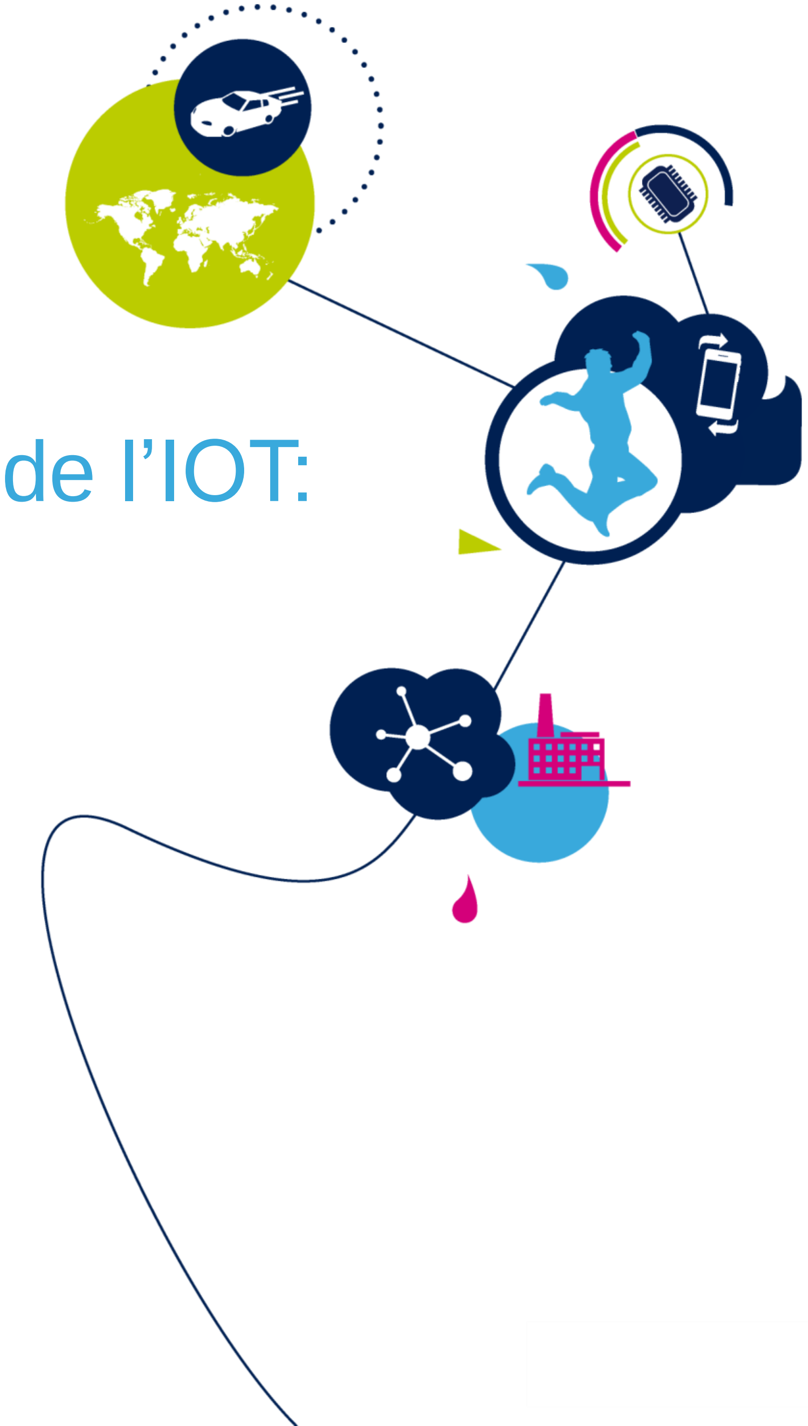
Au coeur du monde connecté, les défis de l’IOT:
STMicroelectronics STM32Trust

8 oct 2019

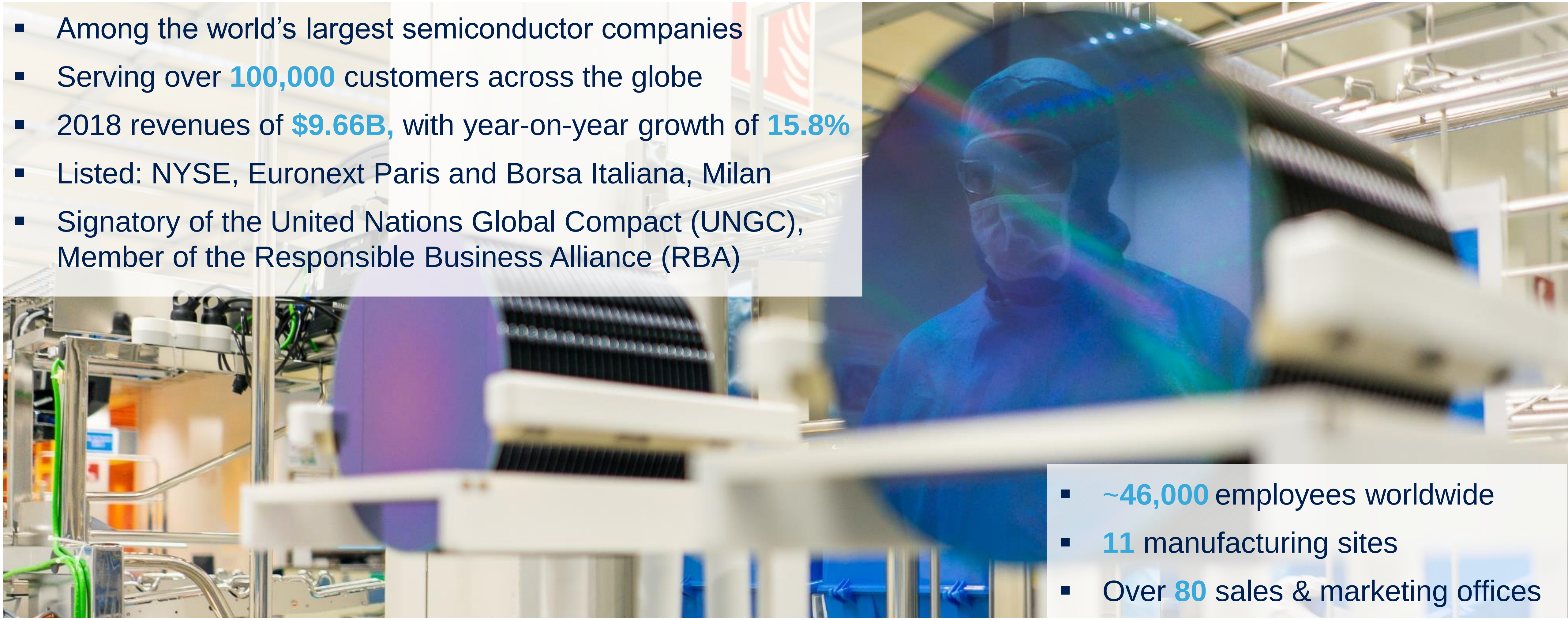
Laurent DESSEIGNES / Christophe MANI



Introduction

life.augmented

STMicroelectronics Presentation



- Among the world’s largest semiconductor companies
- Serving over **100,000** customers across the globe
- 2018 revenues of **$9.66B,** with year-on-year growth of **15.8%**
- Listed: NYSE, Euronext Paris and Borsa Italiana, Milan
- Signatory of the United Nations Global Compact (UNGC), Member of the Responsible Business Alliance (RBA)

