Cybersecurity Threats and Risks; International Regulatory Developments; PQC (Post-Quantum Cryptography)

Global Technical & Cybersecurity Advisor
Dennis Kengo Oka
dennis.kengo.oka@iav.jp

GlobalPlatform Cybersecurity Vehicle Forum
May 15, 2025, Shanghai, China

Introduction of IAV

Founded

1983

Berlin

Software Systems & Connectivity

Vehicle Solutions & Autonomous Driving

Powertrain Systems

6,600

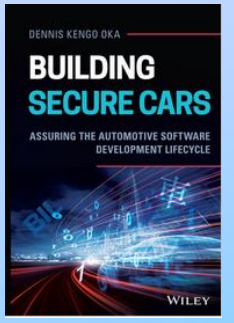
Employees

26

Locations worldwide

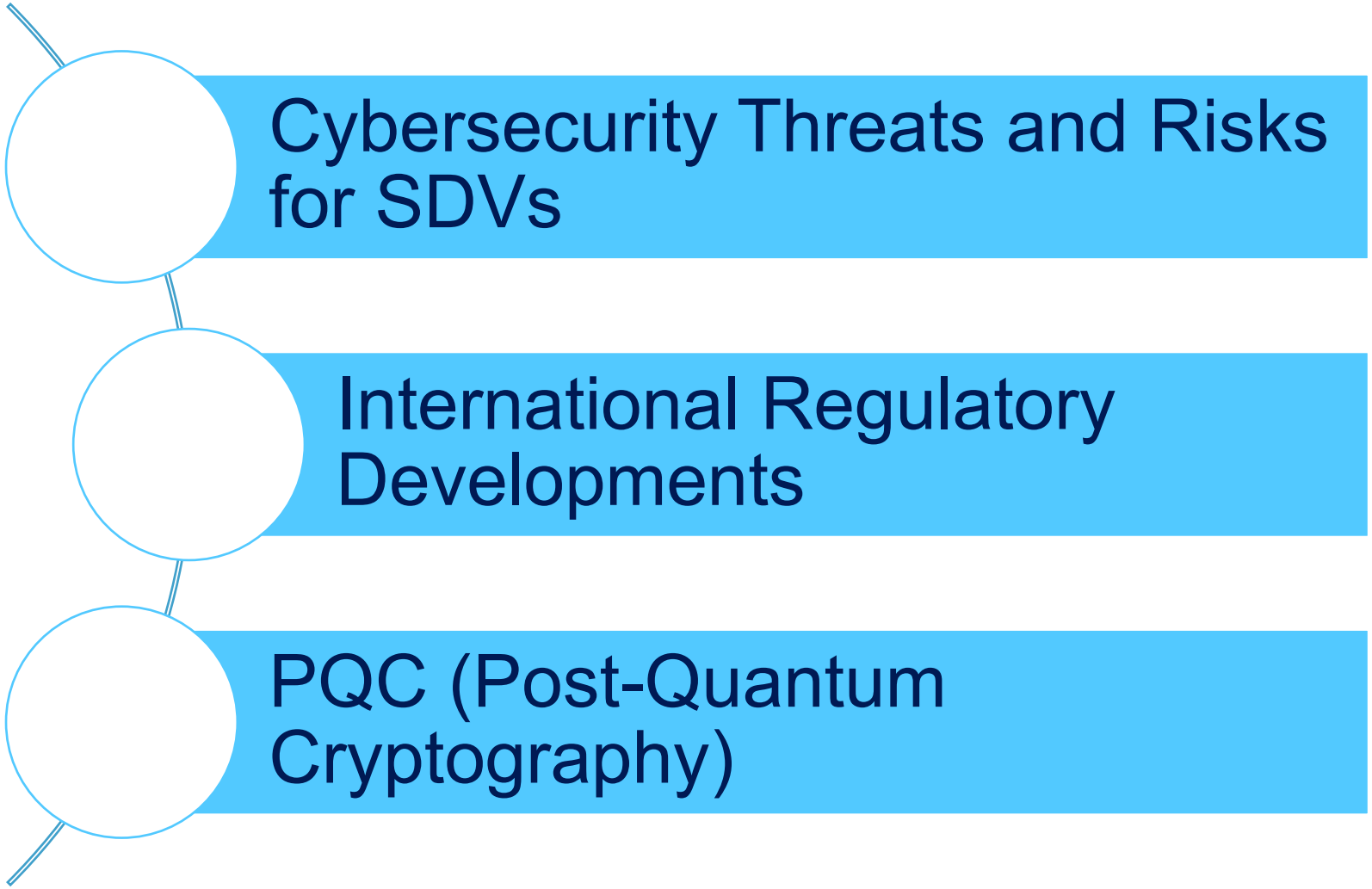
Dr. Dennis Kengo Oka

- Started working on automotive security in 2006
- Involved in standardization and best practices activities
- 70+ publications and presentations at events
- Global Technical & Cybersecurity Advisor

