Rise to Automotive Security Challenges
迎接汽车信息安全挑战

Jing Zhe, Bosch China, AUTOSAR

@Cybersecurity Vehicle Forum, Global Platform, Beijing 2023.10.24

BOSCH

Overview of Bosch Product Security

Agenda

- Automotive Cybersecurity Standards/Regulations
  - International cybersecurity regulation:WP.29/R155
  - CN cybersecurity vehicle type approval standard
  - Overall CN automotive cybersecurity standard system
- Bosch Coping Strategy
  - Security Engineering Process (Comply to ISO21434)
  - Security Features
  - Monitoring & Maintenance(Operation)
- Outlook - Quantum Computers and their Cybersecurity Impact

BOSCH

Automotive Cybersecurity Standards/Regulations

-International cybersecurity regulation:WP.29/R155
-CN cybersecurity vehicle type approval standard
-CN automotive cybersecurity standard system

BOSCH

Automotive Cybersecurity Standards/Regulations

International cybersecurity regulation:WP.29/R155

BOSCH

Automotive Cybersecurity Standards/Regulations

International cybersecurity regulation:WP.29/R155

UNECE

Cyber Security Regulation

Cybersecurity Management System

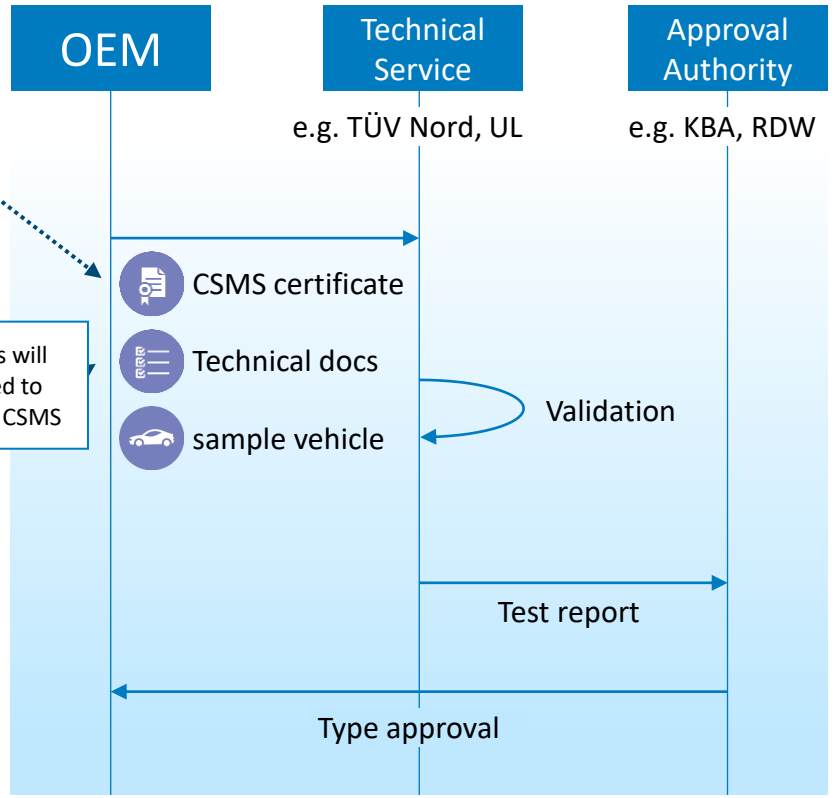
- Processes for
  - Managing cyber security
  - Identifying risks
  - Assessing, categorizing, treating risks
  - Verifying appropriate risk management
  - Testing of security
  - Keeping assessments of risks & of effectiveness of measures up to date
  - Continuous monitoring & detecting of cyber attacks, cyber threats, and vulnerabilities
  - Responding within reasonable timeframe
- Managing dependencies with suppliers and service providers
- Entire life-cycle (development, production, post-production)
- Target is vehicle type (i.e. CSMS ≠ ISMS)

Vehicle Type Security

- "Application of CSMS to vehicle type at time of type approval"

