

CRESITT INDUSTRIE

Centre de Ressources
Technologiques en Électronique



Smart Industrie sécurisée : Sécurisation de solutions électroniques et impacts

S. ROUXEL – 07 10 2021 – v 1.0

Réf du document : DT_PPT_SR_Smart_Indus_Sec_v1.0_20211007

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.

- Risques Cyber
- Solutions de sécurisation
- Impacts des solutions
- Exemple de mise en oeuvre

- 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

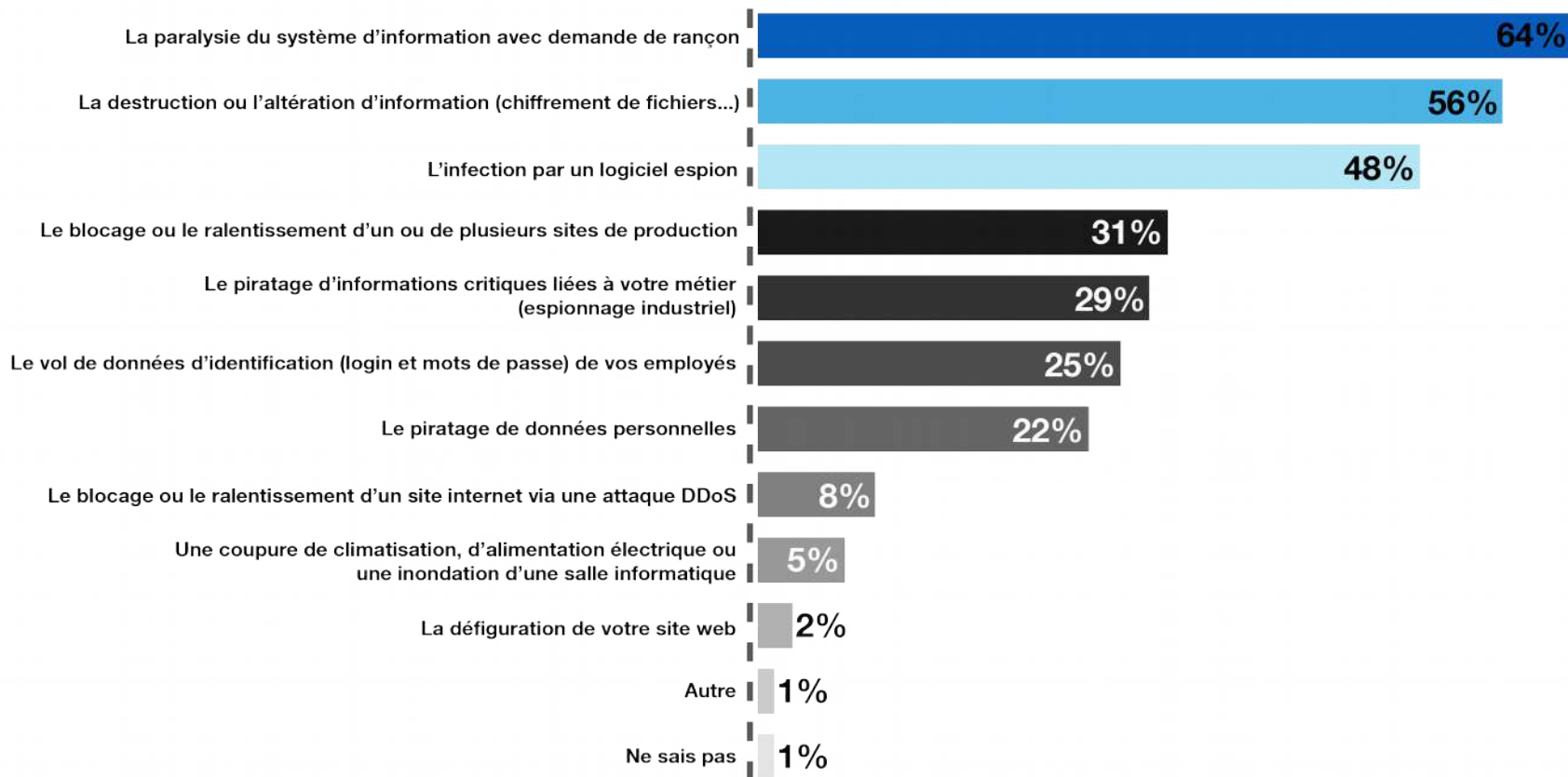
- DdoS, DoS
- Ransomware
- Malware (trojan, worms, virus)
- Spambots
- Backdoors
- Hameçonnage
- Destruction de données



src : [hiscox](#), [cyberexperts.tech](#), [orangecyberdefense.com](#)

- 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](http://cybermalveillance.gouv.fr))





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

- Détournement des matériels

- Productivité

Conséquences possibles d'une attaque de cybersécurité réussie contre des systèmes d'automatisation / de robotique





