THE FUTURE OF AUTOMOTIVE TECHNOLOGY
HOW TO ENSURE SECURITY & SAFETY?

Hassan TRIQUI – *CEO & Co-founder of Secure-IC*

GSA International Summit – Shanghai

October 28, 2024

Version 1.1

AGENDA

1. What is at stake?

2. What about regulations?

3. How does Secure-IC address those challenges?

4. Key takeaways

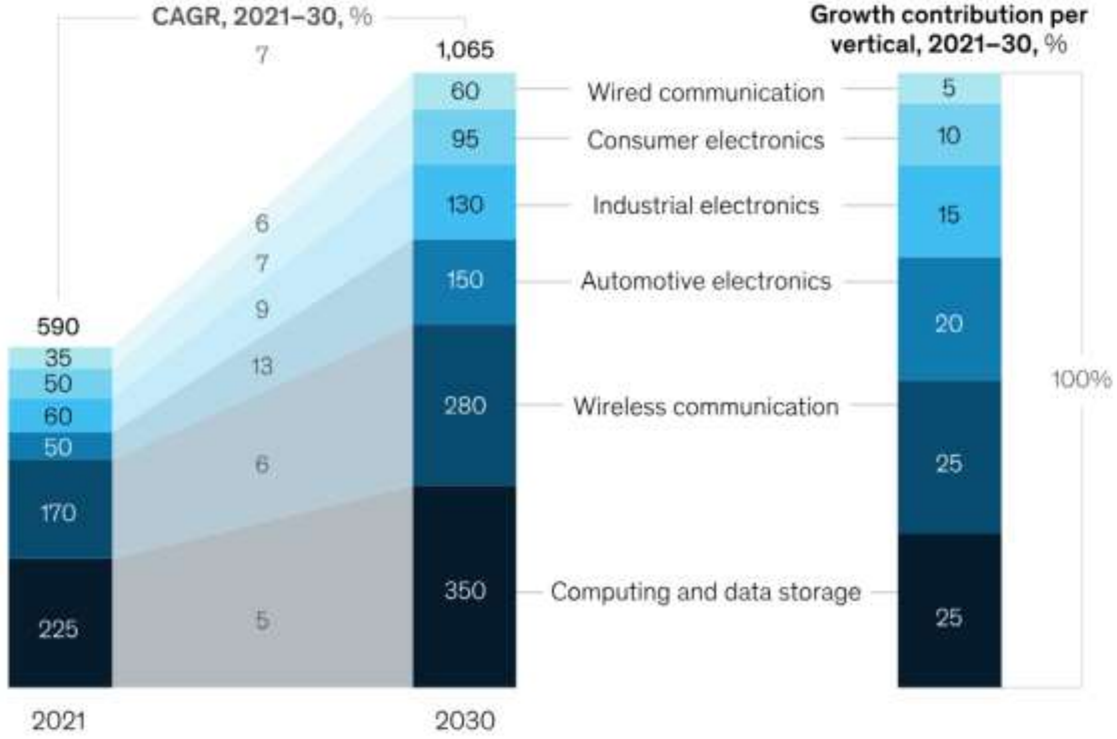
1. WHAT IS AT STAKE?

WHAT IS AT STAKE?

US EXECUTIVE FORUM

THE SEMICONDUCTOR DECADE: A TRILLION-DOLLAR INDUSTRY

Global semiconductor market value by vertical, indicative, $ billion



Note: Figures are approximate.

McKinsey & Company

Source: McKinsey & Company – The Semiconductor Decade: a Trillion-Dollar Industry (April 2022)

WHAT IS AT STAKE FOR THE AUTOMOTIVE INDUSTRY?