Suppliers will also need to operate a CSMS

Type Approval*

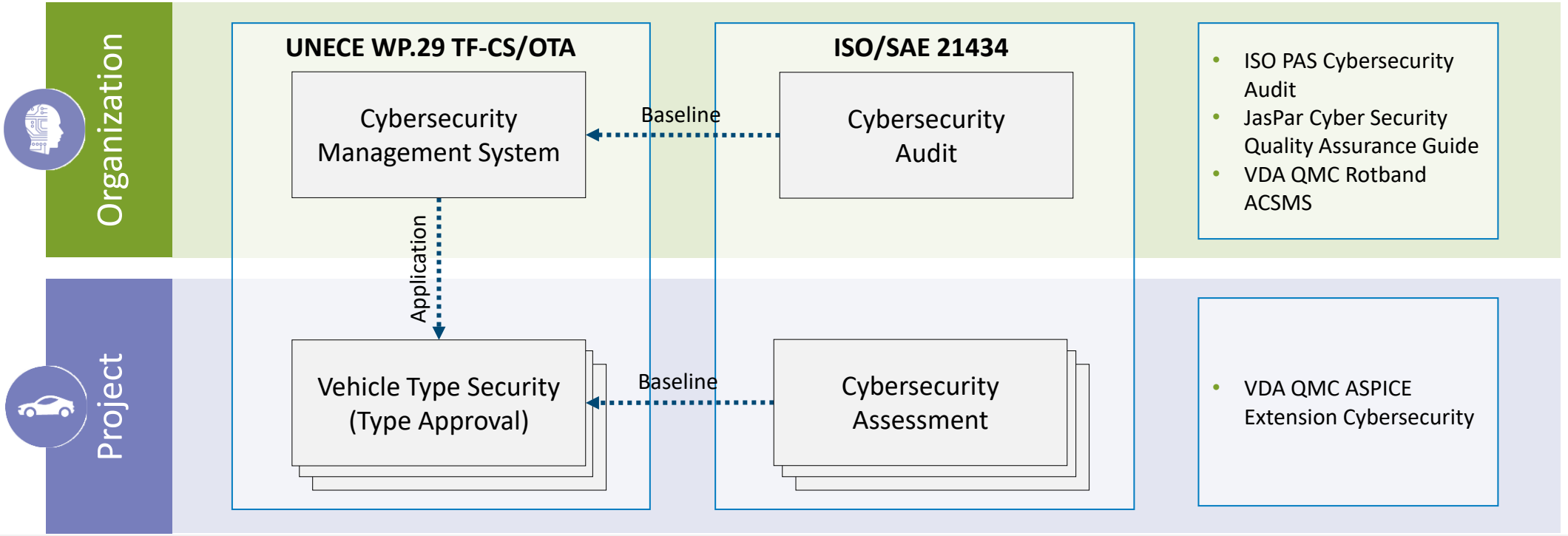


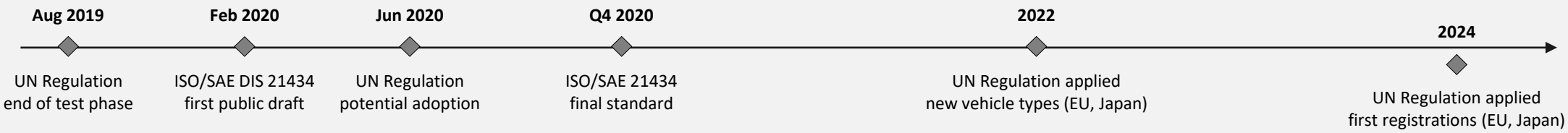
* Applicable in EU, JP, KR, UK and further markets