- Sécurisation du matériel

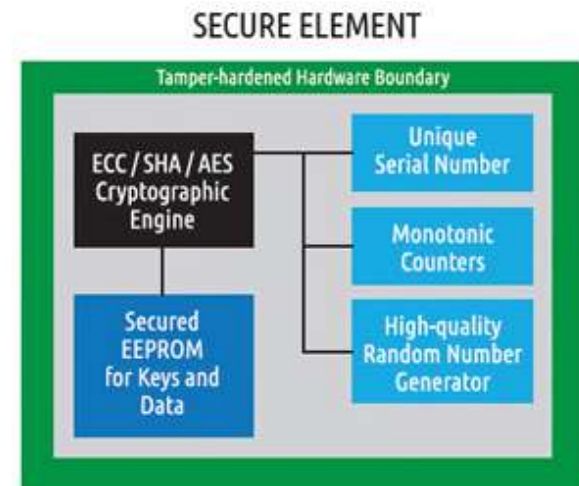
- Fonctions intégrées
 - Secure element
 - Jtag sécurisé
 - Ressources de chiffrement
 - TrustZone
- Critères communs : niveaux d'assurance (>EAL5)



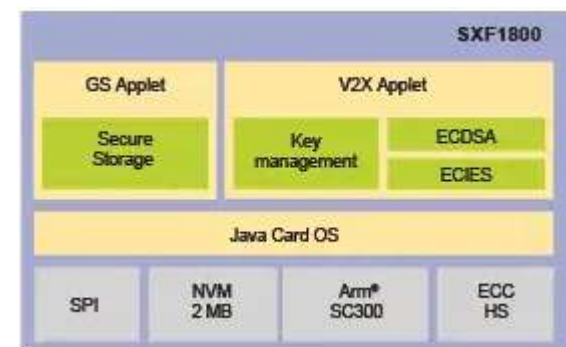
- Sécurisation logicielle

- Bootloader sécurisé
- Mémoires compartimentées
- Blockchain
- Trusted Execution Environment (TEE), MPU (Memory Protection Unit), firewall, tamper detection,,,

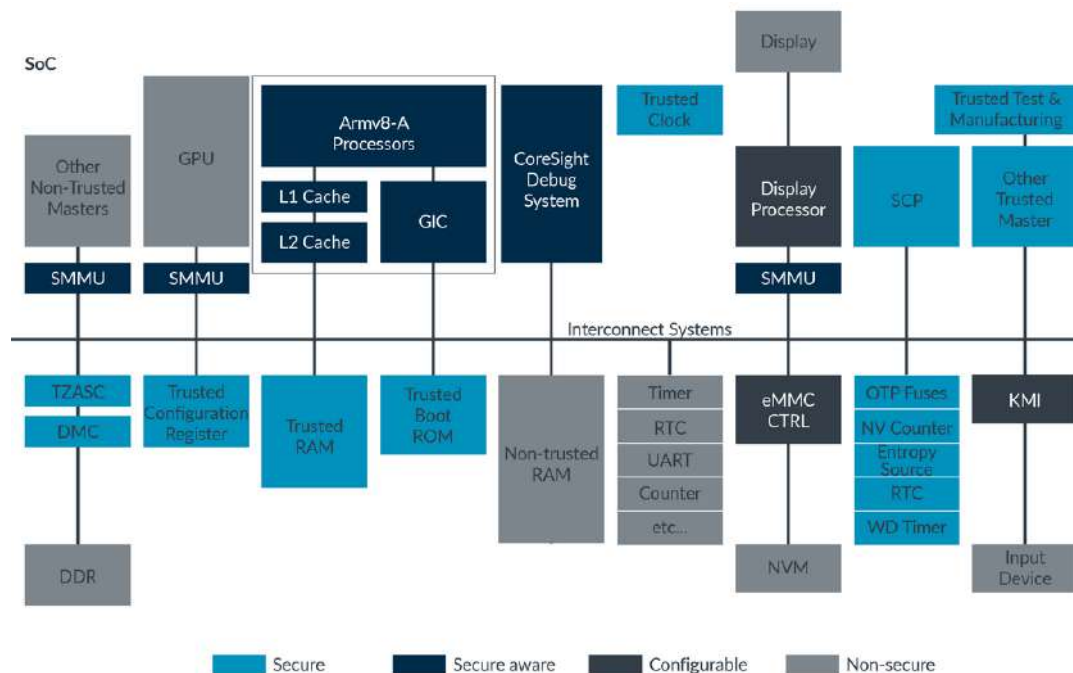
- Sécurisation du matériel
 - Secure element
 - Protection des données
 - Garantir l'intégrité et l'authentification
 - Démarrage sécurisé
 - Stockage sécurisé (clefs, certificats)
 - Fournir des ressources de chiffrement
 - Execution d'application sécurisée (type bancaire)



