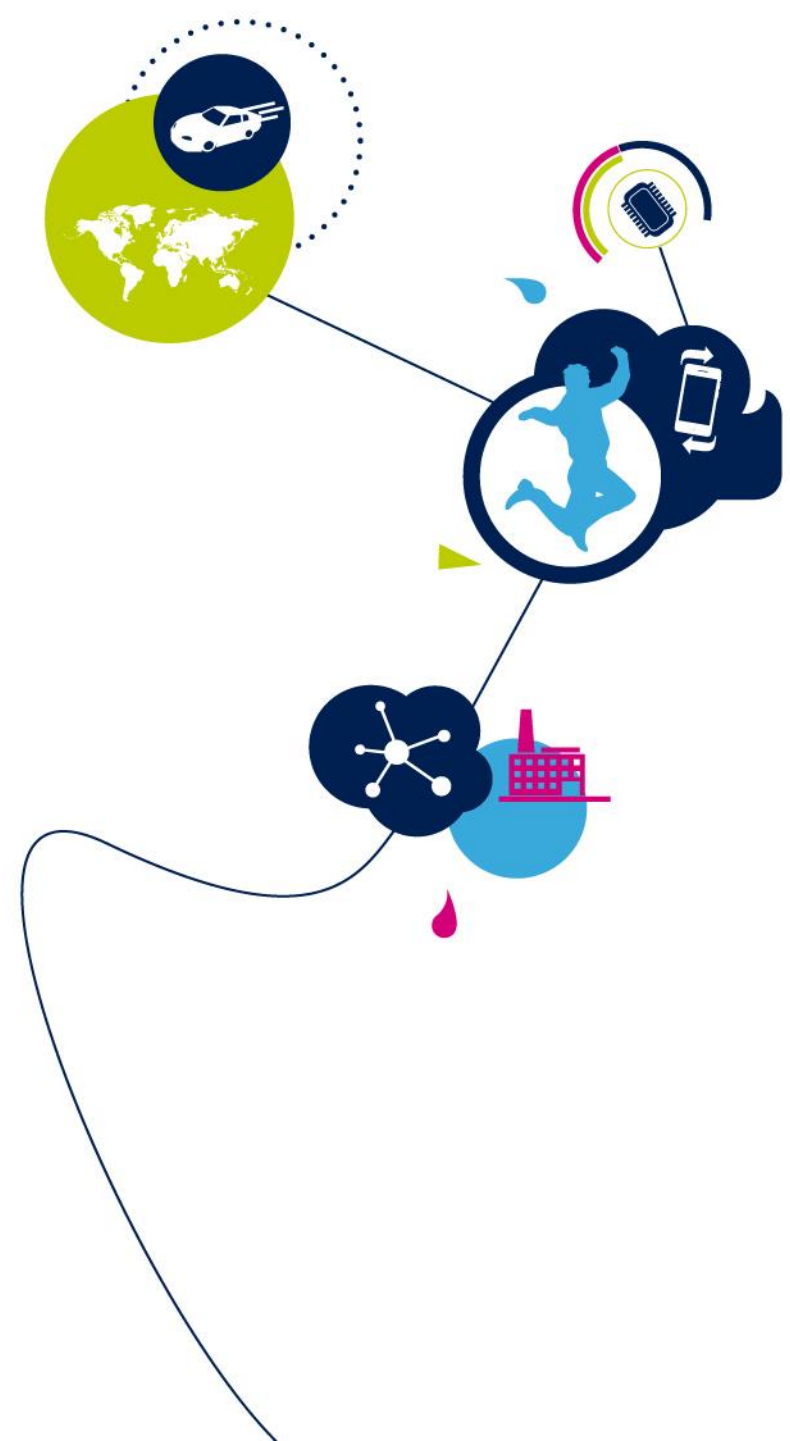


STM32 Ecosystem Enables Customers to Secure Their IoT Applications

STM32生态系统帮助客户实现安全的物联网应用

Stephane Rainsard

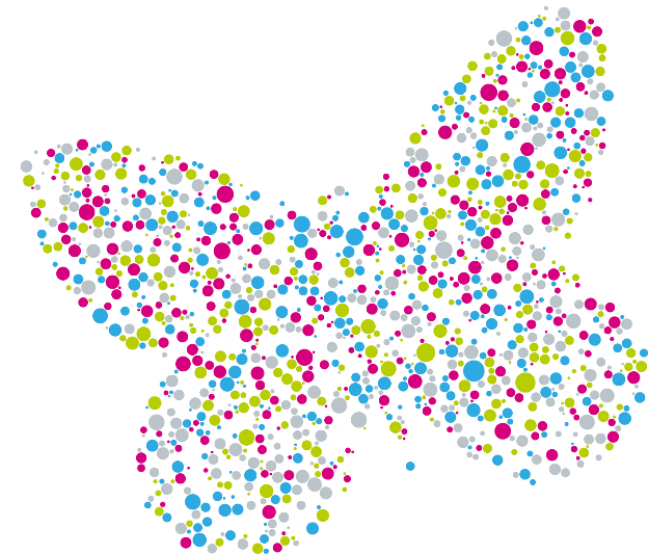
Technical Marketing Manager
APAC Region



13 Product Series
More than 50 Product Lines

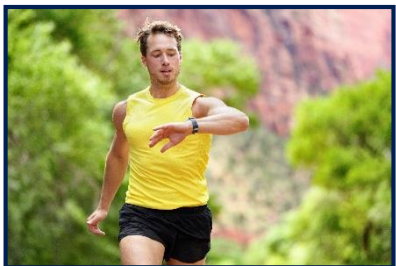
Great Investment

4



Great Investment

5



具体系统需要具体分析

让我们一起查看STM32生态系统如何帮助客户实现安全的物联网应用

安全：是一个生态系统

6



Security

ST最佳
产品组合



New products announced

New products with new IPs

ST
软件库



Mass Market
SW Libraries
(X-Cube-CryptoLib)

大众市场
解决方案



New solutions available

Secure Firmware Install
Secure Boot – Secure Firmware Upgrade

现场培训



Field Training

合作伙伴

 Alibaba Cloud

 **arm** 
PROVE & RUN



 **SECURE
THINGZ**

And more...