- ~**46,000** employees worldwide
- **11** manufacturing sites
- Over **80** sales & marketing offices

Smart Things

Smart Home & City

Smart Industry

Smart Driving

IoT / Smart Connected Objects

300 million in 2017

800 million in 2021

Wearable computing devices

0.4 billion in 2017

1.8 billion in 2021

Excluding PCs & digital home

4 billion in 2017

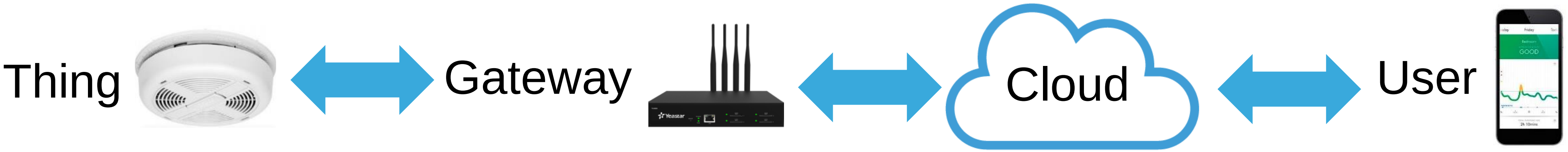
10 billion in 2021

Retail, advertising, supply chain & Industrial IoT

1.1 billion in 2017

2.2 billion in 2021

The IoT Topology and Equation



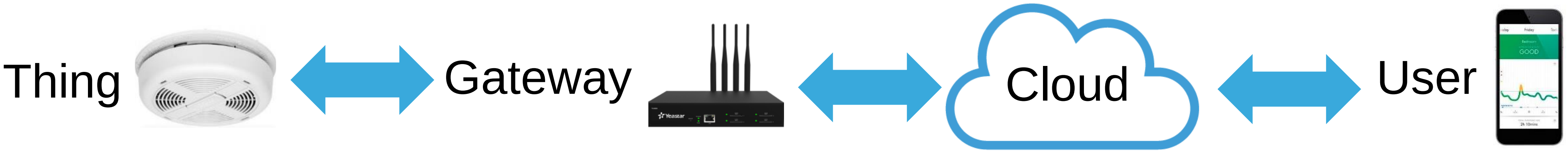
Thing

Gateway

Cloud

User

The IoT Topology and Equation

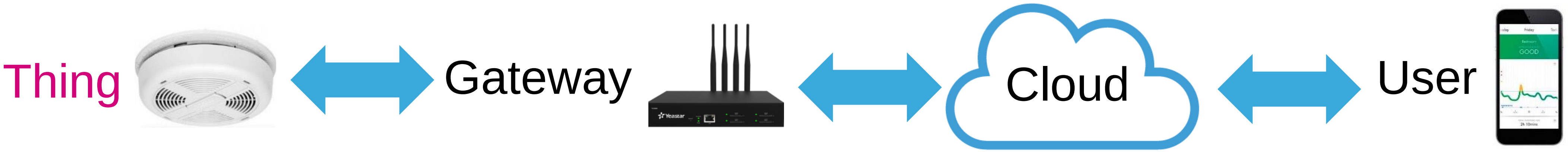


Thing ↔ Gateway ↔ Cloud ↔ User

The IoT Equation:

IoT =

The IoT Topology and Equation

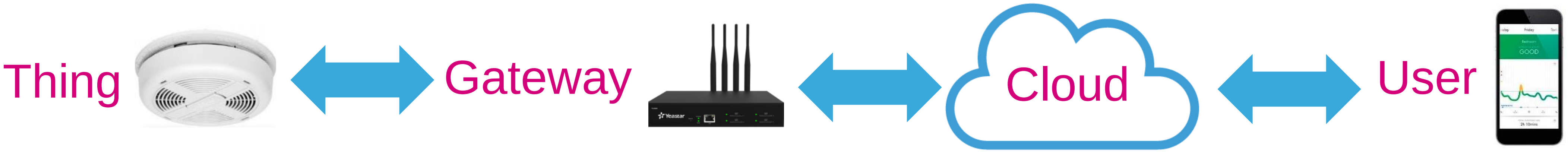


Thing ⟷ Gateway ⟷ Cloud ⟷ User

The IoT Equation:

IoT = Data +

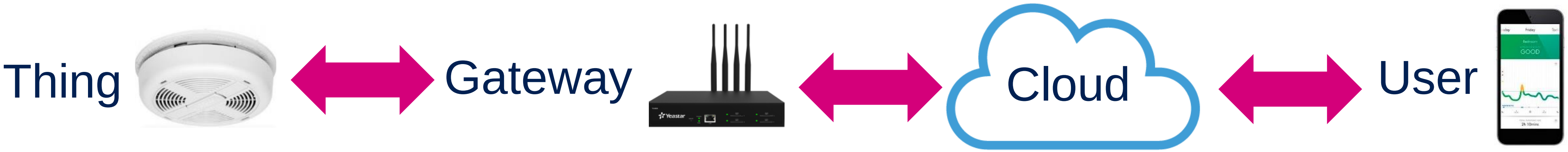
The IoT Topology and Equation



The IoT Equation:

IoT = Data + Processing +

The IoT Topology and Equation

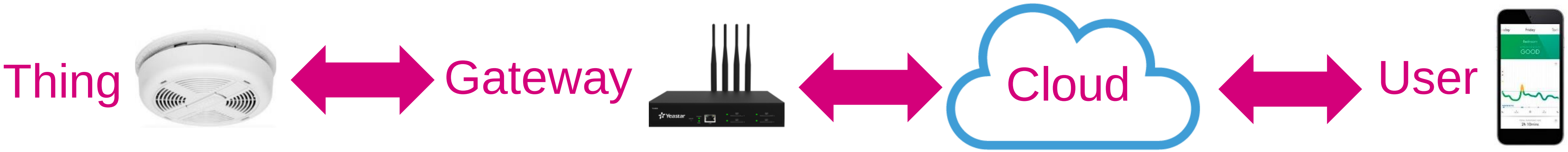


Thing ⟷ Gateway ⟷ Cloud ⟷ User

The IoT Equation:

IoT = Data + Processing + Connectivity +

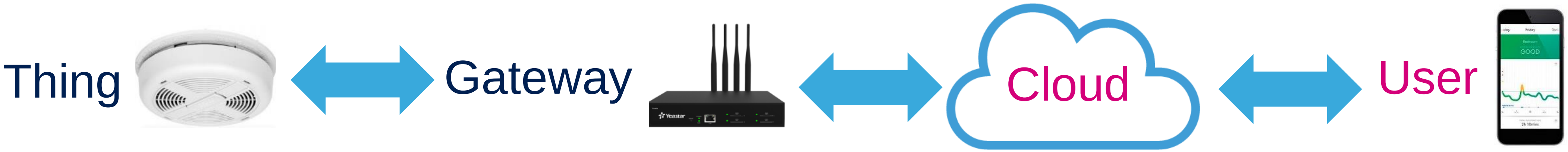
The IoT Topology and Equation



The IoT Equation:

IoT = Data + Processing + Connectivity + Security +

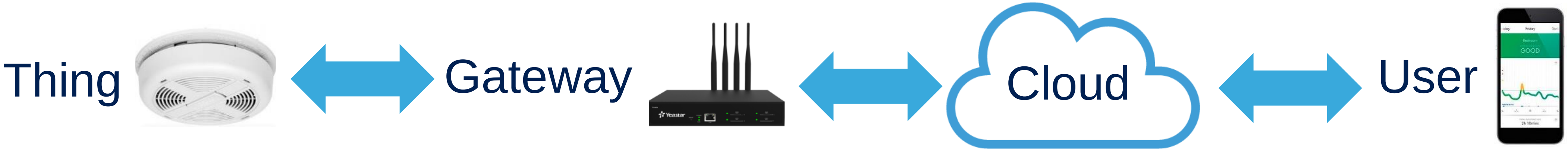
The IoT Topology and Equation



The IoT Equation:

IoT = Data + Processing + Connectivity + Security + Services

The IoT Topology and Equation

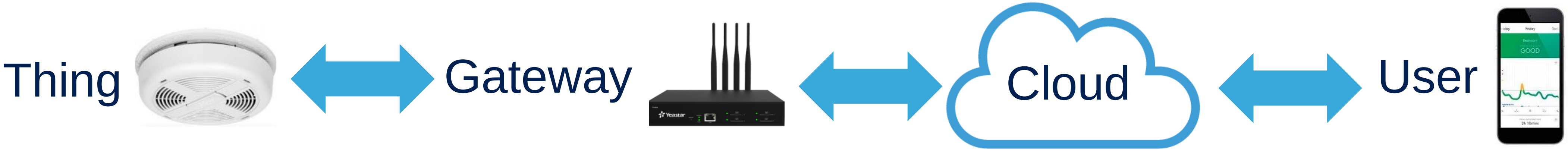


Thing ⟷ Gateway ⟷ Cloud ⟷ User

The IoT Equation:

IoT = Data + Processing + Connectivity + Security + Services

The IoT Topology and Equation



Thing

Gateway

Cloud

User

The IoT Equation:

IoT = Data + Processing + Connectivity + Security + Services

Focus for this presentation, with Microcontrollers offers

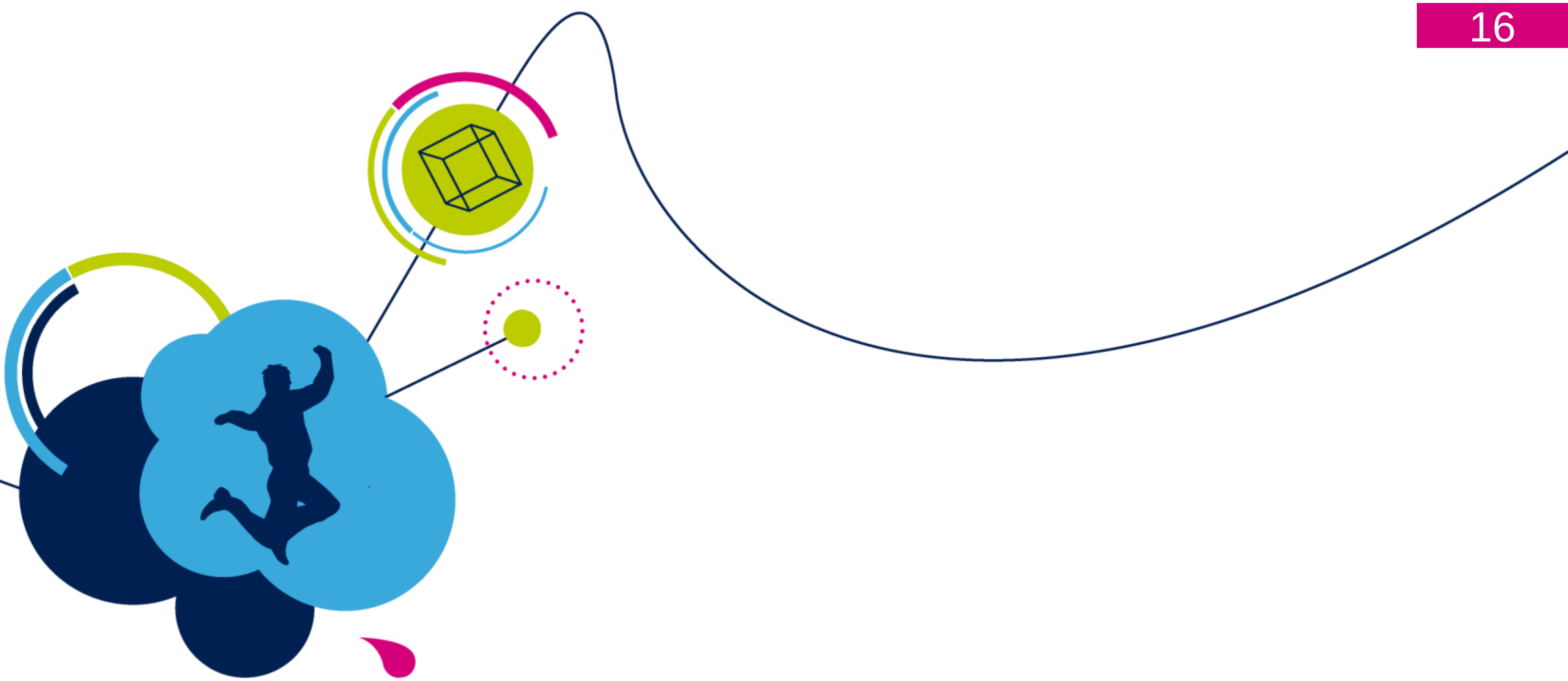
ST: A serious player in Processing & Security

General Purpose Microcontrollers
(GP MCUs)

#2 world-wide in 2018

Secure Microcontrollers
(Secure MCUs)