Performance

Security

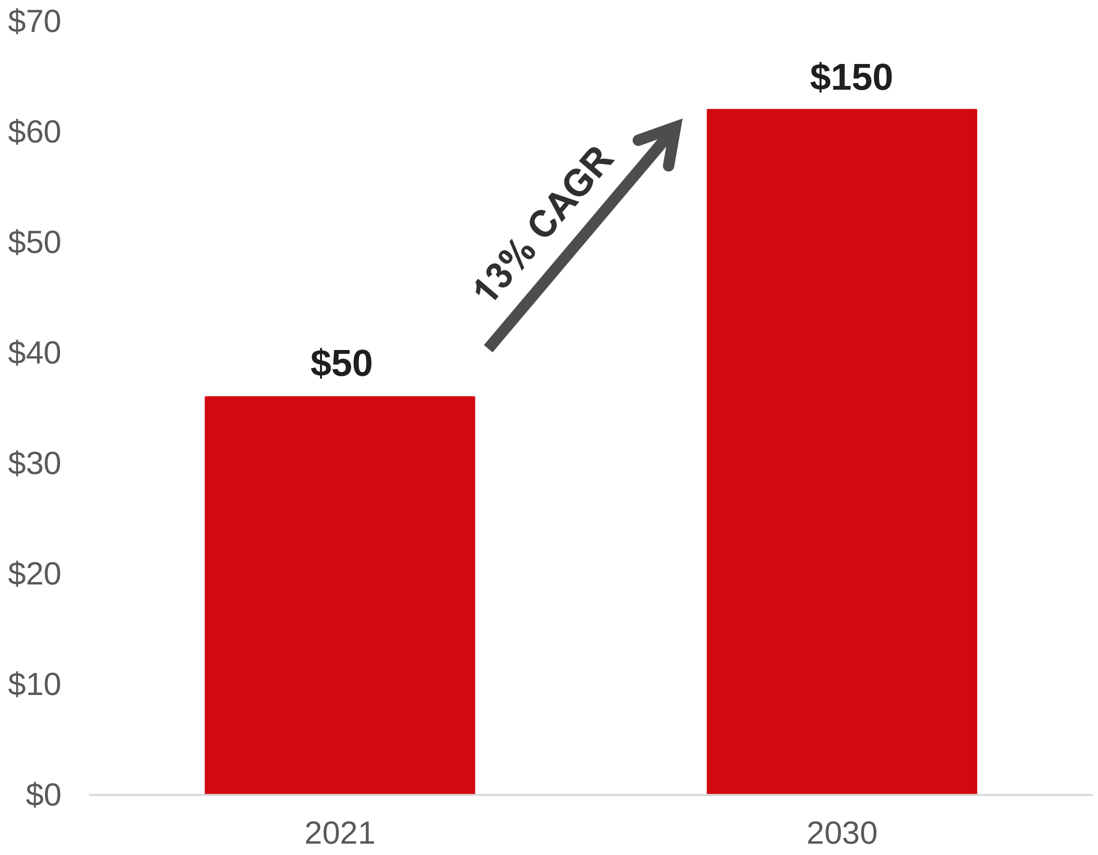
Safety

Softwarization

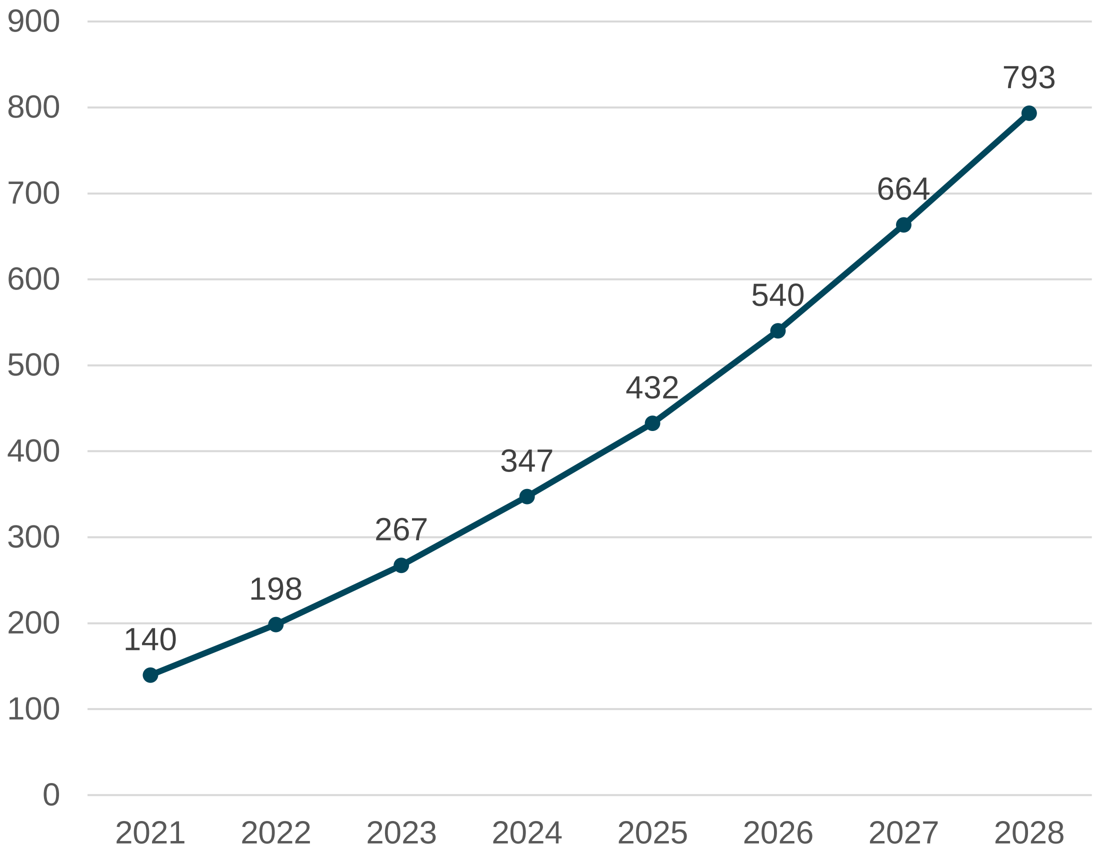
Source: Motor Authority

AUTOMOTIVE MARKET

Global Automotive Semiconductor Market ($B)



Number of Automotive IoT Connections (M units)



Sources: Source: IHS (Aug 2021) & GlobalPlatform SESIP
Automotive IoT - Worldwide, , n.d.. [Online]. Available: https://www-statista-com/outlook/tmo/internet-of-things/automotive-iot/worldwide

AUTOMOTIVE MARKET OPPORTUNITY

80 ECUs

Up to 80 ECUs in modern vehicles with sub-system dedicated to one or more features of an automotive system

Security Standards

Organizational & Development flow-oriented standards

ISO
