life.augmented

Security Framework for Embedded Systems

Sridhar Ethiraj

3rd Aug 2022

Agenda

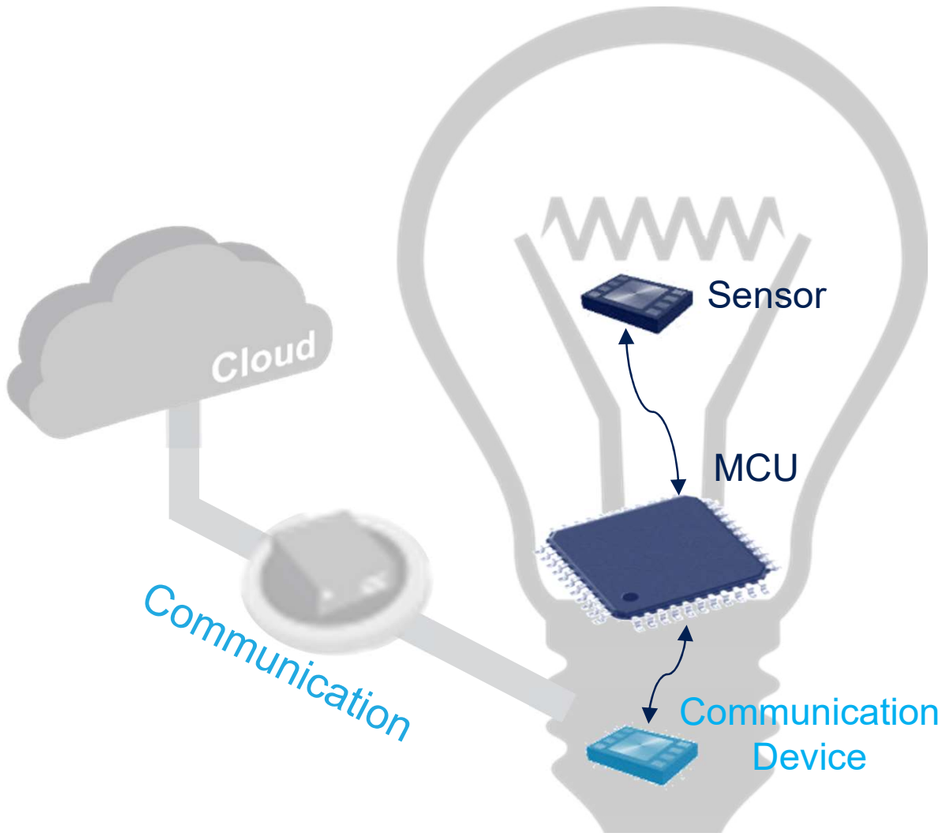
1. Introduction
2. Security threats and counter measures
3. Security layering and Protection
4. Security Functions
5. Security Assurance Levels and Certifications
6. Take away

