life.augmented

IoT Security Standards & Regulations A Focus on EU RED

Bruno MUSSARD

Wireless MCU Security Manager

STMicroelectronics

Agenda

1 About ST & STM32

2 Certifications & regulations

3 Focusing on RED

4 Meeting RED with SESIP

Q&A session

life.augmented

About ST & STM32

life.augmented

We are creators and makers of technology

One of the world’s largest semiconductor companies

48,500+ employees of which **8,400+** in R&D

$17.29B revenues in 2023

Over **80** Sales & Marketing offices serving over **200,000** customers across the globe

13 manufacturing sites

Signatory of the United Nations Global Compact (UNGC)
Member of the Responsible Business Alliance (RBA)

life.augmented

All flagship products targeting SESIP3

STM32 portfolio

MPU

- **STM32MP1** — Up to 1 GHz Cortex-A7, 209 MHz Cortex-M4
- **STM32MP2** — Dual 1.5 GHz Cortex-A35, 400 MHz Cortex-M33

High-performance MCUs

- STM32F7 — 1082 CoreMark, 216 MHz Cortex-M7
- **STM32H7R/S** — Up to 3224 CoreMark, Up to 600 MHz Cortex -M7, 240 MHz Cortex -M4
- **STM32N6** — MCU with neural processing unit
- STM32F2 — Up to 398 CoreMark, 120 MHz Cortex-M3
- STM32F4 — Up to 608 CoreMark, 180 MHz Cortex-M4
- **STM32H5** — Up to 1023 CoreMark, 250 MHz Cortex-M33

Mainstream MCUs

- STM32F3 — 245 CoreMark, 72 MHz Cortex-M4
- **STM32G4** — 569 CoreMark, 170 MHz Cortex-M4
- **STM32C0** — 114 CoreMark, 48 MHz Cortex M0+
- STM32F0 — 106 CoreMark, 48 MHz Cortex-M0
- **STM32G0** — 142 CoreMark, 64 MHz Cortex-M0+
- STM32F1 — 177 CoreMark, 72 MHz Cortex-M3

All new products targeting SESIP3

Ultra-low-power MCUs

- STM32L0 — 75 CoreMark, 32 MHz Cortex-M0+
- **STM32U0** — 140 CoreMark, 48 MHz Cortex-M0+
- STM32L4 — 273 CoreMark, 80 MHz Cortex-M4
- STM32L4+ — 409 CoreMark, 120 MHz Cortex-M4
- STM32L5 — 443 CoreMark, 110 MHz Cortex-M33
- **STM32U5** — 651 CoreMark, 160 MHz Cortex-M33

