



Fastrack your embedded security journey with STM32 solutions

Anna RAFFALLI
APeC STM32 Security Marketing
STMicroelectronics



What is security?

Security is about ensuring:



Confidentiality

Protecting sensitive data and ensuring secrecy.



Integrity

Safeguarding data accuracy and protecting it from any modification.



Availability

Ensuring that functionality and/or data is available when it is needed.



IoT growth puts security at the forefront

1 trillion IoT products to be deployed within the next 10 years

96 % of IoT products are deployed without any security expertise.

In 2025, there are 152,200 IoT devices connecting to the internet per minute.*

The number of IoT monthly attacks in the world reached over 10.54 million in December 2022**



Source:

*<https://dataprot.net/statistics/iot-statistics/>

**<https://www.statista.com/statistics/1322216/worldwide-internet-of-things-attacks/>

Industry-Driven Cybersecurity Standards



Consumer & IoT

Severs & Data Centers

Industrial & Automation

Biometric Authentication

Payment & Banking

Global Platform™

CSA connectivity standards alliance

OPEN Compute Project®

DMTF

IEC 62443-4

ETSI EN 303 645

fido ALLIANCE

MOSIP

PCI

EMVCO

Cybersecurity Regulations and Labels

Managed by governments

EU RED new cyber requirements

- All products embedding or connected to an antenna of a radio equipment and connected directly or indirectly to internet



EU CRA

- All products with digital elements, connected directly or indirectly to another device or network



US Cyber Trust Mark

- Voluntary cybersecurity labeling program initiated by the White House
- Targets IoT devices for smart home

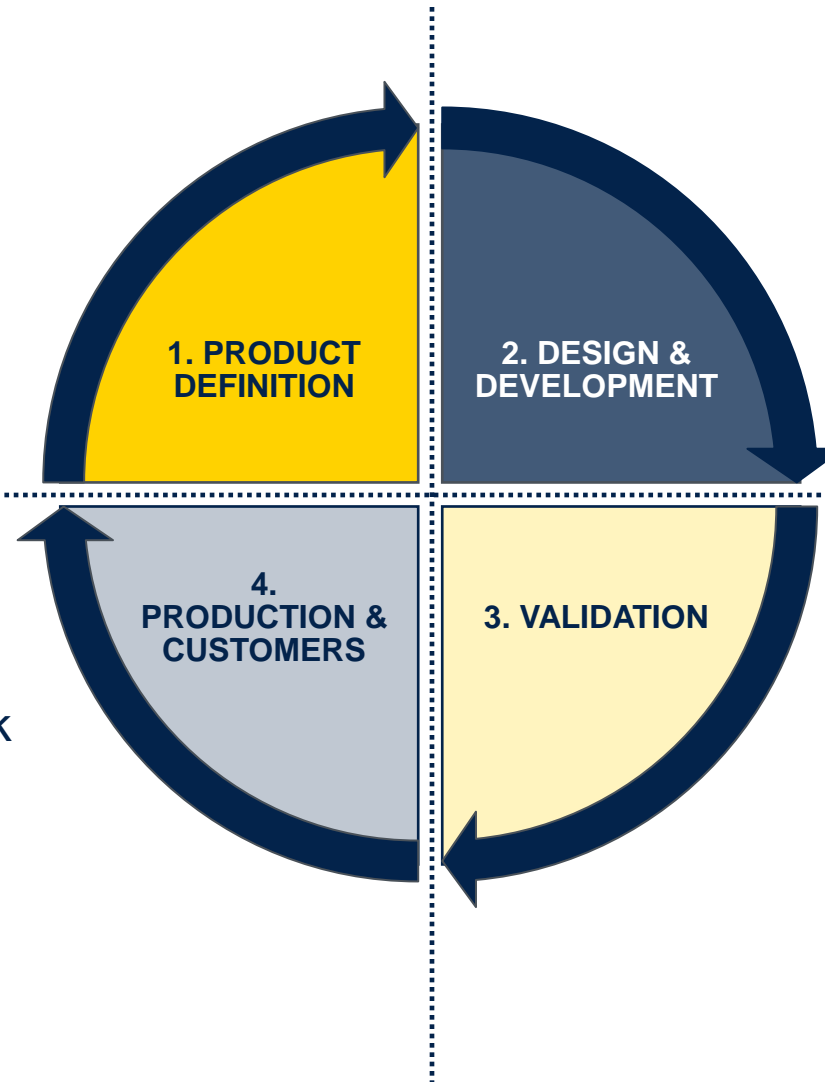


Question for the audience

Have you ever faced the requirement to comply to a cybersecurity regulation or standard? If yes, which one?

