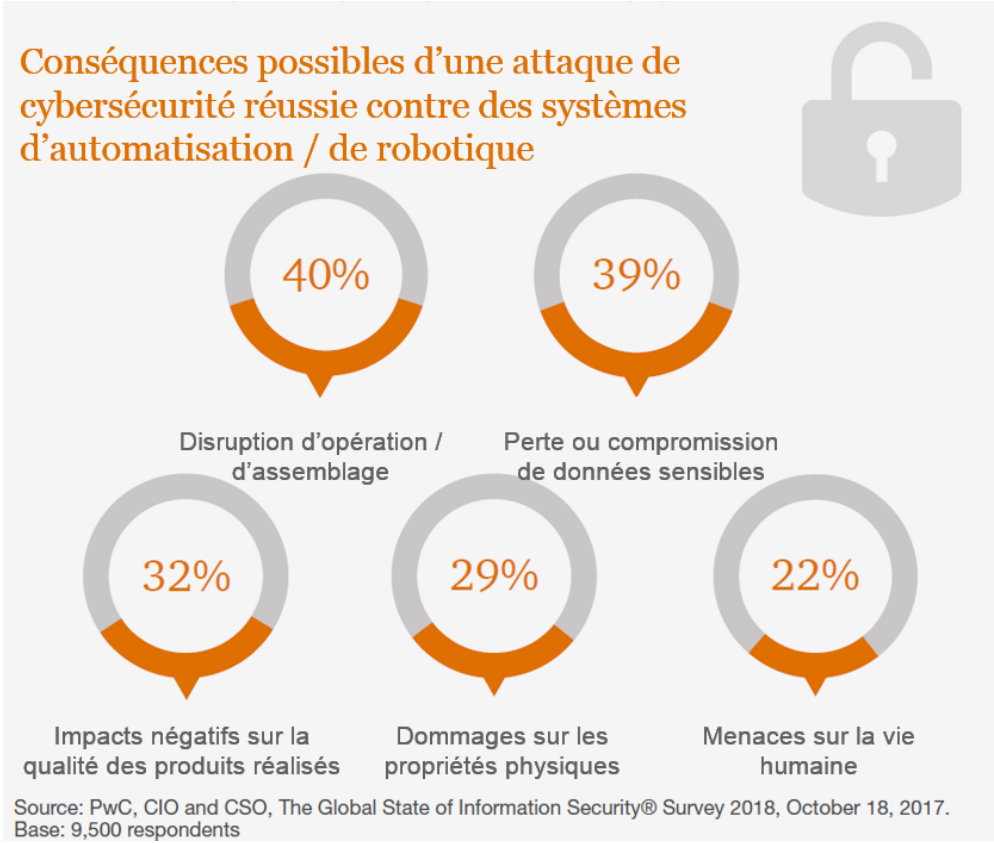


Sondage réalisé par Orange Business Services, L'Usine Nouvelle et B2B Intelligence, 2018.