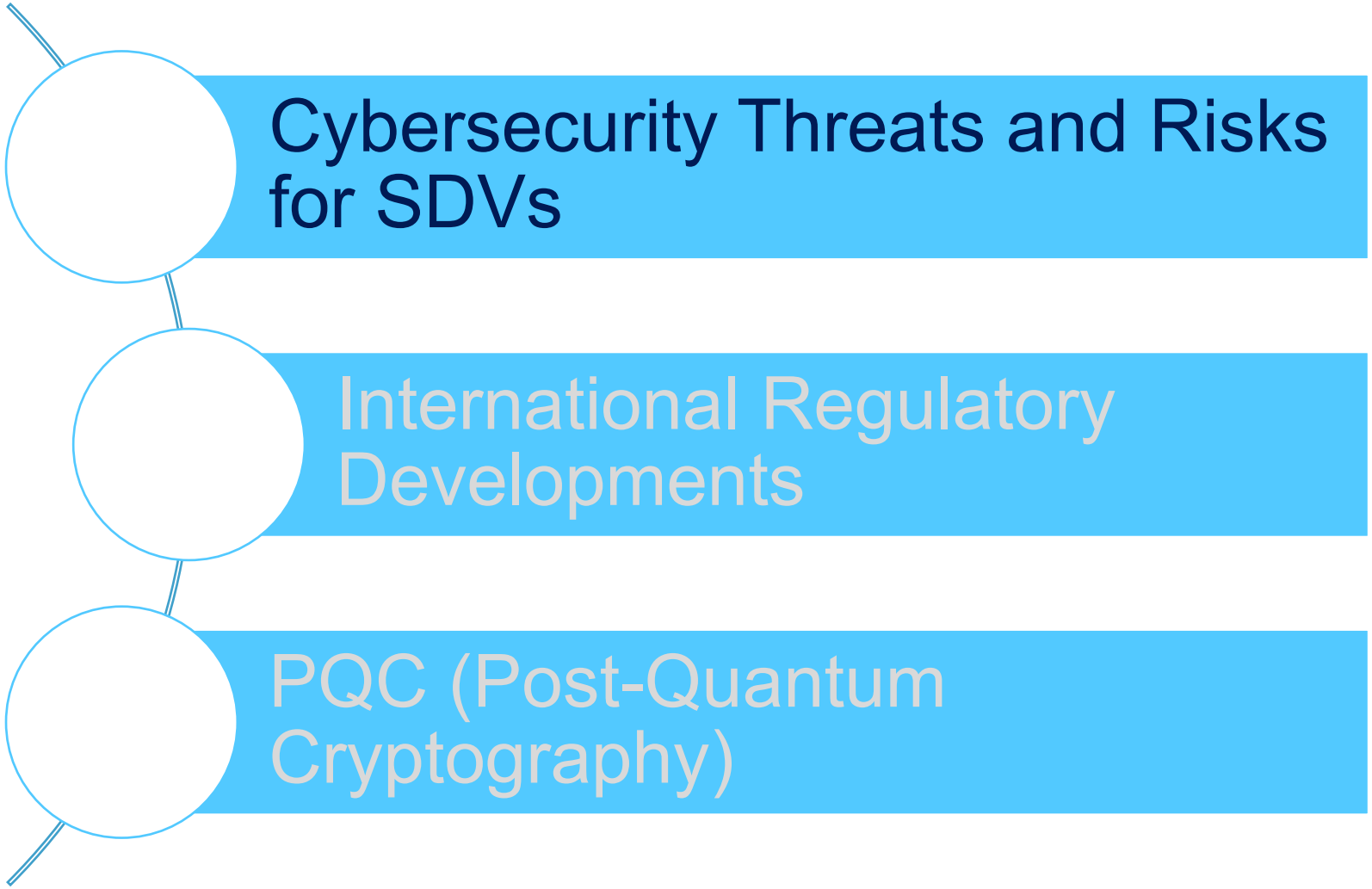


Author of books: "*Building Secure Cars: Assuring the Automotive Software Development Lifecycle*" and "*Building Secure Automotive IoT Applications: Developing Robust IoT Solutions for Next-Gen Automotive Software*"

Agenda

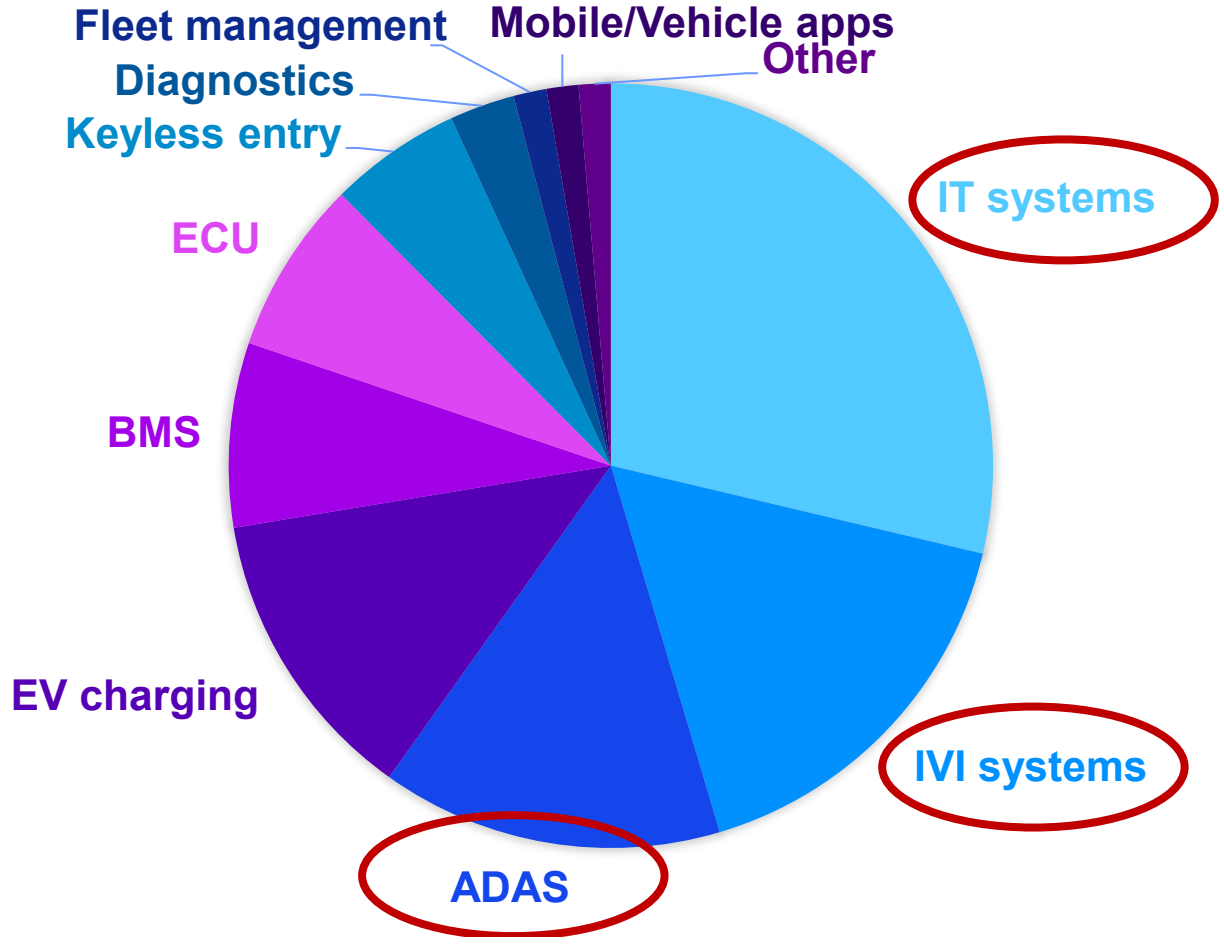

Cybersecurity Threats and Risks for SDVs
International Regulatory Developments
PQC (Post-Quantum Cryptography)

Agenda


Cybersecurity Threats and Risks for SDVs
International Regulatory Developments
PQC (Post-Quantum Cryptography)

ECU: Electronic Control Unit
BMS: Battery Management System
EV: Electric Vehicle
ADAS: Advanced Driver Assistance System
IVI: In-Vehicle Infotainment