ST最佳
产品
组合

ST
软件库

大众市场
解决方案

现场
培训

合作伙伴



最佳产品组合

7

ST's best in
class portfolio

ST最佳
产品组合

基于Cortex-M33的第一款STM32

8

- More security with TrustZone and ST security implementation
 - HW to resist to Logical and board level attack
- Lower Power consumption
 - STM32 ultra-low-power technology
- Integration, Size, performance
 - More performance, high memory size and wide portfolio



ST最佳
产品
组合

STM32 L5

ST
软件库

大众市场
解决方案

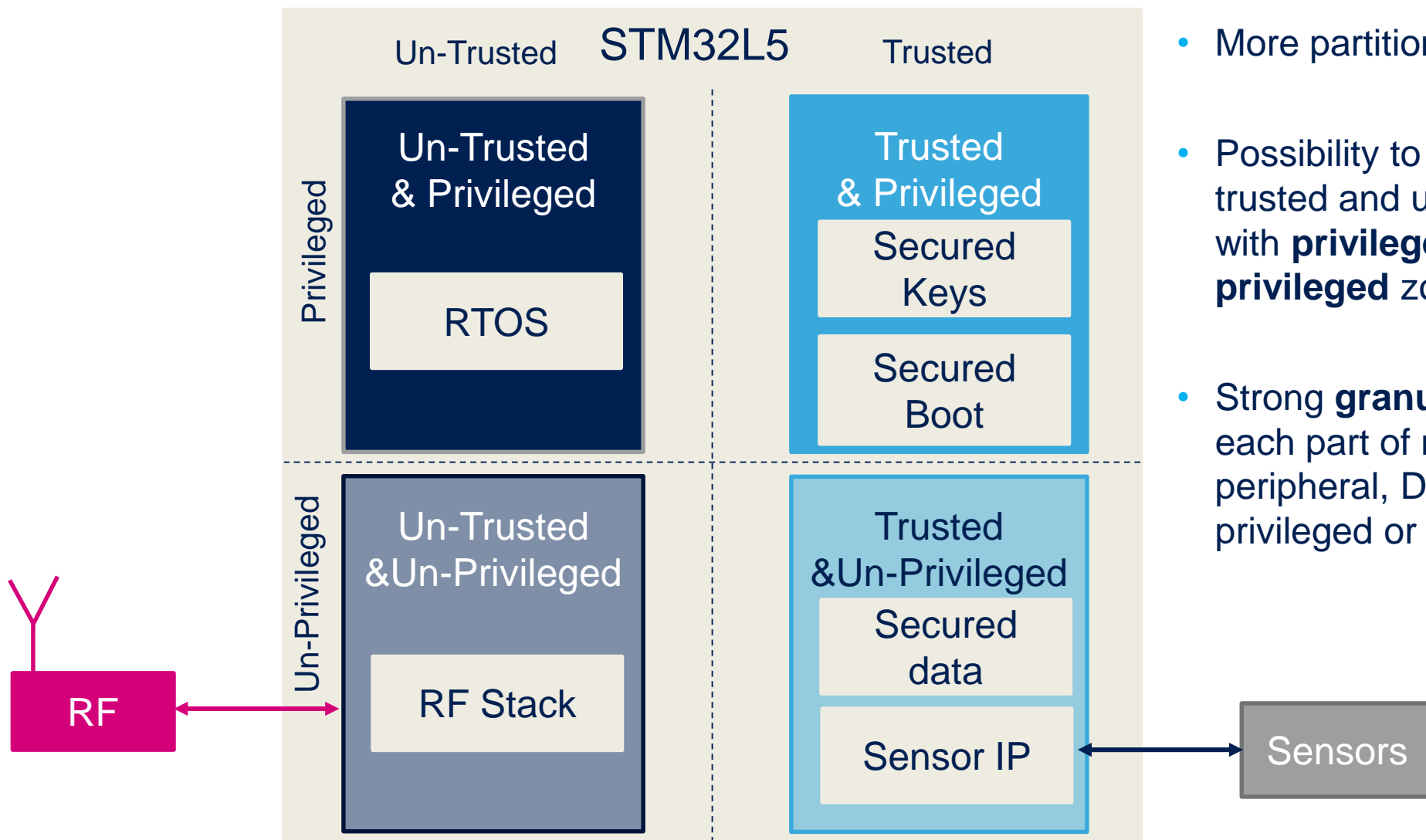
现场
培训

合作伙伴



TrustZone: 例子

9



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

ST最佳
产品
组合



ST
软件库

大众市场
解决方案

现场
培训

合作伙伴

一整套安全技术

10



ENCRYPTION DECRYPTION AUTHENTICATION

- AES-128/256 Encryption
- SHA-256 Authentication
- **Private Key Acceleration (PKA): for RSA, Diffie-Hellmann or ECC (Elliptic Curve Cryptography)**
- Certified Crypto library
- True Random Number Generator
- Unique ID
- OTP Zone