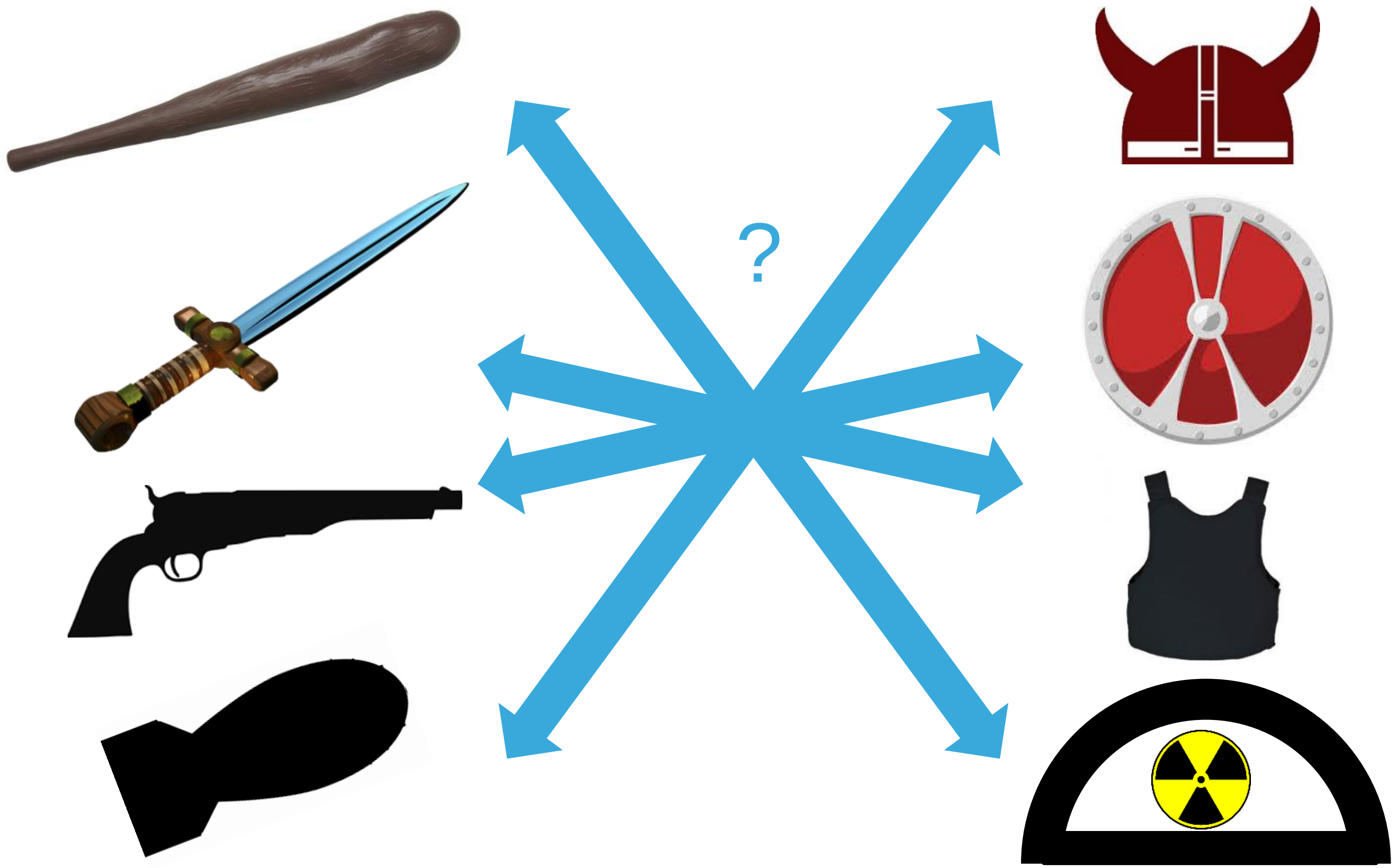
#3 world-wide in 2018



STM32Trust

Security: Introduction

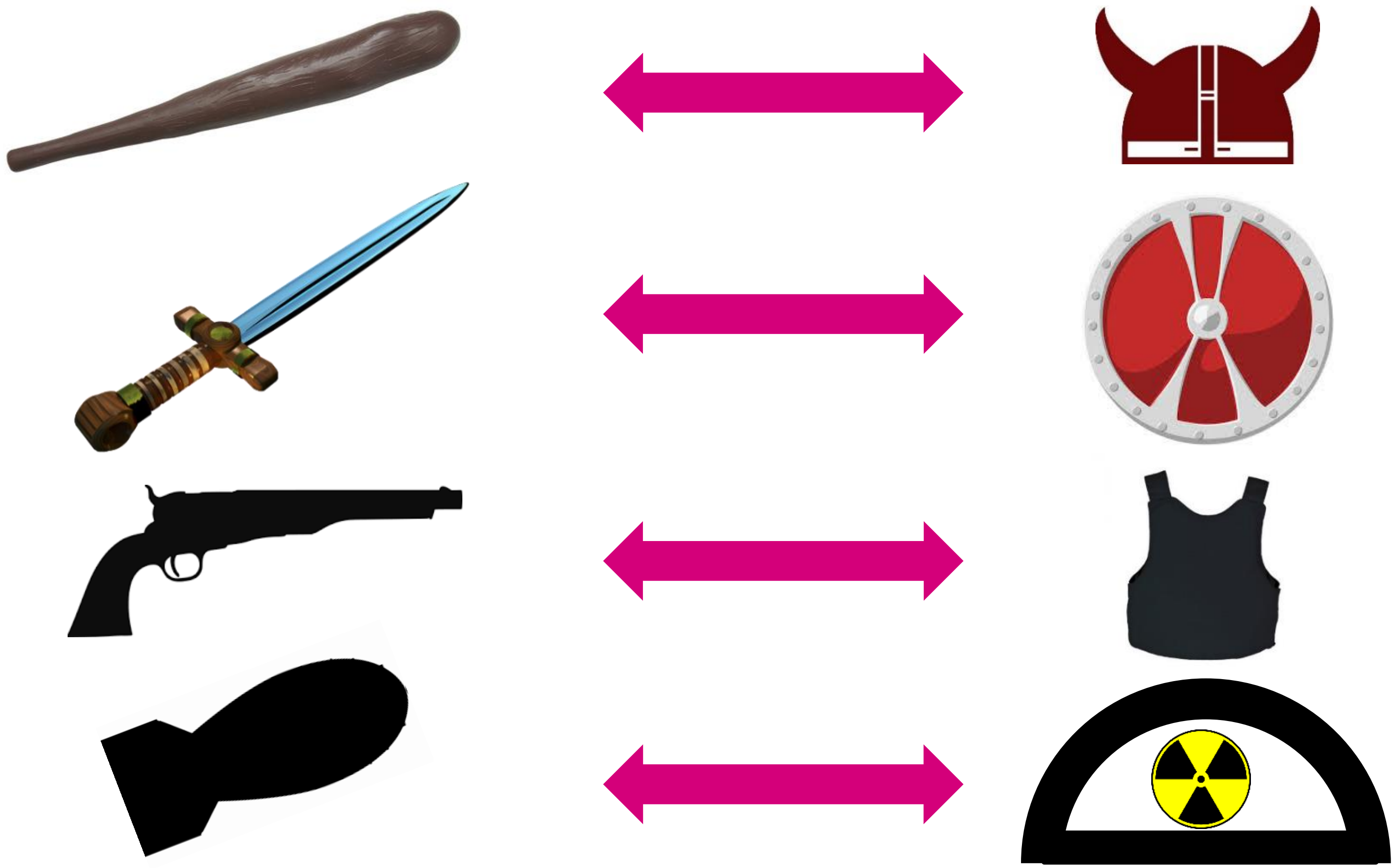
Security is an endless war, similar to the one of Weapon and Shield