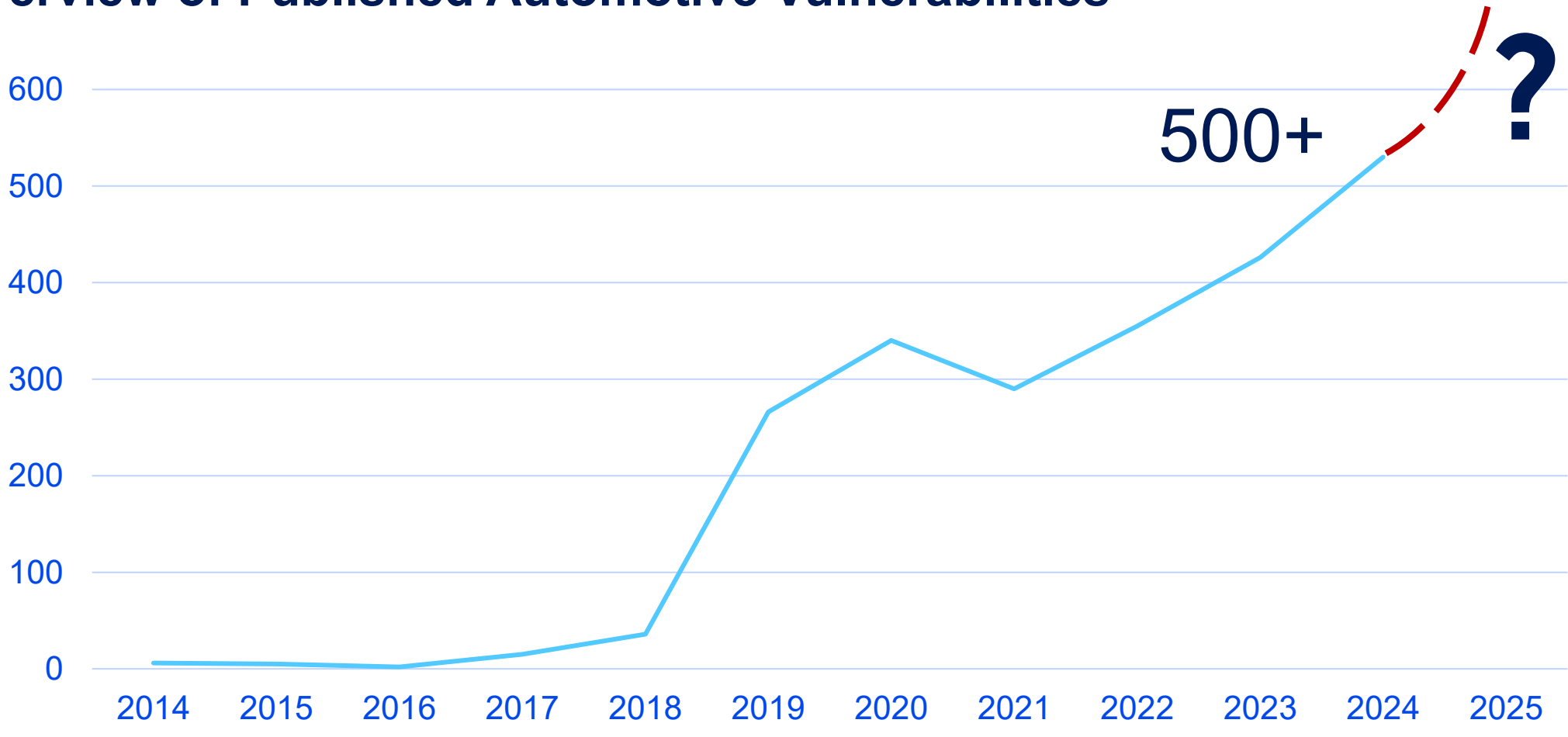
Overview of Automotive Threats in 2024



Incidents targeting IT systems, IVI systems and ADAS were most prevalent

Ref: VicOne 2025 Automotive Cybersecurity Report
VIcOne Automotive Cybersecurity Snapshot

Overview of Published Automotive Vulnerabilities

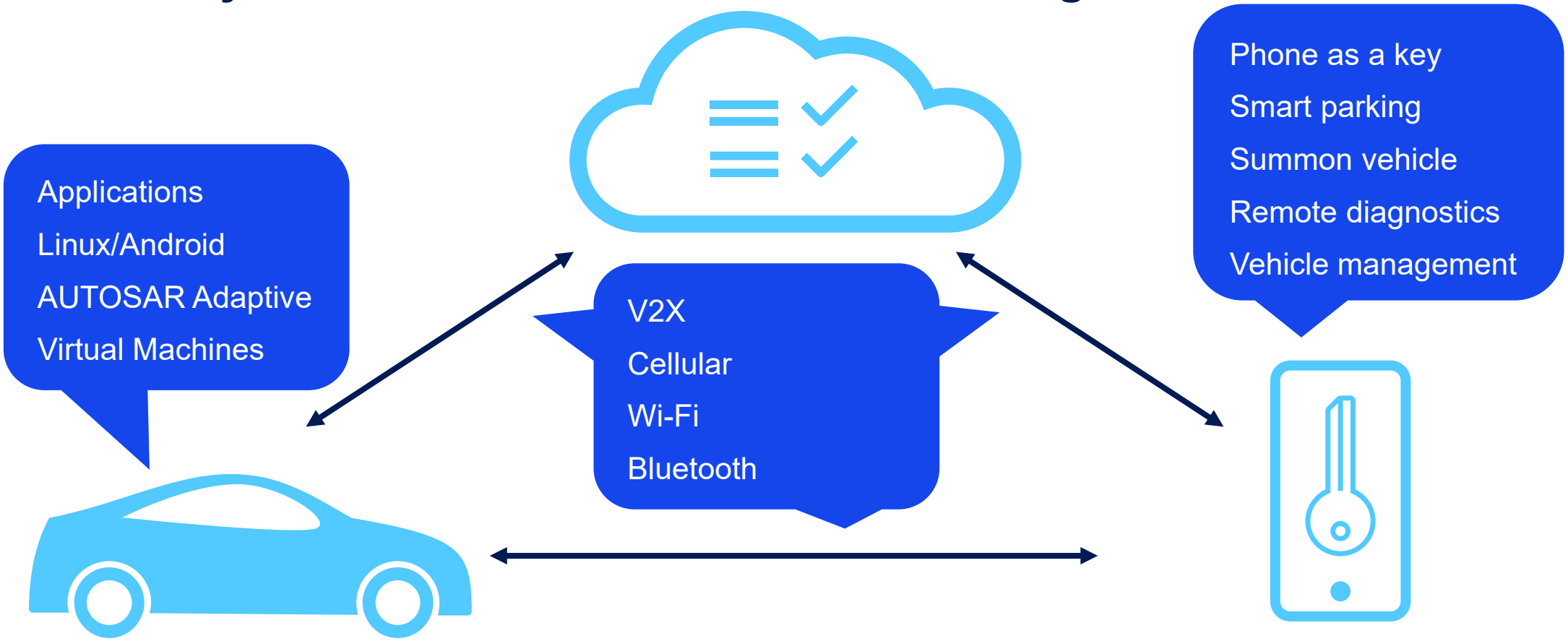


Increasing number of automotive vulnerabilities published year over year

Ref: VicOne 2025 Automotive Cybersecurity Report
VIcOne Automotive Cybersecurity Snapshot

SDV: Software-Defined Vehicle
V2X: Vehicle to X

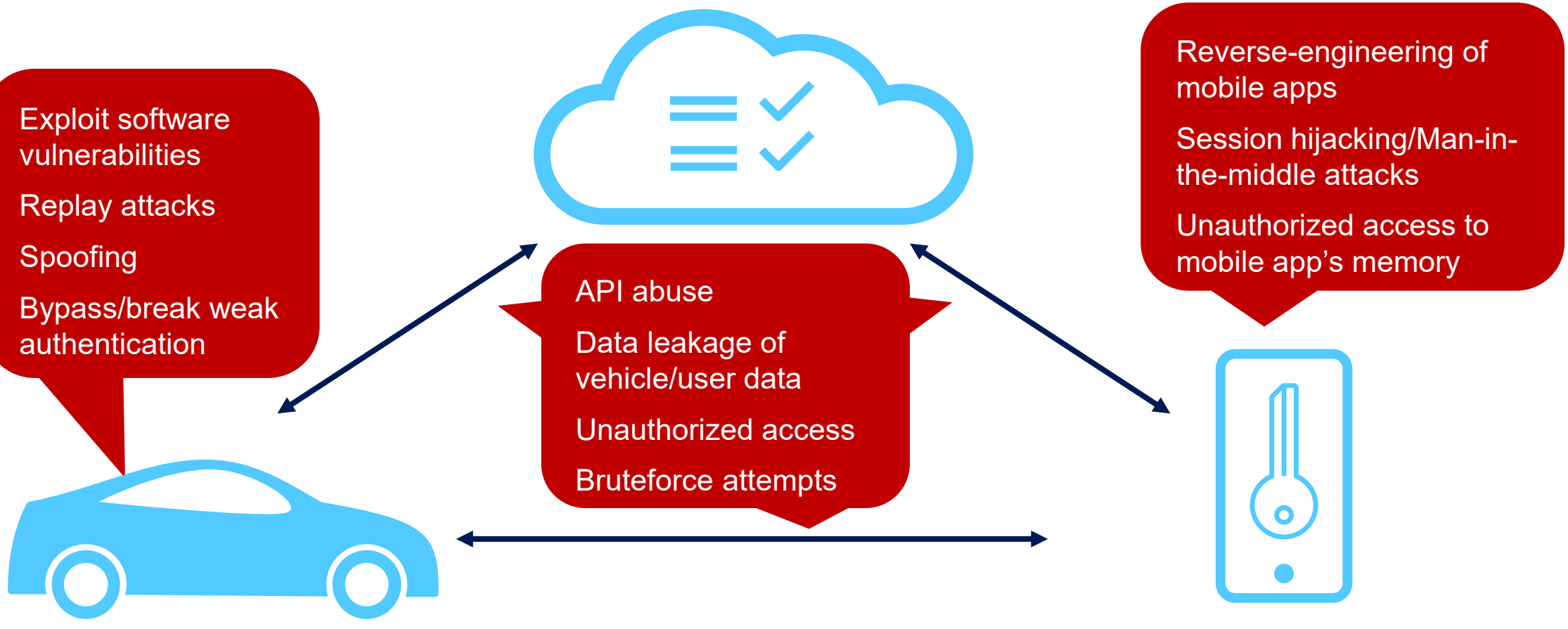
SDV Ecosystem – New Use Cases and Technologies