- Détournement des matériels

Risques Cyber

- Productivité



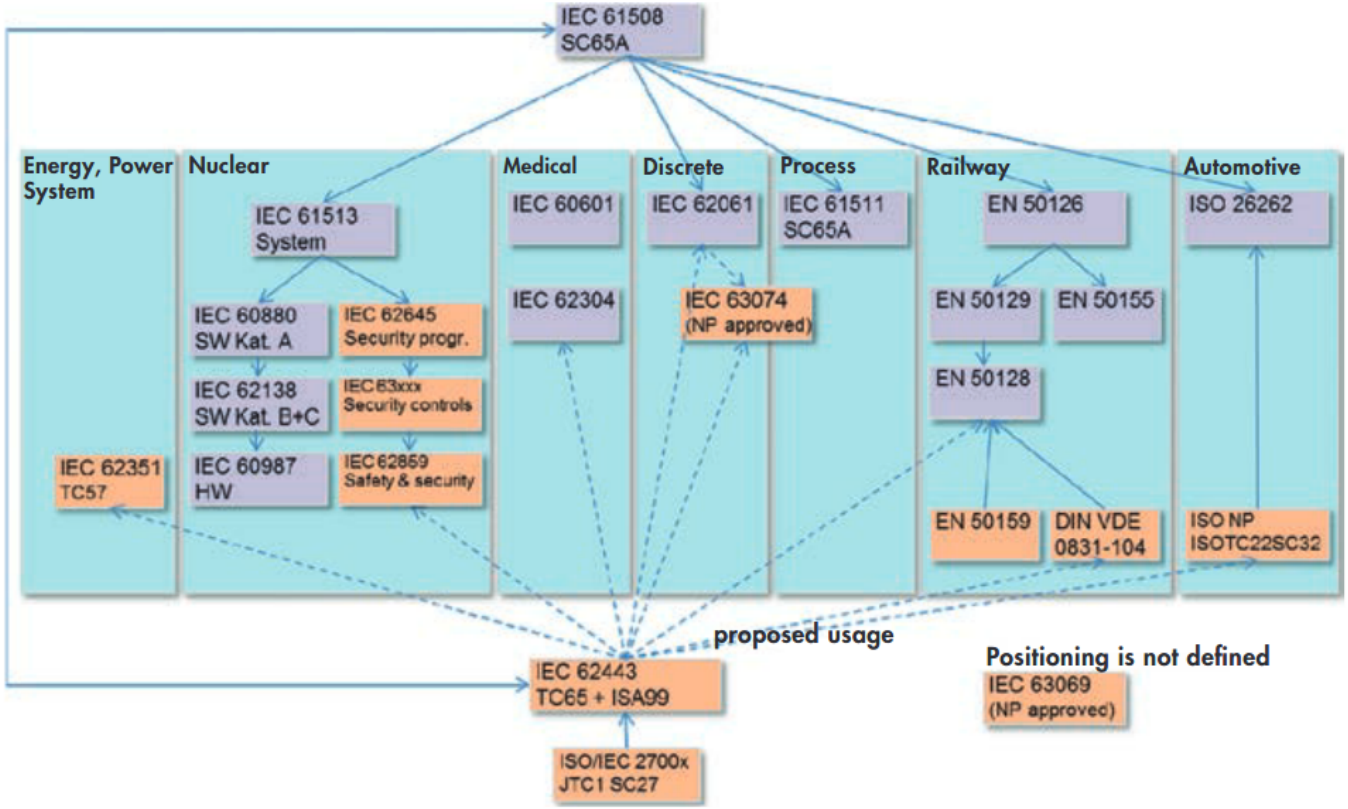
Risques Cyber

- Cibles : Tout le monde depuis 2017
  - Airbus, Saint-gobain, Fleury-Michon, Renault, Maerks, SNCF, Orange, Altran, MMA, MisterFly, CHU Rouen, agglomération de Grand Cognac, etc...
  - Particuliers +210 % en 2019 (*cybermalveillance.gouv*)

Directive cybersecurité

Directive cybersecurité

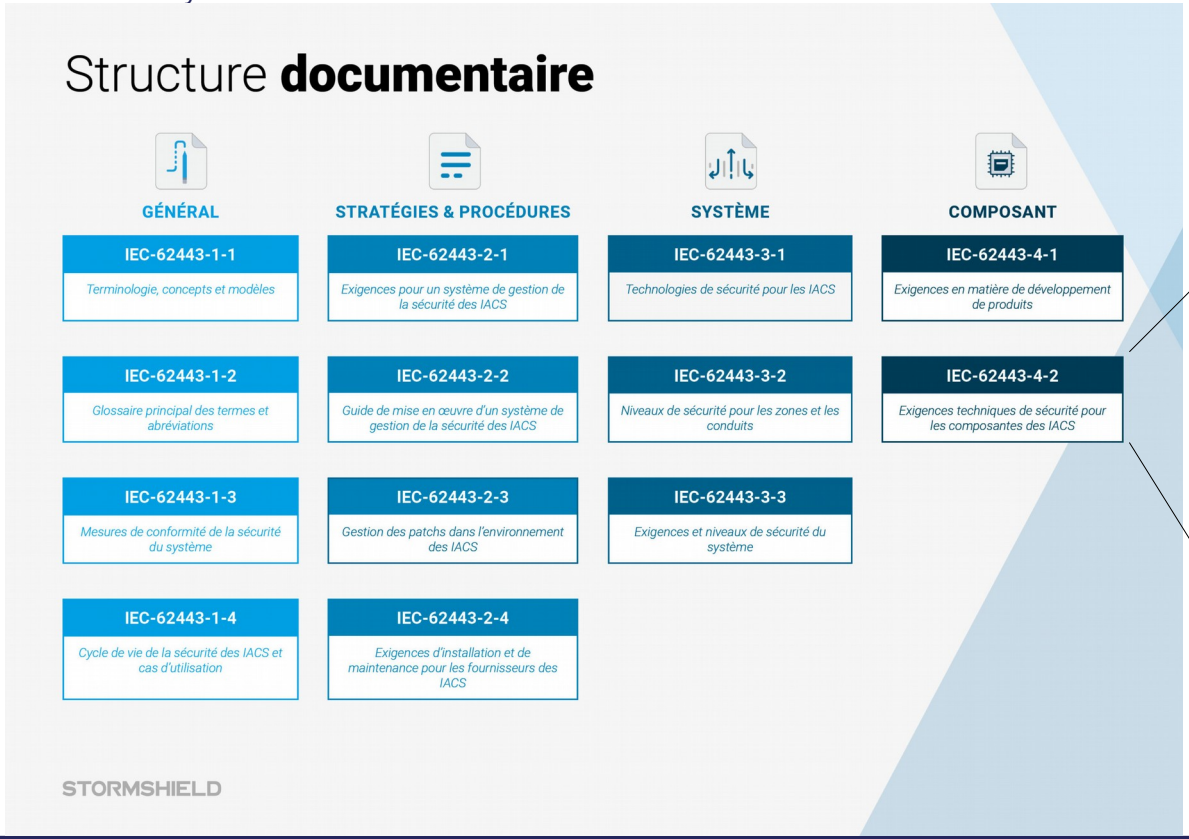
- Référentiel normatif à la sécurité fonctionnelle des systèmes électroniques relatifs à la sécurité
  Analyse du système face aux agressions internes et externes