BOSCH

Automotive Cybersecurity Standards/Regulations

International cybersecurity regulation:WP.29/R155

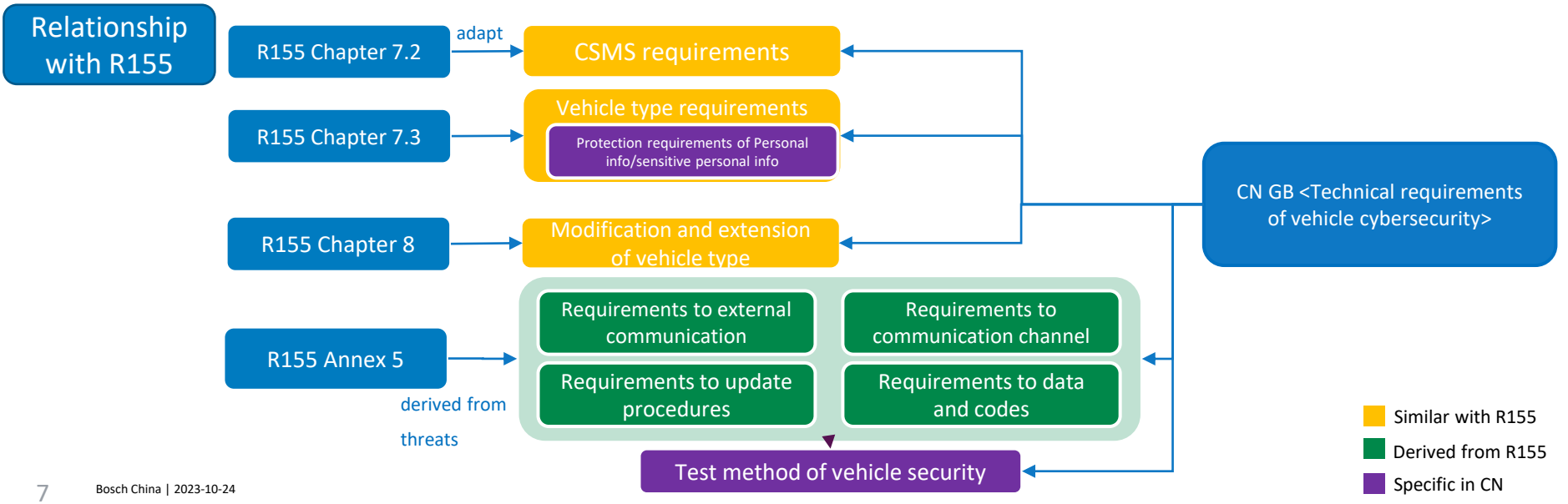




Automotive Cybersecurity Standards/Regulations

CN cybersecurity vehicle type approval standard

- The standard GB <Technical requirements for vehicle cybersecurity> derived from R155 will be a compulsory standard and used for CN vehicle type approval, plan to be released Middle of 2024:
  - CSMS(Cyber Security Management System) and Vehicle type requirements are required refer R155 → Indirect request Tier to implement CSMS and develop products based on CSMS
  - Technical requirements are derived from the threats in UNECE R155 annex 5 with tailoring.
    - The initial approach: Each threat in annex 5, at least one requirement created in this standard
  - Test methods specific in CN are defined based on technical requirements, which will be used for vehicle type approval
  - Data security requirements are compulsory in CN cybersecurity vehicle type approval → Refer to <Personal info/sensitive personal info protection> in GB/T<ICV - General requirements of data>.