MEMORY and IP PROTECTION

- **Active and static Anti-tamper detection**
- Memory Protection Unit (MPU)
- Secure Boot
- Read and Write Protection
- **HDP (Hide Protect)**
- **OTFDEC (On-the-fly decryption) on Octo SPI to protect external memory**
- JTAG fuse
- **TrustZone**
- **Unique Boot Entry**

选择STM32WB系列

7个关键点让我们脱颖而出

ST最佳
产品
组合



ST
软件库

大众市场
解决方案

现场
培训

合作伙伴



Open 2.4 GHz radio
Multi-protocol



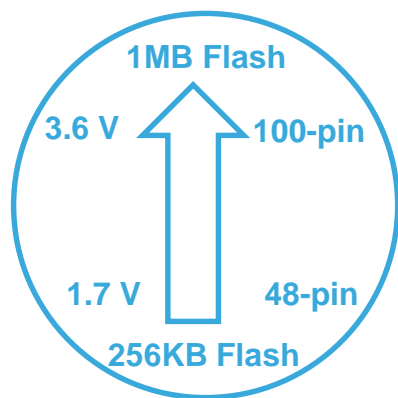
Dual-core / Full control
Ultra-low-power



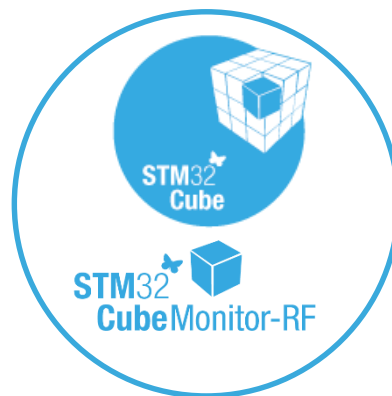
IoT Protection ready



Massive integration
Cost saving



A large offer



Advanced RF tool, Energy control
with C code generation

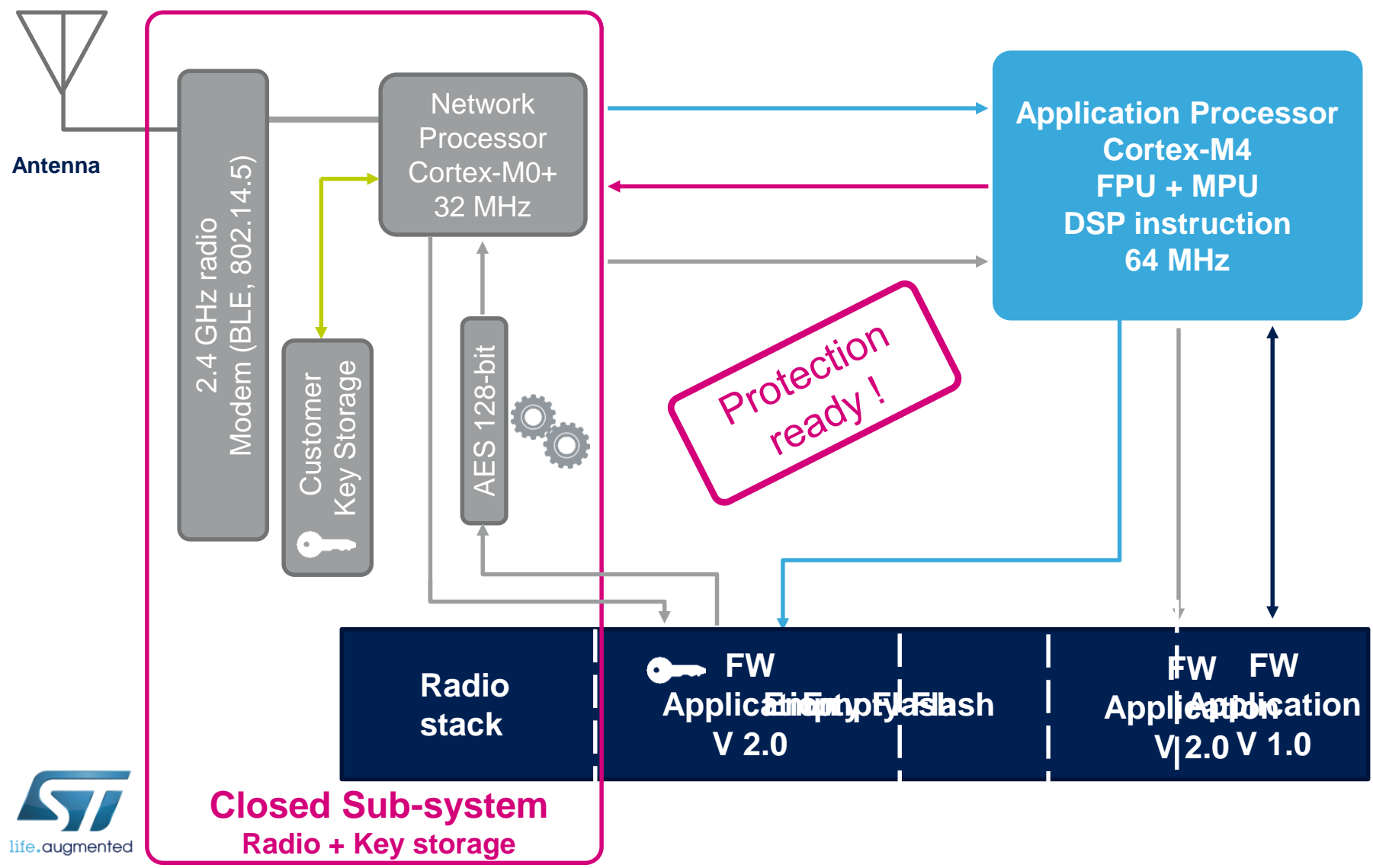


No matter what!