src : Safety and security Interface at the Standards Level (© IEC TC65)

NF EN IEC 62443 : Cybersécurité des installations industrielles

La sécurité des systèmes automatisés de contrôle



Fournit les ressources pour :

- La protection de la chaîne logistique
- La lutte anti-intrusion / sabotage
- L'intégrité du démarrage
- La sécurité des applications utilisateur

Directive cybersecurité

NF EN IEC 62443-4-2 : **7 Exigences Fondamentales (FR)**

- FR1 : Identification and authentication control (IAC),
- FR2 : Use Control (UC),
- FR3 : System Integrity (SI),
- FR4 : Data Confidentiality (DC),
- FR5 : Restricted Data Flow (RDF),
- FR6 : Timely Response to Events (TRE)
- FR7 : Resource Availability (RA).

Directive cybersecurité

NF EN IEC 62443-4-2 : **5 Niveaux de Sécurité (SL)**

- SL-0 : Pas d'action spécifique ou de protection de sécurité nécessaire
- SL-1 : Protection contre les violations occasionnelles ou fortuites
- SL-2 : Protection contre les violations utilisant des moyens simples avec peu de ressources, peu de compétence et des compétences générales
- SL-3 : Protection contre les violations intentionnelles utilisant des moyens sophistiqués avec des ressources modérées, des compétences spécifiques IACS et une motivation modérée
- SL-4 : Protection contre les violations intentionnelles utilisant des moyens sophistiqués avec des ressources étendues, des compétences spécifiques IACS et une forte motivation

Directive cybersecurité

NF EN IEC 62443-4-2 : **4 Types de composants**

- Embedded Device : surveille, contrôle, commande le process industriel
  => Contrôleur de logique programmable (PLC), Système de contrôle distribué (DSC)
- Network Device : facilite ou restreint le flot de données
  => firewall, routeur, passerelle, switch...
- Host Device : élément qui exécute des applications
  => pc, serveur, data centers...
- Software Application : logiciel interfacé avec le process ou le système de contrôle (exécuté sur l'embedded ou le host device)
  => SCADA, data logger...

Directive cybersecurité

NF EN IEC 62443-4-2 : Technical security requirements for IACS component

- FR1 : Identification and authentication control (IAC) (Capabilities for Tests)
  - Identification / authentification utilisateur
  - Identification / authentification application / appareil
  - Gestion de compte
  - Gestion d'identifiant
  - Gestion de l'authentification sécurisée
  - Accès sans fil
  - Robustesse des mots de passe
  - Certificat PKI
  - Robustesse des clefs
  - Masquer les informations d'authentification
  - Gérer les tentatives de login
  - Surveillance des réseaux

Directive cybersecurité

NF EN IEC 62443-4-2 : Technical security requirements for IACS component

- FR2 : Use control (UC) (Key point for control Tests)

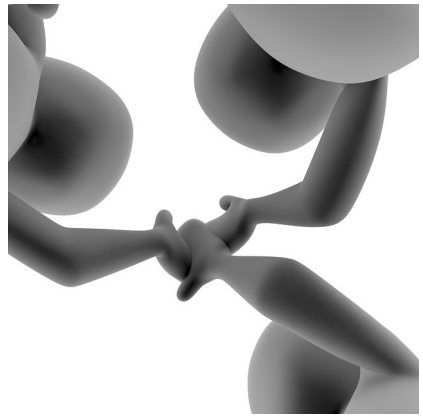
Contrôle l'usage de l'utilisateur identifié