Version simplifiée



- Sécurisation du matériel
 - Microcontrôleurs avec sécurisation
 - Solution ARM : Cortex-A (application) & Cortex-M (microcontroller)



src : arm

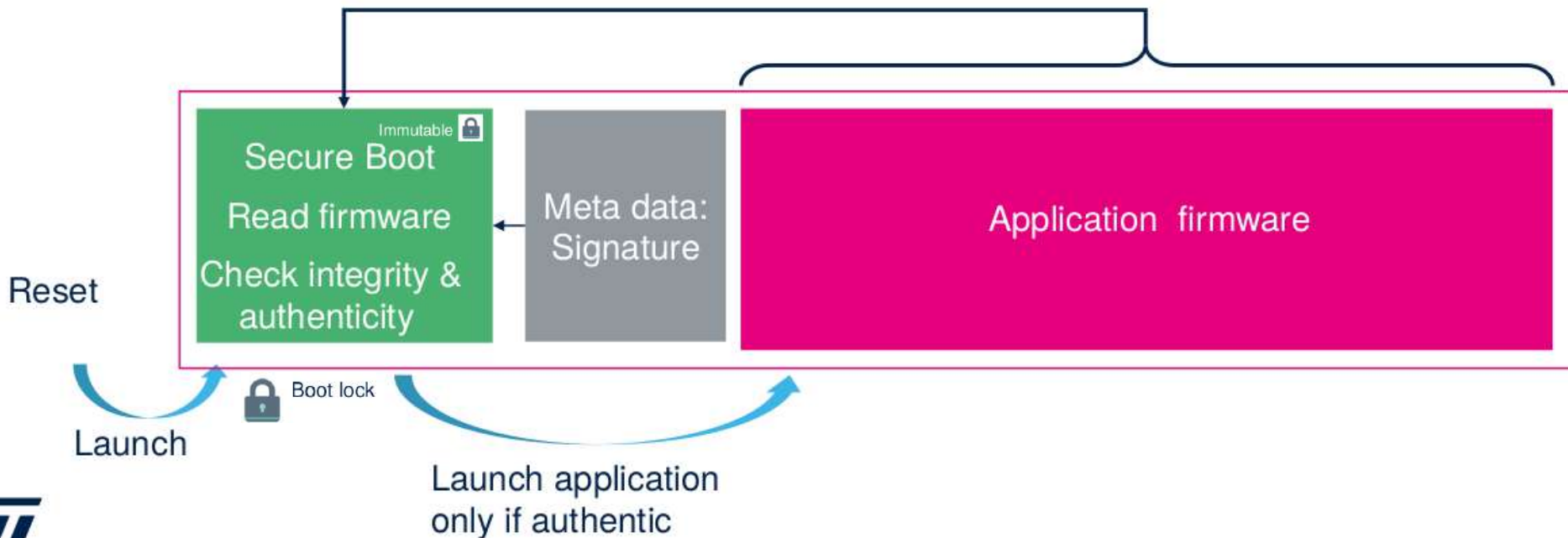
- Sécurisation du matériel
 - Microcontrôleur avec sécurisation
 - Solution ARM : Cortex-A (application) & Cortex-M (microcontroller)
- Sécurisation du firmware
- Sécurisation de l'exécution



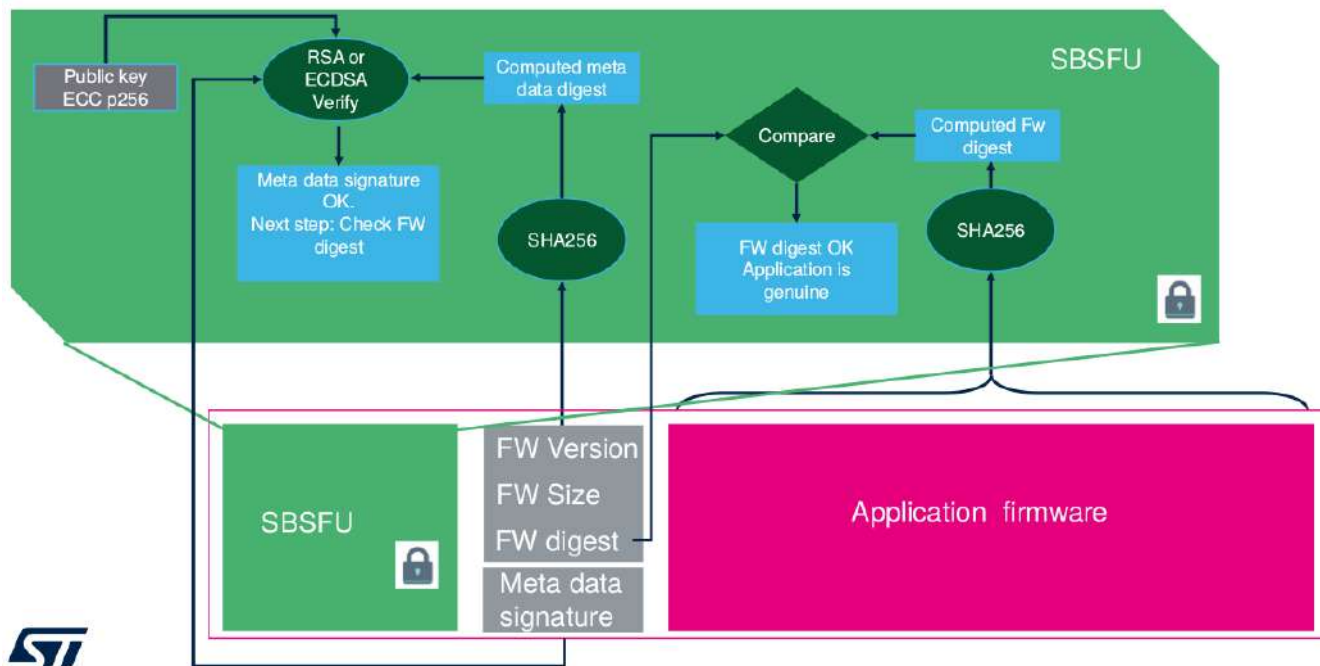
- Sécurisation du matériel
 - Microcontrôleur avec sécurisation
 - Secure Boot (SB) & Secure Firmware Update (SFU)
 - Intégrité du firmware
 - Authenticité du firmware
 - Update d'un firmware chiffré possible
 - Hash et signature avec clef