完备的IoT安全防护

Radio Stack And/or Application FW Update



- 1 New FW package received
- 2 New FW detected Update is launched
- 3 App Processor initiate FW update (include send New FW package signature for authentication)
- 4 Authentication signature matches preprogrammed key Case not, the process is aborted and device resets
- 5 New FW package is decrypted with proprietary Key. Device upload on going.



ST最佳
产品
组合

ST
软件库

大众市场
解决方案

现场
培训

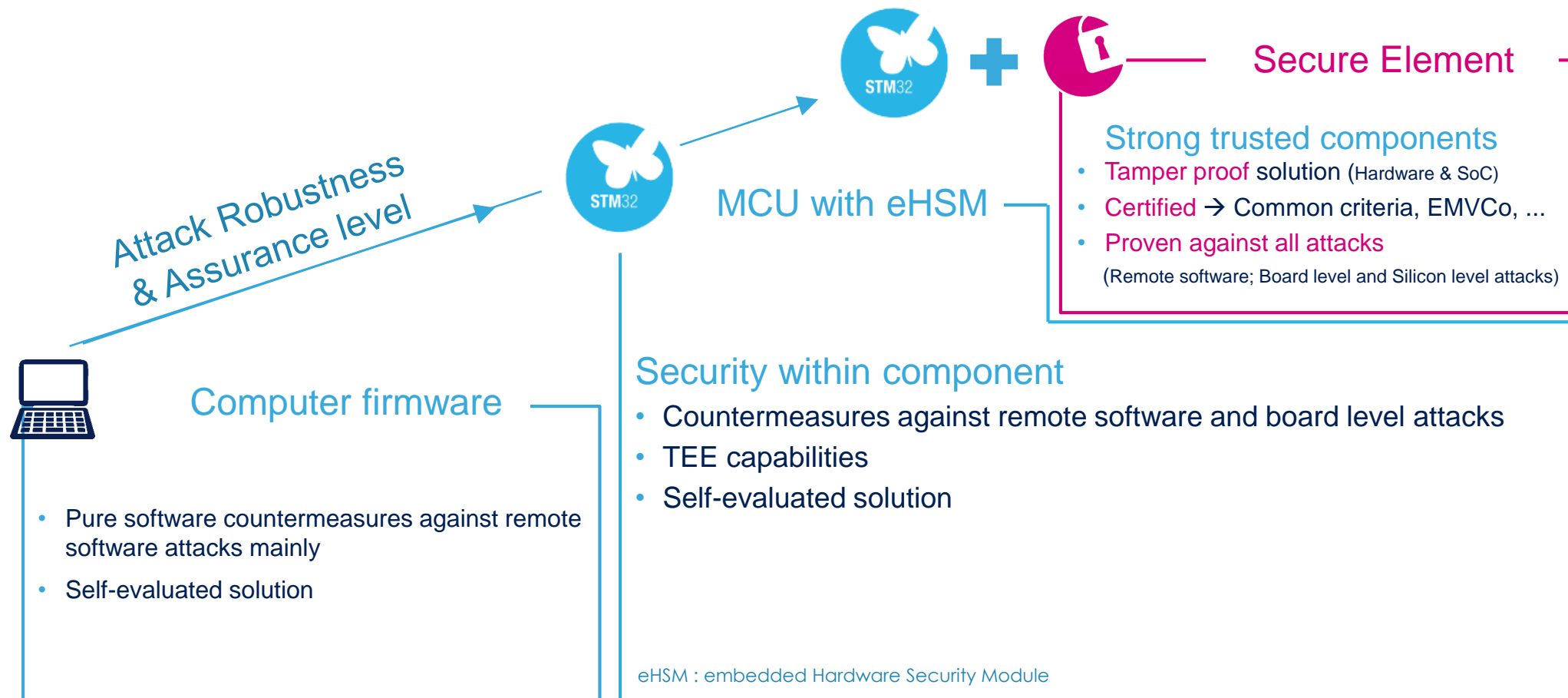
合作伙伴



Solution choice depends of Attack
Robustness & Assurance level
customer demand

灵活的 安全解决方案

14



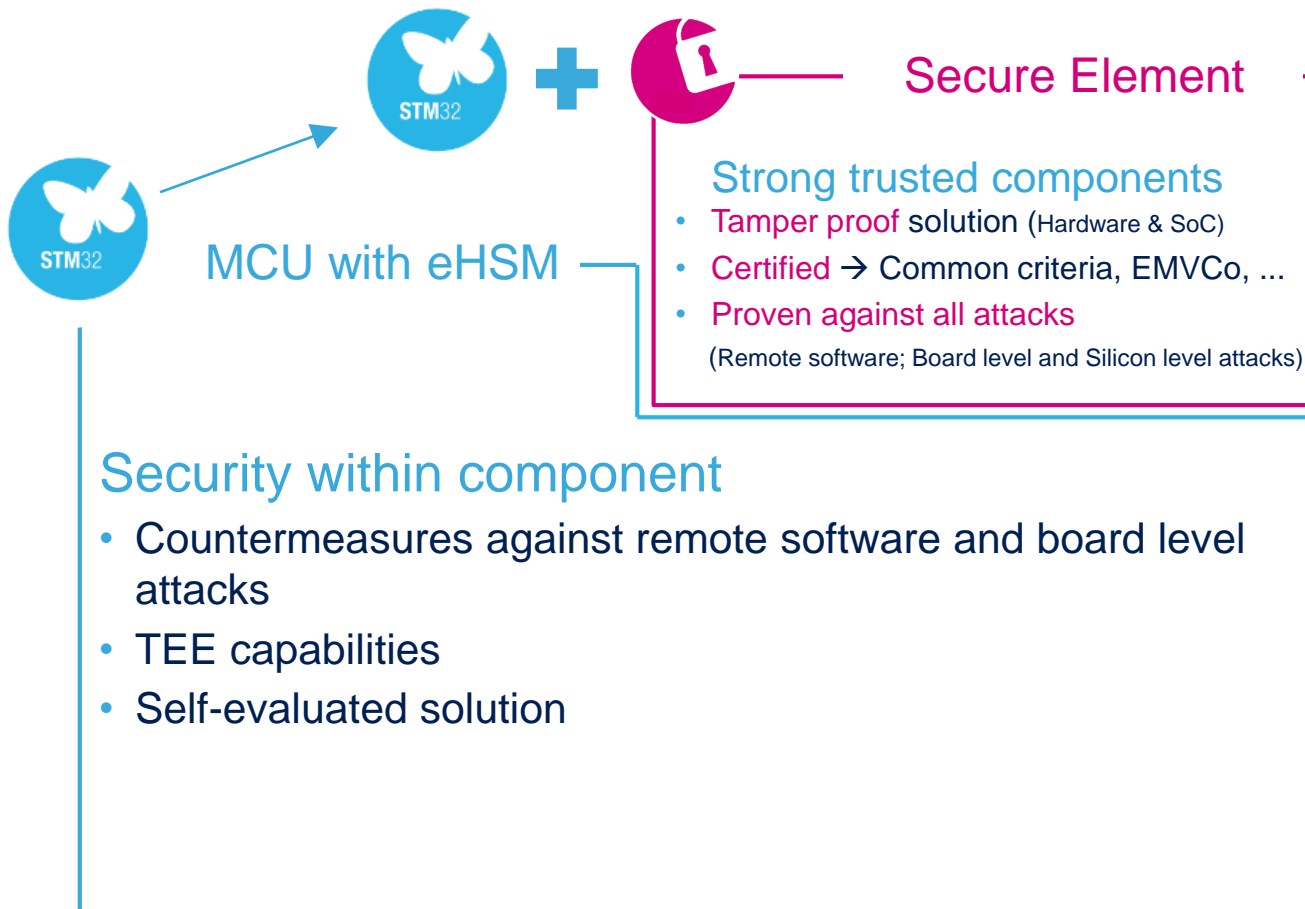
ST最佳
产品
组合

ST
软件库

大众市场
解决方案

现场
培训


合作伙伴



灵活的 安全解决方案

15

Tamper-proof secure element

- System-on-Chip with Secure MCU
- Secure embedded OS
- Optimized for IoT devices
- Certified security 

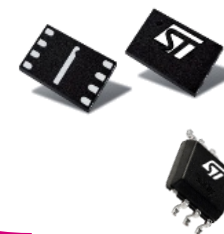


&



Complete
ecosystem

- Personalization service
- GP MCU integration libraries
- STM32 MCU expansion board



ST最佳
产品
组合

ST
软件库

大众市场
解决方案

现场
培训

合作伙伴



ST软件库

16

ST Software
Libraries
ST软件库

ST最佳
产品
组合

ST
软件库

大众市场
解决方案

现场
培训

合作伙伴



X-Cube-CryptoLib
Available on all STM32

所有STM32可用的软件库

17

- AES-128, AES-192, and AES-256
 - ECB (Electronic Codebook Mode)