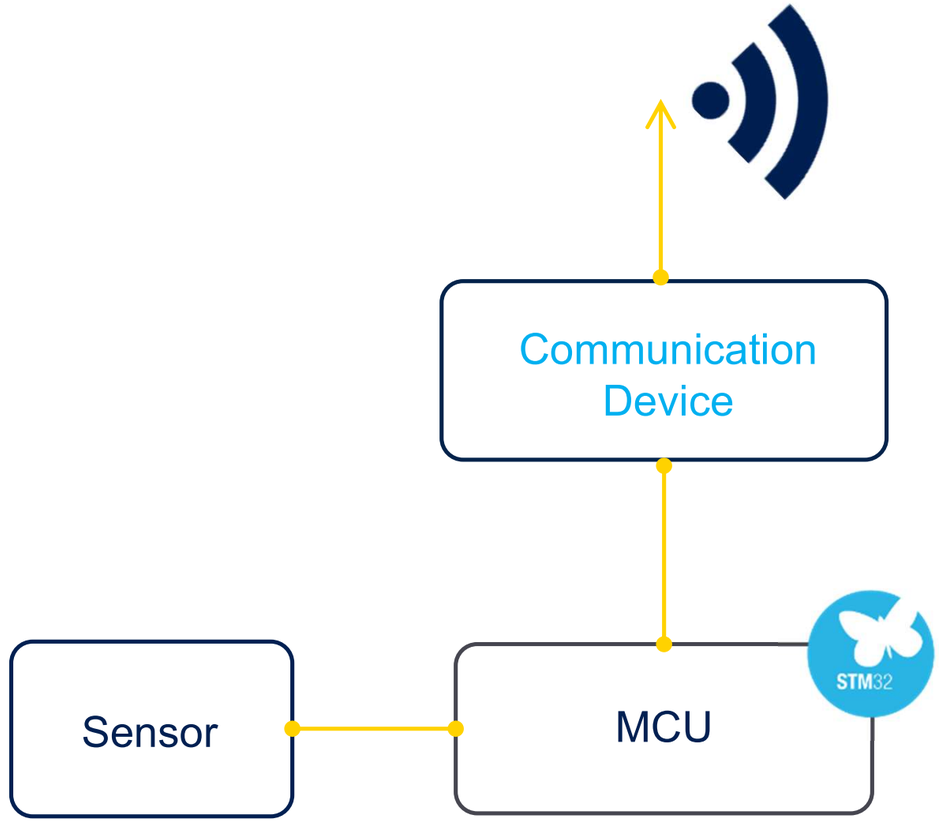
life.augmented

Introduction

life.augmented

Simple IoT Device





Connected objects
Our concern for tomorrow

2020

Operating system -based solutions

65%

Connected objects

20 billion

2025

Embedded solutions

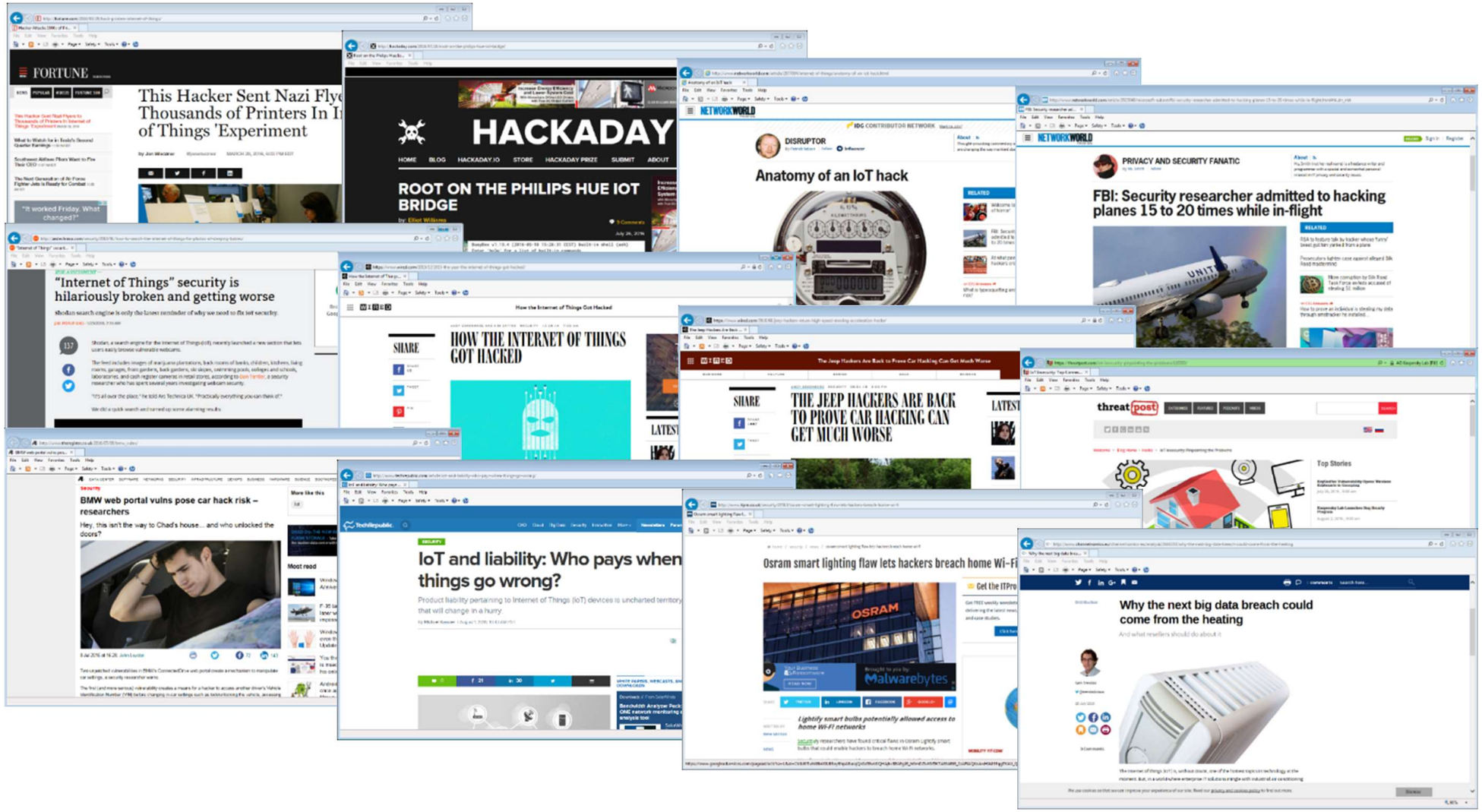
65%

Connected objects

48 billion

life.augmented

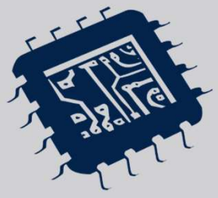
In the news


FORTUNE
This Hacker Sent Nazi Flyers to Thousands of Printers In Internet of Things 'Experiment
HACKADAY
ROOT ON THE PHILIPS HUE IOT BRIDGE
NETWORKWORLD
Anatomy of an IoT hack
PRIVACY AND SECURITY FANATIC
FBI: Security researcher admitted to hacking planes 15 to 20 times while in-flight
"Internet of Things" security is hilariously broken and getting worse
How the Internet of Things Got Hacked
HOW THE INTERNET OF THINGS GOT HACKED
THE JEEP HACKERS ARE BACK TO PROVE CAR HACKING CAN GET MUCH WORSE
threatpost
Top Stories
BMW web portal vulns pose car hack risk – researchers
Techrepublic
IoT and liability: Who pays when things go wrong?
Osram smart lighting flaw lets hackers breach home Wi-Fi
Why the next big data breach could come from the heating

Categories of attacks

95% of IoT attacks today

Cloning attacks



Logical

- Local or remote
- Open ports
- SW bugs
- Debug I/Fs

and more…

Board-level

- Memory probing
- “Mod-chips”
- Fault injection
- Side-channels

and more…

Chip-level

- Probing
- Laser
- FIB
- Reverse eng.

and more…

Cost and expertise of attack materials

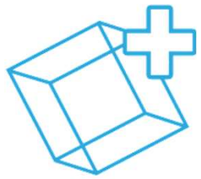
- **Logical attack**
  From outside the box
- **Board-level attack**
  From Inside the box
- **Chip-level attack**
  From Inside the chip

Secure Boot
Root of Trust

life.augmented

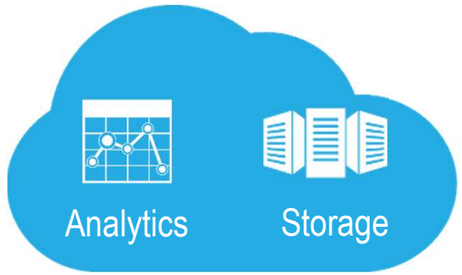
End-to-end security in the IoT

Securing the IoT means securing every stage

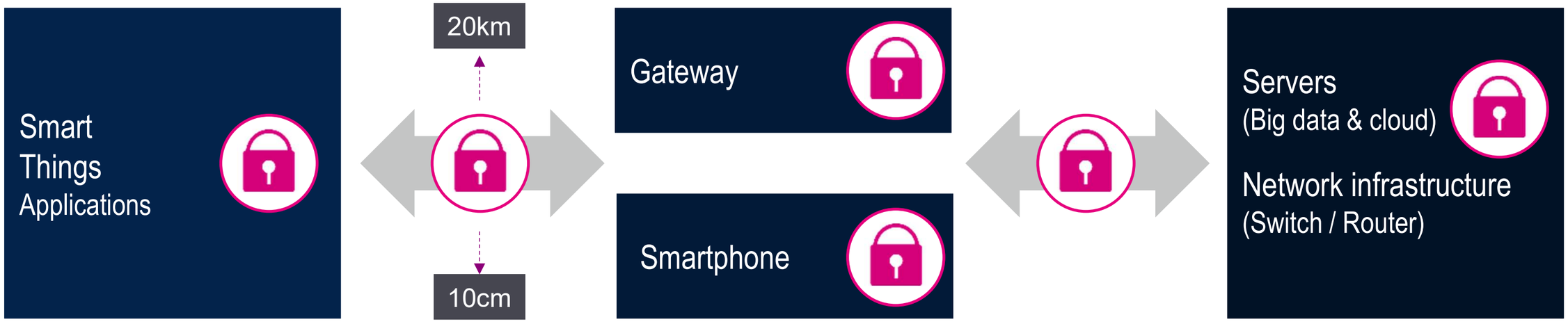


Nodes
(Billions)

Gateways
(Millions)



Cloud



life.augmented

Challenges of embedded systems and IoT devices

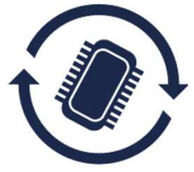
Many applications, many customers

End-to-end security

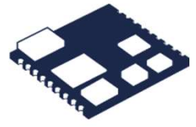
Limited security know-how of implementers in many cases