ISO 26262
Road Vehicles - Functional Safety
UNECE

Security features & Resistance oriented standards

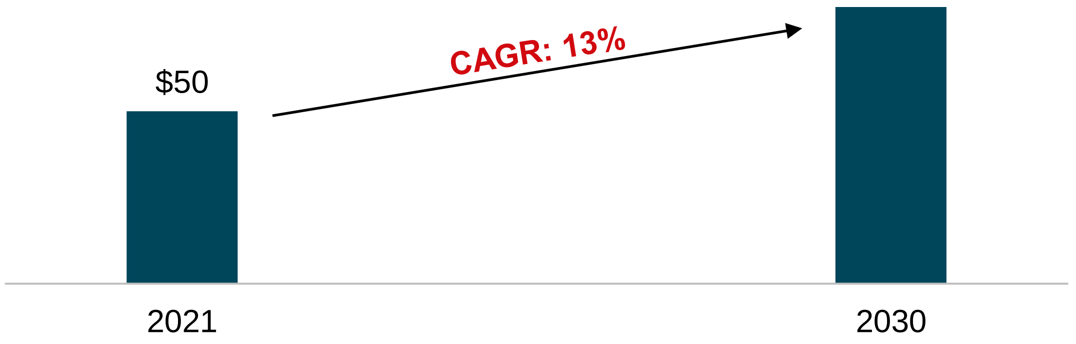
SAE INTERNATIONAL
Protection Profile V2X Hardware Security Module
CAR 2 CAR Communication Consortium
CAR 2 CAR COMMUNICATION CONSORTIUM
Singapore Standards Council
evita
AUTOSAR
AUTOMOTIVE SPICE®

Automotive Electronic Design Main Players and Scope → SECURE-iC Solutions

Actors	Domain	Threats
OEM	Vehicle	Bypassing Security Policy
OEM / Tier 1	Subsystem	Fuzzing, DoS
Tier 1	ECU	Counterfeiting
Silicon Vendor	Component	Trojan Horse

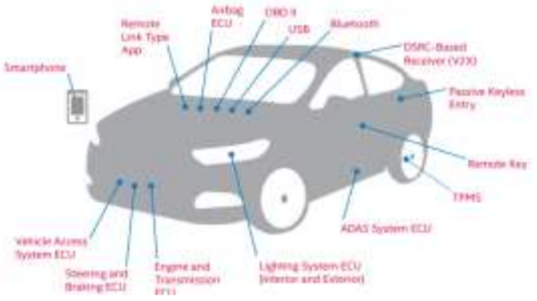
SECURYZR™
LABORYZR™
EXPERTYZR™

Global Automotive Semiconductor Market ($B)