 - CBC (Cipher-Block Chaining) with support for ciphertext stealing
 - CTR (Counter Mode)
 - CFB (Cipher Feedback)
 - OFB (Output Feedback)
 - CCM (Counter with CBC-MAC)
 - GCM (Galois Counter Mode)
 - CMAC
 - KEY WRAP
 - XTS (XEX-based tweaked-codebook mode with ciphertext stealing)
- DES and TripleDES:
 - ECB (Electronic Codebook Mode)
 - CBC (Cipher-Block Chaining)
- ARC4
- Random bit generator engine based on DRBG-AES-128
- Hash function: HKDF-SHA-512
- Hash functions with HMAC support:
 - MD5
 - SHA-1
 - SHA-224
 - SHA-256
 - SHA-384
 - SHA-512
- RSA with PKCS#1v1.5
 - Encryption/decryption
 - Signature
- ECC (Elliptic Curve Cryptography):
 - Key generation
 - Scalar multiplication (the base for ECDH)
 - ECDSA
- ChaCha20
- Poly1305
- Chacha20-Poly1305
- ED25519
- Curve25519

CAVP
Certified

ST最佳
产品
组合

ST
软件库

大众市场
解决方案

现场
培训

合作伙伴



X-Cube-CryptoLib
Available on all STM32
CAVP Certified

美国密码算法验证体系 (CAVP)

18

- Provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and their individual components
- Issues validation certificates
- Maintains a list of validated algorithms
- Validated **X-CUBE-CRYPTOLIB** algorithms for STM32
 - AES: #3971
 - RSA: #2036
 - ECDSA: #874
 - SHS: #3275
 - DRBG: #1165
 - HMAC: #2589