Fragmented asset value & protection accountability

Long device cycles, requiring field upgrade



Large number of devices



life.augmented

Supporting the security process
Security along the product life cycle

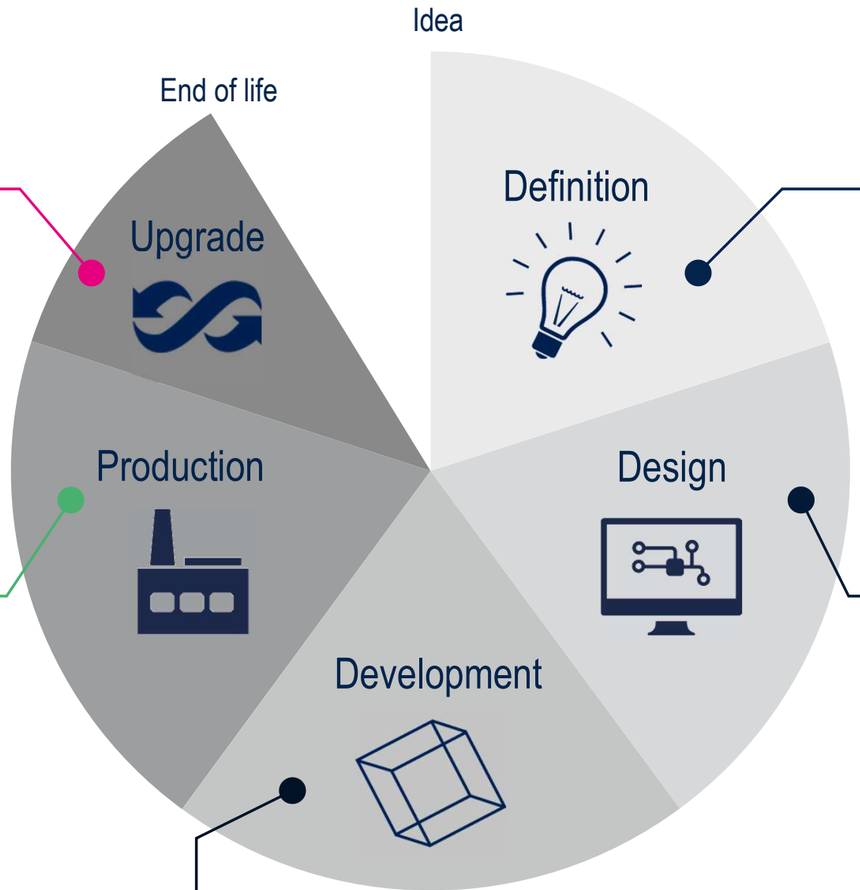
Secure firmware upgrades and secure end-to-end communication

Secure production environment, secure firmware installation, and certifications

Selection of secure components & processes solving customer security needs

Leveraging ST's security ecosystem and strong know-how

Support in defining the appropriate level of security



life.augmented

Security threats and counter measures

life.augmented

Why security matters

Security is about protecting assets

Information, capabilities, features, financial or technical resources
digital (software sources), physical (a car or a server) or commercial (brand) assets
that may be damaged, lost or disrupted

Consumer private information	A product or solution	Health and safety	The work place
Finances, health, location, passwords, accounts	Processes, services, intellectual property, firmware, brands	Medical devices, manufacturing processes and equipment, transport & vehicles	Production equipment, environmental and access controls

life.augmented

The threats & consequences

Threats	Device cloning & counterfeiting	Data corruption	Data breaches
What we need to protect against	**Compromises** OEM **devices** and **revenues** of service providers	Can introduce **misinterpretation** at the service level	Breaches can **expose private end user data** impacting people's lives
	Can lead to **data breaches** and **loss of privacy**	Can **damage service quality** and reputation	Stolen data can **impact the service provider's liability**
	Causes service **quality issues** and potential **denial of services**	Can potentially **impact end-user safety**	Stolen data can **impact the service provider's reputation**

life.augmented

Functional countermeasures

Threats

- Device cloning & counterfeiting
- Data corruption
- Data breaches

Functional countermeasures

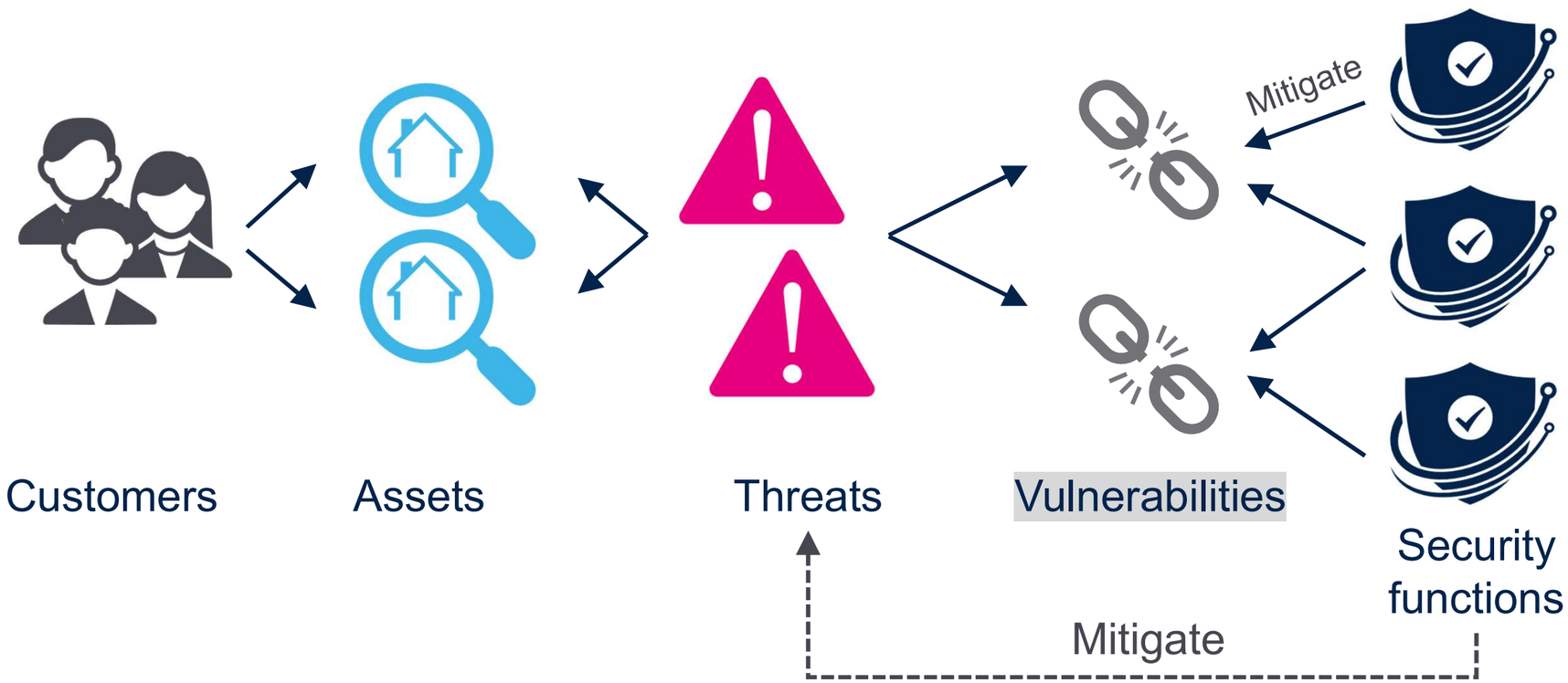
- Data / Identity protection
- Secure boot
- Secure storage
- Secure firmware upgrade
- Secure communication
- Code & execution protection
- Authentication

Protecting assets ensures

- Confidentiality
- Integrity
- Availability

life.augmented

Security services mitigate risks



Threats exploit **vulnerabilities** and damage **assets**.