Resource

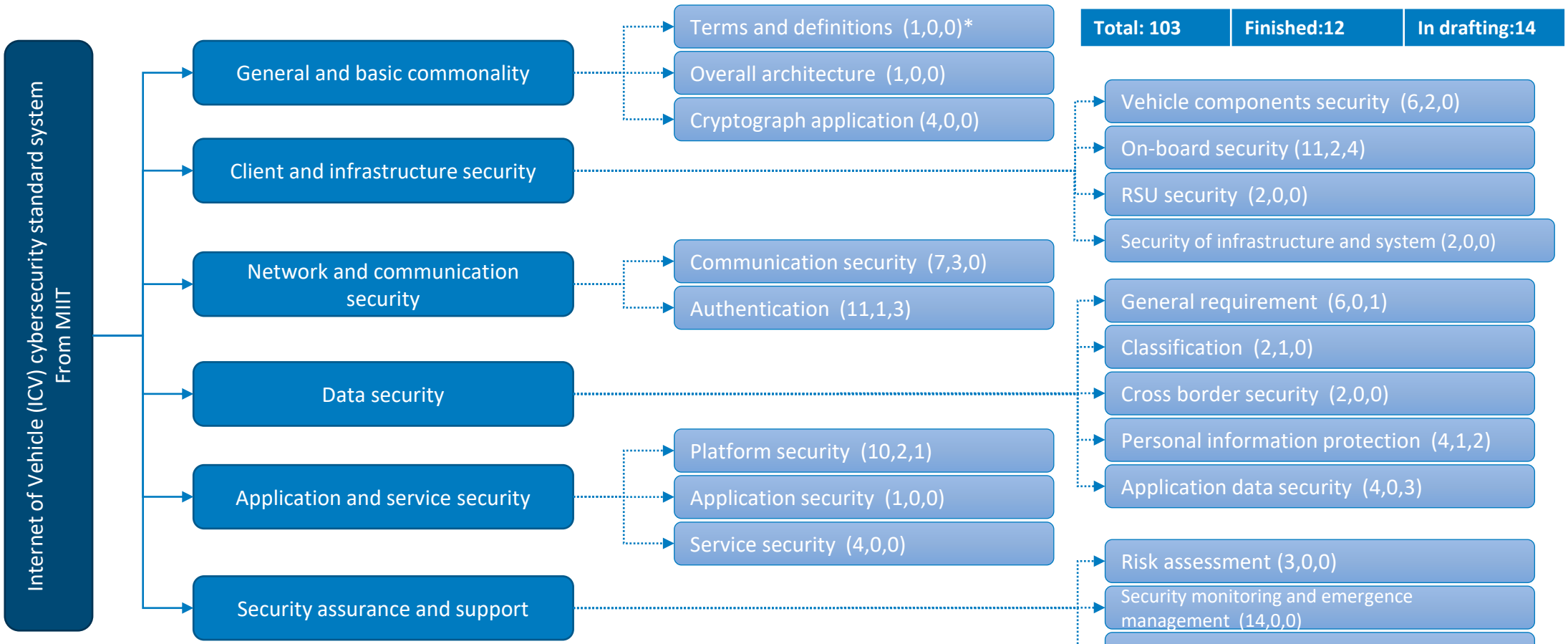
TC114 Workgroup of Standard

History

- 2019.11: GB/T phase started
- 2021.7: Switch from GB/T to GB
- 2021.9: Working group task force
- 2022.4: verification with OEMs
- 2022.6: Draft available for WG comments
- 2023.8: Submit for approval
- 2023.8: Approved
- *M2024: released*

Cybersecurity Standards/Regulations in Automotive

CN automotive cybersecurity standard system -updated in Feb.2023



*(X,Y,Z): x->Num of all standards, Y-> Num of standards finished, Z-> Num of standards in drafting