Security: Introduction

Security is an endless war, similar to the one of Weapon and Shield

Need for having the correct Shield versus a given Weapon



The Attack Levels

Cost and expertize of attack materials

Today 95% of IoT attacks

Logical

- Local or remote
- Open ports
- Software Bugs
- Debug Interfaces
- Etc.

Board-level

- Local
- Memory probing
- Fault injection
- Side-channels attacks
- Etc.

Chip-level

- Local
- Probing
- Laser
- Reverse Engineering
- Etc.

General Purpose Microcontrollers (MCUs)

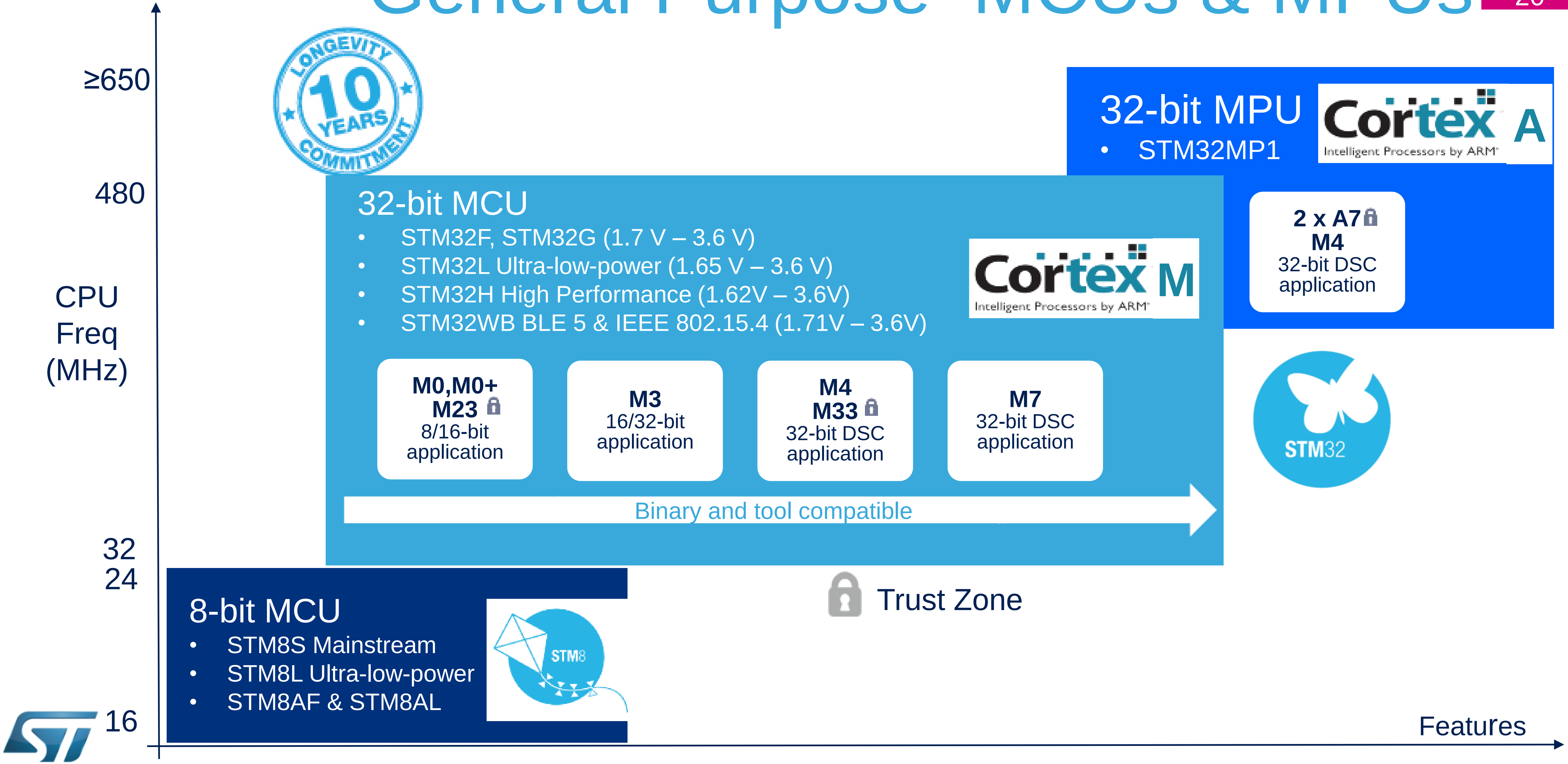
On-going…

Secure Microcontrollers (MCUs)

Focus for this presentation

life.augmented

General Purpose MCUs & MPUs


≥650
480
CPU Freq (MHz)
32
24
16
Features
LONGEVITY 10 YEARS COMMITMENT
Cortex A Intelligent Processors by ARM
Cortex M Intelligent Processors by ARM
STM32
STM8

32-bit MPU

- STM32MP1

2 x A7 🔒
M4
32-bit DSC application

32-bit MCU

- STM32F, STM32G (1.7 V – 3.6 V)
- STM32L Ultra-low-power (1.65 V – 3.6 V)
- STM32H High Performance (1.62V – 3.6V)
- STM32WB BLE 5 & IEEE 802.15.4 (1.71V – 3.6V)

M0,M0+
M23 🔒
8/16-bit application

M3
16/32-bit application

M4
M33 🔒
32-bit DSC application

M7
32-bit DSC application

Binary and tool compatible

8-bit MCU

- STM8S Mainstream
- STM8L Ultra-low-power
- STM8AF & STM8AL

🔒 Trust Zone

STM32 General Purpose MCUs

2007	vs	2018
#11	GP MCU Ranking ST Rank	#2
5 %	MCU Market Share ST Share	20 %
0 %	Cortex-M Market Share ST Share	41%
0	STM32 Part Numbers	1 600
0	Shipped STM32	>3 Billion

STM32 General Purpose MCUs & Security

Historically addition of Security Ingredients: Not readable by customers…

- MPU – Memory Protection Unit
- Firewall
- RDP – Read Protection
- PcRoP- Proprietary Code Protection
- Execute Only
- Debug Lock

- Tamper detection
- Tamper sensors
- Unique Identifiers
- Crypto accelerators
- Hash accelerators
- …

life.augmented

Macro cases: What to protect in MCUs ?