Protections mitigate **vulnerabilities** and therefore can mitigate **threats**.

Identify assets, threats and vulnerabilities to define protection strategies and countermeasures that reduce risks to an acceptable level

life.augmented

Security Framework

A security framework to protect embedded systems

1. Identify threats according to the different types of customer assets
2. Propose mitigation strategies via **Security Functions & Services**
3. Rely on recognized **Security Assurance levels**

Goal: help customers protect their assets and reach the required Security Assurance levels

life.augmented

Our goal: protect customer assets

Data

Confidentiality

Secrets

Regulations

Authenticity

IP

Software

Data

Processes

Secrets

Connectivity

Regulations

Network access

Data transfer

Confidentiality

Availability

System trust

Regulations

Reliability

Availability

Authentication

Confidentiality

https://www.st.com/content/st_com/en/ecosystems/stm32trust.html

Security Layering & Protection

life.augmented

Security layering

- MCU security features
  - Used to establish a robust platform on which trusted processes and associated cryptography can be performed
- Cryptographic functions
  - Preserve confidentiality, verify integrity, authenticity
- Secure Boot (SB) and Secure Firmware Update (SFU)
  - Establishing a Root of Trust
  - Building a system that can evolve to counter new threats, add new functionality, fix bugs in a controlled and secure way once device is in the field

Application
- Features / Services
- Communication (TLS)

Security Services
- Secure Boot, Secure Firmware Update

Cryptographic functions
- Confidentiality, Integrity, Availability

MCU Security Features

Firewall | PCROP | RDP | WRP | MPU

Static security protection

STM32 static memory protections

Readout Protection (RDP)

- Level 0: no readout protection
- Level 1: memory readout protection
- Level 2: chip readout protection
- Level 0.5: Secure Debug Protection (NEW)

→ Flash code and registers (+ SRAM2 in L4) can’t be dumped through JTAG/SWD or by the CPU itself booted from other memories than internal flash

Proprietary code Read Out Protection (PcROP)

- Specific configurable area
- 1 each per Flash bank

→ Flash code is only executable, cannot be read and dumped by the CPU

Write protection (WRP)

- 1 each per Flash / SRAM sector

→ Flash code is protected from unwanted write/erase operations

Dynamic security protection

STM32 dynamic protections

Firewall

- Code or data protection in Flash or SRAM

→ Single call-gate interface
Trusted execution region
Ideal to protect sensitive function and IP from the rest of the application

MPU

- Memory isolation
- Hard-fault or core lock-up in case of violation

→ Read, Write, execute attribute per region
Prevent Stack Overflow
System protection against unintended modification

Backup domain and Anti-Tamper

- Independent voltage
- RTC, Backup SRAM
- Tamper detection pin

→ Detection of tamper event
Reset of all backup register
Time stamp event

Security functions and ST offer

life.augmented

From assets to security functions

STM32Trust simplifies the mitigation model analysis with:

- Pre-analyzed threats and vulnerabilities
- Mitigation with ready to use Security Functions & Services

Data

Connectivity

IP

System trust

Threats	Vulnerabilities
Data confidentiality	Device identity
Data integrity	Software & Updates
Denial of Service	Debug access
Impersonation	Secret storage
Software integrity	Lifecycle
Malware Intrusion	Open Communication
Software copy	Monitoring
License fraud	Shared memories
Cloning	Untrusted environment

STM32Trust Security Functions

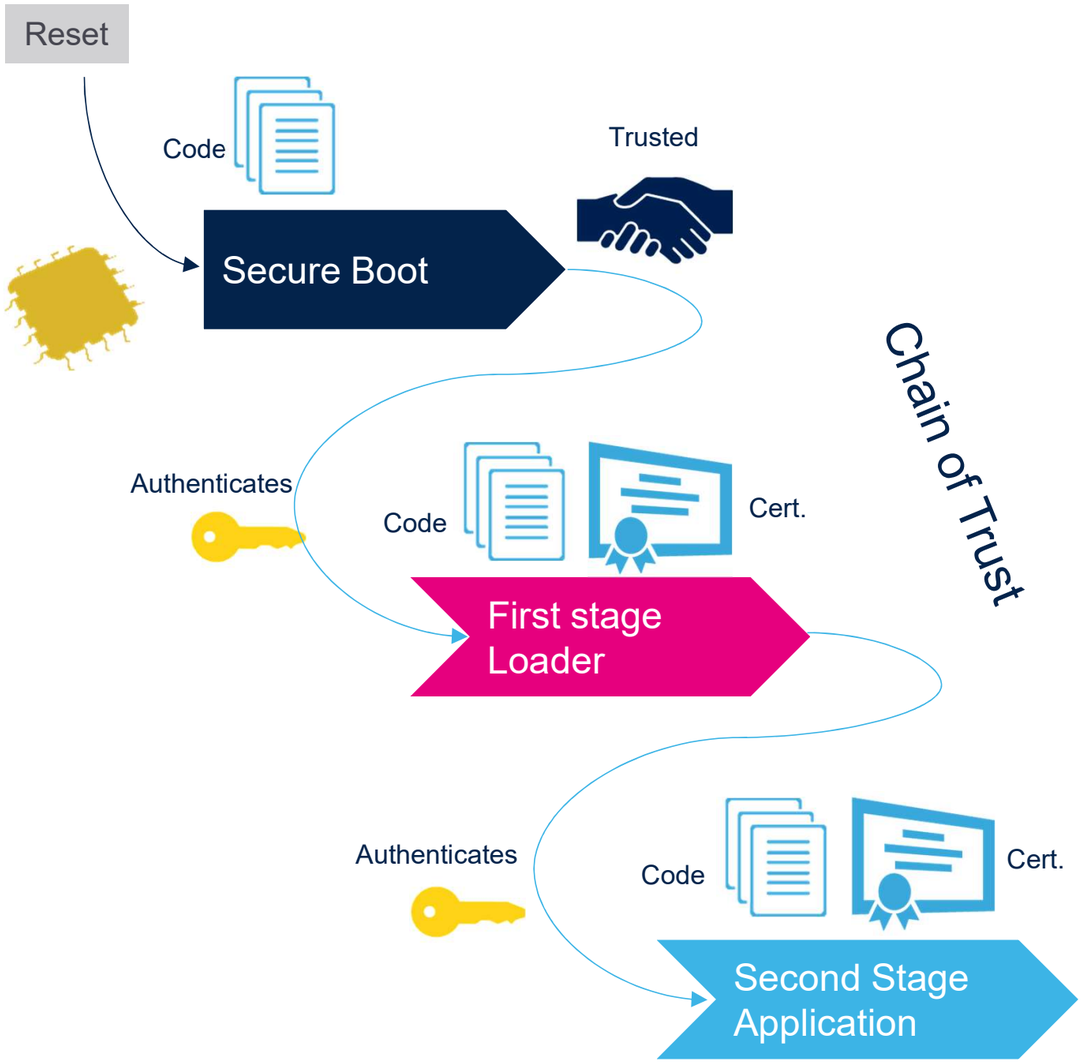
- Identification / Authentication / Attestation
- Application Life Cycle
- Secure Manufacturing
- Software IP Protection
- Silicon Device Life Cycle
- Secure Install / Update
- Secure Storage
- Isolation
- Abnormal Situation Handling
- Secure Boot
- Crypto Engine
- Audit / Log