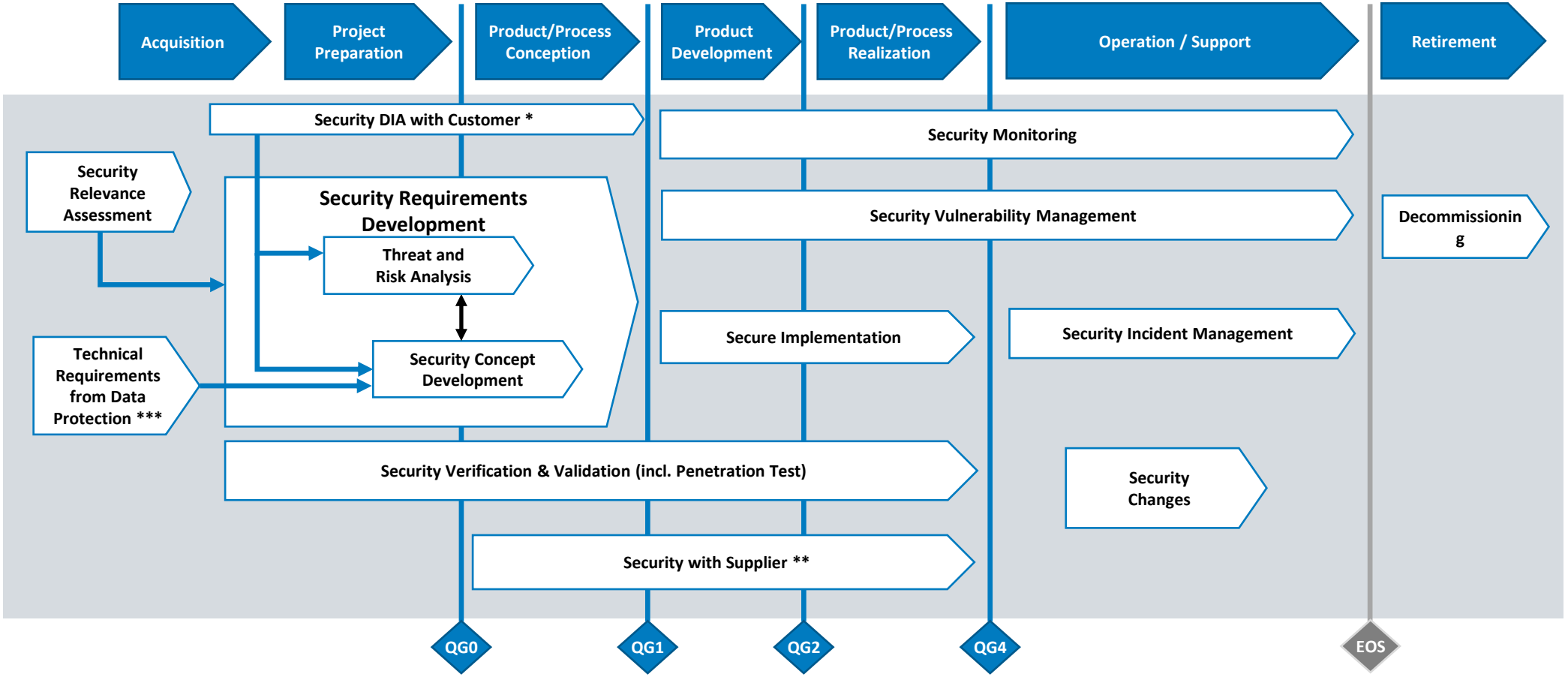
Bosch Coping Strategy

-Security Engineering Process (Comply with ISO21434)
-Categorized Security Measures
-Monitoring & Maintenance(Operation)

BOSCH

Security Engineering Process-Comply with ISO21434

Bosch Security Engineering Process



BOSCH

Bosch Coping Strategy

Put Products into Categories

1) Sensors, actuators and System ASICs

NEW

- High degree of ASIC and sensor functionality, Not programmable via automotive Bus systems (e.g., CAN, LIN, Ethernet, etc.)

2) Classic deeply Embedded ECUs (AUTOSAR- or Non-AUTOSAR based)

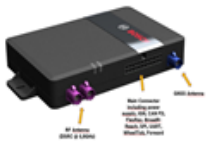
- Integrated inside automotive E/E architecture, uP or uC based, no direct Internet connection

3) Deeply embedded ECUs with higher attack potential (due to regulations and/or norms)

- Integrated inside E/E architecture, uP or uC based, no direct Internet connection, regulations on SW integrity protection

4) ECUs with Internet-connectivity

- Integrated inside E/E architecture, mainly uP-based, with Internet Connectivity