Wireless MCUs

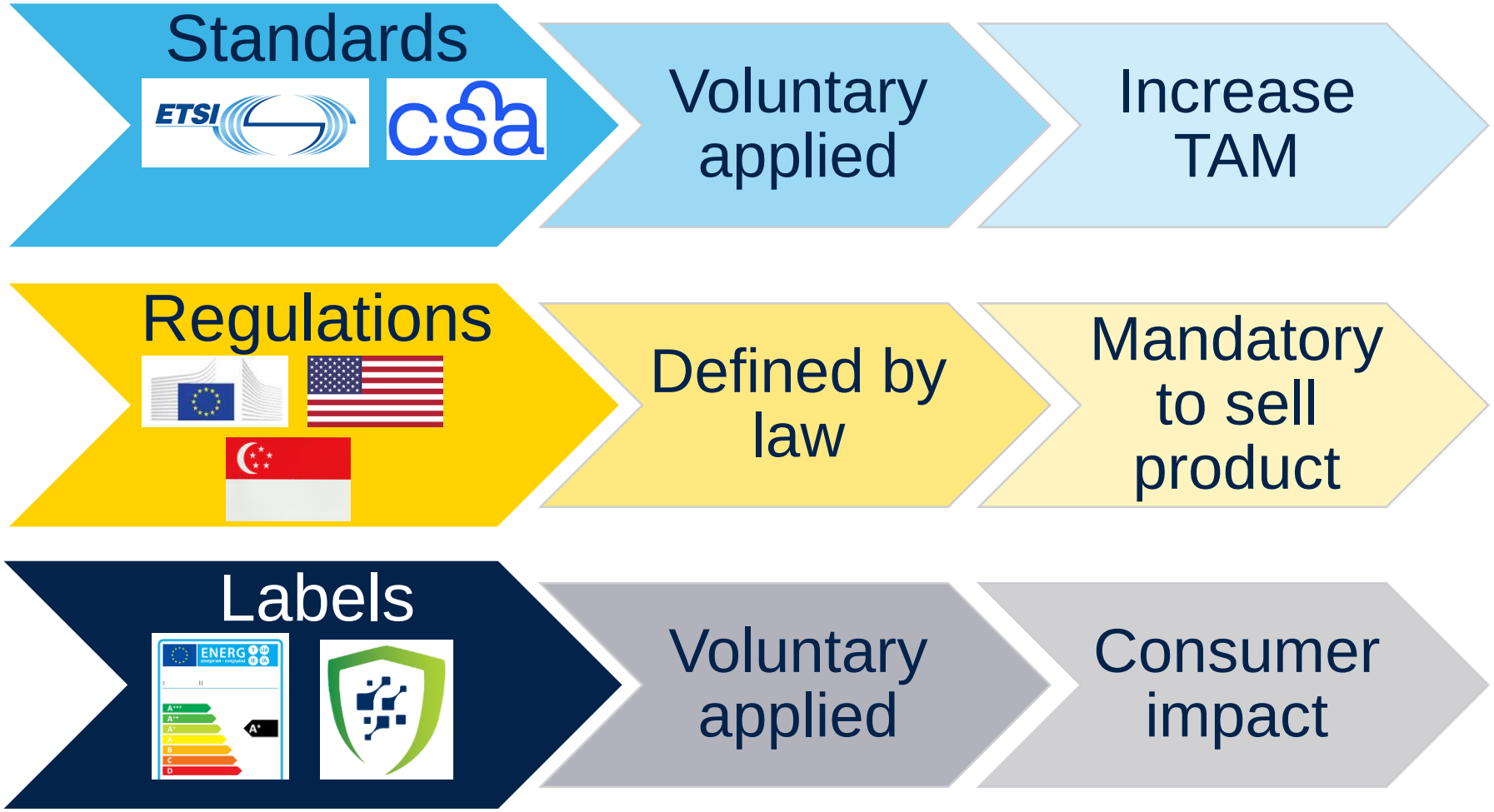
- **STM32WL** — 162 CoreMark, 48 MHz Cortex-M4, 48 MHz Cortex-M0+
- **STM32WB0** — 64 MHz Cortex-M0+
- **STM32WB** — 216 CoreMark, 64 MHz Cortex-M4, 32 MHz Cortex-M0+ (Radio co-processor only)
- **STM32WBA5/6** — 407 CoreMark, 100 MHz Cortex-M33

Latest product generation · Radio co-processor only · New series & lines introduced in 2024 · Pre-announcement

life.augmented

Certifications & Regulations

Standards / Regulations / Labels



RED & CRA

Radio Equipment Directive (RED)

Essential requirements for radio equipment

- EMC, safety/health, privacy & fraud protection
- **No known vulnerability** at product launch
- Be capable to **update/patch** the products
- Conformity assessment with **risk-based** approach
  - HW component: N/A
  - IoT consumer & industrial devices: self-declaration
  - Medical devices & auto: exemption

Cyber Resilience Act (CRA)

Ensures secure HW & SW products on the market

- **Active monitoring** of vulnerabilities
- Provide **update/patch** for products
- Different security levels according to **predefined categories**
  - Hardware component: Third-party evaluation
  - IoT consumer devices: self-declaration
  - IoT industrial devices: Third-party evaluation

August 1, 2025

CRA should repel RED

life.augmented

US Cyber Trust Mark

IoT security labeling program

- Voluntary cybersecurity labeling program initiated by the White House based on NIST 8425
- Targets IoT devices for smart home
- Operated by FCC operational in 2024

Connectivity Standards Alliance (CSA) Consortium

- Security certification program
- Covering NIST 8425, ETSI 303 645 & Singapore CSA CLS
  - Pilot program started in Sept. 23