life.augmented

Security functions

1- Secure Boot	2- Secure Install / Update	3- Secure Storage	4- Isolation
Ability to ensure the authenticity and integrity of an embedded application	Installation or update of firmware with initial integrity and authenticity checks before programming and execution	Ability to securely store secrets like data or keys	Isolation between trusted and non-trusted parts of an application
5- Abnormal Situation Handling	**6- Crypto engine**	**7- Audit / Log**	**8- Identification / Authentication / Attestation**
Ability to detect and react to abnormal hardware and software situations	Ability to process cryptographic algorithms, as recommended by security assurance schemes	Keep trace of security events in an unchangeable way	Unique identification of a device and/or software, and ability to detect its authenticity
9- Silicon Device Life Cycle	**10- Software IP Protection**	**11- Secure Manufacturing**	**12- Application Life Cycle**
Control states to securely protect silicon device assets through its lifetime	Ability to protect a section or the whole software package against external or internal reading. Can be multi-tenant	Device provisioning or personalization in untrusted environment with overproduction control	Define unchangeable incremental states to securely protect application states and assets

Goal of Secure Boot / Root of Trust

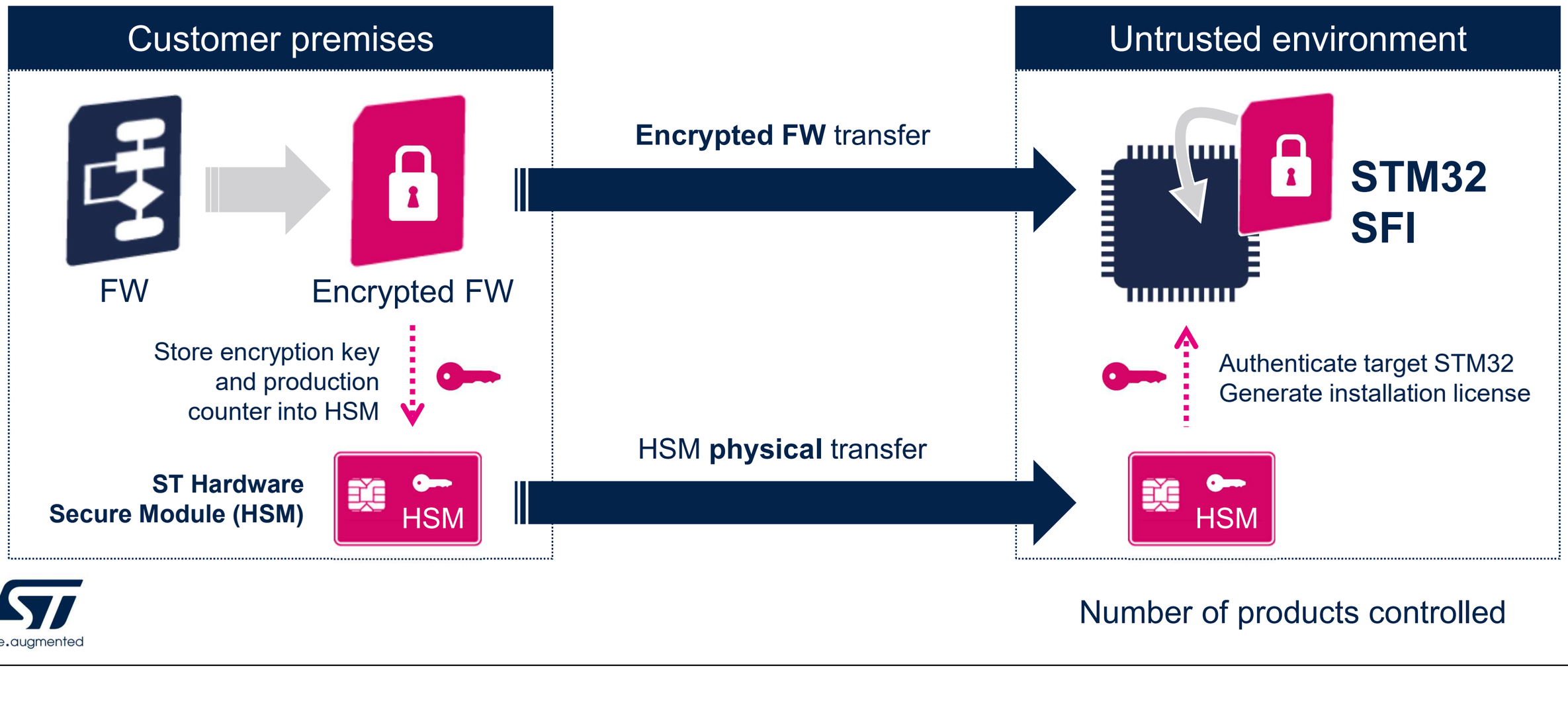


- Immutable Secure Boot code
- Executed first at reset
- Verify platform integrity
  - Clock settings
  - Register configurations
  - Memory protection
- Launch Root-of-Trust services
  - Code authentication
  - Uses cryptographic keys and encryption functions