BOSCH

Bosch Coping Strategy

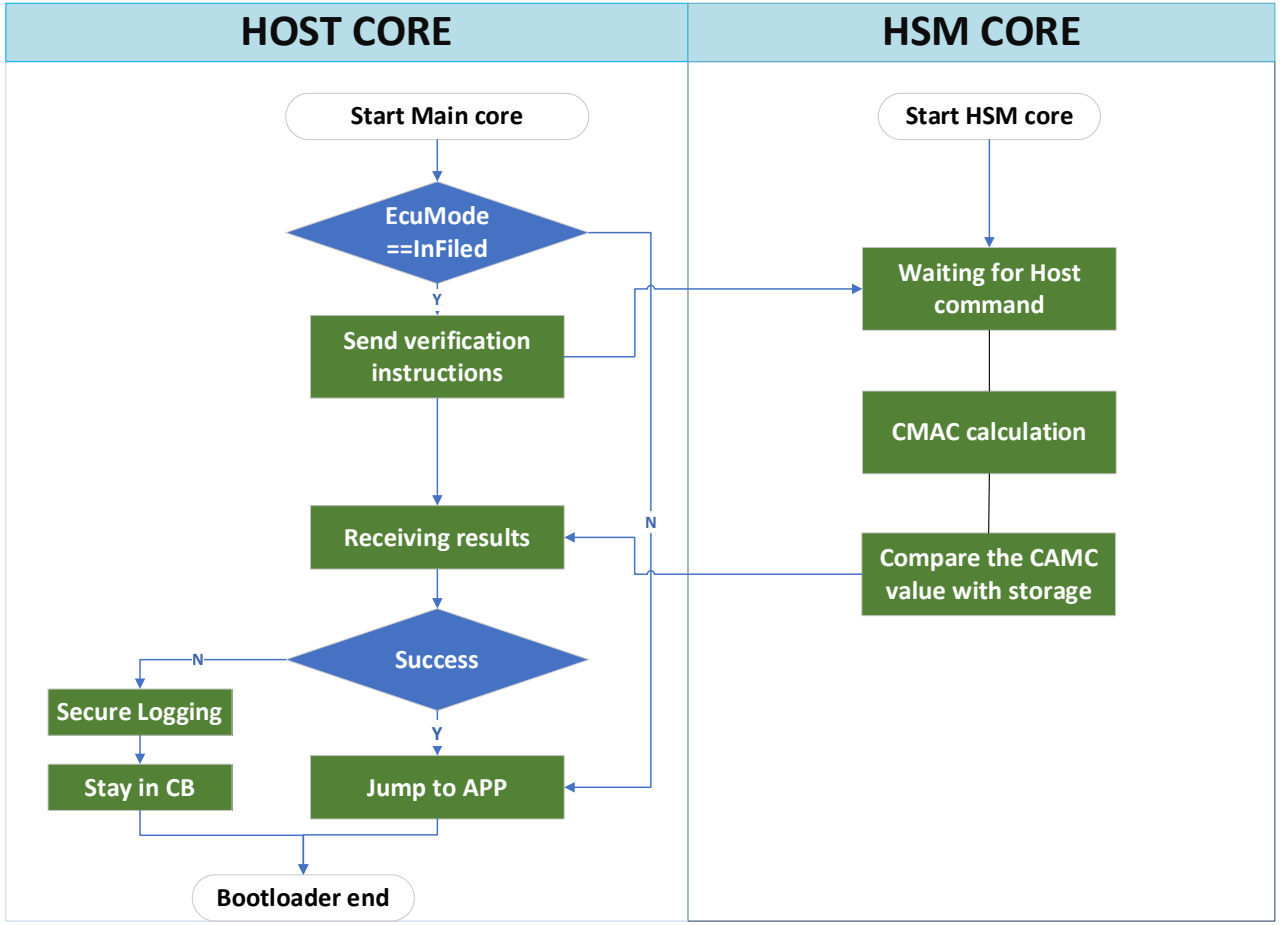
Security Portfolio Covers Product Needs

Secure Flashing	Secure Access	Secure Debug	Flash Protection	Secure Com
Ensure software authentication and integrity via **digital signatures**	Authenticated access for diagnosis services (incl. reprogramming)	Protect the JTAG port from unauthorized usage	Prevent flash from unauthorized programming	Authenticity and Integrity for vehicle internal communication

Secure Storage Secure Logging	Key Management	Software Encryption	Secure Boot	HSM Firmware Update
Ensure authenticity and confidentiality of secure stored data	Store and protect key	Encryption and decryption mechanism of delivered software to protect for theft on transport	Secure boot of initial code combined with parallel verification of further executables	HSM config area update or vulnerability escalation

Bosch Coping Strategy

Example: Secure Boot



Secure Boot

Secure boot of initial code combined with parallel verification of further executables

Key Feature:

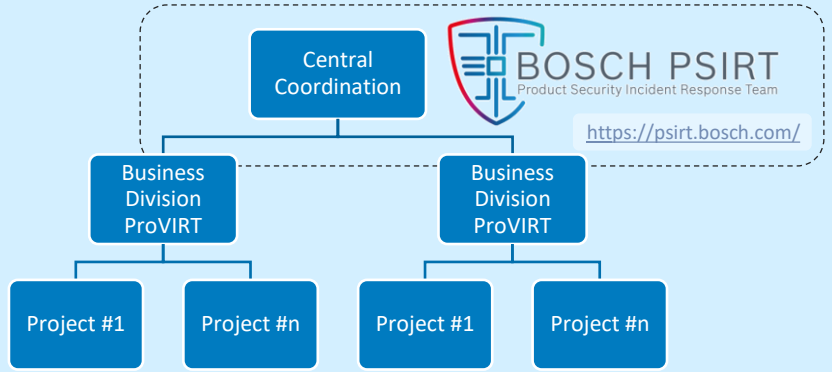
- Lifecycle switch
- Reference table update
- CMAC value calculate

Bosch Coping Strategy
Actively Monitor Vulnerabilities

Bosch has established a layered organizational structure for vulnerability management and incident response.