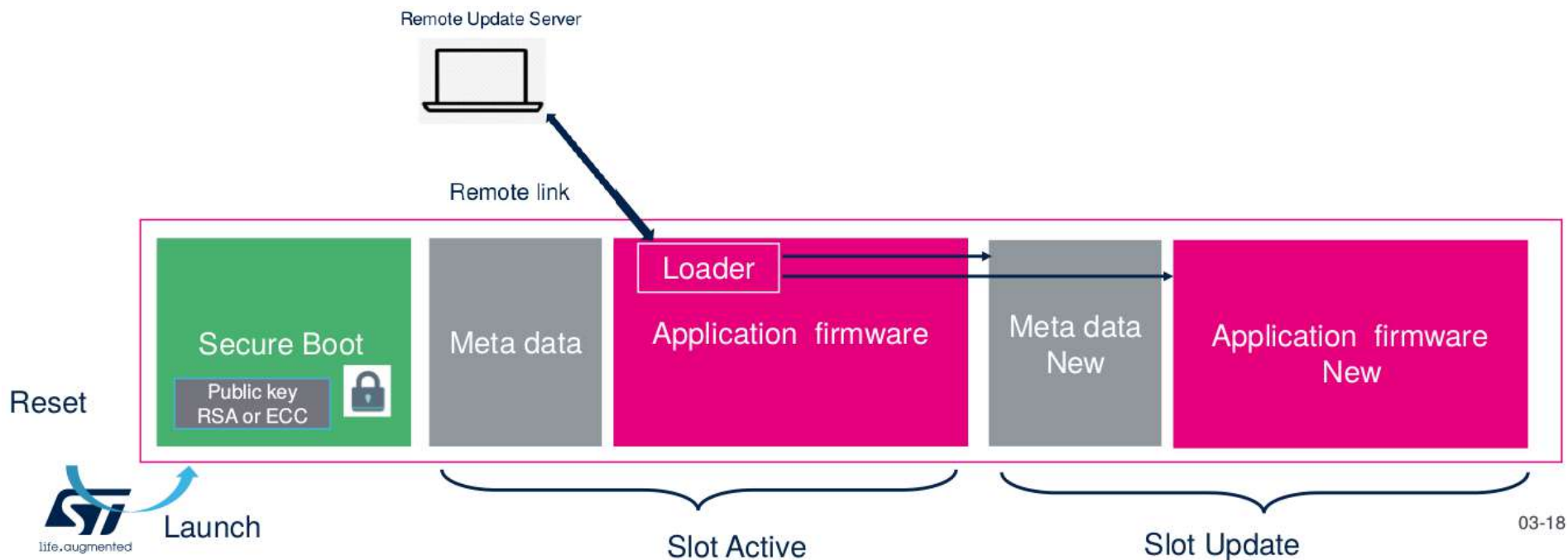
- Sécurisation du matériel
 - Microcontrôleur avec sécurisation
 - Principes : **Secure Boot (SB)** & Secure Firmware Update (SFU)



- Sécurisation du matériel
 - Microcontrôleur avec sécurisation
 - Principes : **Secure Boot (SB)** & Secure Firmware Update (SFU)



- Sécurisation du matériel
 - Microcontrôleur avec sécurisation
 - Principes : Secure Boot (SB) & **Secure Firmware Update (SFU)**