Customer values	Needed Protection
Whole code running in MCU	Ability to not expose the code
Partial code running in MCU	Ability to isolate trusted code from non-trusted
Full control of their devices	Authenticity and integrity of programmed code
Secret data stored in MCU	Ability to not expose secret
User data	Ability to not expose data

Macro cases: What to protect in MCUs ?

Customer values	Needed Protection	ST Answer today
Whole code running in MCU	Ability to not expose the code	STM32 + STM32 Trust
Partial code running in MCU	Ability to isolate trusted code from non-trusted	STM32 + STM32 Trust
Full control of their devices	Authenticity and integrity of programmed code	STM32 + STM32 Trust
Secret data stored in MCU	Ability to not expose secret	STM32 + STSAFE
User data	Ability to not expose data	STM32 + STSAFE

Introducing STM32Trust

Consistent Security ecosystem around STM32

Code Protection

Means in Silicon, Software, Tools and Service to **Trust** the firmware programming action:

- **SFI** - Secure Firmware Install solution
- Libraries for **SBSFU** - Secure Boot / Secure Firmware Update
- Tools for SFI/SBSFU:
  - STM32CubeProgrammer and STM32HSM

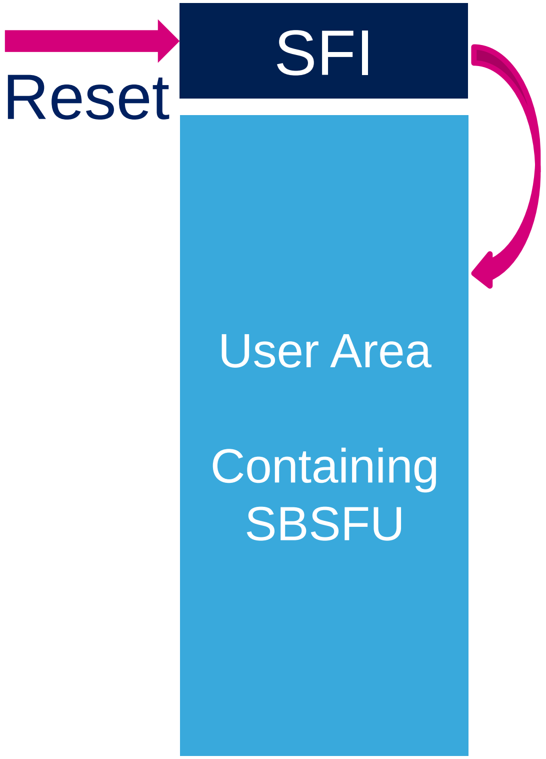
Execution Protection

Means in Silicon, Software, Tools and Service to **Trust** the firmware execution:

- Control over Debug
- Secure Boot / Root of Trust
- Isolation: MPU, Dual Core, Firewall, TrustZone

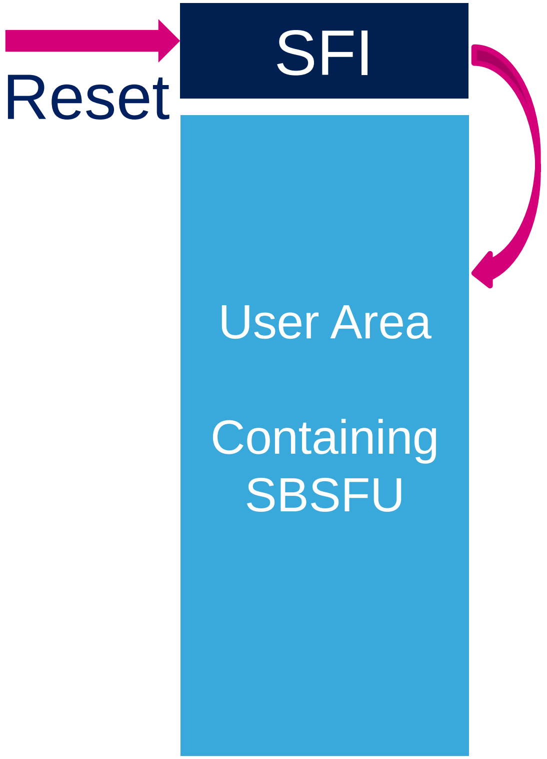
SFI and SBSFU (1/4)

- SFI – Secure Firmware Install
    - A **native** software service built-in latest STM32 MCUs
        - “Temporal” isolation at boot
    - Made to ensure 1st programmation of a firmware securely, i.e.:
        - No access to software from Manufacturer
        - Limited counted occurrences of software by Manufacturer
    - Achieved via full ecosystem provided by ST and partners



- SBSFU – Secure Boot / Secure Firmware Update
    - A **reference code** to let customer make his own implementation
    - Examples of implementations with different transport medias

SFI and SBSFU (2/4)



Reset

SFI

User Area

Containing SBSFU

STM32
Secure Loader

Loading of Code for user area

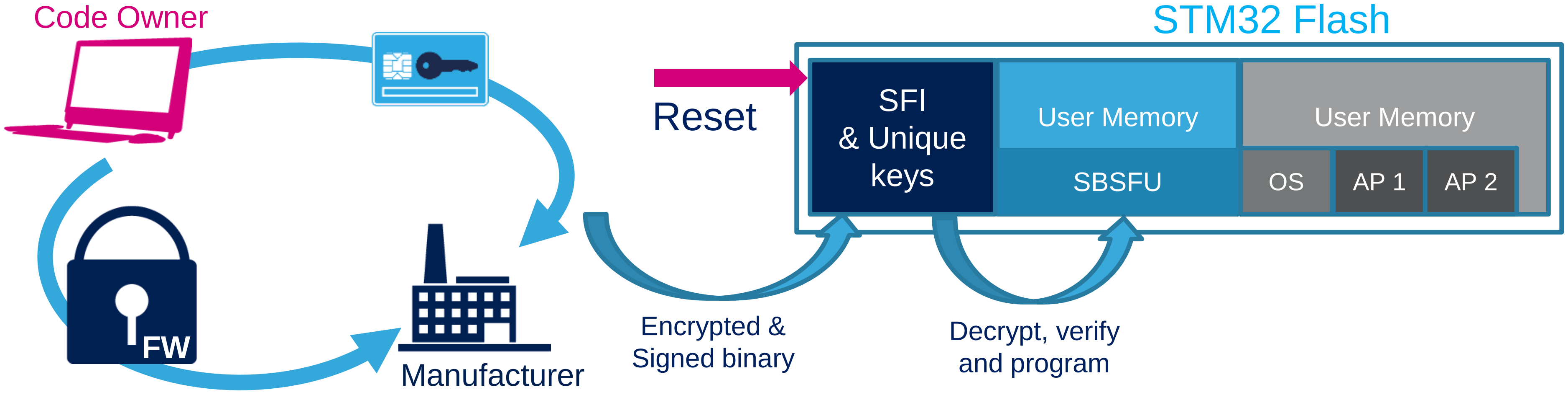
Supported Communication interface
UART / SPI / USB