Advanced software and increased connectivity to support new SDV use cases

SDV: Software-Defined Vehicle
API: Application Programming Interface

Increased Attack Surface

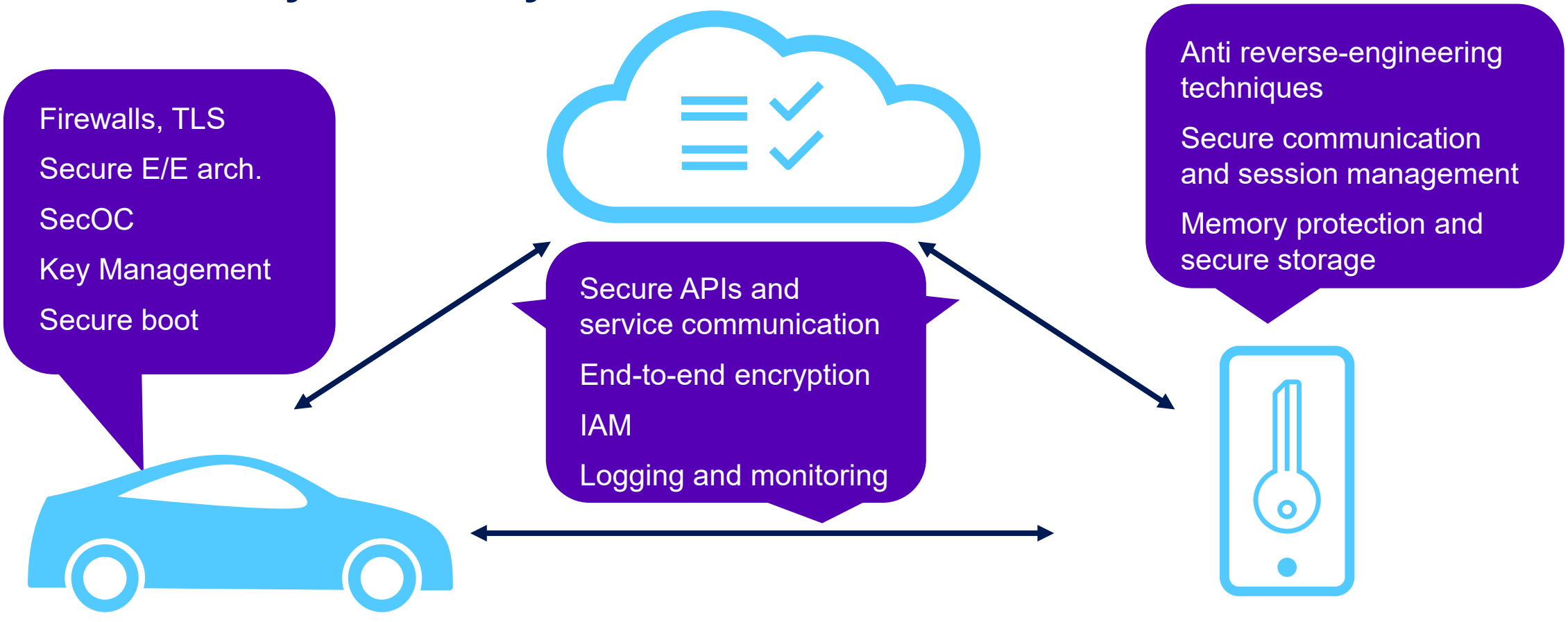


Advanced software and increased connectivity lead to increased attack surface

SDV: Software-define vehicle
TLS: Transport Layer Security
SecOC: Secure Onboard Communication

API: Application Programming Interface
IAM: Identity and Access Management

End-to-End Cybersecurity Solutions



End-to-end cybersecurity solutions are needed to reduce the risks

TARA: Threat Analysis and Risk Assessment
SecOC: Secure Onboard Communication
IDS: Intrusion Detection System
TEE: Trusted Execution Environment
CI/CD: Continuous Integration/ Continuous Delivery
CSMS: Cybersecurity Management System
SUMS: Software Update Management System
VSOC: Vehicle Security Operations Center
OTA: Over the Air
ECU: Electronic Control Unit

Secure End-to-End Lifecycle

Security Functions

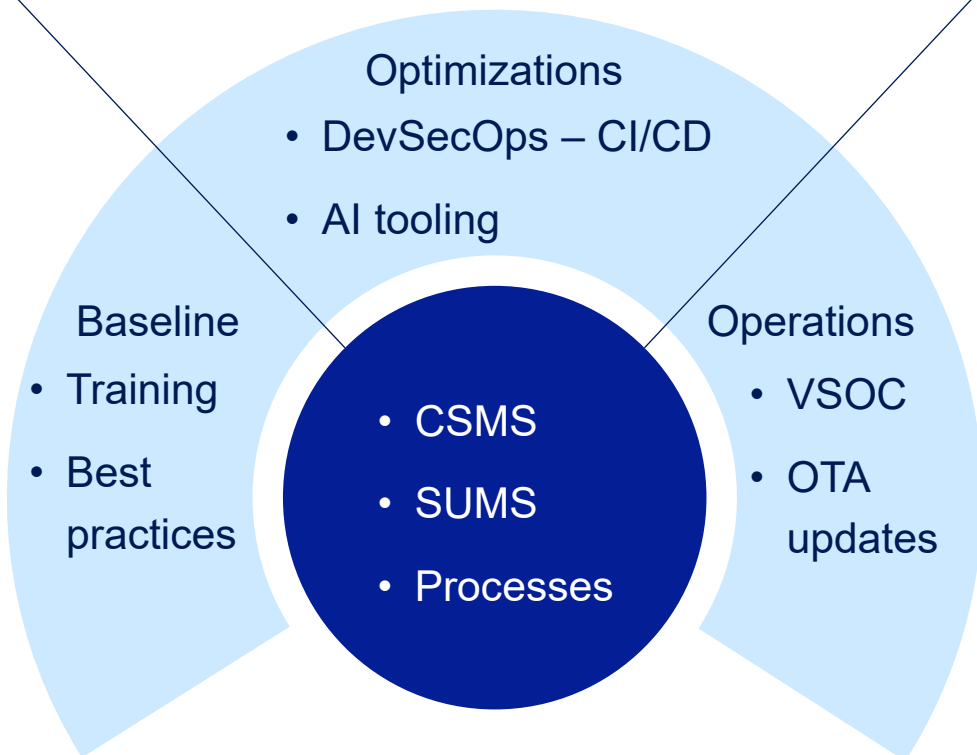
- Digital Vehicle Key
- Key Management
- SecOC
- End-to-End Encryption
- IDS
- Secure Boot
- Secure Communication
- Secure APIs