CAVP
Certified

ST最佳
产品
组合

ST
软件库

大众市场
解决方案

现场
培训

合作伙伴



大众市场解决方案

19

Mass
Market
Solutions

大众市场
解决方案

ST最佳
产品
组合

ST
软件库

大众市场
解决方案

现场
培训

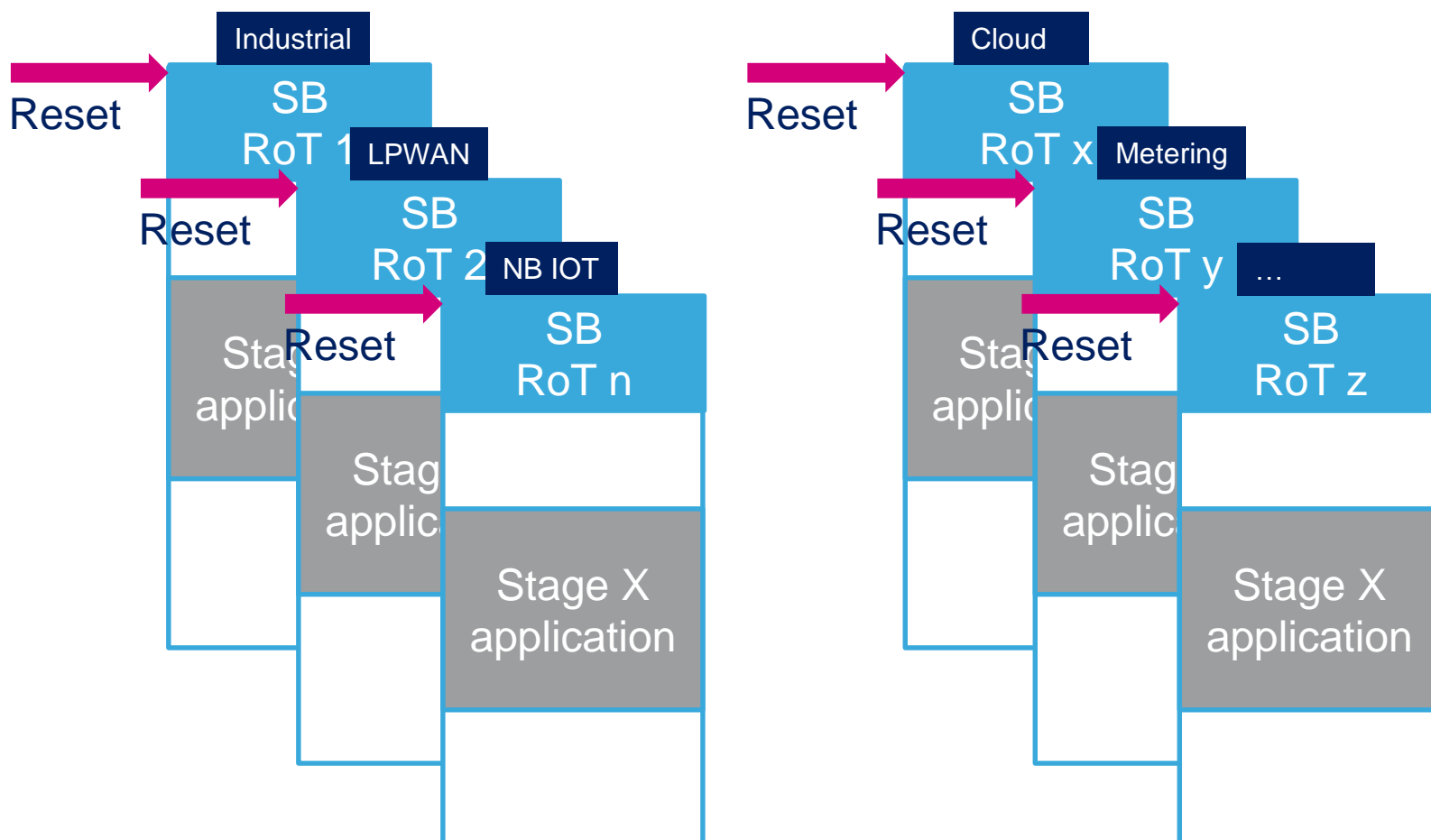
合作伙伴



大众市场解决方案

20

The context : not a single standardized
Secure Boot / Root of Trust model





如何支持该方法

21

- Embedded ROMed code

SB / RoT approach	feasibility	remarks
One code on all STM32	☺	May not be market acceptable
Multiple code on STM32	☹	Diversify products Increase development, qualification, certification, cost

- ST proposal

- Allow Industries to develop their own Secure Boot / Root of Trust method ➡ X-Cube-SBSFU
- Propose a way to securely load it into the STM32 ➡ SFI
- Propose a way to isolate and securely execute it within STM32 ➡ STM32