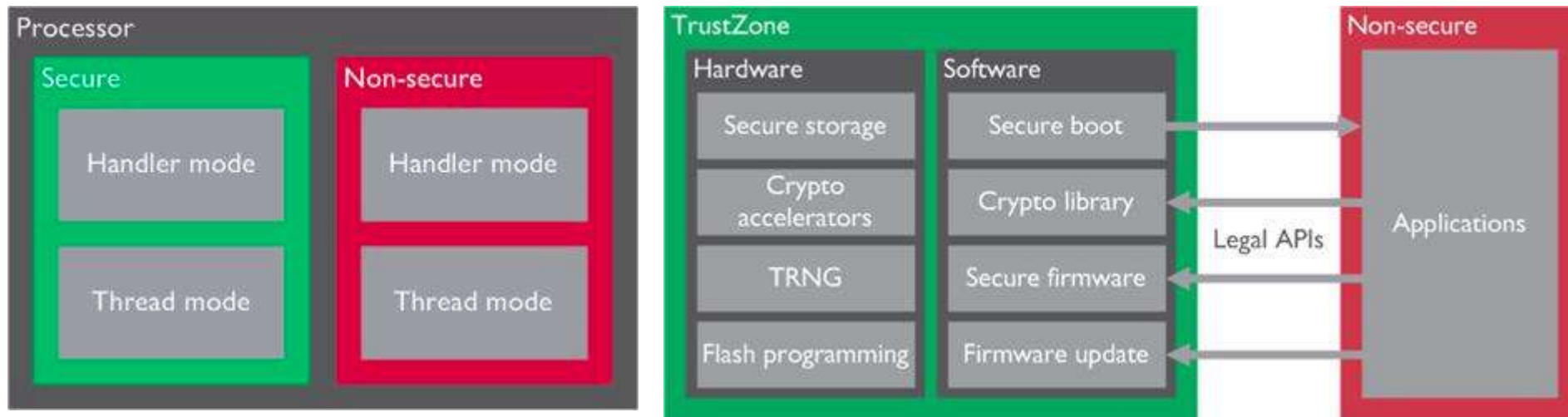


03-18

- Sécurisation du matériel
 - Microcontrôleur avec sécurisation
 - TrustZone :
 - Sécurisation des données et des échanges
 - Exécution en zone protégée du code critique (pas d'altération)
 - Cycle de vie d'application garantie
 - Détection des situations anormales



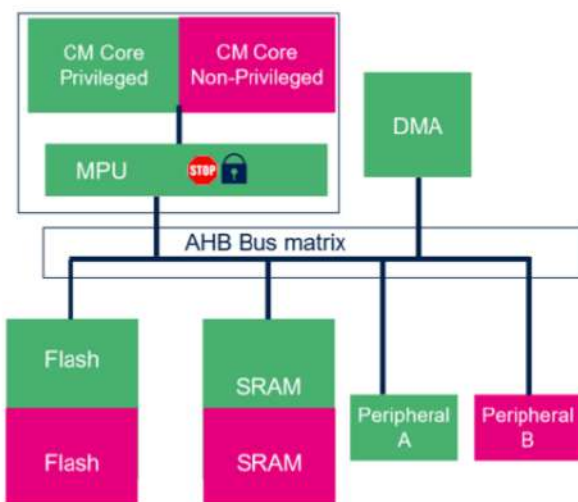
- Sécurisation du matériel
 - Microcontrôleur avec sécurisation – Exécution Sécurisée
 - TrustZone isolation renforcée par le matériel
 - Monde sécurisé S (vert), et non sécurisé NS (rouge)



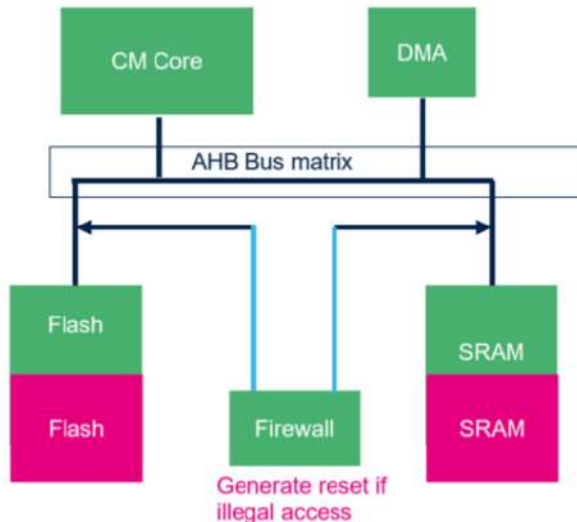
src : arm

- Sécurisation du matériel
 - Microcontrôleur avec sécurisation
 - TrustZone - Isolation : 3 mécanismes

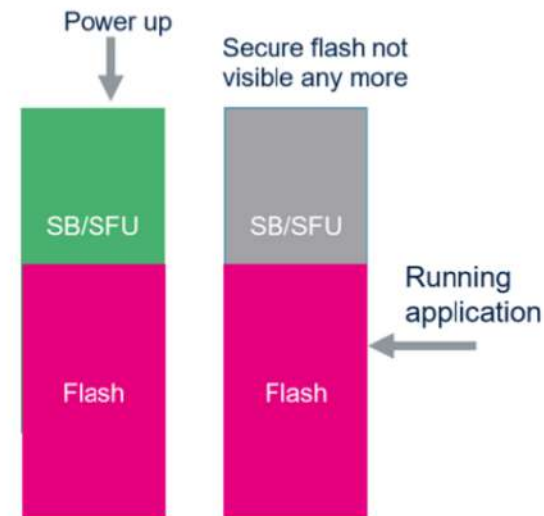
Memory Protection Unit (MPU) – Firewall - Flash