Security by design and for lifetime

- Define the product usage
- Perform a risk assessment



- Implement the product security features
- Secure SW development
- Create SBoM
- Identify of inherited vulnerabilities and remediation

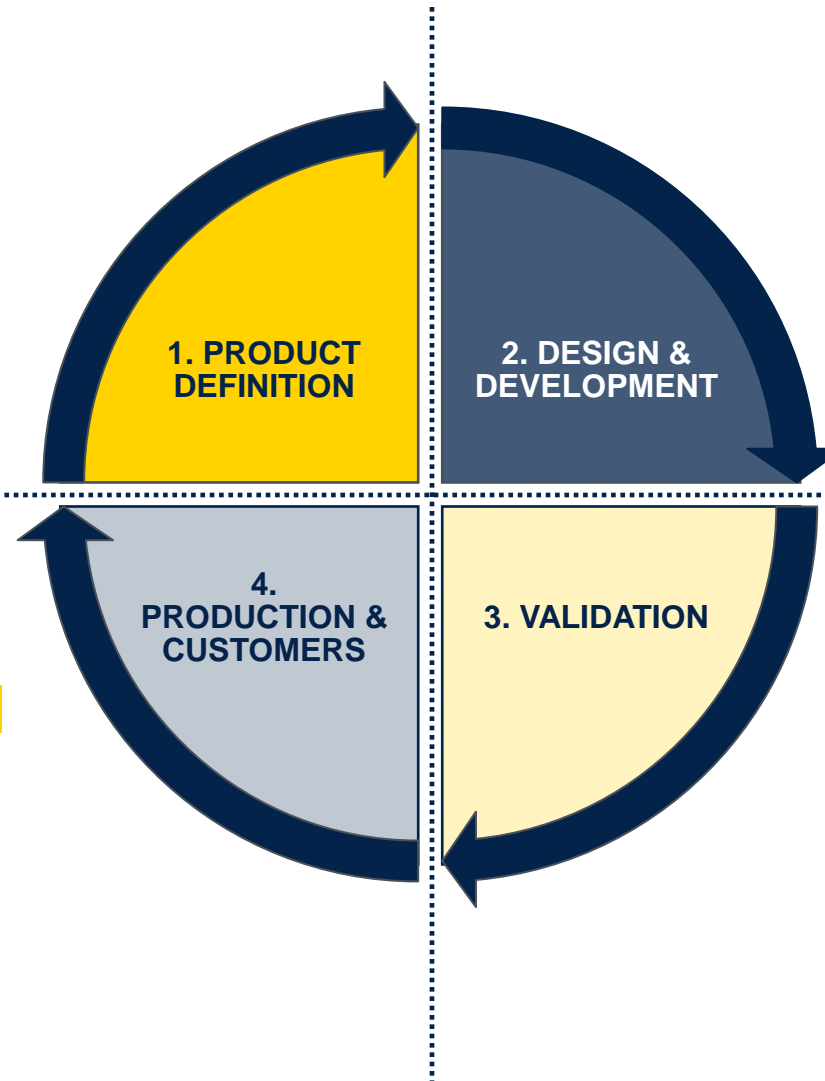
- Track vulnerabilities through regular scans
- Handle vulnerabilities on a risk basis
- Deploy firmware updates
- Report actively exploited vulnerabilities

- Perform functional validation
- Static and dynamic application testing (SAST and DAST), penetration testing

Security by design and for lifetime

ST Contribution

- Define the product usage
- Perform a risk assessment



- **Implement the product security features**
- **Secure SW development**
- **Create SBoM**
- **Identify of inherited vulnerabilities and remediation**