CA certificate, key and SFI services
Provisioned by ST in standard STM32
➔ Mass Market approach

SFI and SBSFU (3/4)

The loading process

- At manufacturing:



Code Owner

Manufacturer

Encrypted & Signed binary

Reset

STM32 Flash

SFI & Unique keys

User Memory

SBSFU

User Memory

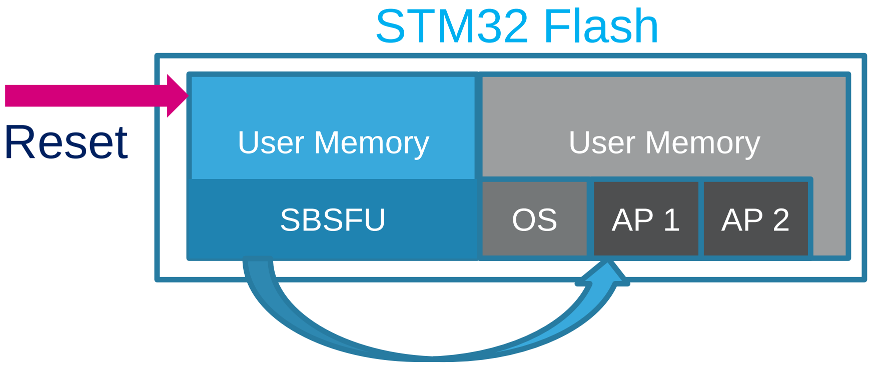
OS

AP 1

AP 2

Decrypt, verify and program

- During Device life time:
  - SFI removed
  - Protected by Secure Boot
  - Optional Secure Updates



STM32 Flash

Reset

User Memory

SBSFU

User Memory

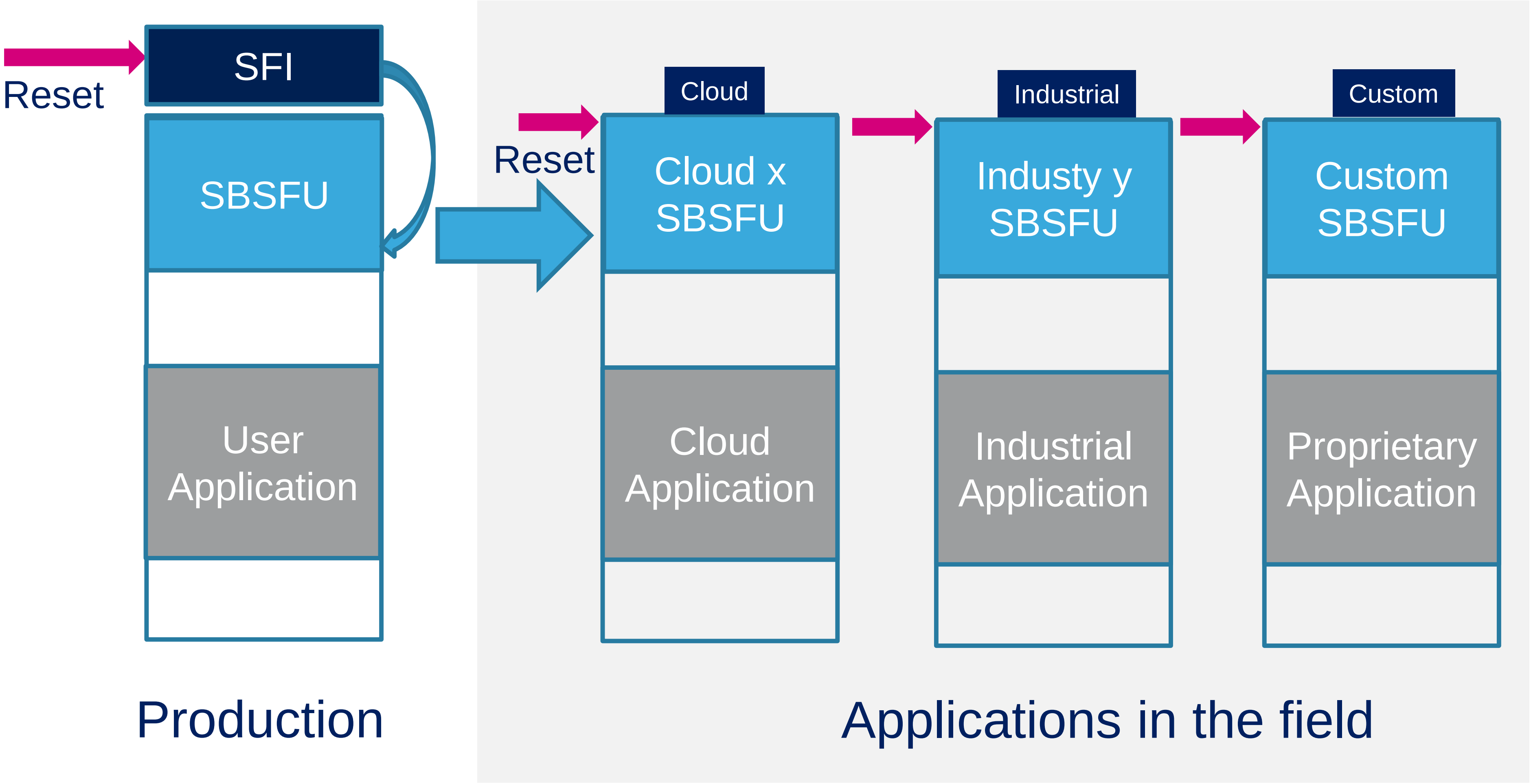
OS

AP 1

AP 2

SFI and SBSFU (4/4)