MPU



Firewall



Flash

• Sécurisation du matériel

◦ TrustZone - Isolation :

- Accès mémoire sécurisés par des attributs (secure, unsecure, non-secure callable)
- SAU (Secure Attribution Unit) + IDAU (Implementation Device Attribution Unit)
 - SAU configuration arm de 8 régions mémoires
 - IDAU configuration particulière du fabricant pour l'extension des zones

Figure 9-2 Simple memory map created by a minimal IDAU design

Address	Type	Security
0xFFFFFFF	Device system	Various (CPU controlled)
0xF000000		Secure
0xE000000		Non-secure
0xD000000	Device system	Secure
0xC000000		Non-secure
0xB000000		Secure
0xA000000	RAM (WB)	Secure
0x9000000		Non-secure
0x8000000		Secure
0x7000000	RAM (WT)	Non-secure
0x6000000		Secure
0x5000000		Non-secure
0x4000000	Device	Secure
0x3000000		Non-secure
0x2000000		Secure
0x1000000	Code	Non-secure
0x0000000		Secure

src : arm

Ex: bit[28] spécifie secure/non-secure (NXP)

SAU		IDAU		End result
Secure	+	Secure	=	Secure
NS	+	Secure	=	Secure
Secure	+	NS	=	Secure
NS	+	NS	=	NS
NSC	+	Secure	=	Secure
NSC	+	NS	=	NSC

src : NXP

- Sécurisation du matériel
 - TrustZone - Isolation :
 - Passages Secure => Non-secure
 - API function
 - Interruption

Figure 6-1 Security state transitions

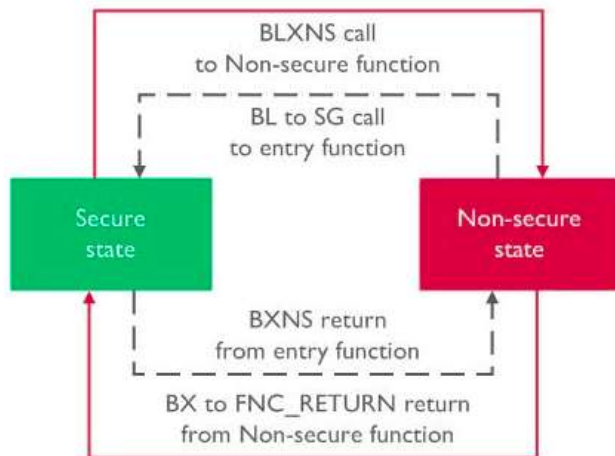
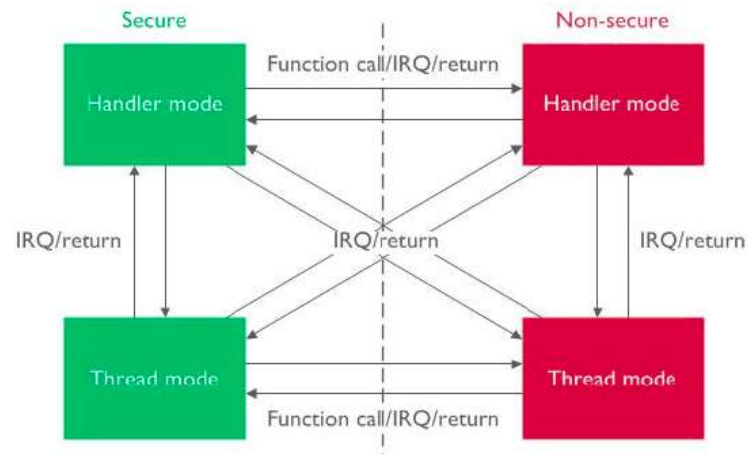


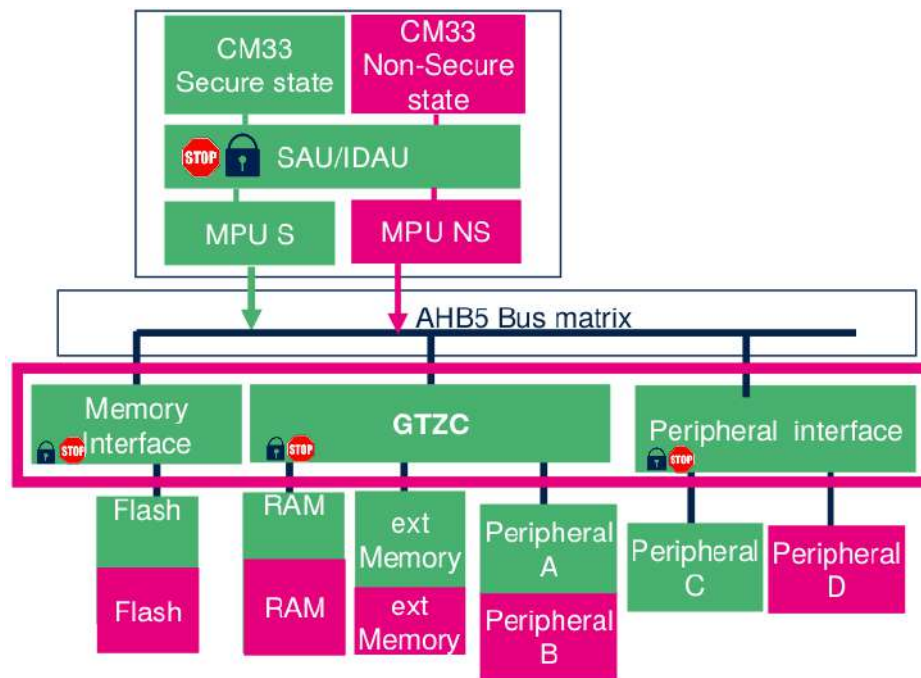
Figure 6-4 Forms of transition between Secure and Non-secure worlds