Cybersecurity Labelling Scheme
BY CYBER SECURITY AGENCY OF SINGAPORE

Singapore CLS

Cyber Security Agency

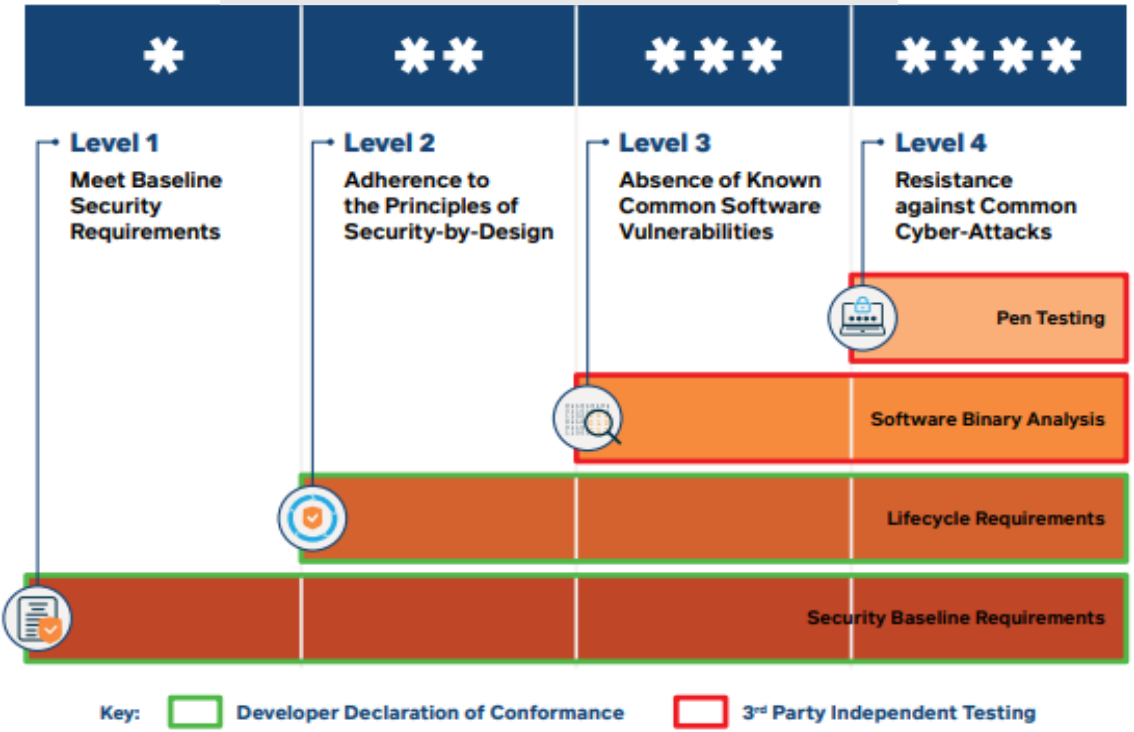
Cybersecurity Labeling Scheme (CLS)

- provide an indication of the security level of IoT products to consumer
- Incentivize developers/manufacturers to deliver enhanced cybersecurity provisions