Different security requirements for each type of ECU (Electronic Control Units)

Complex Modern Architecture



The increased connectivity and use of modern technologies multiplicated attacks entry point in vehicle, amplifying the need for a higher level of security needed

Source: industry research reports

SECURE-iC
THE SECURITY SCIENCE COMPANY

2. WHAT ABOUT REGULATIONS?

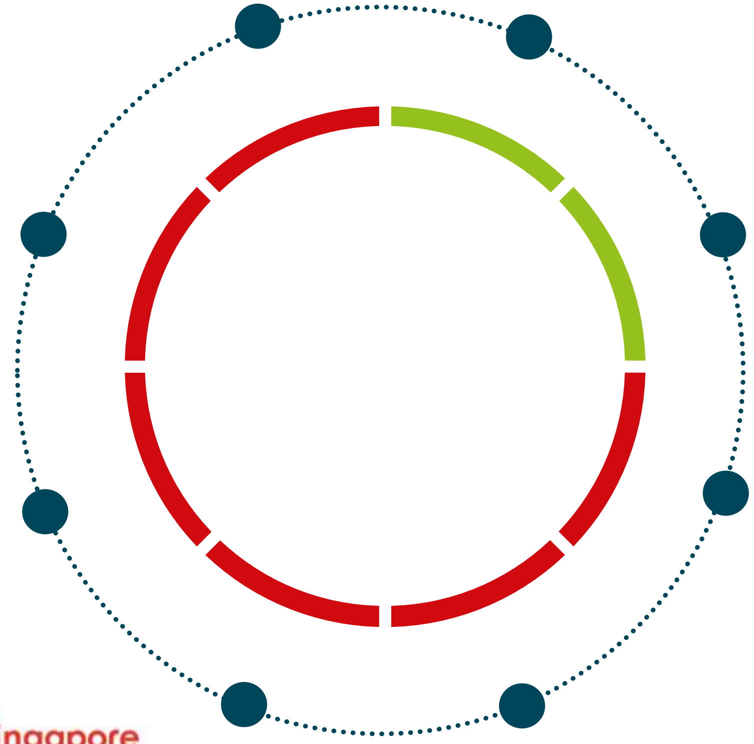
AUTOMOTIVE
GLOBAL SECURITY STANDARDS

ASPICE

Automotive SPICE is a maturity model adapted for the automotive industry. It assesses the maturity of development processes for electronic and software-based systems (e.g., ECUs). It is based on an initiative of the Special Interest Group Automotive and the Quality Management Center (QMC) in the German Association of the Automotive Industry (VDA).

UN WP29

Inside the World Forum for Harmonization of Vehicle Regulations, this working group produced recommendations on cyber security to be applied to vehicle components. It provides organizational requirements and Security-by-Design approach.



AUTOSAR

global development partnership founded in 2003 by automotive manufacturers, suppliers and other companies from the electronics, semiconductor and software industries. Its purpose is to develop and establish an open and standardized software architecture for automotive electronic control units (ECUs).

ISO 21434

ISO level of vehicle cybersecurity engineering best practices. It is mandatory in Europe, Japan, Korea… Provides rules and requirements for the whole cybersecurity development process. Based on Threat Analysis Risk Assessment approach and Design for Security.

EVITA

European project documentation describing recommendations in terms of architecture, features and API for vehicle security. Three levels (low, medium, full) corresponding to different types of ECU.

SAE J3101

Common set of Requirements to be applied to hardware assisted functions to ensure the security of cars and other vehicles against cyber security threats.

TR68

Singaporean standard for autonomous vehicle regulation. Technical Reference for autonomous vehicle.

Protection Profile V2X Hardware Security Module
CAR 2 CAR Communication Consortium

CC V2X PP

Protection Profile V2X Hardware Security Module for Common Criteria, based on EAL4+, AVA_VAN.4 and ALC_FLR.1. Sets up the requirements for connected communication modules in the vehicle that must be met to achieve proper security level.