ST最佳
产品
组合

ST
软件库

大众市场
解决方案

现场
培训

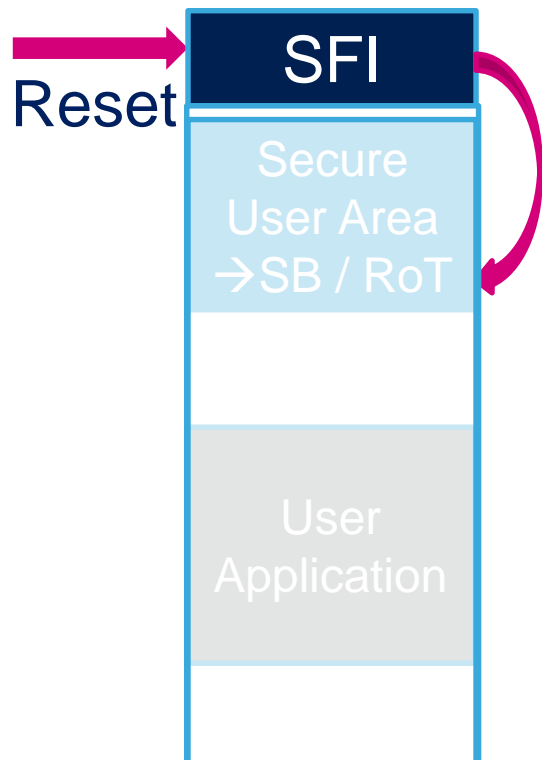
合作伙伴



内建SFI

22

Secure Firmware Install 安全固件安装



STM32
Secure Loader

Loading of Confidential / Authentic SB / RoT binary file into
Secure User Area

Supported Communication interface
UART / SPI / USB

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

ST最佳
产品
组合

ST
软件库

大众市场
解决方案

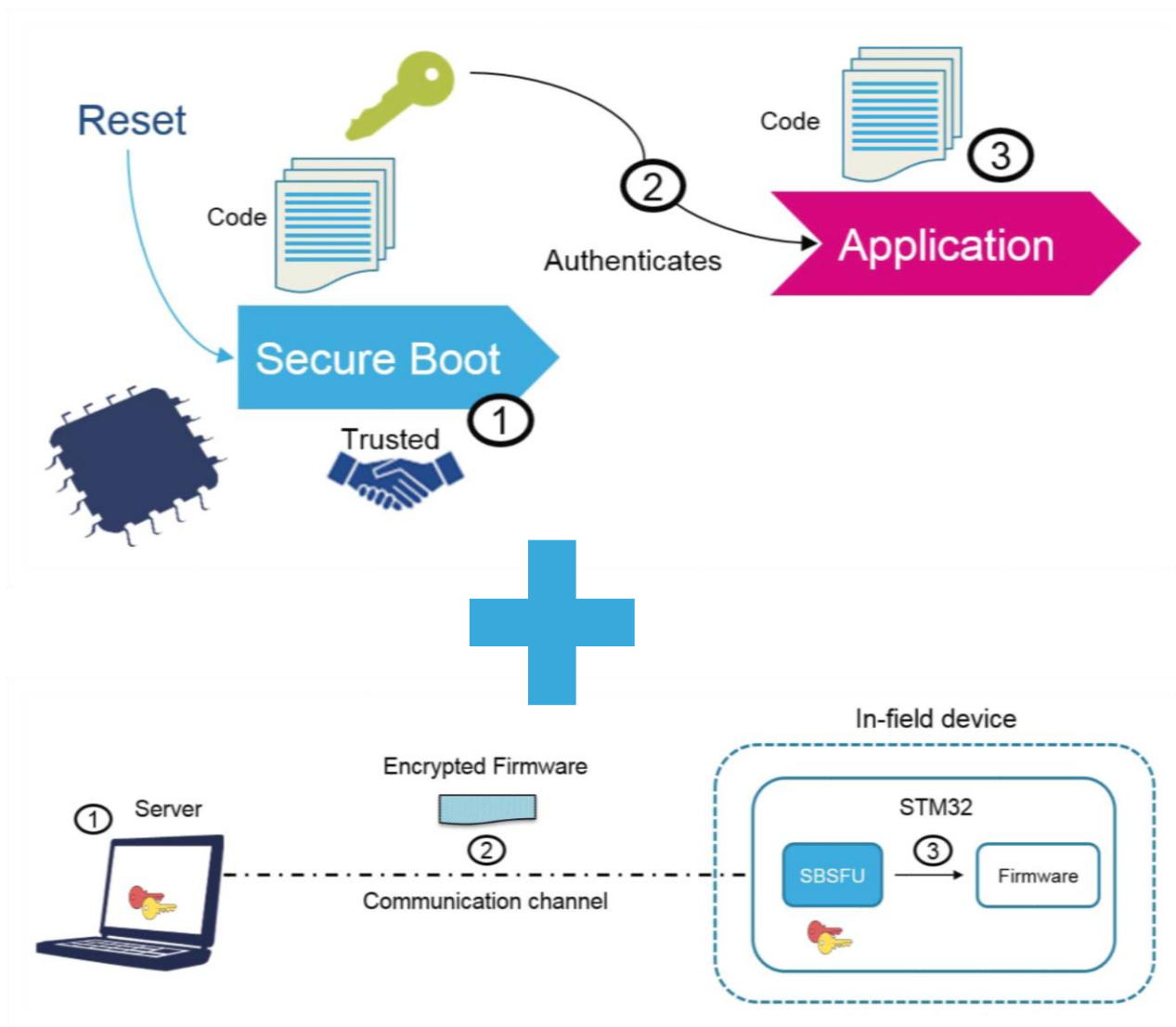
现场
培训

合作伙伴



X-Cube-SBSFU

23



- Secure Boot + Secure Firmware Update
- X-Cube-SBSFU package available on www.st.com
- Provided as source code
- Tools and documentation available
- Already for STM32L4, many more to come...