- Autorisations (privilèges/droits)
- Usage des communications sans fil
- Appareils portables et mobiles (restriction des utilisations)
- Exécution de code sur mobile
- Verrouillage de sessions
- Sessions distantes (contrôle)
- Information d'audits (rapports, analyse)
- Horodatage
- Non-répudiation des actions des utilisateurs
- Protection des interfaces
- Contrôle des périphériques (nb limité, exécution de code interdit)
- Accès système limité (gestion de droits)

Directive cybersecurité

NF EN IEC 62443-4-2 : Technical security requirements for IACS component

- FR3 : System integrity (SI) (Key point to protect integrity)
  - Communication
  - Protection contre code malveillant
  - Vérification des fonctions de sécurité
  - Intégrité du logiciel , des sessions
  - Validation des signaux/valeurs des entrées
  - État de sortie déterminé
  - Identification et traitement des conditions d’erreurs
  - Audit (accès protégés)
  - Mise à jour (composant, firmware)
  - Altération physique (détecter, prémunir)
  - Confiance des éléments des fournisseurs
  - Intégrité du mécanisme de démarrage
  - Intégrité du reboot
  - Intégrité de la mise à jour



Directive cybersecurité

NF EN IEC 62443-4-2 : Technical security requirements for IACS component

- FR4 : Data confidentiality (DC) (Key point for confidentiality)
  - Protéger les données
  - Suppression des données, purge mémoire en fin de vie du composant
  - Chiffrer les données
    - Bannir MD5, SHA-0, SHA-1, DES, 3DES, et chiffrement propriétaire.
    - Utiliser algorithme à clef asymétrique d'au moins 2048 bits (RSA)
    - Utiliser algorithme à clef symétrique d'au moins 256 bits (AES)

Directive cybersecurité

NF EN IEC 62443-4-2 : Technical security requirements for IACS component

- FR5 : Restricted data flow (RDF) (Key point for control data flow/communication)
  - Segmentation du réseau
  - Firewall
  - Filtrer le contenu utilisateur
  - Protéger le service DHCP
  - Prévenir les boucles de switch

Directive cybersecurité

NF EN IEC 62443-4-2 : Technical security requirements for IACS component

- FR6 : Timely response to events (TRE) (Key point to monitor / recorded security event)
  - Accès au rapport d'audit (read-only)
  - Surveillance continue

- FR 7 : Resource availability (RA) (Key point to protect resource)
  - Protection contre le déni de service
  - Gestion des ressources (priorités)
  - Sauvegarde
  - Rétention des configurations
  - Paramètres des configuration du réseaux et de la sécurité
  - Limiter les fonctionnalités (nb ports ouverts)
  - Inventaire des composants (versionning visible)

Recommandations et leviers

Recommandations et leviers

- Organismes
  - ANSSI :
    - recense les failles de sécurité
    - propose des guides
    - *https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/*
  - NIST :
    - publie manuel de référence, guide sur la sécurité
  - C.E.S.T.I. :
    - laboratoire de THALES pour la certification
    - audit de sécurité (EAL7)

Recommandations et leviers

https://www.keylength.com/fr/

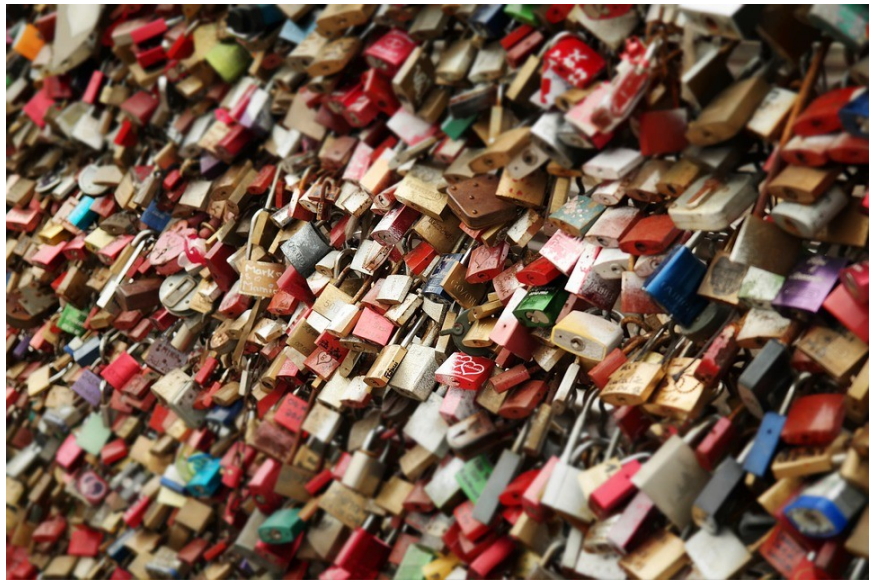
- Recommandation longueur de clefs : NIST