🟥 *Security Features & Resistance oriented standards*

🟩 *Organizational & development flow-oriented standards*

FUNCTIONAL SAFETY + SECURITY

ISO 26262

Road Vehicles - Fuctional Safety

Need to consider Security and Safety jointly

SECURITY ENCOMPASSES SAFETY

GOAL	Guarantee the correct behavior of the system, even if is affected by an electrical or electronic failure
USE	ISO 26262 Standard for Automotive Safety
ACHIEVEMENTS	• Rigorous Design and Evaluation Methodology • Resilience and Fault Tolerance: - Detection of defects in electronic system, - Failures management using Safety Monitor.

SECURE-iC
THE SECURITY SCIENCE COMPANY

SAFETY IN AUTOMOTIVE

ISO 26262
Road Vehicles - Fuctional Safety

Airbag

⚠ Inadvertent deploy

ASIL-D

Instrument Cluster

⚠ Loss of critical data

ASIL-B

Rear Lights

⚠ Both side failure

ASIL-A

Rear View Camera

⚠ No Valid Sensor Data

ASIL-B

Engine Management

⚠ Unwanted Aceleration

ASIL-C to D

Headlights

⚠ Both side failure

ASIL-B

Brake Lights

⚠ Both side failure

ASIL-B

Antilock Braking

⚠ Unintended Full Power Braking

ASIL-D

Active Suspension

⚠ Suspension oscillates

ASIL-B to C

V2X

⚠ Misinterpretation in autonomous drive

ASIL-D

Radar Cruise Control

⚠ Inadvert braking

ASIL-C

Electric Power Steering

⚠ Self-steering

ASIL-D

Vision ADAS

⚠ Incorrect Sensor Feedback

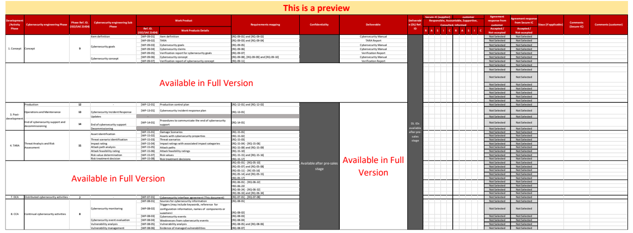
ASIL-B

Source: Embitel.com

SECURITY AND THE EVOLVING GLOBAL VALUE CHAIN

Case Study: Automotive ISO/SAE 21434 Genesis

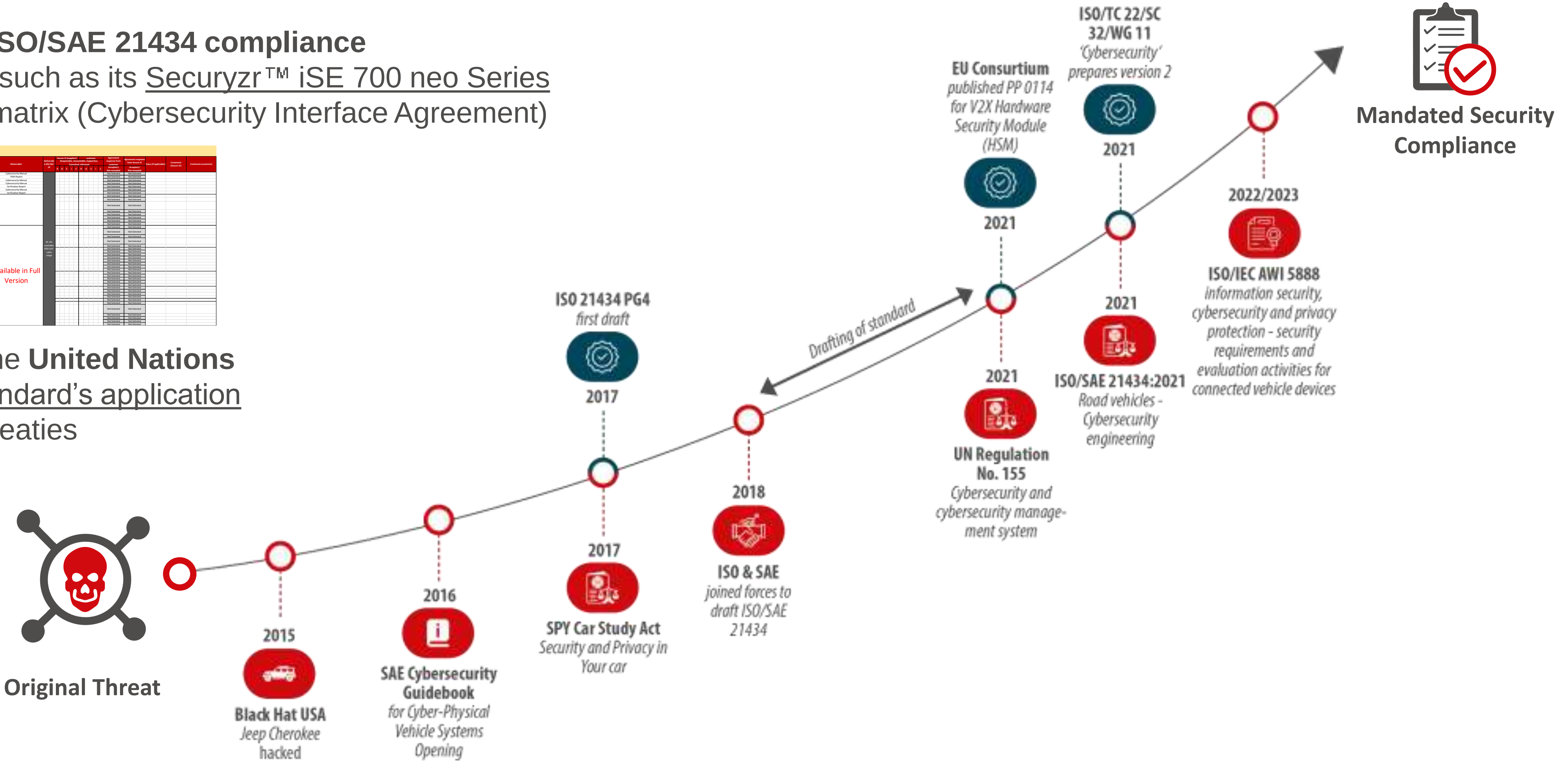
Secure-IC ensures **ISO/SAE 21434 compliance**
for specific products such as its Securyzr™ iSE 700 neo Series
using a compliance matrix (Cybersecurity Interface Agreement)