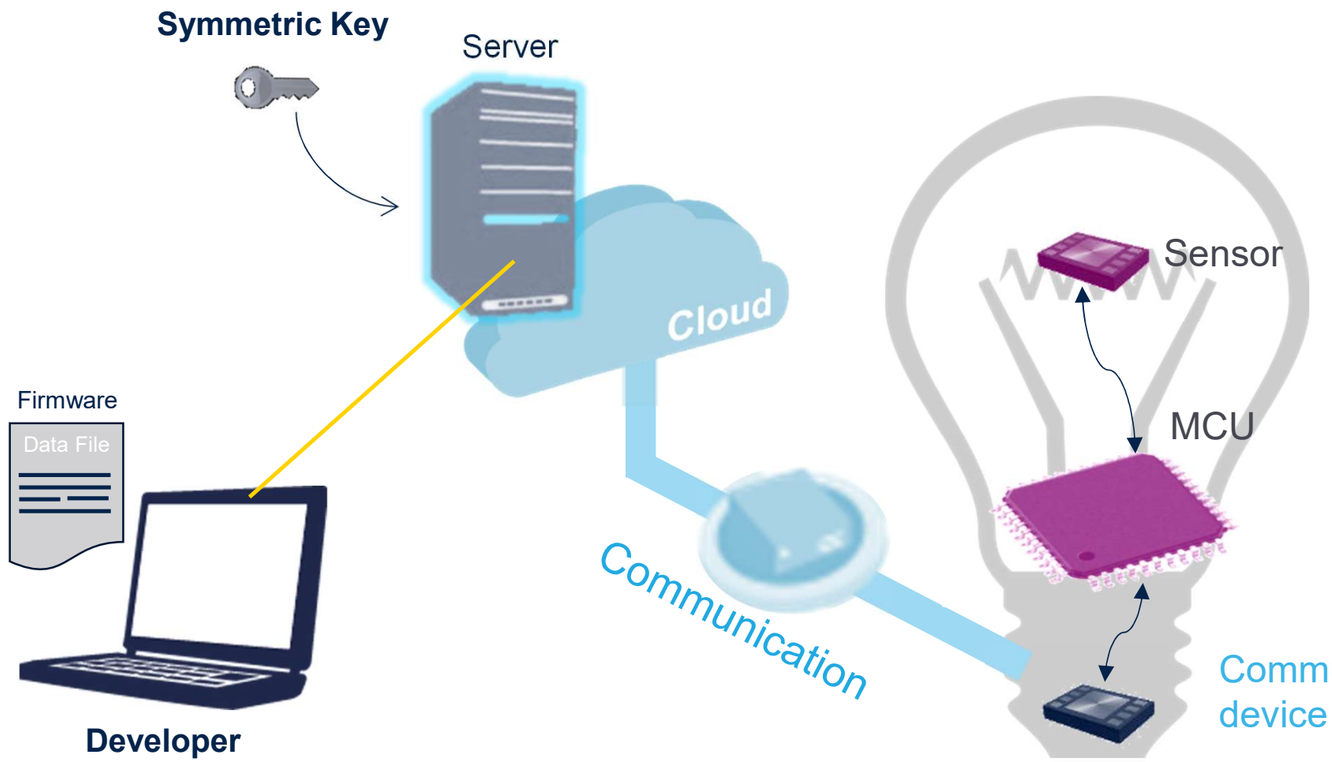
life.augmented

Secure your production flow with Secure Firmware Install (SFI)

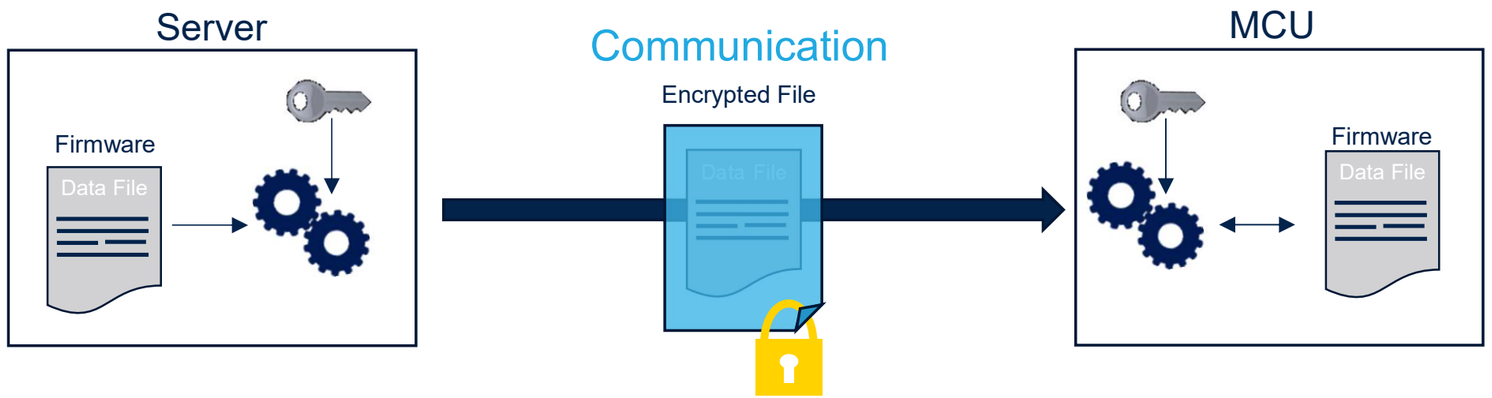
Protect your code and control the number of products manufactured