Cybersecurity Labelling Scheme
BY CYBER SECURITY AGENCY OF SINGAPORE

Singapore CLS

Multiple security levels



Multiple recognition

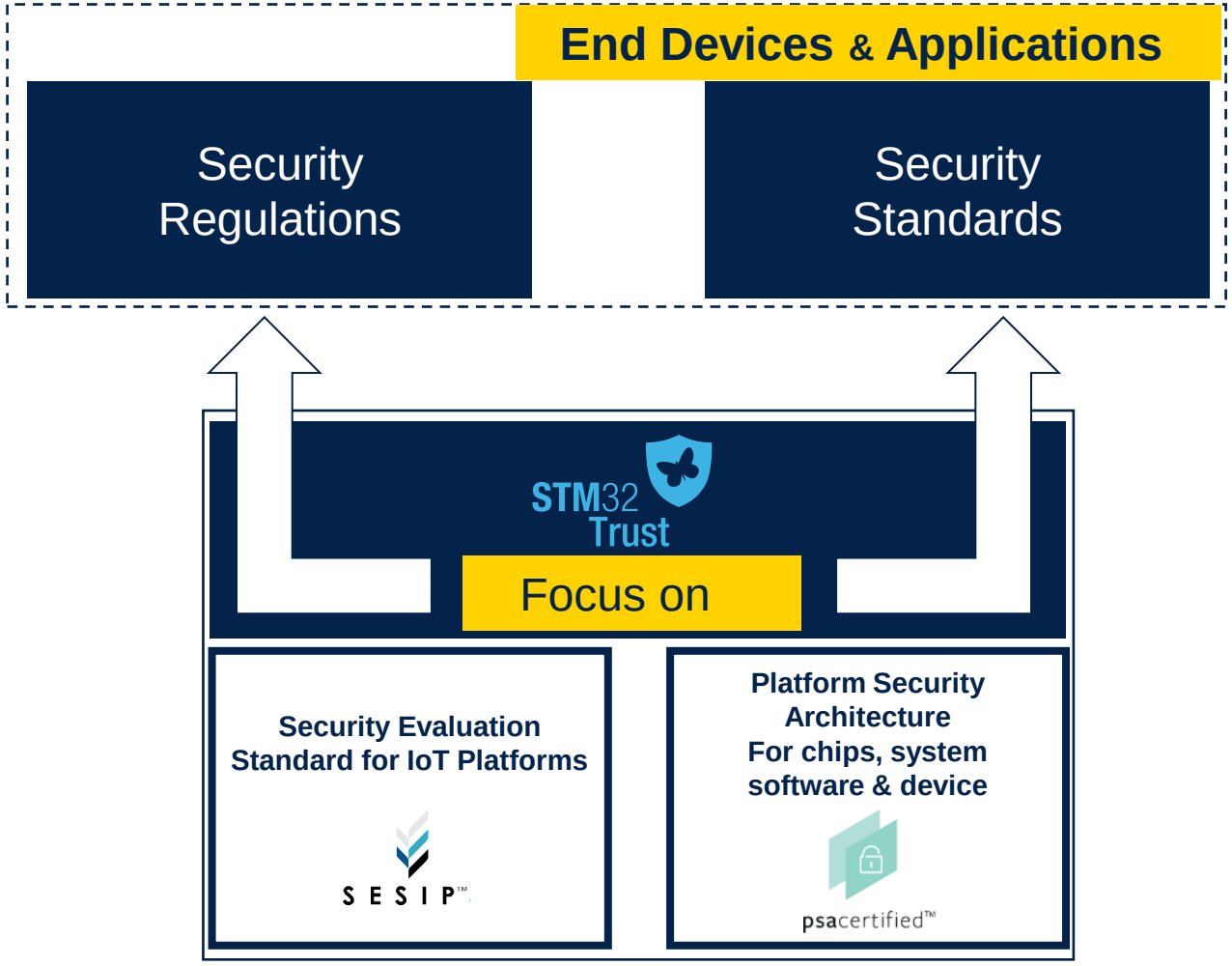
- CLS Level 2 and above with Germany
- CLS Level 3 and above with Finland

CLS-ready program

- Applies to subcomponents
- SESIP methodology may be applicable

life.augmented

ST Objective ➔ To cover all programs



Focusing on RED

Product harmonization legislation in the EU

LEGISLATION

MANDATORY

STANDARDS

VOLUNTARY

CONFORMITY ASSESSMENT

MARKET SURVEILLANCE

Focusing on RED

The Radio Equipment Directive

- Initial regulatory framework in Directive 2014/53/EU
- Cybersecurity requirements added on October 2021 ➔ Article 3(3) points (d), (e) and (f)
- Objective: To protect the user from cybersecurity risk

(d) Does not harm the network

(e) Personal data and privacy of the user & subscriber are protected

(f) Ensuring protection from fraud

Focusing on RED

Radio equipment categories

- EU delegated regulations 2022/30 & (EU) 2023/2444
- All products with an antenna

Connected directly
or indirectly to the Internet

Handling personal
or childcare data

Processing financial
transactions

Exemptions

Medical
devices

Civil
aviation

Motor
vehicles

Toll
systems

Full exemption

Partial exemption on 3.3(e) and (f) but (d) is enforced

Focusing on RED

From essential requirements to standardization requests

- Legal requirements to be supported by the harmonized standards
- Technical specifications covering article 3(3) points (d), (e) and (f), and test methods