This is a preview

Development /Activity Phase	Cybersecurity engineering Phase	Phase Ref. ID. (ISO/SAE 21434)	Cybersecurity engineering Sub Phase	Work Product		Requirements mapping	Confidentiality	Deliverable	Deliverable (DL) Ref. ID	Secure-IC (supplier)					customer					Agreement response from customer	Agreement response from Secure-IC	Staus (if applicable)	Comments (Secure-IC)	Comments (customer)
										Responsible, Accountable, Supportive, Consulted, Informed														
				Ref. ID. (ISO/SAE 21434)	Work Products Details					R	A	S	I	C	R	A	S	I	C	Accepted / Not-accepted	Accepted / Not-accepted			
1. Concept	Concept	9	Item definition	[WP-09-01]	Item definition	[RQ-09-01] and [RQ-09-02]		Cybersecurity Manual	DL IDs available after pre-sales stage											Not Selected	Not Selected			
			Cybersecurity goals	[WP-09-02]	TARA	[RQ-09-03] and [RQ-09-04]		TARA Report												Not Selected	Not Selected			
				[WP-09-03]	Cybersecurity goals	[RQ-09-05]		Cybersecurity Manual												Not Selected	Not Selected			
				[WP-09-04]	Cybersecurity claims	[RQ-09-06]		Cybersecurity Manual												Not Selected	Not Selected			
				[WP-09-05]	Verification report for cybersecurity goals	[RQ-09-07]		Verification Report												Not Selected	Not Selected			
			Cybersecurity concept	[WP-09-06]	Cybersecurity concept	[RQ-09-08], [RQ-09-09] and [RQ-09-10]		Cybersecurity Manual												Not Selected	Not Selected			
				[WP-09-07]	Verification report of cybersecurity concept	[RQ-09-11]		Verification Report												Not Selected	Not Selected			
Available in Full Version																				Not Selected	Not Selected			
																				Not Selected	Not Selected			
																				Not Selected	Not Selected			
																				Not Selected	Not Selected			
																				Not Selected	Not Selected			
																				Not Selected	Not Selected			
																				Not Selected	Not Selected			
																				Not Selected	Not Selected			
3. Post-development	Production	12	-	[WP-12-01]	Production control plan	[RQ-12-01] and [RQ-12-02]	Available after pre-sales stage	Available in Full Version												Not Selected	Not Selected			
	Operations and Maintenance	13	Cybersecurity Incident Response	[WP-13-01]	Cybersecurity incident response plan	[RQ-13-01]														Not Selected	Not Selected			
			Updates	-																Not Selected	Not Selected			
	End of cybersecurity support and decommissioning	14	End of cybersecurity support	[WP-14-01]	Procedures to communicate the end of cybersecurity support	[RQ-14-01]														Not Selected	Not Selected			
			Decommissioning	-																Not Selected	Not Selected			
4. TARA	Threat Analsyis and Risk Assessment	15	Asset identification	[WP-15-01]	Damage Scenarios	[RQ-15-01]														Not Selected	Not Selected			
				[WP-15-02]	Assets with cybersecurity properties	[RQ-15-02]														Not Selected	Not Selected			
			Threat scenario identification	[WP-15-03]	Threat scenarios	[RQ-15-03]														Not Selected	Not Selected			
			Impact rating	[WP-15-04]	Impact ratings with associated impact categories	[RQ-15-04] - [RQ-15-06]														Not Selected	Not Selected			