The Active Monitoring service will provide additional information for the OEM vehicle-level vulnerability management process.

Bosch organizational set up



Active Monitoring (recommended service, offered as a subscription model)

Sources *(illustrative)*

- NIST NVD
- Bosch Vulnerability Database
- Auto-ISAC (NA & EU)
- Supplier notifications/errata
- Customer reports
- Additional sources

Monitoring frequency
Automated screening, triage on working days (e.g., 7 hours 5 days per week)

Preliminary report
in case of an incident (e.g., 6 working days for an incident, in average)

Final report
for relevant vulnerabilities reasonable time (typically <4 weeks for root cause analysis)

Customer Benefits

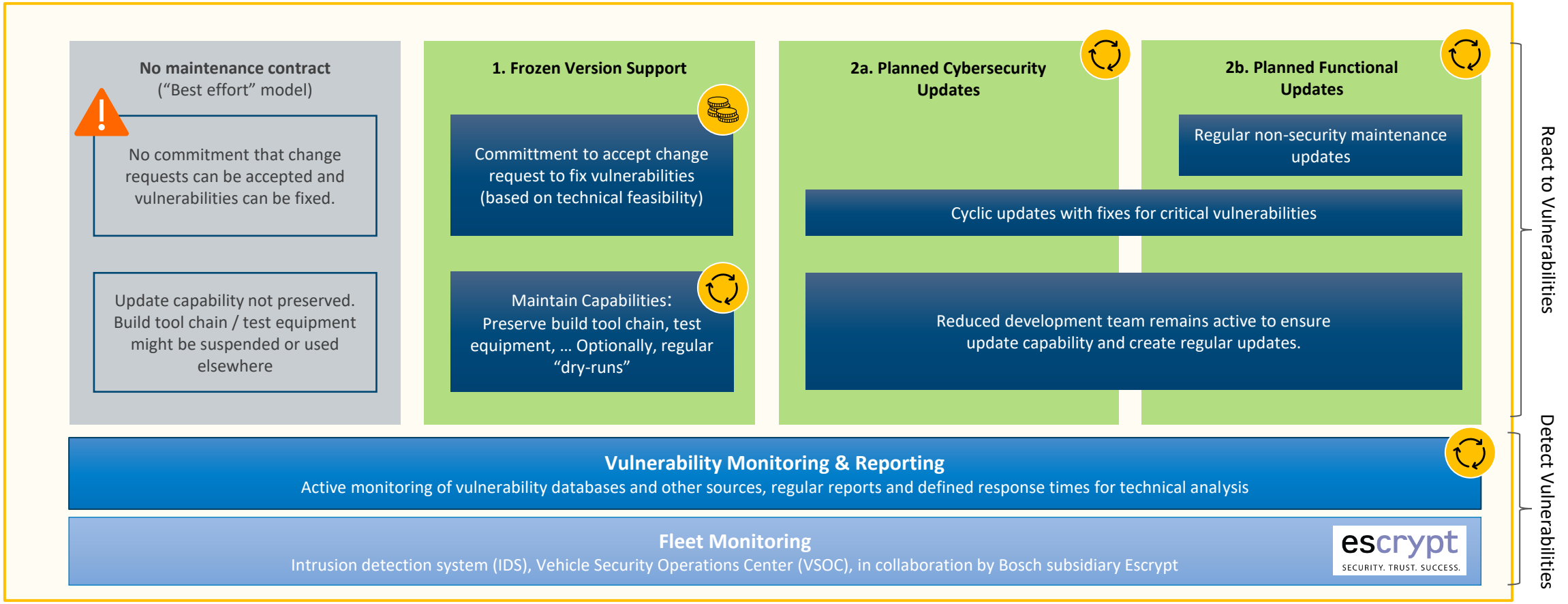
- Support to fulfill regulatory obligations (e.g., UNECE R155 and GDPR)
- Ability to react fast on security vulnerabilities/ incidents and to establish mitigations quickly.
- Access to a unique information source of a global company with many diverse customers and domains
- Reduced efforts and costs