Date	Niveau de Sécurité	Algorithme symétrique	Factorisation Module	Logarithme discret Clef	Logarithme discret Groupe	Courbe elliptique	Hash (A)	Hash (B)
Legacy (1)	80	2TDEA	1024	160	1024	160	SHA-1 (2)	
2019 - 2030	112	(3TDEA) (3) AES-128	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2019 - 2030 et au-delà	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1 KMAC128
2019 - 2030 et au-delà	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224 SHA3-224
2019 - 2030 et au-delà	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-256 SHA3-384 SHA3-512 KMAC256

Solutions

Préconisations matérielles

- Sécurisation du matériel
  - Fonctions intégrées
    - secure element
    - bootloader sécurisé
    - jtag sécurisé
    - mémoires compartimentées
    - ressources de chiffrement
  - Critère commun > EAL5



- Sécurisation logicielle
  - BlockChain
  - Trust zone, Trusted Execution Environment (TEE), MPU (Memoy Protection Unit), firewall, tamper detection,,,

Préconisations matérielles

- Exemple de composants
  - **SE050** de chez **NXP** : secure element iot prêt à l'emploi conforme IEC 62443-4-2 eal 6+

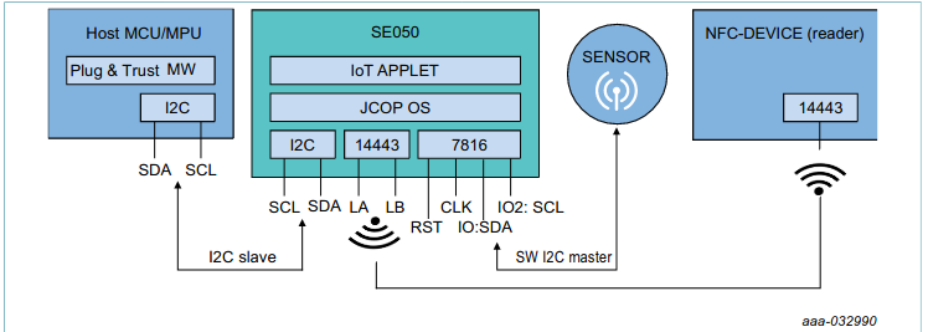


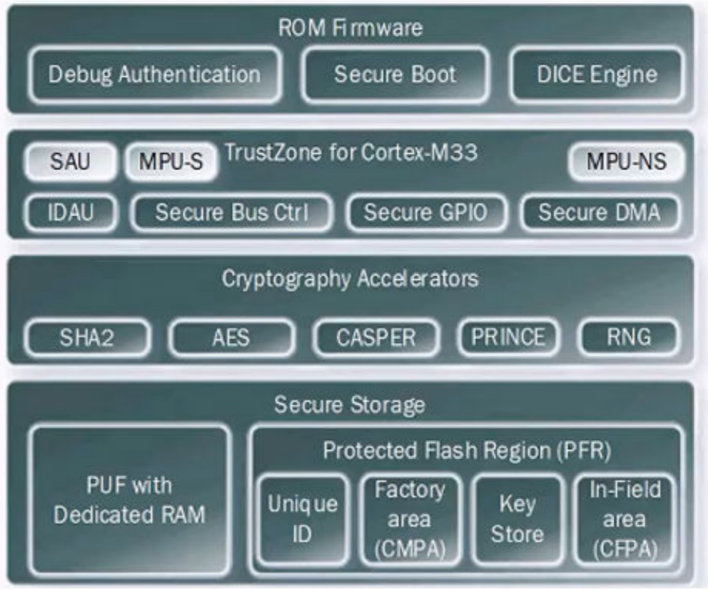
Figure 1. SE050 solution block diagram

The SE050 IoT applet supports:

- Generic module management
  - Lifecycle management
  - Session management
  - Timer functionality
  - Access control
  - Secure import/export of keys or files
- Applet Secure Channel management
  - AESKey sessions (previously called SCP03)
  - ECKey sessions (previously called FastSCP)
- Random number generation
- Key management (ECC, RSA, AES, DES, etc.): write, read, lock, delete
- Elliptic curve cryptographic operations
- RSA cryptographic operations
- AES/DES cryptographical operations (AES ECB, CBC, CTR)
- Binary file creation and management
- UserID creation and management
- Monotonic counter creation and management
- PCR creation and management
- Hash operations
- Message authentication code generation
  - CMAC
  - HMAC
- Key derivation functionality
  - HKDF
  - PBKDF2
- Specific use case support
  - TLS PSK master secret calculation
  - MIFARE DESFire protocol support
  - I2C Master support

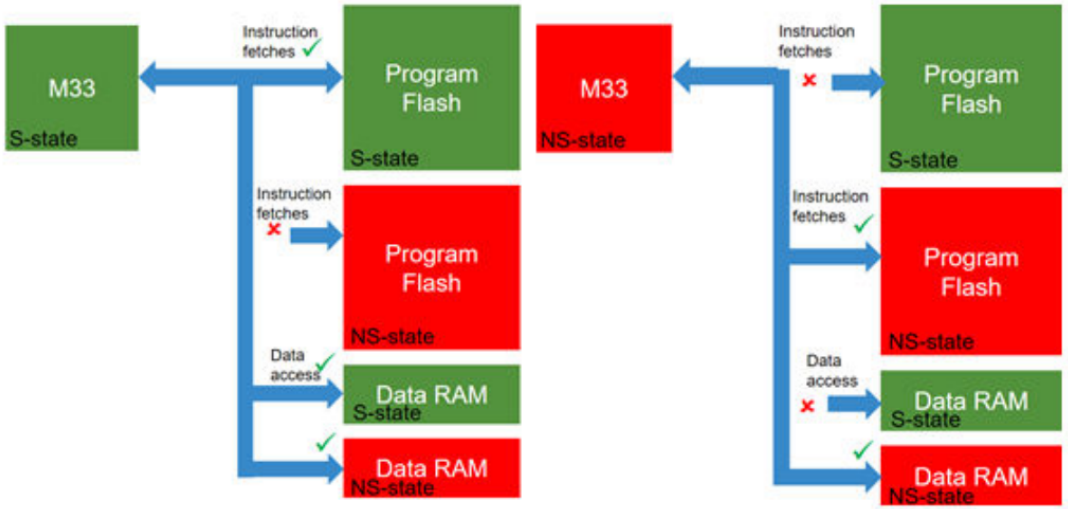
Préconisations matérielles

- Exemple de composants...
  - **LPC55Sxx** de chez **NXP** : System on Chip (Soc) pour la sécurisation de systèmes embarqués