- Secure loading adapting real applications cases

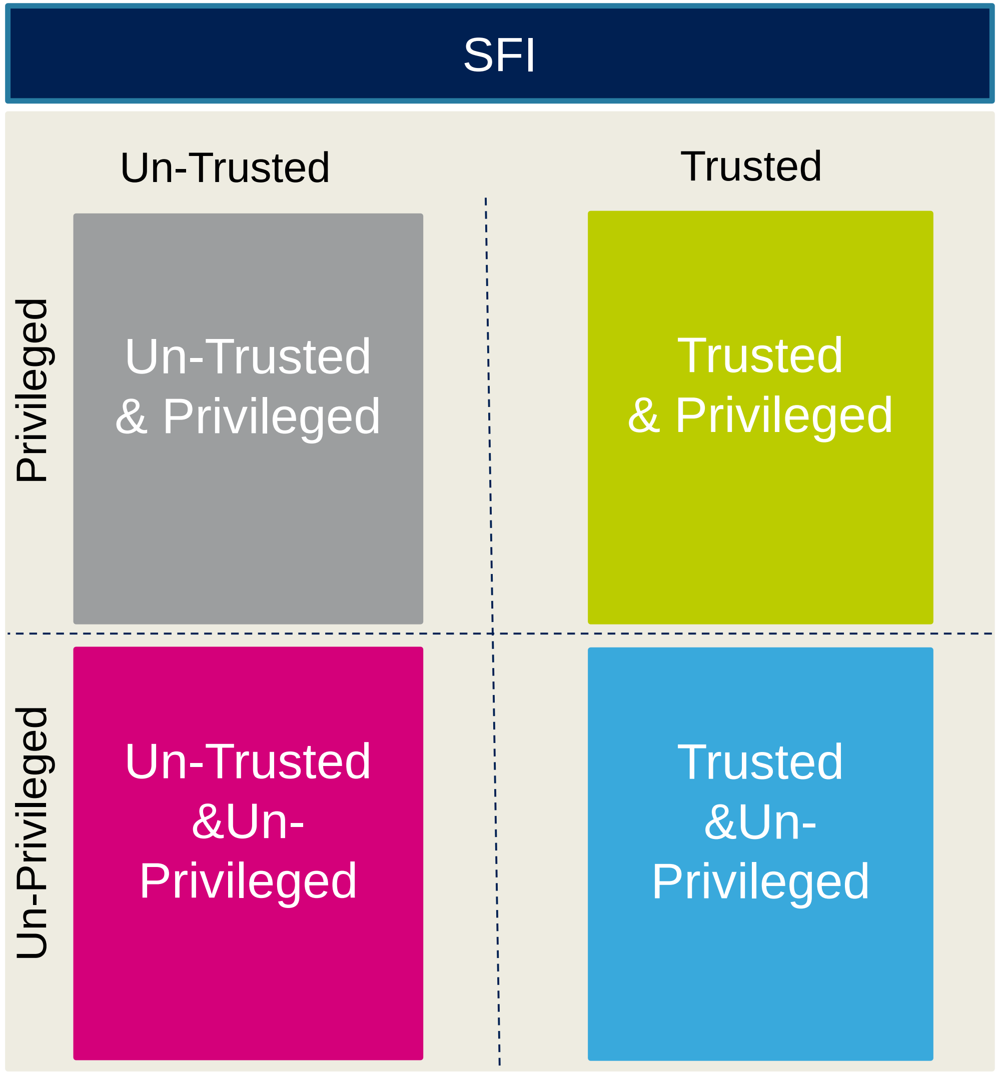


More information ?

www.st.com/stm32trust

One last word:
Upcoming new offers & Certifications

Newcoming STM32L5: more isolations



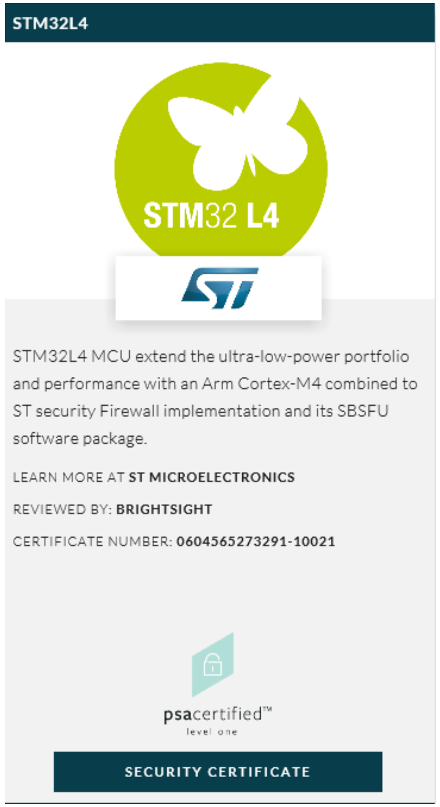
SFI

	Un-Trusted	Trusted
Privileged	Un-Trusted & Privileged	Trusted & Privileged
Un-Privileged	Un-Trusted &Un-Privileged	Trusted &Un-Privileged

- More partitioning
- Possibility to separate the trusted and un-trusted area with **privileged and un-privileged** zone
- And still SFI / SBSFU !

Certifications / Evaluations

- Evaluations are done by some external companies, 100% independently
- Certifications Targets: arm PSA (Levels 1 and 2) and SESIP (1 to 3)
  Currently:



STM32L4

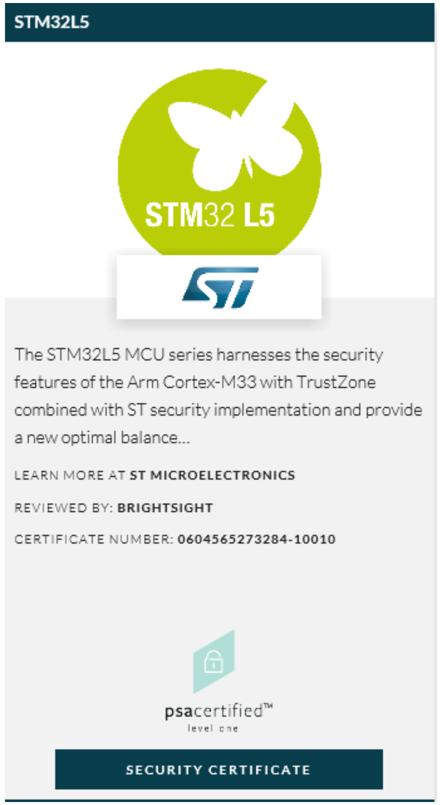
STM32L4 MCU extend the ultra-low-power portfolio and performance with an Arm Cortex-M4 combined to ST security Firewall implementation and its SBSFU software package.

LEARN MORE AT **ST MICROELECTRONICS**

REVIEWED BY: **BRIGHTSIGHT**

CERTIFICATE NUMBER: **0604565273291-10021**

SECURITY CERTIFICATE



STM32L5

The STM32L5 MCU series harnesses the security features of the Arm Cortex-M33 with TrustZone combined with ST security implementation and provide a new optimal balance...

LEARN MORE AT **ST MICROELECTRONICS**

REVIEWED BY: **BRIGHTSIGHT**

CERTIFICATE NUMBER: **0604565273284-10010**

SECURITY CERTIFICATE

Thank you ! Questions ?

/STM32 @ST_World community.st.com