Fallback if Active Monitoring service is not in place:

- No committed service levels, response times or reports
- Reactive and limited approach only, no proactive monitoring included

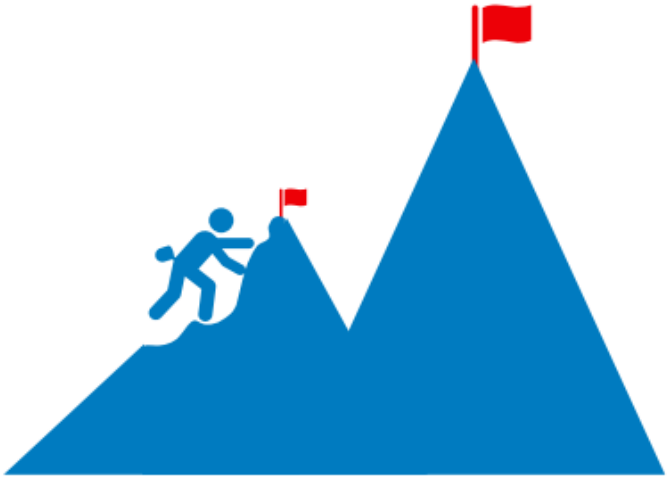
Bosch Coping Strategy

Building Blocks for Monitoring & Maintenance



Bosch Coping Strategy
Long Term Monitoring & Maintenance

Delivery a Safe/Secure vehicle



Next challenge:

Ensure Safety/Security in all Lifecyle of vehicle

Long term monitoring & maintenance must be there

Outlook - Quantum Computers and Their Cybersecurity Impact

BOSCH

Quantum Computers and their Cybersecurity Impact

Post Quantum Cryptography (PQC)

Cybersecurity attacks supported by Quantum Computers can disrupt our security building blocks. Means the integrity of our products could not be ensured any more, which implies pot. liability issues and worst-case scenarios.

Irrespective of the issues with Quantum Computers, we should be prepared for the worst-case scenario. Means we should analyze & pot. change:

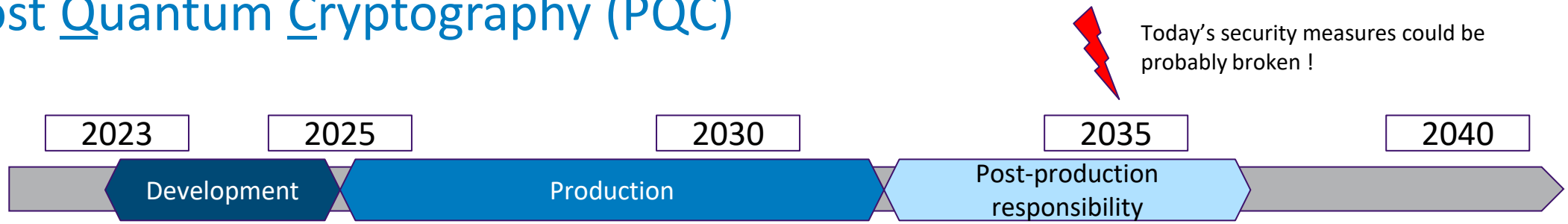
- our contracts,
- our HW,
- our security concepts and
- our key management.

SW updates in field will not solve the issue!

A PQC Strategy must be defined & established soon!

Quantum Computers and their Cybersecurity Impact

Post Quantum Cryptography (PQC)



- Quantum computers could cause cybersecurity real-world impacts in 2035, with a 50% likelihood !
- The products which are in field 2035, are designed today !

→ to avoid costly maintenance activities in field or the loose of assets, the QC resilience should be improved in the next 3 years!

The US NIST did a recommendation about new PQC resilient crypto primitives, recently.

An industrialization strategy in the units should be defined **soon**!

Thank you!

BOSCH