Security Engineering

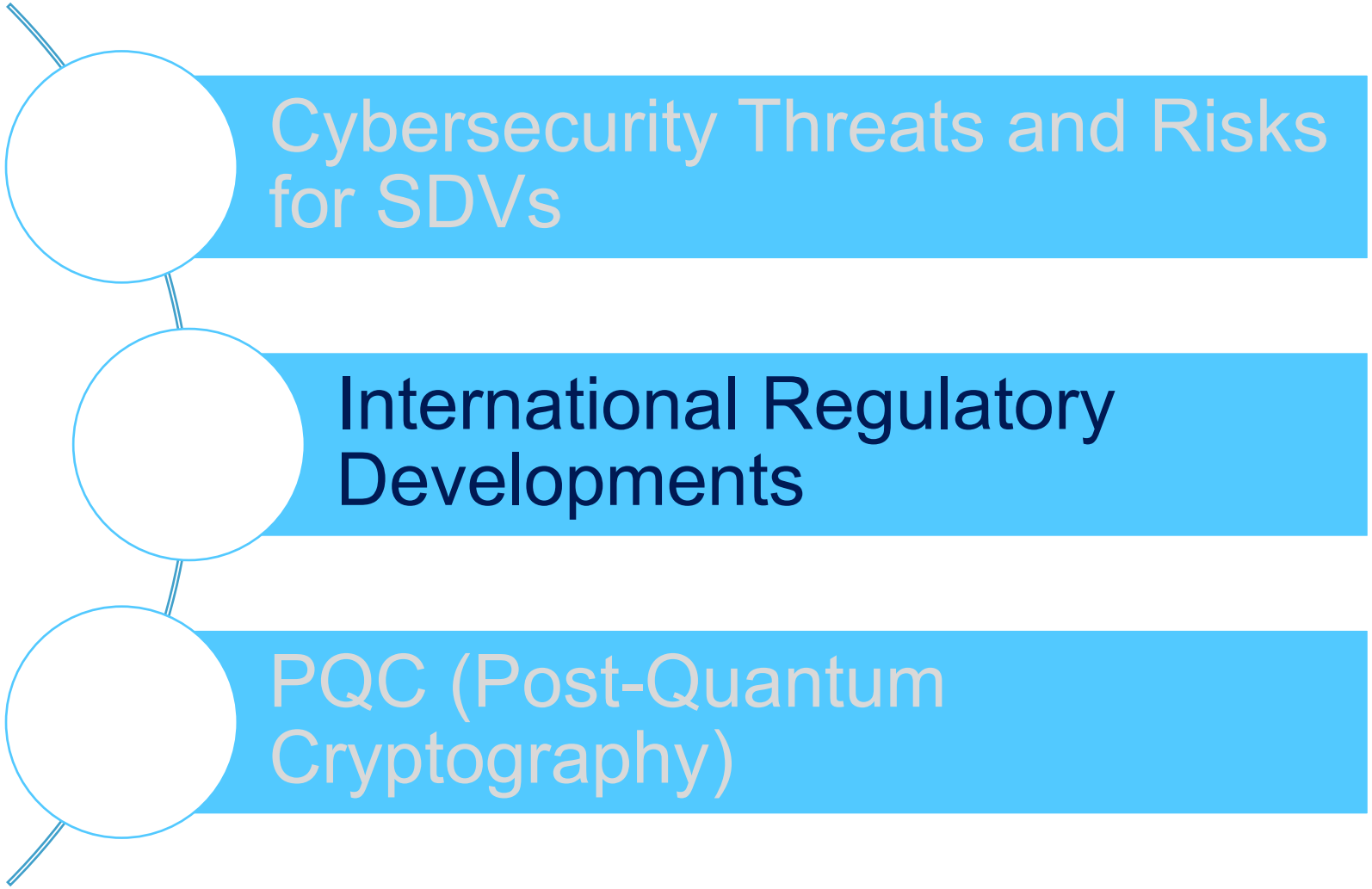
- TARA
- Security Requirements
- Security Concepts

Security Testing

- Code Review
- Functional Security Tests
- Fuzz Testing
- Pentesting (full vehicle/ ECU/cloud/mobile apps)



Agenda


Cybersecurity Threats and Risks for SDVs
International Regulatory Developments
PQC (Post-Quantum Cryptography)

Security Regulations Worldwide at a Glance

Cybersecurity – R155 vs. CRA vs. GB-44495 (1)

Legend:
Less strict
More strict

Topic	UN R155	CRA	GB-44495
Products effected	Road vehicles (M, N, O (at least one ECU), L)	Products with digital elements	Road vehicles (M, N, O (at least one ECU))
Required management system	Mandates formal CSMS certification, renewal every 3 years	Approved quality system would be sufficient	Requires CSMS audit but does not issue certificate, expects renewal every 3 years
Risk assessment	Risk assessment as part of CSMS alongside with mitigation	Simple risk assessment sufficient; needs to be part of technical documentation	Requires risk assessment of threats and vulnerabilities for products and systems

Cybersecurity – R155 vs. CRA vs. GB-44495 (2)