- **Track vulnerabilities through regular scans**
- **Handle vulnerabilities on a risk basis**
- **Deploy firmware updates**
- **Report actively exploited vulnerabilities**

- Perform functional validation
- **Static and dynamic application testing (SAST and DAST), penetration testing**

Question for the audience

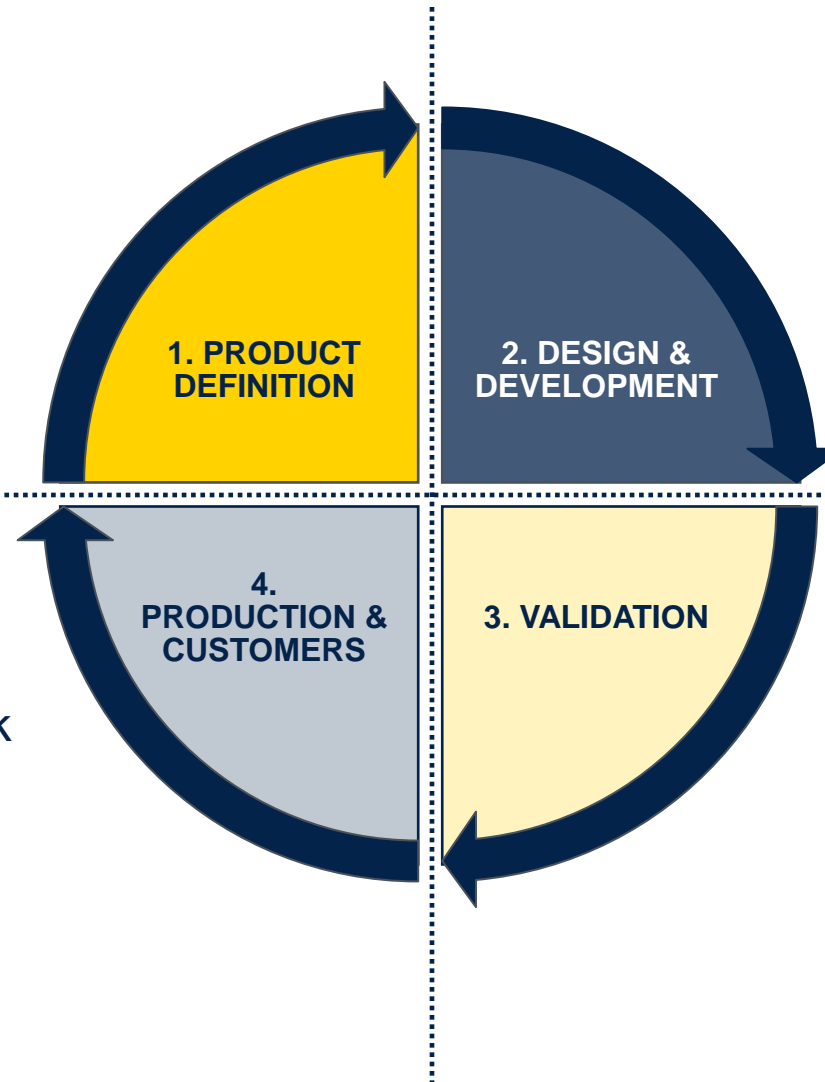
What is the most important aspect to take care of when designing a secure product:

- (1) Risk assessment
- (2) Secure Development Process
- (3) Implementation of Security Features
- (4) Vulnerability tracking through the product lifecycle
- (5) All of the above