			Attack path analysis	[WP-15-05]	Attack paths	[RQ-15-08] and [RQ-15-09]														Not Selected	Not Selected			
			Attack feasibility rating	[WP-15-06]	Attack feasibility ratings	[RQ-15-10]														Not Selected	Not Selected			
			Risk value determination	[WP-15-07]	Risk values	[RQ-15-15] and [RQ-15-16]														Not Selected	Not Selected			
			Risk treatment decision	[WP-15-08]	Risk treatment decisions	[RQ-15-17]														Not Selected	Not Selected			
Available in Full Version						[RQ-05-01] - [RQ-05-10]														Not Selected	Not Selected			
						[RQ-05-07] and [RQ-05-08]														Not Selected	Not Selected			
						[RQ-05-11] - [RC-05-16]														Not Selected	Not Selected			
						[RQ-05-14] and [RQ-05-15]														Not Selected	Not Selected			
						[RQ-05-17]														Not Selected	Not Selected			
						[RQ-06-01] - [RQ-06-22]														Not Selected	Not Selected			
						[RQ-06-23]														Not Selected	Not Selected			
						[RQ-06-24] - [RQ-06-32]														Not Selected	Not Selected			
						[RQ-06-33] and [RQ-06-34]														Not Selected	Not Selected			
7. DCA	Distributed cybersecurity activities	7	-	[WP-07-01]	Cybersecurity interface agreement (This document)	[RQ-07-01] - [RQ-07-08]														Not Selected	Not Selected			
8. CCA	Continual cybersecurity activities	8	Cybersecurity monitoring	[WP-08-01]	Sources for cybersecurity information	[RQ-08-01]														Not Selected	Not Selected			
				[WP-08-02]	Triggers (may include keywords, reference for configuration information, names of components or suppliers)	[RQ-08-02]														Not Selected	Not Selected			
				[WP-08-03]	Cybersecurity events	[RQ-08-03]														Not Selected	Not Selected			
			Cybersecurity event evaluation	[WP-08-04]	Weaknesses from cybersecurity events	[RQ-08-04]														Not Selected	Not Selected			
			Vulnerability analysis	[WP-08-05]	Vulnerability analysis	[RQ-08-05] and [RQ-08-06]														Not Selected	Not Selected			
			Vulnerability management	[WP-08-06]	Evidence of managed vulnerabilities	[RQ-08-07]														Not Selected	Not Selected			

US Congress and the **United Nations**
are enforcing the standard's application
thanks to laws and treaties



Original Threat

2015
Black Hat USA
Jeep Cherokee hacked

2016
SAE Cybersecurity Guidebook
for Cyber-Physical Vehicle Systems Opening

ISO 21434 PG4
first draft
2017

2017
SPY Car Study Act
Security and Privacy in Your car

2018
ISO & SAE
joined forces to draft ISO/SAE 21434

Drafting of standard

EU Consurtium
published PP 0114 for V2X Hardware Security Module (HSM)
2021

2021
UN Regulation No. 155
Cybersecurity and cybersecurity management system

ISO/TC 22/SC 32/WG 11
'Cybersecurity' prepares version 2
2021

2021
ISO/SAE 21434:2021
Road vehicles - Cybersecurity engineering

2022/2023
ISO/IEC AWI 5888
Information security, cybersecurity and privacy protection - security requirements and evaluation activities for connected vehicle devices

Mandated Security Compliance

Pathway from Threat to Mandated Compliance Illustrated by Automotive ISO/SAE 21434