Legend:
Less strict
More strict

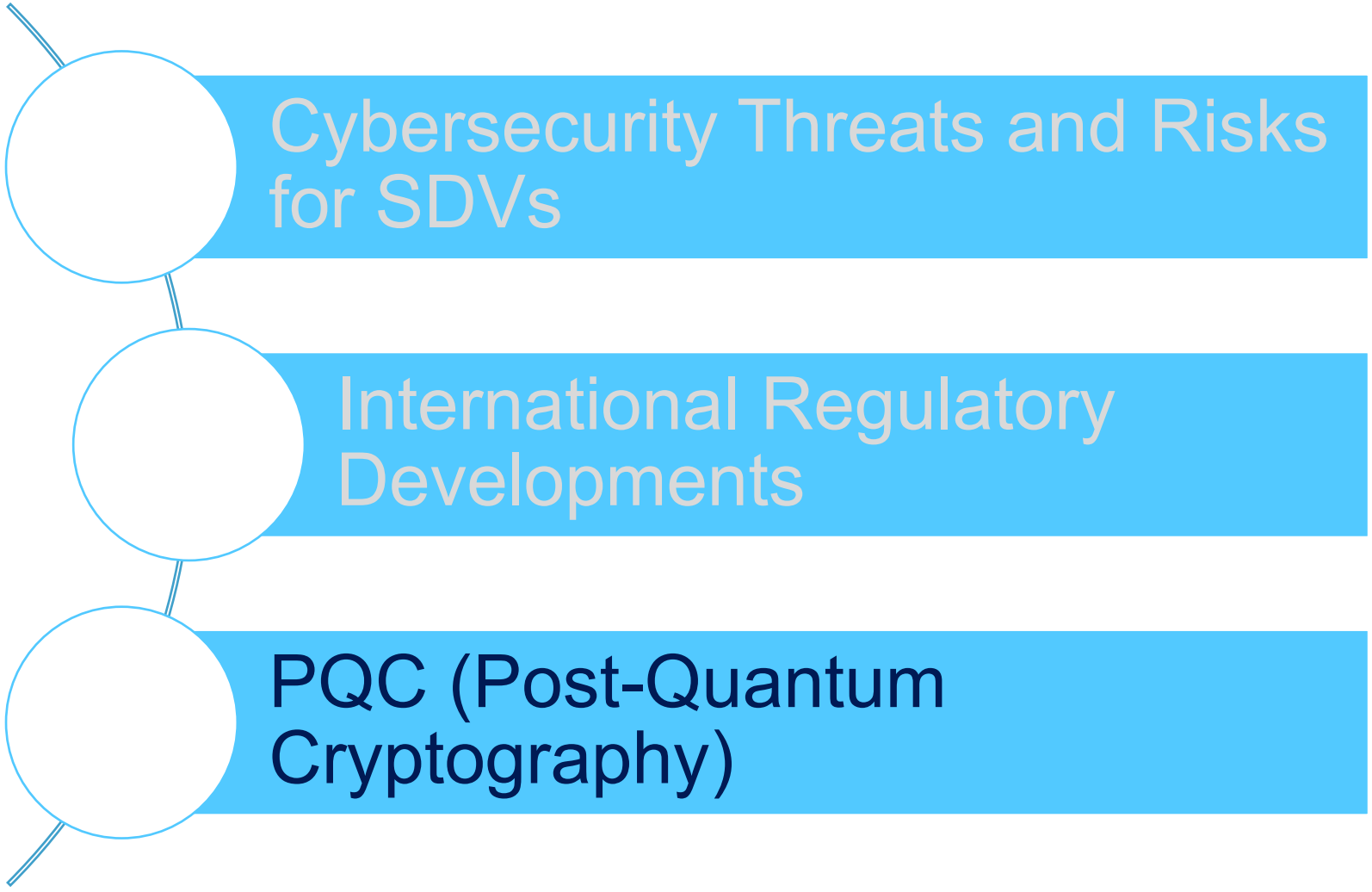
Topic	UN R155	CRA	GB-44495
Technical requirements	Threats and abstract countermeasures specified in Annex 5	Essential abstract requirements are defined in Annex I	Includes specific technical controls, such as authentication protocols, intrusion detection, and data security measures
Testing and certification	CSMS & Vehicle Types needs to be tested by technical service and certified by approval authority	Depending on type of product: self-declaration, third-party conformity assessment, or European cybersecurity certification	Testing of cybersecurity functions is required based on 27 defined security tests (e.g., external interfaces, access control, communications security); third-party labs may conduct evaluations
Cryptography requirements	Does not mandate specific algorithms but expects appropriate cryptographic measures aligned with best practices	No fixed algorithms, but secure, up-to-date cryptographic standards must be used	Specifies international, national or industry standard crypto modules (e.g., Chinese cryptographic algorithms)

Cybersecurity – R155 vs. CRA vs. GB-44495 (3)

Legend:
Less strict
More strict

Topic	UN R155	CRA	GB-44495
Reporting obligations	OEM to report yearly new attacks and actions effectiveness of implemented mitigation / additional actions	Manufacturer to report actively exploited vulnerabilities or severe incidents to ENISA within 24 hours, and more detailed incident notification within 72 hours	Processes in place for vulnerability management but no specific reporting timelines or authorities to report to
Fixing vulnerabilities	Remediation of threats and vulnerabilities in the product within a reasonable timeframe	Manufacturers shall ensure that vulnerabilities of that product, including its components, are handled effectively	Must implement vulnerability handling processes (e.g., NVDB-CAVD); known high-risk vulnerabilities must be fixed within 6 months
Service duration	… until end-of-life of all vehicles	Support period shall be at least 5 years... If expected to be in use for longer, support period shall correspond to the expected usage time	No specific minimum update period but manufacturers are expected to maintain processes that ensure continued cybersecurity of vehicles throughout their operational life

Agenda


Cybersecurity Threats and Risks for SDVs
International Regulatory Developments
PQC (Post-Quantum Cryptography)

Future Technologies – Quantum Computing

Microsoft's Majorana 1 chip carves new path for quantum computing

Written by

Catherine Bolgar

Published

February 19, 2025

Check out the world's first Quantum Operating System

2441 Views | 24 Apr 2025, 06:00 PM | Abhijeet V Singh

Fujitsu and RIKEN develop world-leading 256-qubit superconducting quantum computer

Kawasaki and Wako, Japan, April 22, 2025

New advancements in Quantum Computing

Ref: https://content.techgig.com/technology/the-dawn-of-quantum-computing-introducing-qnodeos-the-first-quantum-operating-system/articleshow/120586133.cms
https://news.microsoft.com/source/features/innovation/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing/
https://www.fujitsu.com/global/about/resources/news/press-releases/2025/0422-01.html

RSA: Rivest Shamir Adleman
ECC: Elliptic Curve Cryptography
AES: Advanced Encryption Standard

Quantum Computing Impact on Cybersecurity

Shor's algorithm

- Can factor large integers exponentially faster than best-known classical algorithms
- Affects: Asymmetric encryption algorithms that rely on the difficulty of factoring large integers or finding discrete logarithms
- Result: Big threat – e.g., RSA and ECC could be completely broken – private keys can be extracted from public keys

Grover's algorithm

- Can speed up bruteforce attacks (but only by a square root)
- Affects: Symmetric encryption algorithms that rely on key size and infeasibility of bruteforcing all possible keys
- Result: Partial threat – e.g., AES-128 would be weakened to half the security (64-bit strength)