Security by design and for lifetime

ST Contribution

- Define the product usage
- Perform a risk assessment

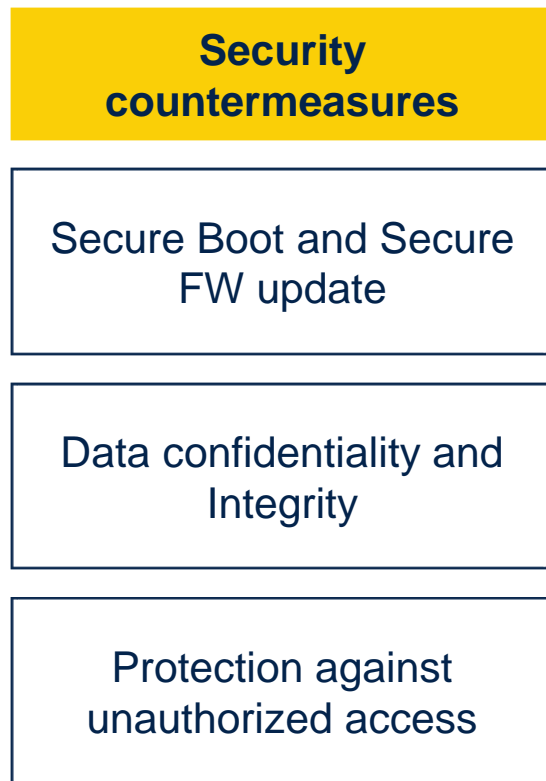


- **Implement the product security features**
- Secure SW development
- Create SBoM
- Identify of inherited vulnerabilities and remediation

- Track vulnerabilities through regular scans
- Handle vulnerabilities on a risk basis
- **Deploy firmware updates**
- Report actively exploited vulnerabilities

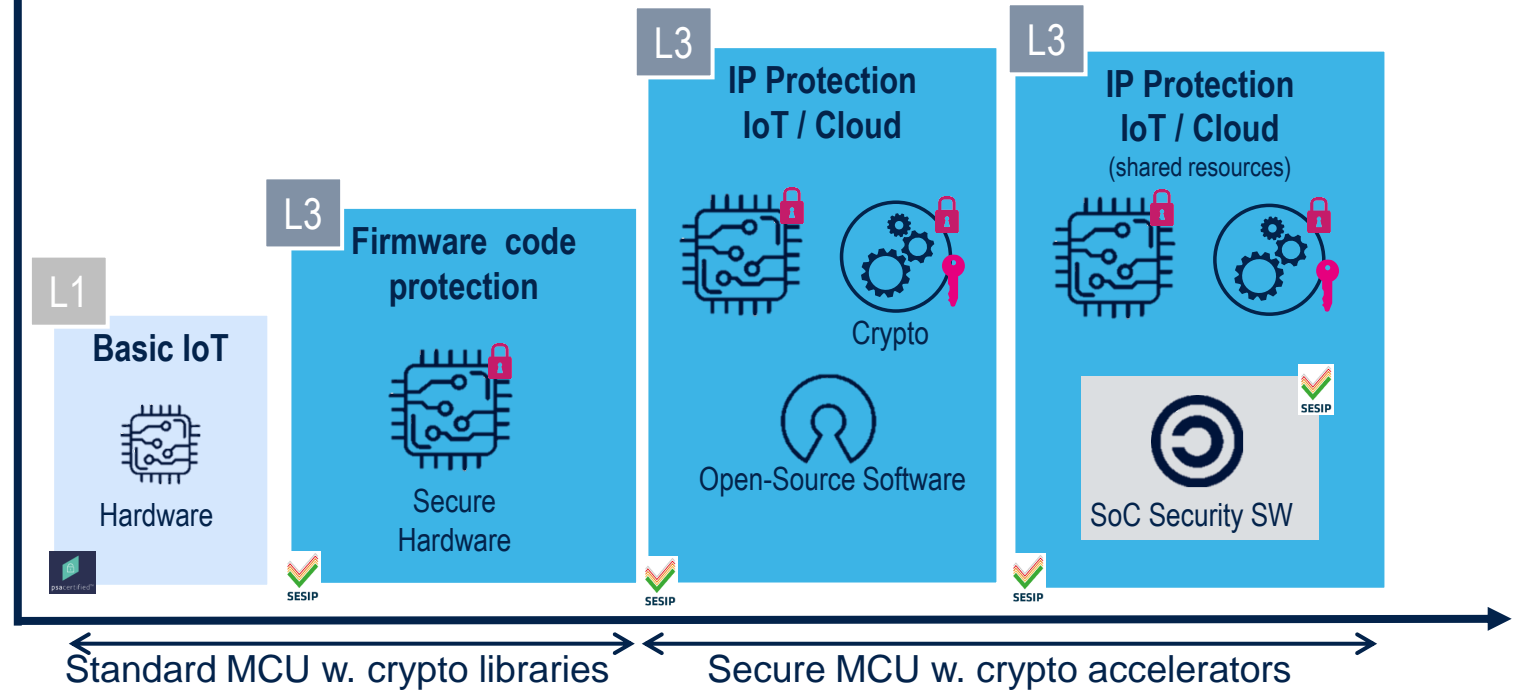
- Perform functional validation
- Static and dynamic application testing (SAST and DAST), penetration testing