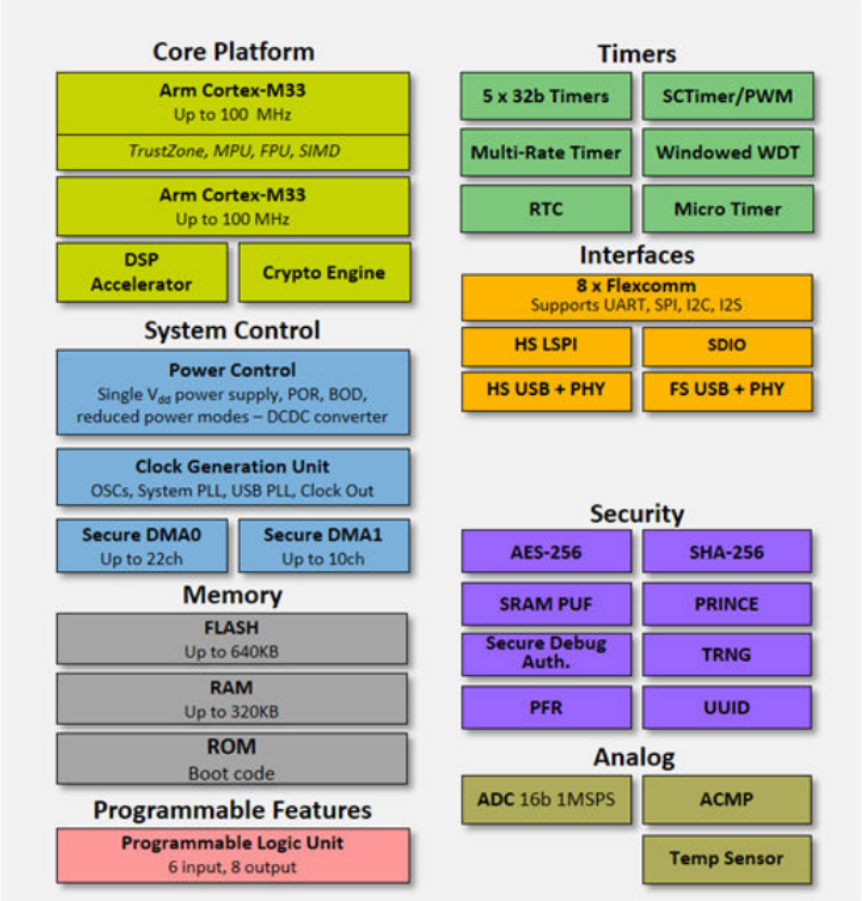
Préconisations matérielles

- Exemple de composants...
  - **LPC55Sxx** de chez **NXP** :
    Etats du cpu sécurisés et non sécurisés



Préconisations matérielles

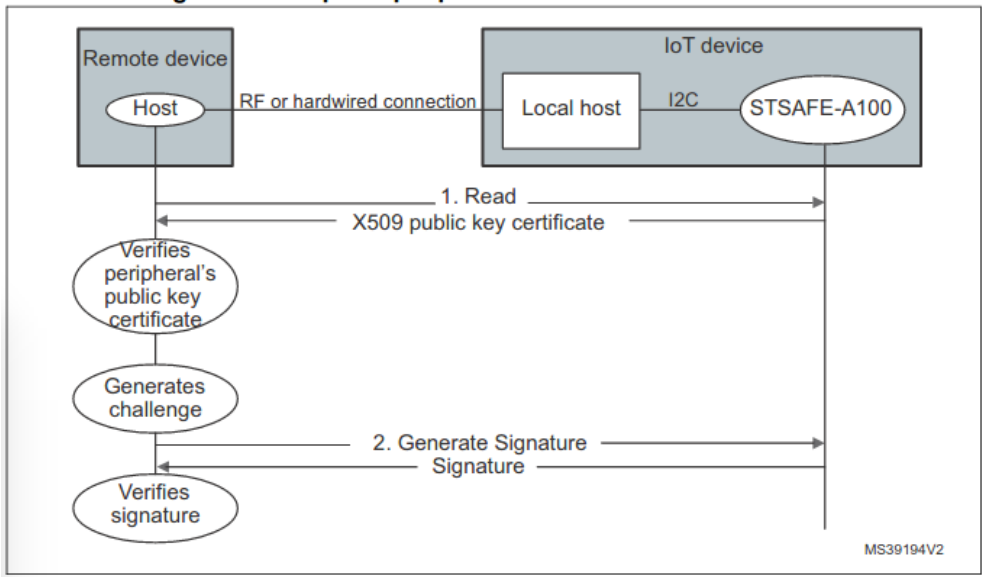
- Exemple de composants...
  - **LPC55Sxx** de chez **NXP** : Architecture des LPC55S6x



Préconisations matérielles

- Exemple de composants...
  - **STSAFE-A/J/TPM** de chez **ST** : pour l'authentification et l'établissement d'une connexion sécurisée distante