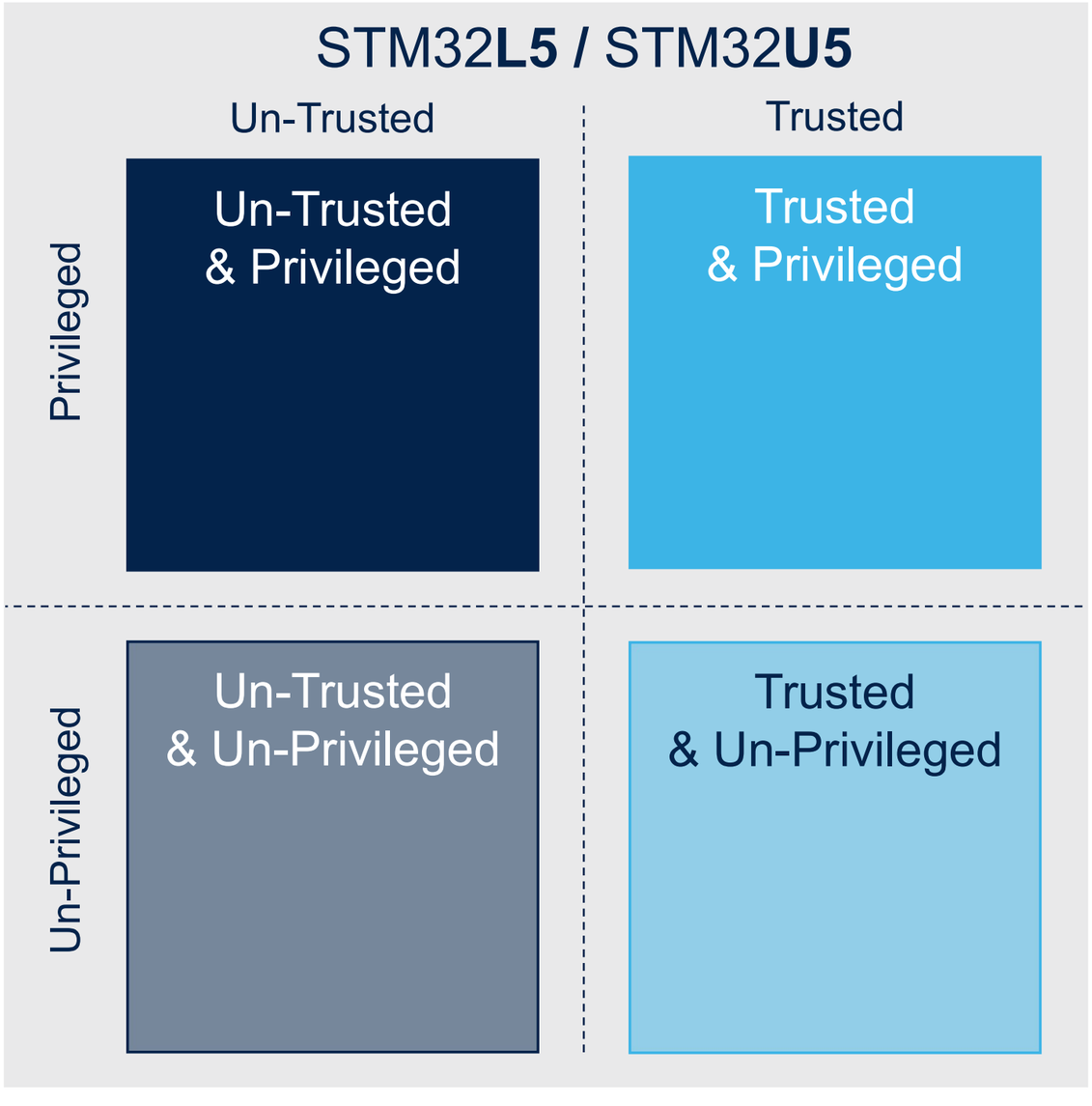
Secure Firmware Update



- Server sends firmware package
- Device receives, stores new firmware package and executes it

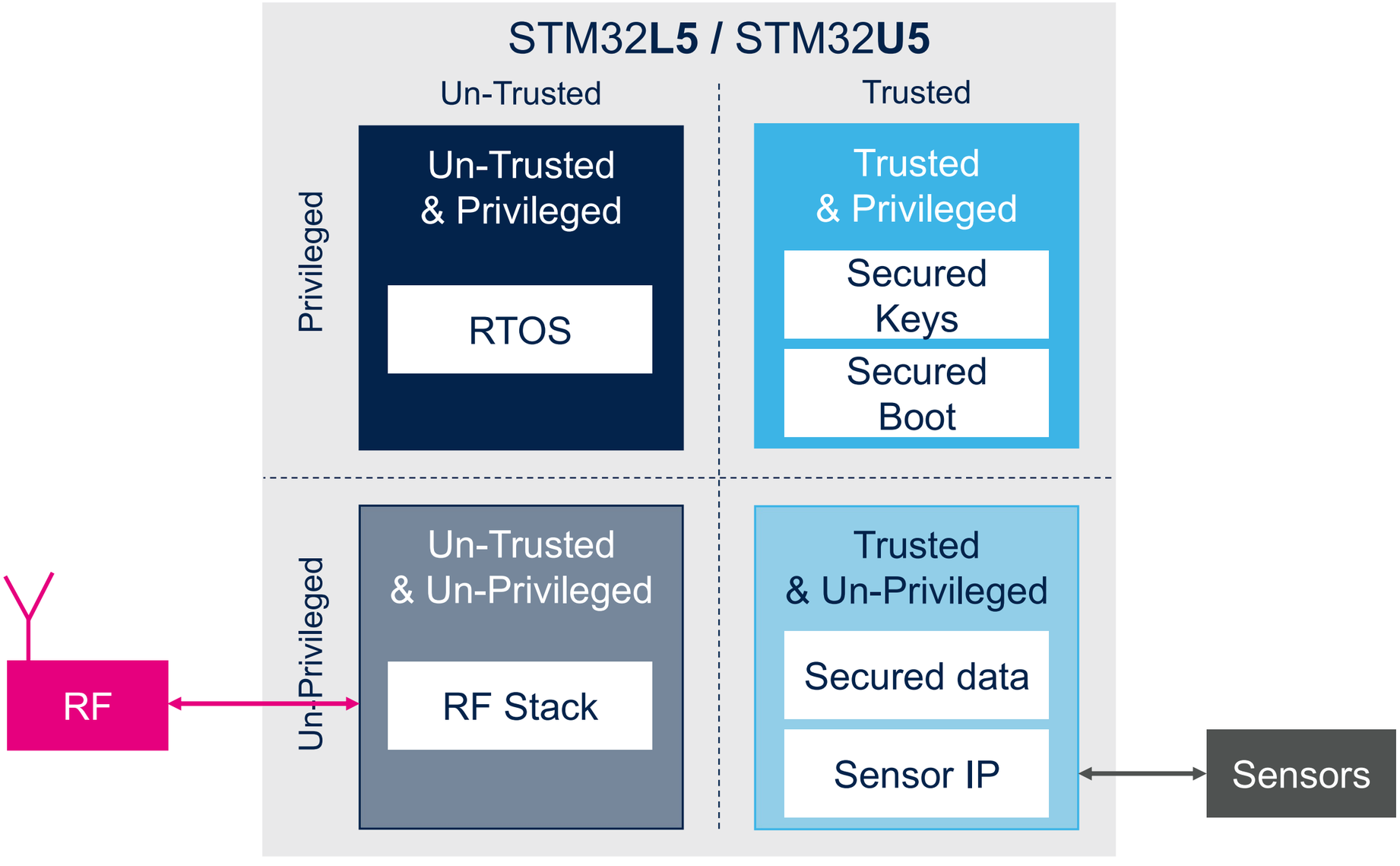


Secure Storage & Isolation



- More partitioning
- Possibility to separate the trusted and un-trusted areas with **privileged and un-privileged** zones
- Strong **granularity** to define each part of memory or each peripheral, DMA channel as privileged or un-privileged

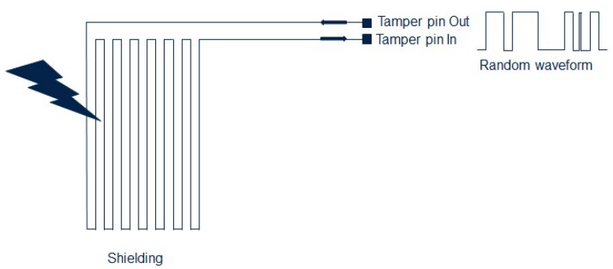
Example: TrustZone Isolation in Cortex-M33