From basic SW-based implementations to advanced embedded HW functions reaching SESIP L3 assurance, and certified secure FW packages



Protection against attacks on chip

Protection against remote attacks





STM32 MCU/MPU

Target certifications

MPU

PSAL1	PSAL1	PSAL1	PSAL3	SESIP3	PCI ready	PSAL3	SESIP3	PCI ready
STM32MP15 – CA7/CM4	STM32MP13 – A7	STM32MP25 – A35/M33						
Native Secure Boot TF-A + OPTEE	Native secure Boot External Memory encryption	Native secure Boot External Memory encryption						

High Perf MCUs

	PSAL1		PSAL3	SESIP3	PSAL3	SESIP3
	STM32F7 – CM7	STM32H7 – CM7/CM4	STM32N6 – CM55			
			PSAL3	SESIP3	PSAL3	SESIP3
	STM32F2 – CM3	STM32F4 – CM4	STM32H5 – CM33	STM32H7S – CM7		
			Native Secure Boot New product life cycle Secure Manager+ST-RoT	Native Secure Boot ROMless		

Mainstream MCUs

			PSAL1			
		STM32F3 – CM3	STM32G4 – CM4			
			Memory Hide Protect Feature			
PSAL1	SESIP3		PSAL1			
STM32C0 – CM0+	STM32F0 – CM0	STM32G0 – CM0	STM32F1 – CM3			
Memory Hide Protect Feature		Memory Hide Protect Feature				

Ultra-low Power MCUs

	PSAL1	PSAL1	PSAL1	SESIP3	PSAL3	SESIP3	PCI ready	
	STM32L4 – CM4	STM32L4+ – CM4	STM32L5 – CM33	STM32U5 – CM33	STM32U3 – CM33			
	X-Cube-SBSFU with STSAFE support		1 st STM32 With CM33 core	1 st STM32 with Secure storage HW	1 st MCU with attestation			
					PSAL3	SESIP3		
					STM32U0 M0+			