ST最佳
产品
组合

ST
软件库

大众市场
解决方案

现场
培训

合作伙伴

Field
Training
现场培训

ST最佳
产品
组合

ST
软件库

大众市场
解决方案

现场
培训

合作伙伴

为中国各地提供培训

25

2018
Sessions: 47

Training Form:

- Whole day
- Theory + Hands-on

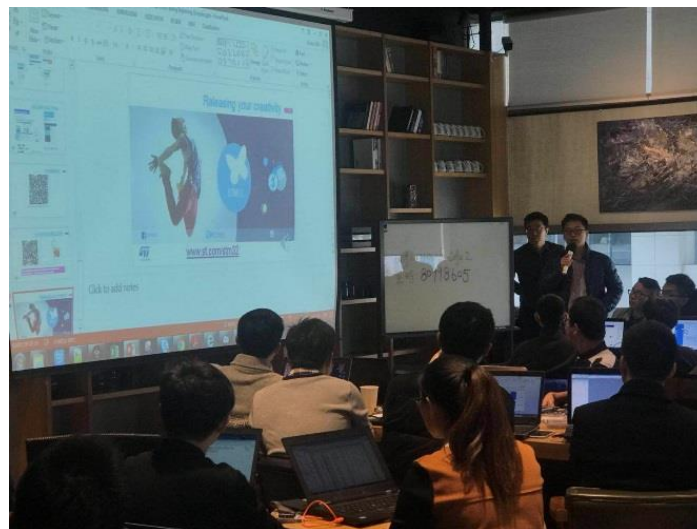
City:

Tier-1 City:

- Shanghai, Shenzhen, Beijing

Tier-2 City:

- 9 cities including :
Guangzhou, Chengdu, Wuhan,
Xi'an, Qingdao ...



ST最佳
产品
组合

ST
软件库

大众市场
解决方案

现场
培训

合作伙伴



合作伙伴

26

Partners
合作伙伴

ST最佳
产品
组合

ST
软件库

大众市场
解决方案

现场
培训

合作伙伴



合作伙伴

27



PROVE & RUN



And more...

ST is addressing your application needs by integrating industry's best practices and innovative solutions into a complete ecosystem.

ST enables your next idea by bringing ST's portfolio, software and tools together with Partner's solutions

ST最佳
产品
组合

ST
软件库

大众市场
解决方案

现场
培训

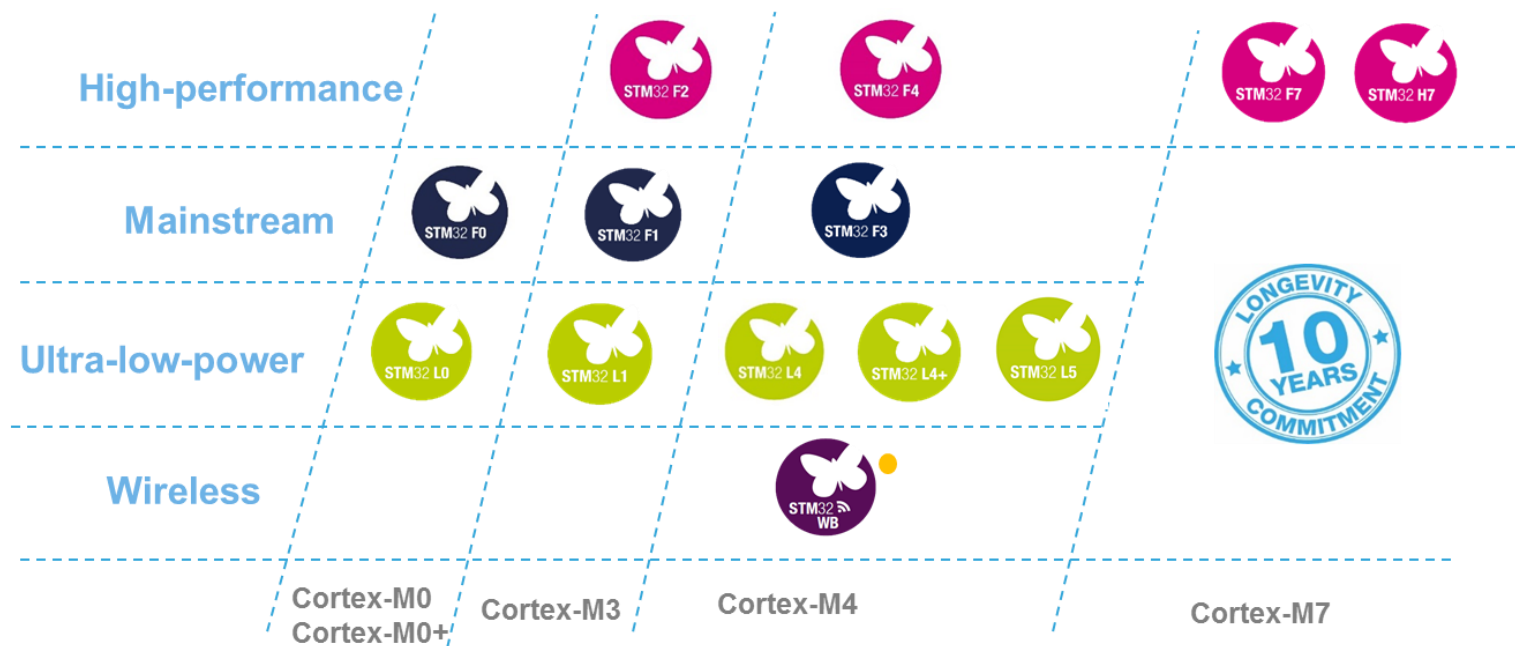
合作伙伴



Providing Security IPs,
Libraries, Solutions
across our portfolio

Great Investment

28



- New Products
- SW Libraries
available for all STM32
- SFI
大众市场方案
- SBSFU
大众市场方案
- Trainings
- Partners

Releasing Your Creativity

29



www.st.com/stm32