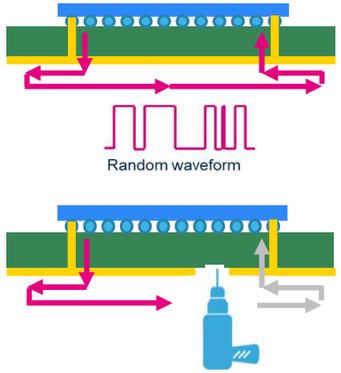


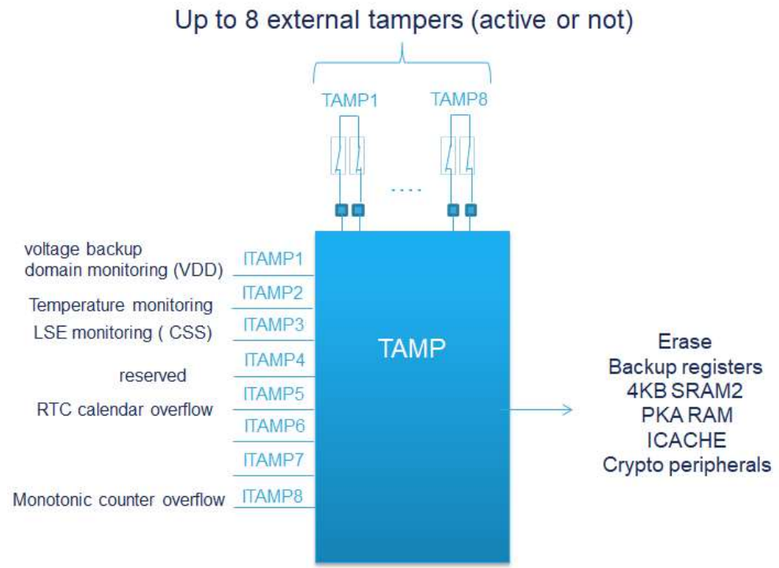
Abnormal situation handling

Active Tamper Feature in STM32

STM32 Silicon Feature	Benefit for Security Function
Anti tamper / Active tamper / Backup registers	Protect against a wide range of physical attacks on HW system outside the MCU. Erases backup registers information when tamper attempt is detected
RTC (Alarm timestamp)	Timestamp on tamper events, or internal events
GPIO Locking	Lock of selected GPIO. Impossible to unlock until next reset. Ability to lock communication channels after tamper detection
CSS (Clock Security System)	Internal clock available for secured program execution independently from external source clock
ECC (Error Correction Code)	Robust memory integrity. Hardened protection against fault injection attacks thanks to error detection
Temperature Sensor	Check if device is operating in expected temperature range. Hardened protection against temperature attacks
Watchdogs	Independent watchdog and window watchdog for software timing control.
PVD (Power Voltage Monitoring)	Monitors changes on power







life.augmented

Security assurance levels & certifications

life.augmented

From device to application security assurance level

- STM32Trust focuses on two de-facto product certification schemes:

SESIP	**Security Evaluation Standard for IoT Platforms** (SESIP) Published by Global Platform for IoT devices
psacertified™	**Platform Security Assurance** by ARM® (PSA) Focusing to protect IoT devices

- Compliant with multiple national & applicative security standards
- In keeping with the security requirements of most applications

enisa THE EU CYBERSECURITY AGENCY
GLOBALPLATFORM
TRUSTED COMPUTING GROUP
PCI
ETSI EN 303 645
GSMA
UL 2900-1
FIPS Level 1 Validated 140-2
Common Criteria
IEC IEC 62443
EMVCo

Security assurance & certifications

STM32 Trust

STM32 MCUs & MPUs

STSECURE

STSAFE Secure Element

Product Security Assurance*	psacertified™ SESIP3	Common Criteria EAL**5+**

Bridge for Application Assurance level

Application Security Assurance	enisa THE EU CYBERSECURITY AGENCY; GLOBALPLATFORM; TRUSTED® COMPUTING GROUP; PCI; ETSI; GSMA; UL® 2900-1; FIPS Level 1 Validated 140-2; Common Criteria; IEC 62443; EMVCo.

** product certifications depends on each products*

- **Security Evaluation Standard for IoT Platforms (SESIP)**
  - Published by Global Platform to align protection profiles to multiple security assurance schemes
- **Platform Security Assurance (PSA) by ARM©**
  - Focus on protecting IoT devices
- **Common Criteria EAL5+**
  - Enhance security with highest hardware resistance based on secure elements (STM32 companion chips)

life.augmented

STM32U5 - Enhanced security

Extensive functionality to protect your assets

Isolation

TrustZone®
Secure Peripherals
Secure DMA

Cryptography

Side channel AES, PKA
Additional AES, PKA, SHA, and TRNG
CAVP certified CryptoLib

Security assurance level

L3 psacertified™

L3 SESIP

1st MCU to reach Level 3

Lifecycle

RDP: **4 protection level states**
Password-based regression

Memory protections

OTP, HDP, WRP, RDP, and MPU
Ext. Flash encryption OTFDec
Secure Debug

Active tamper

4x active pairs of tamper pins.
Volt. &Temp. monitoring (**Vbat**)
Total tamper I/Os: **8**

Trust anchor

TF-M, Secure Boot,
Secure Firmware Install
Hardware Unique Keys

New features for STM32 in bold

life.augmented

Product certification status

Certifications	Available Now	
ARM PSA • Level 1 (Self Assessment) • Level 2 (White box – Time Limited) • Level 3 (Physical attack)	ARM PSA Level 1 • STM32L4 • STM32L5 • STM32G0 • STM32G4 ARM PSA API Compliant • STM32L5 (TF-M)	ARM PSA Level 2 • STM32L5 (TF-M) ARM PSA Level 3 • STM32U585 (TF-M)
SESIP • Level 1 (Self Assessment) • Level 2 (Black box) • Level 3 (White box – Time Limited) • Level 4 (White box) • Level 5 (Smartcard-like EAL4+)	SESIP Level 1 • STM32L4 (SBSFU)	SESIP Level 3 • STM32L4 (SBSFU) • STM32L5 (TF-M) • **STM32U585 (TF-M)**
	CC EAL5+ • STSAFE-A110 • STSAFE-TPM • ST4SIM FIPS-140-2 • STSAFE-TPM TCG • STSAFE-TPM GSMA • ST4SIM	

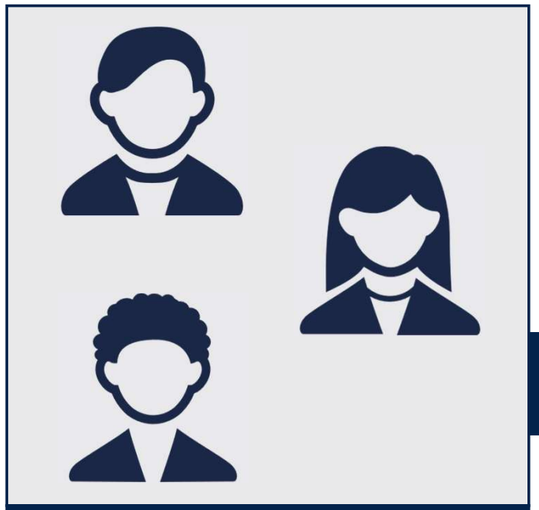
Evaluations	Available Now	
PCI POS Point of Sale application	• STM32L4	• Certification documents and links available at www.st.com/stm32trust • Evaluation material is not public

Takeaways

life.augmented

STM32Trust security framework to implement security

Security framework reaching up to PSA Level 3 and SESIP Level 3



Customer security needs

- Isolation
- Secure Boot
- Secure Storage
- Crypto Engine
- Identification/Authentication
- Secure Manufacturing
- ...

12 core security functions to address needs

Implementation on **STM**32 and ST**SAFE**

Strong certification

STM32

psacertified™

STM32L5+TFM: Level **2**

SESIP3

STM32L4+SBSFU: Level **3**

STSAFE

Common Criteria

EAL**5+**

life.augmented

www.st.com/STM32Trust

PSA = **P**latform **S**ecurity **A**rchitecture, by ARM
SESIP = **S**ecurity **E**valuation **S**tandard for **I**oT Platforms, by Global Platform

Our technology starts with You

Find out more at www.st.com

life.augmented