Wireless MCUs

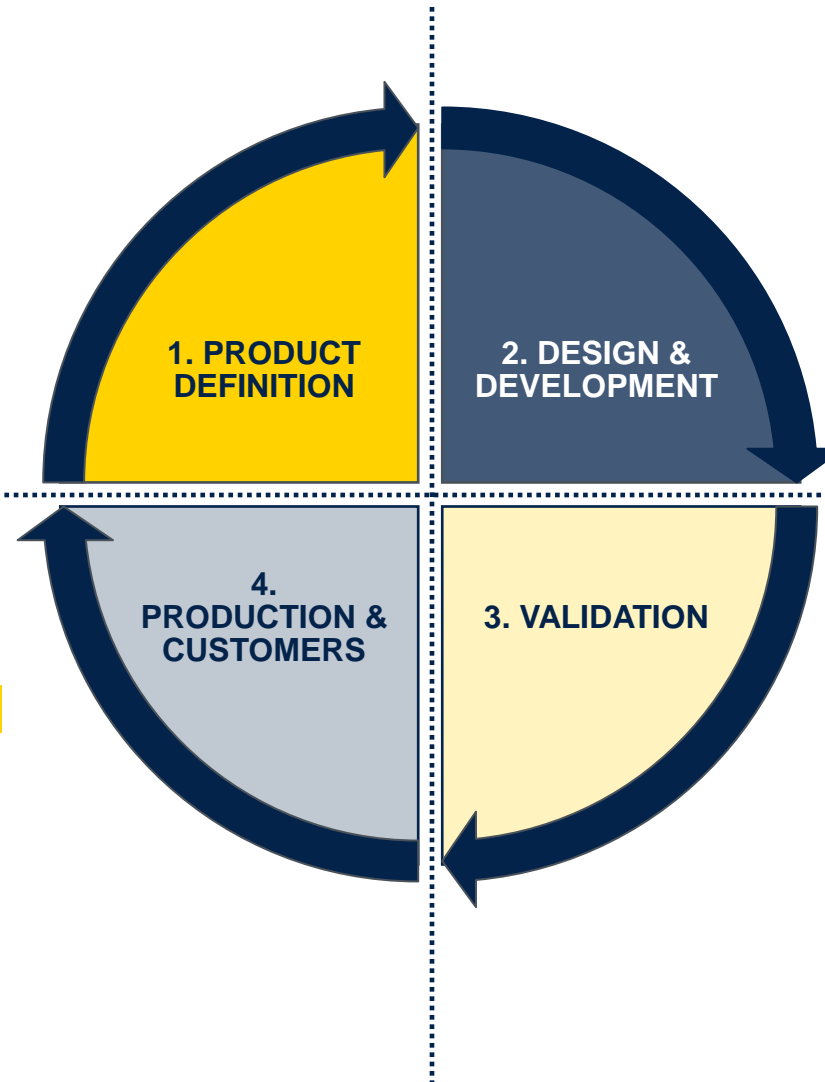
STM32WL5 - CM4/CM0+	STM32WL3 - CM0+	STM32WB5 - CM4/CM0+	STM32WB0 - CM0+	PSAL1	SESIP3
X-Cube-SBSFU	Secure Bootloader	X-Cube-SBSFU with Customer Key Storage	Secure Bootloader	STM32WBA – CM33	
				Wireless STM32 With Secure Storage HW	