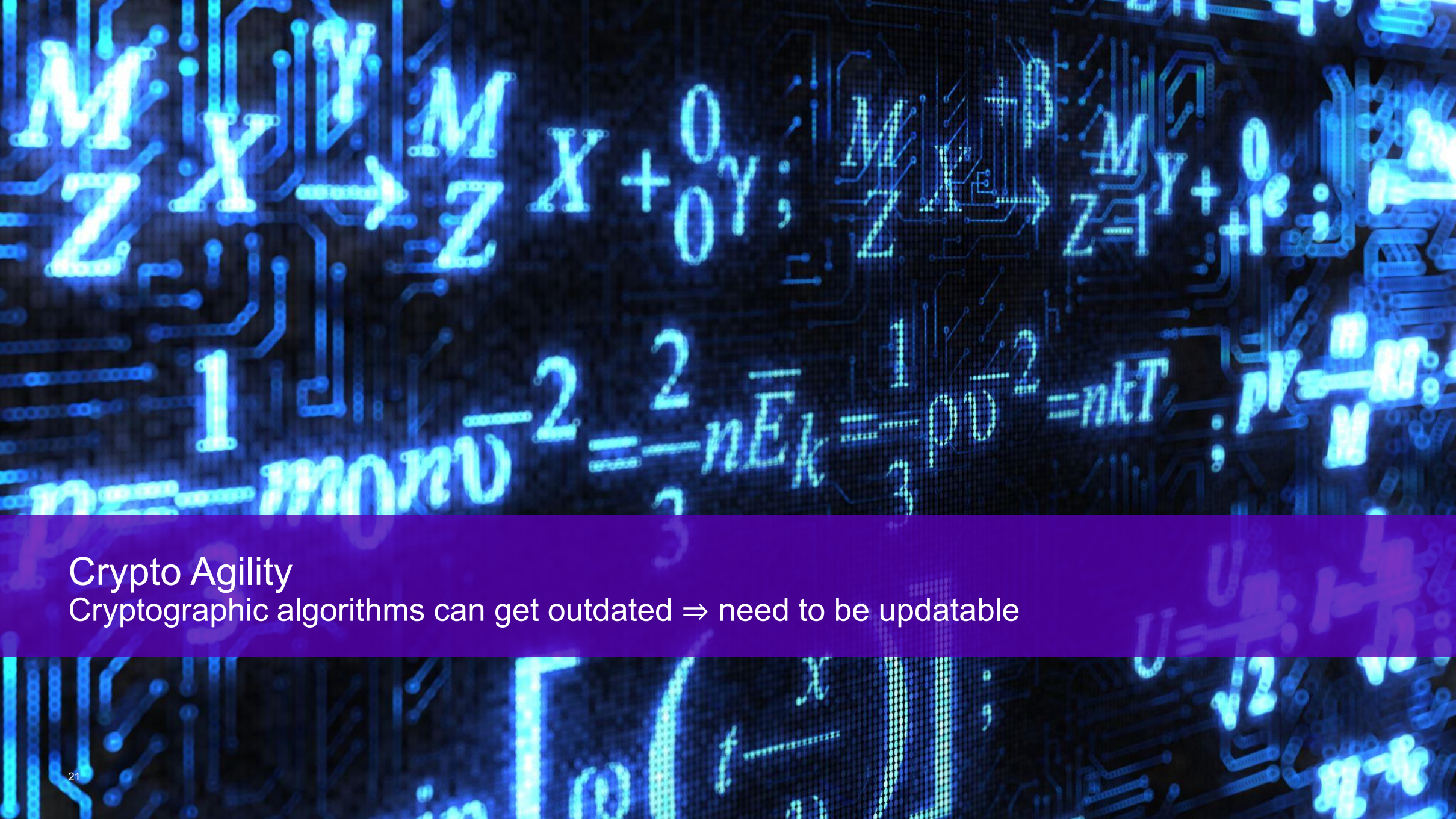
Quantum Computing has severe impact on Cybersecurity

PQC Approaches

PQC: Post-Quantum Cryptography
RSA: Rivest Shamir Adleman
ECC: Elliptic Curve Cryptography
ECDSA: Elliptic Curve Digital Signing Algorithm
ECDH: Elliptic Curve Diffie Hellman
AES: Advanced Encryption Standard
SHA: Secure Hash Algorithm
HMAC: Hash-based Message Authentication Code

Traditional Algorithm	Quantum Vulnerability	PQC Approach
RSA	Broken by Shor's algorithm	CRYSTALS-Kyber (key exchange)
ECC (ECDSA, ECDH)	Broken by Shor's algorithm	CRYSTALS-Dilithium (signatures)
AES-128	Grover's algorithm halves security (64 bits)	Use AES-256
SHA-2 (SHA-256)	Grover's algorithm halves preimage resistance (128 bits)	Continue with SHA-2 or use SHA-512 for extra margin
SHA-3-256	Grover's algorithm halves preimage resistance (128 bits)	Continue with SHA-3-256 or use SHA-3-512 for extra margin
HMAC	Depends on underlying hash (SHA-2 or SHA-3)	See above for SHA-2 and SHA-3-256
ChaCha20 (256 bits)	Grover's algorithm halves security (128 bits)	Continue with ChaCha20 (256 bits)

Post Quantum Computing Crypto solutions are needed to address the risks

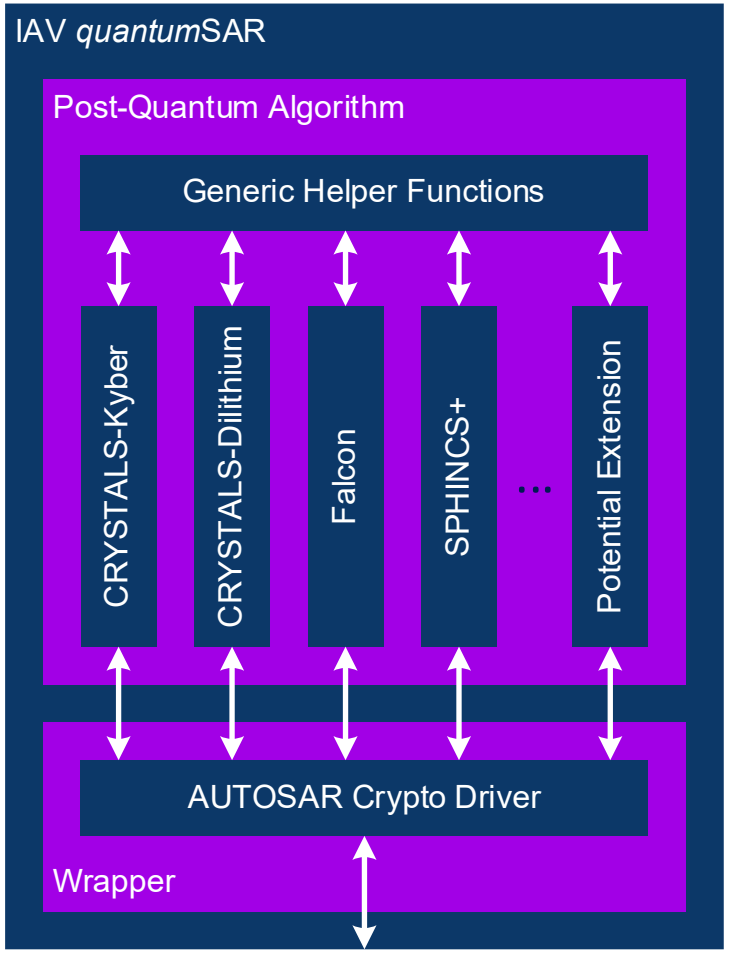


Crypto Agility

Cryptographic algorithms can get outdated ⇒ need to be updatable

NIST: National Institute of Standards and Technology
PQC: Post-Quantum Cryptography