configurable par registre Interrupt Target Non-secure (NVIC_ITNS)

src : arm

- Sécurisation du matériel
 - Microcontrôleur avec sécurisation
 - TrustZone – Exemple Cortex M33 :



src : arm

- Sécurisation du matériel
 - Microcontrôleur avec sécurisation
 - Exemples :
 - ST Microelectronics : STM32L4x, STM32L5x
 - NXP : LPC55S69
 - Renesas : RA4M3, RA6M4, RA6M5
 - Cypress : PSoC 64 secure
 - Silicon labs : wireless gecko serie 2
 - Infineon : Aptiga trust
 - Microchip : ATECC608A
 - Texas Instrument : Sitara AM43x

- Sécurisation du matériel
 - Microcontrôleur avec sécurisation
 - TrustZone - Isolation :

Memory Protection Unit (MPU) – Firewall - Flash

	STM32 Series	Isolation features				
		Secure mem/HDP	MPU	Firewall	Trustzone	Arm Cortex®
 Available on all devices  Depends on device part number	STM32 F0					M0
	STM32 F1					M3
	STM32 F2					M3
	STM32 F3					M4
	STM32 F4					M4
	STM32 F7					M7
	STM32 L0					M0+
	STM32 L1					M3
	STM32 L4					M4
	STM32 L5					M33
	STM32 H7					M7/M4
	STM32 G0					M0+
	STM32 G4					M4
	STM32 WB					M4/M0+

Available on all devices

Depends on device part number

- Recommandations ANSSI

- Guide « RECOMMANDATIONS RELATIVES À LA SÉCURITÉ DES (SYSTÈMES D') OBJETS CONNECTÉS »
ANSSI-PA087 2021-08-27
 - R24-25 Protections de données (clefs et chiffrement)
 - R26 Minimisation de la surface d'attaque
 - R27 Chaîne de démarrage sécurisée
 - R28-29-30-31-32 Mise à jour authentifiée avec versionning et anti-rollback
 - R33 Mémoire compartimentée
 - R45 Protection de communication inter-composants
 - R53 Protocole de communication sécurisée



- Coûts

- Consommation

- Consommation supérieure avec SBSFU et la trustzone et le chiffrement

- Ressource mémoire

- Besoin de plus de ressources mémoire (SBSFU)

- Temps d'exécution

- Temps de démarrage allongé par les vérifications du bootloader sécurisé

- Prix

- Plus cher qu'une solution sans sécurisation (12-17€ le micro)
 - Devrait certainement évoluer à la baisse à cause des régulations à venir et des normes existantes
 - NF EN IEC 62 443, NF EN IEC 61508, ETSI EN 303 645, ISO SAE 21434:2021...

Exemple de mise en oeuvre

- Exemple de réalisation : Secure By Design

- Matériel

- Kit STM32WL55
- Accéléromètre LIS3DH
- Ultrason (distance) MB1200

- Sécurisation

- SBSFU
- Communication LoRaWan
- Chiffrement des datas (AES256)

Sécurisation du bout en bout



SBSFU + LoRaWAN
STM32WL55



LIS3DH



MB1200

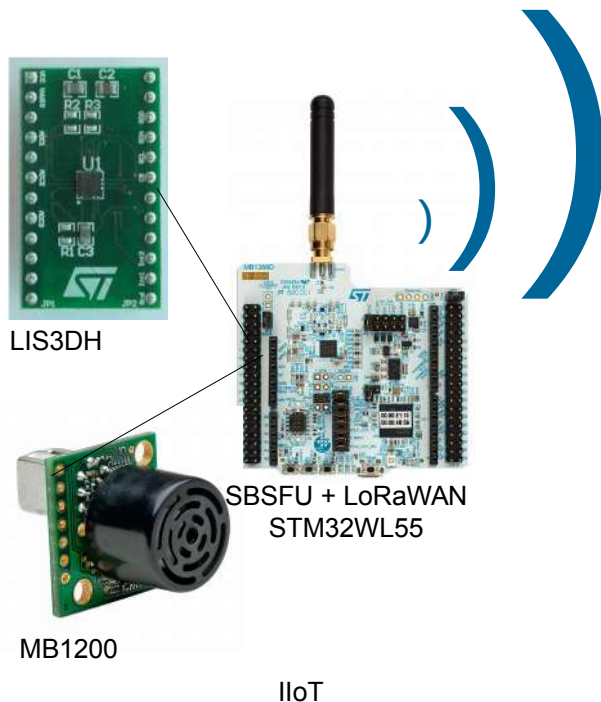
- Exemple de réalisation : Secure By Design