Harmonized Standards

They ensure that the radio equipment

- ► includes elements to monitor and control network traffic, including the transmission of outgoing data, for item (d)
- ► is designed to mitigate the effects of ongoing denial of service attacks: for point (d)
- ► implements appropriate authentication and access control mechanisms: for point (d)/(e)/(f)
- ► is provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards harm to the points (d)/(e)/(f)
- ► are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to points (d)/(e)/(f)
- ► protects stored, transmitted or otherwise processed (e)/(f) against accidental or unauthorised storage, processing, access, disclosure, unauthorized destruction, loss or alteration or lack of availability of points (e)/(f)
- ► includes functionalities to inform the user of changes that may affect data protection and privacy: for point (e)
- ► logs the internal activity that can have an impact on points (e)/(f)
- ► allows users to easily delete their stored personal data, enabling the disposal or replacement of equipment without the risk of exposing personal information, for point (e)

Excerpt from Annexes 1& 2 to the Commission Implementing Decision C(2022) 5637 final

Meeting RED with SESIP

SESIP: explicit security functions

A baseline for IoT platform certification

Identification and attestation of platforms and applications

- ▶ Verification of platform identity
- ▶ Verification of platform instance identity
- ▶ Verification of platform genuineness
- ▶ Security initialization of the platform
- ▶ Attestation of platform state
- ▶ Attestation of application genuineness
- ▶ Attestation of application state

Secure communication

- ▶ Secure communication support
- ▶ Secure communication enforcement

Managed by ST

Product life cycle: factory reset / install / update / decommission

- ▶ Factory reset of platform
- ▶ Secure install of application
- ▶ Secure update of the platform
- ▶ Secure uninstall of application
- ▶ Decommission of platform
- ▶ Field Return of Platform

SESIP™

life.augmented

SESIP: Explicit Security Functions

A baseline for IoT platform certification

Extra attacker

- ▶ Limited physical attacker resistance
- ▶ Physical attacker resistance
- ▶ Software attacker resistance: isolation of platform
- ▶ Software Attacker resistance: isolation of platform parts
- ▶ Software attacker resistance: isolation of application parts

Cryptographic functionality

- ▶ Cryptographic operation
- ▶ Cryptographic key generation
- ▶ Cryptographic keystore
- ▶ Cryptographic Random Number Generation

SESIP™

Managed by ST

Compliance functionality

- ▶ Secure trusted storage
- ▶ …

Access control

- ▶ Privileged access control
- ▶ …

Availability

- ▶ Secure Communication Enforcement
- ▶ …

SESIP to be recognized as an EN security standard !

life.augmented

SESIP ➔ RED

SESIP3 certification target

SESIP Security Functions

- ► Verification of platform identity
- ► Verification of platform instance identity
- ► Verification of platform genuineness
- ► Security initialization of the platform
- ► Attestation of platform state
- ► Secure update of the platform
- ► Physical attacker resistance
- ► Software attacker resistance: isolation of platform
- ► Cryptographic operation
- ► Cryptographic key generation
- ► Cryptographic keystore
- ► Cryptographic Random Number Generation
- ► Field return of Platform
- ► Secure trusted storage

RED Technical Specifications

- ► include elements to monitor and control network traffic, including the transmission of outgoing data, for item (d)
- ► is designed to mitigate the effects of ongoing denial of service attacks : for point (d)
- ✓ ► implement appropriate authentication and access control mechanisms: for point (d)/(e)/(f)
- ✓ ► are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards harm to the points (d)/(e)/(f)
- ✓ ► are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to points (d)/(e)/(f)
- ✓ ► protect stored, transmitted or otherwise processed (e)/(f) against accidental or unauthorised storage, processing, access, disclosure, unauthorised destruction, loss or alteration or lack of availability of points (e)/(f)
- ✓ ► include functionalities to inform the user of changes that may affect data protection and privacy: for point (e)
- ✓ ► log the internal activity that can have an impact on points (e)/(f)
- ✓ ► allow users to easily delete their stored personal data, enabling the disposal or replacement of equipment without the risk of exposing personal information, for point (e)

life.augmented

3 KeyTakeaways

How to meet RED coming regulation ? The answer is STM32 w/SESIP

#1: SESIP supports & speeds up conformance to RED

- Key security functions supported
- SESIP is now the European standard EN 17927

#2: ST as the key supplier for RED conformance

- Thanks to STM32 HW/SW security features
- SESIP target in mind from the ground-up

#3: Some limitations

- Some RED requirements covered at the app level only
- Evaluation to be managed by the OEM

life.augmented

Q&A

life.augmented

Our technology starts with You

life.augmented