Note: information reflects highest die security features

Security by design and for lifetime

ST Contribution

- Define the product usage
- Perform a risk assessment

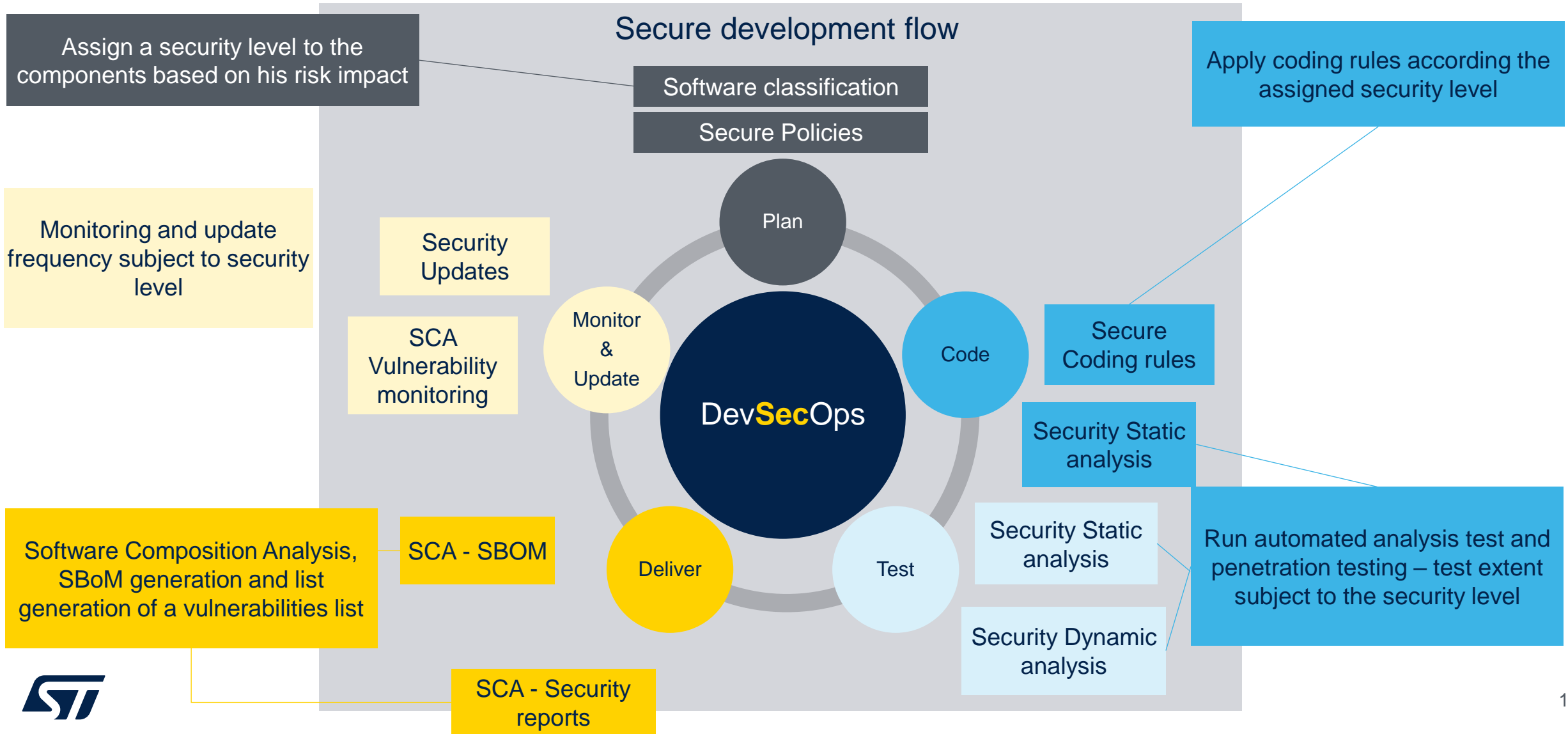


- **Implement the product security features**
- **Secure SW development**
- **Create SBoM**
- **Identify of inherited vulnerabilities and remediation**

- **Track vulnerabilities through regular scans**
- **Handle vulnerabilities on a risk basis**
- **Deploy firmware updates**
- **Report actively exploited vulnerabilities**

- Perform functional validation
- **Static and dynamic application testing (SAST and DAST), penetration testing**

STM32Trust software security policies: ST leading the way



Question to the audience

How does ST support me in my journey to make a secure product? (check all that apply)

- Risk assessment
- Secure Development Process
- Implementation of Security Features
- Vulnerability tracking through the product lifecycle

Future-proof your device with PQC

X-CUBE-PQC ACTIVE Save to myST

STM32 Post Quantum Cryptographic firmware library software expansion for STM32Cube

[Get Software](#) [Download databrief](#)

[Overview](#) [Documentation](#) [Tools & Software](#)



**POST-QUANTUM
CRYPTOGRAPHY**

- With the advent of quantum computers, traditional asymmetric cryptographic algorithms such as RSA, ECC, DH, ECDH, and ECDHE become vulnerable.
- NIST has selected a new set of algorithms designed to be resistant to quantum computing attacks
- The STM32 post-quantum cryptographic library package (X-CUBE-PQC) includes all the major security algorithms for encryption, hashing, message authentication, and digital signing.
- The library includes the PQC Leighton-Micali signature (LMS) verification method, which is used mainly for secure boot code authentication.
- This package contains an example of LMS signature verification using the STM32 cryptographic accelerator running on the STM32H563ZI microcontroller

STM32 products are fully committed toward security

ST develop products and solutions to ease device conformance



STM32 Trust Security Functions: from basic solutions up to a robust HW based solution owned and maintained by ST

STM32Trust software security policies: unparalleled level of secure process support

STM32 products and solutions offer the highest level of security in being compliant with the most stringent certifications

STM32 is the safest way for security certifications



If you would like to reach out and have a dedicated discussion, please shared your contact details.

Our technology starts with You



Find out more at www.st.com

© STMicroelectronics - All rights reserved.

ST logo is a trademark or a registered trademark of STMicroelectronics International NV or its affiliates in the EU and/or other countries.

For additional information about ST trademarks, please refer to www.st.com/trademarks.

All other product or service names are the property of their respective owners.