- STM32WL55JC1

- M0+ : LoRa, pile LoRaWan
 - M4 : application
 - AES256
 - I2c (LIS3DH)
 - Uart (ultrason)

Control - Power supply 1.8 to 3.6 V w/ DCDC+ LDO POR/PDR/PVD/BOR - Crystal oscillators 32 MHz (Radio + HSE) 32.768 KHz (LSE) - Internal RC oscillators 32.768 KHz + 16 MHz + 48 MHz ± 1% acc. over V and T(°C) - RTC/AWU/CSS - PLL - SysTick timer 2 watchdogs (WWDG/IWDG) 43 GPIOs - Cyclic redundancy check - Voltage scaling (2 modes)	Arm® Cortex®-M4 DSP 48 MHz - Nested vector interrupt controller (NVIC) - Memory protected unit (MPU) - JTAG/SW debug	Memory - Up to 256-Kbyte Flash - Up to 64-Kbyte SRAM - CM4 or CM0 Boot_Lock - Boot loader - Hide protect
Security - AES 256-bit + TRNG + PCROP - Tamper Detection - Secure Areas - Secure FW Install - Debug control - Boot Selection - Secure Sub-GHz, MAC Layer, SFI - Key Management services	Radio - LoRa®, (G)FSK, (G)MSK, BPSK +15dBm & +22dBm Power Outputs -148 dBm sensitivity (LoRa) 150 MHz to 960 MHz	Timers 1 x 32-bit timer 3x 16-bit timers 3x ULP 16-bit timers
	Arm® Cortex®-M0+ 48 MHz - Nested vector interrupt controller (NVIC) - Memory protected unit (MPU) - SW debug	Analog 1x 12-bit ADC SAR 2.5 Msps 12-bit DAC 2x ULP comparators - Temperature sensor
		Connectivity 2x SPI, 3x I2C 2x USART LIN, smartcard, IrDA, Modem control 1x ULP UART

- Exemple de réalisation : Secure By Design
 - Systeme complet

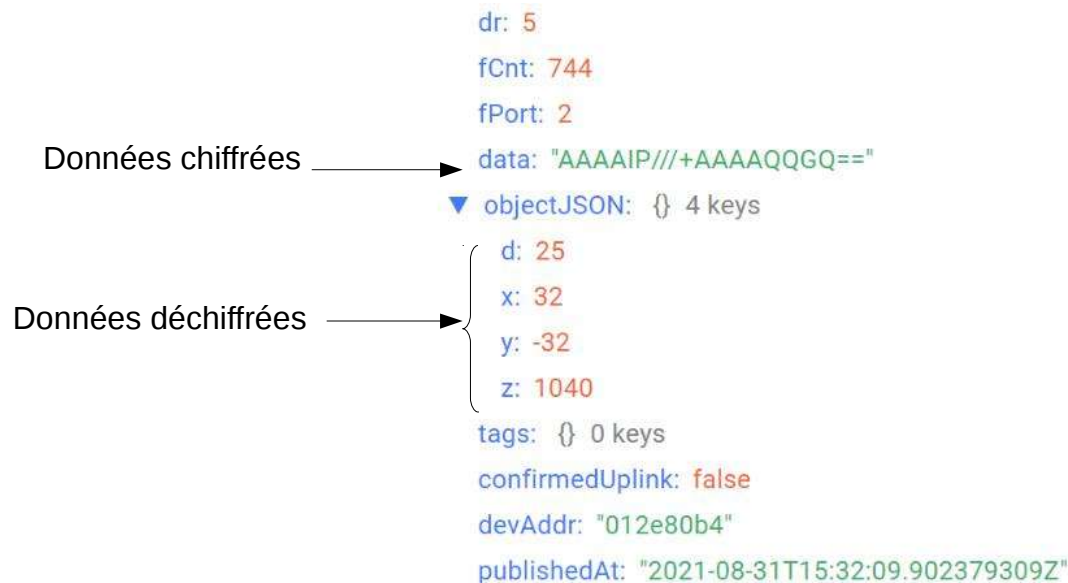


Passerelle LoRaWan
=
Bridge
+
serveur réseau
+
serveur d'application

Plate-forme interne
et/ou
Serveur(s) Cloud



- Exemple de réalisation : Secure By Design
 - STM32WL55JC1
 - Données chiffrées de bout en bout



CRESITT INDUSTRIE

Centre de Ressources
Technologiques en Électronique



FIN

Smart Industrie sécurisée : Sécurisation de solutions électroniques et impacts



S. ROUXEL – 07 10 2021 – v 1.0

Réf du document : DT_PPT_SR_Smart_Indus_Sec_v1.0_20211007

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