Figure 5. Example of peripheral or IoT device authentication



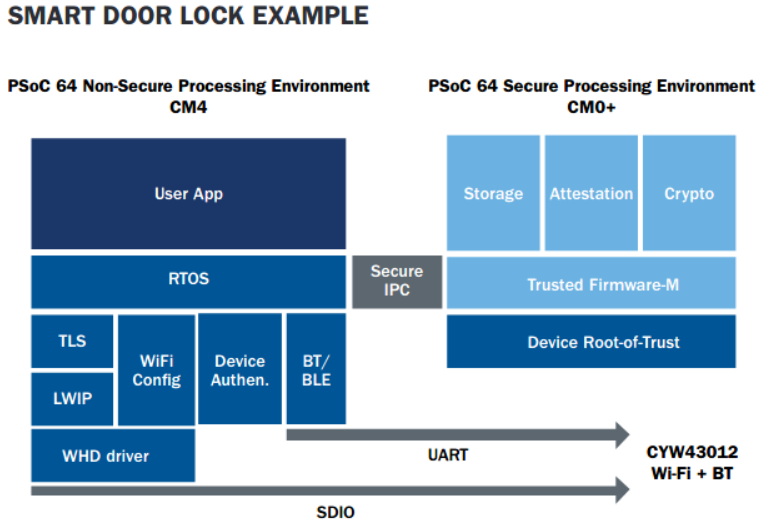
Préconisations matérielles

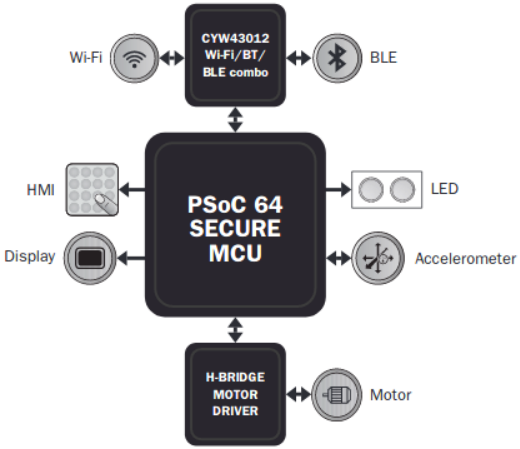
- Exemple de composants...
  - **ATECC608A** de chez **Microchip** : pour l'authentification sécurisée via le réseau et entre accessoires (plate-forme spécifiques Trust Go/Flex/Custom)

- **Network/IoT Node Endpoint Security**
  Manage node identity authentication and session key creation & management. Supports the entire ephemeral session key generation flow for multiple protocols including TLS 1.2 (and earlier) and TLS 1.3
- **Secure Boot**
  Support the MCU host by validating code digests and optionally enabling communication keys on success. Various configurations to offer enhanced performance are available.
- **Small Message Encryption**
  Hardware AES engine to encrypt and/or decrypt small messages or data such as PII information. Supports AES-ECB mode directly. Other modes can be implemented with the help of the host microcontroller. Additional GFM calculation function to support AES-GCM.
- **Key Generation for Software Download**
  Supports local protected key generation for downloaded images. Both broadcast of one image to many systems, each with the same decryption key, or point-to-point download of unique images per system are supported.
- **Ecosystem control and Anti-Counterfeiting**
  Validates that a system or component is authentic and came from the OEM shown on the nameplate.

Préconisations matérielles

- Exemple de composants...
  - **Aptiga trust** de chez **infineon**
  - **PSoC® 64 Secure Microcontrollers** de chez **Cypress**
  - **Wireless Gecko series 2** de chez Silicon Labs
  - ...





Préconisations matérielles

- Exemple de produits
  - **fl MGUARD** RS2000 RS4000 de chez **Phoenix Contact** : routeur conforme IEC 62443-4-2 (vpn, Ipsec, x509.v3)

Table 2-1 CR 1.1 – Human user identification and authentication

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	By default, the mGuard device requires authentication via password for every user interface (SSH, SSL, SNMP or serial console) each time a user logs on. The password for the user can be configured at: **Authentication >> Administrative Users >> Password** (UM: 7.1.1) To avoid insecure authentication, SNMP should be disabled in: **Management >> SNMP >> Query** (UM: 4.6.1)
Reaching SL 2	Additionally required: To reach SL 2, the mGuard device must additionally use an external RADIUS server for unique identification and authentication. The RADIUS server is normally managed by an IT department. It must be ensured that the connection to the RADIUS server is carried out via a VPN tunnel. The integration of an external RADIUS server can be configured at: **Authentication >> RADIUS** (UM: 7.3) **Management >> System Settings >> Shell access** (UM: 4.1.3) **Management >> Web Settings >> Access** (UM: 4.2.2) Configure the mGuard device to allow RADIUS authentication *as only method for password authentication*.
Reaching SL 3 – 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

Préconisations matérielles

- Exemple de produits
  - **GuardLogix 5580** de chez **Rockwell** :
    contrôleur d'automatisme programmable conforme IEC 62443-4-2 (SIL 2, SIL 3)
    - Instructions complémentaires d'intégrité élevée

Préconisations matérielles

- Exemple de produits
  - **Scalance X(x)-200** de chez **Siemens** :
    switch conforme IEC 62443-4-2

FIN

Cybersécurité : Focus extension IEC 62443-4-2
Recommandations et leviers
Solutions matérielles électroniques

S. ROUXEL – 26 11 2020 – v 1.0

Réf du document : DT_PPT_SR_AtelierSecurisation_v1.0_20201006

Le CRT CRESITT est soutenu par :

L'action de diffusion technologique est cofinancée par l'Union européenne.
L'Europe s'engage en région Centre-Val de Loire avec le Fonds européen de développement régional.

Evaluation Assurance Level (EAL)

EAL1 : testé fonctionnellement

EAL2 : testé structurellement

EAL3 : testé et vérifié méthodiquement

EAL4 : conçu, testé et vérifié méthodiquement

EAL5 : conçu de façon semi-formelle et testé

EAL6 : conception vérifiée de façon semi-formelle, et testé

EAL7 : conception vérifiée de façon formelle, et testé