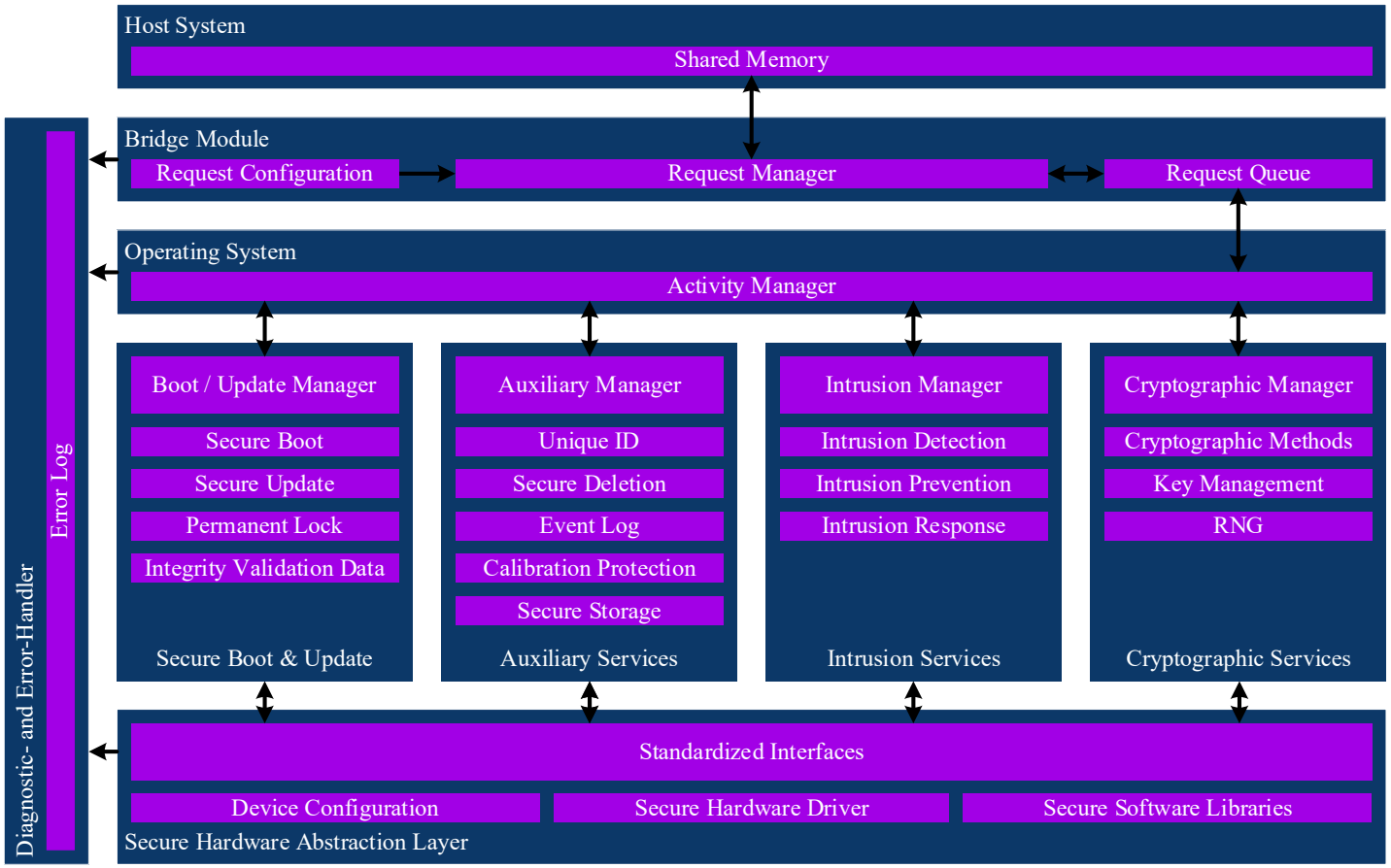
Crypto Agility - IAV *quantum*SAR
Concept



- IAV *quantum*SAR is divided into two parts
  - Post-Quantum Algorithm: platform-independent library with all algorithm standardized by NIST
    - Implemented in C and RUST
    - Available as open-source repository on GitHub (C available now, RUST to follow in 2025)
    - Extendable design for future standardized algorithm (e.g., NIST PQC selection round 4)
  - Wrapper: platform-dependent wrapper for adaption on different software architectures
    - Implementation for AUTOSAR Classic Platform

Crypto Agility - Firmware Security Module

Securable, scalable and updatable Trusted Execution Environment

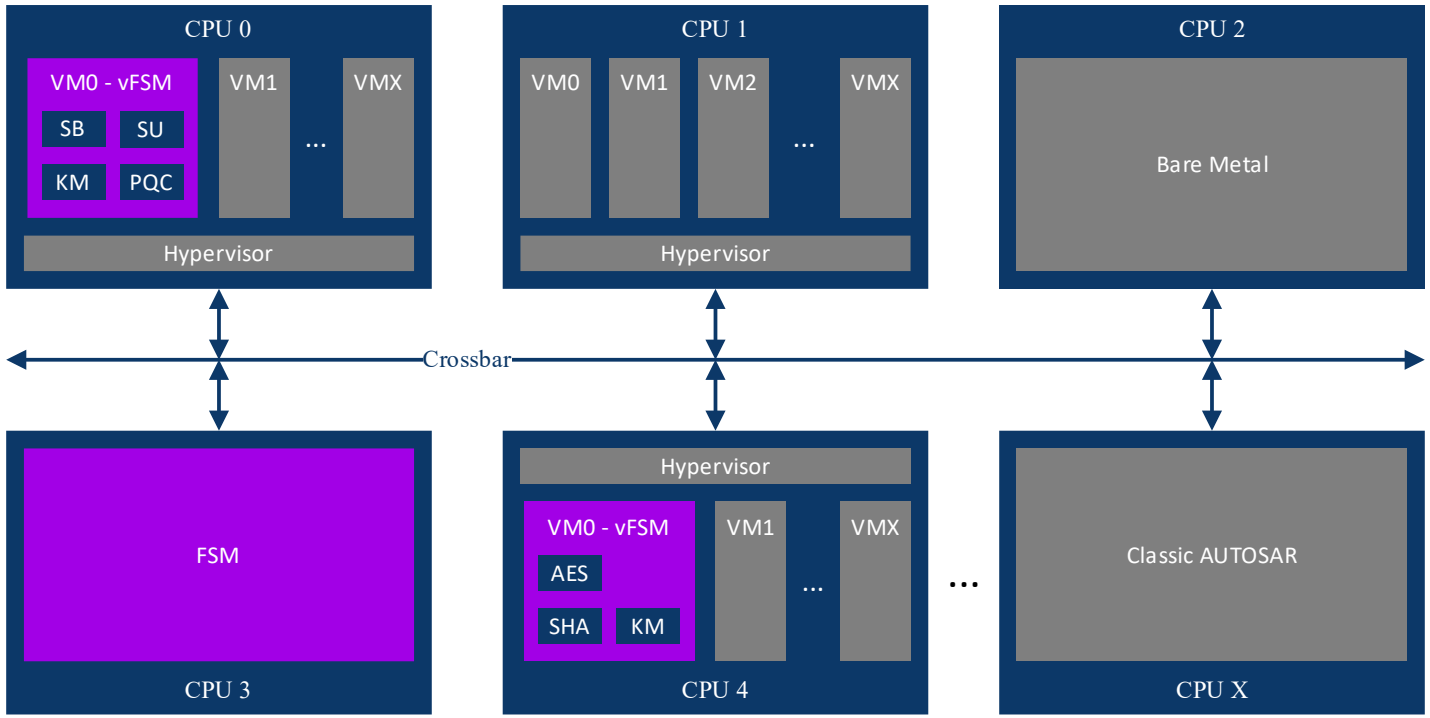


- **Full support of all necessary security functionalities**
  - Secure Boot and Secure Update
  - Secure Logging
  - Intrusion Handling
  - Cryptographic Algorithm
    - Including Post-Quantum Cryptography (PQC)
  - Secure Key Management
  - etc.

HSM: Hardware Security Module
VM: Virtual Machine

Crypto Agility - Firmware Security Module

Securable, scalable and updatable Trusted Execution Environment



- **Integration approaches**
  - Hardware Security Module (HSM)
  - Isolated Main Cores
  - Isolated Virtual Machines (VM)
- **Combination of approaches possible**
  - Adaptable for different system designs
  - Flexible for future extensions

SDV: Software-Defined Vehicle
PQC: Post-Quantum Cryptography

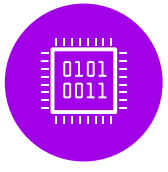
Call to Action

- Stay up-to-date on automotive risks for the SDV ecosystem

- Deploy end-to-end security solutions (vehicle, cloud, mobile device)

- Apply best practices for secure end-to-end development lifecycle

- Be aware of differences in regulatory requirements



- Get ready for PQC

Contact

Dr. Dennis Kengo Oka
IAV Co., Ltd.
dennis.kengo.oka@iav.jp
www.iav.com