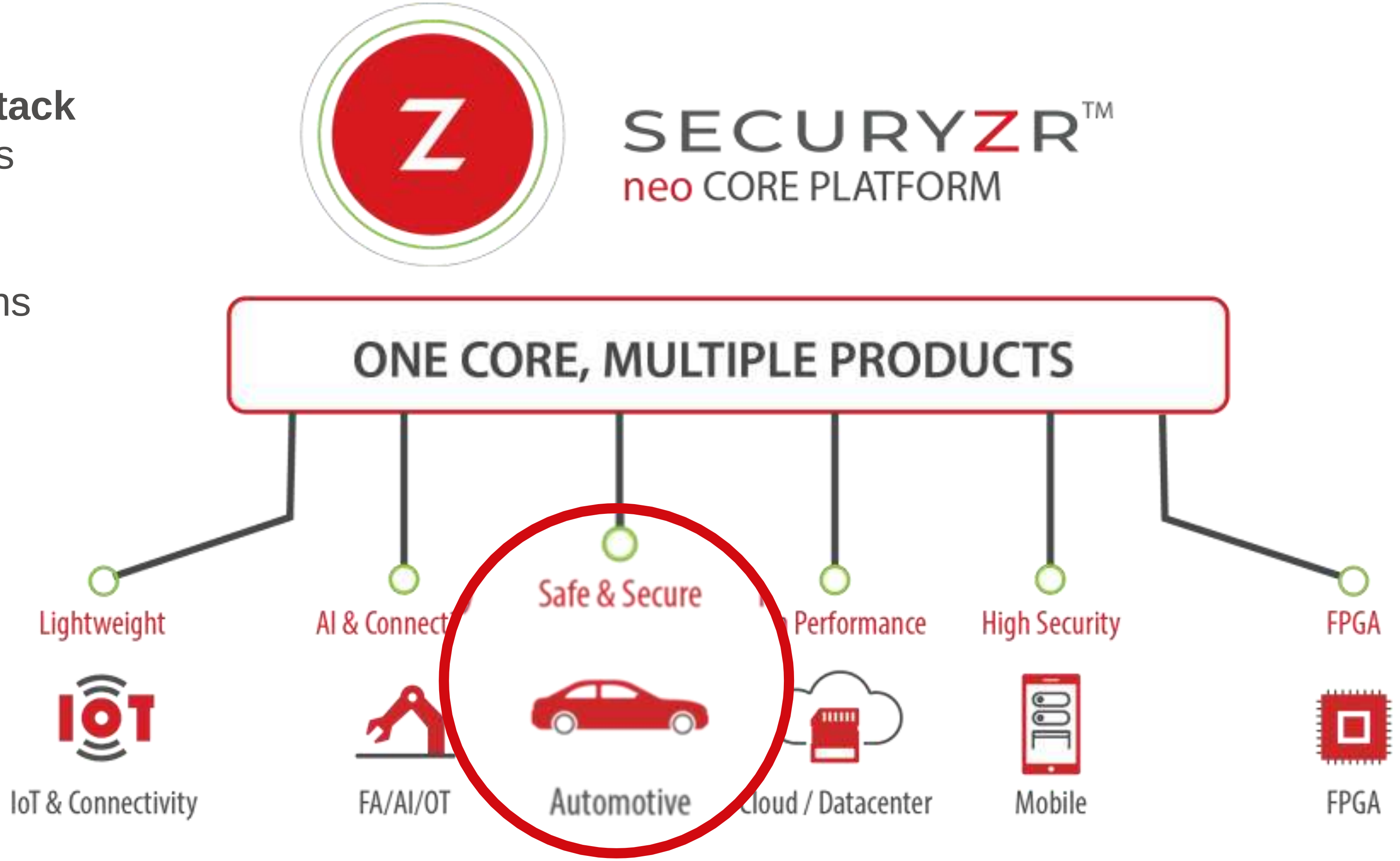
3. HOW DOES SECURE-IC ADDRESS THOSE CHALLENGES?

SECURE-IC
THE SECURITY SCIENCE COMPANY

SECURYZR™ neo CORE PLATFORM

SECURYZR™ neo CORE PLATFORM

Uniform SW stack
for all Series
=
Portability
of applications



SECURYZR™
neo CORE PLATFORM

ONE CORE, MULTIPLE PRODUCTS

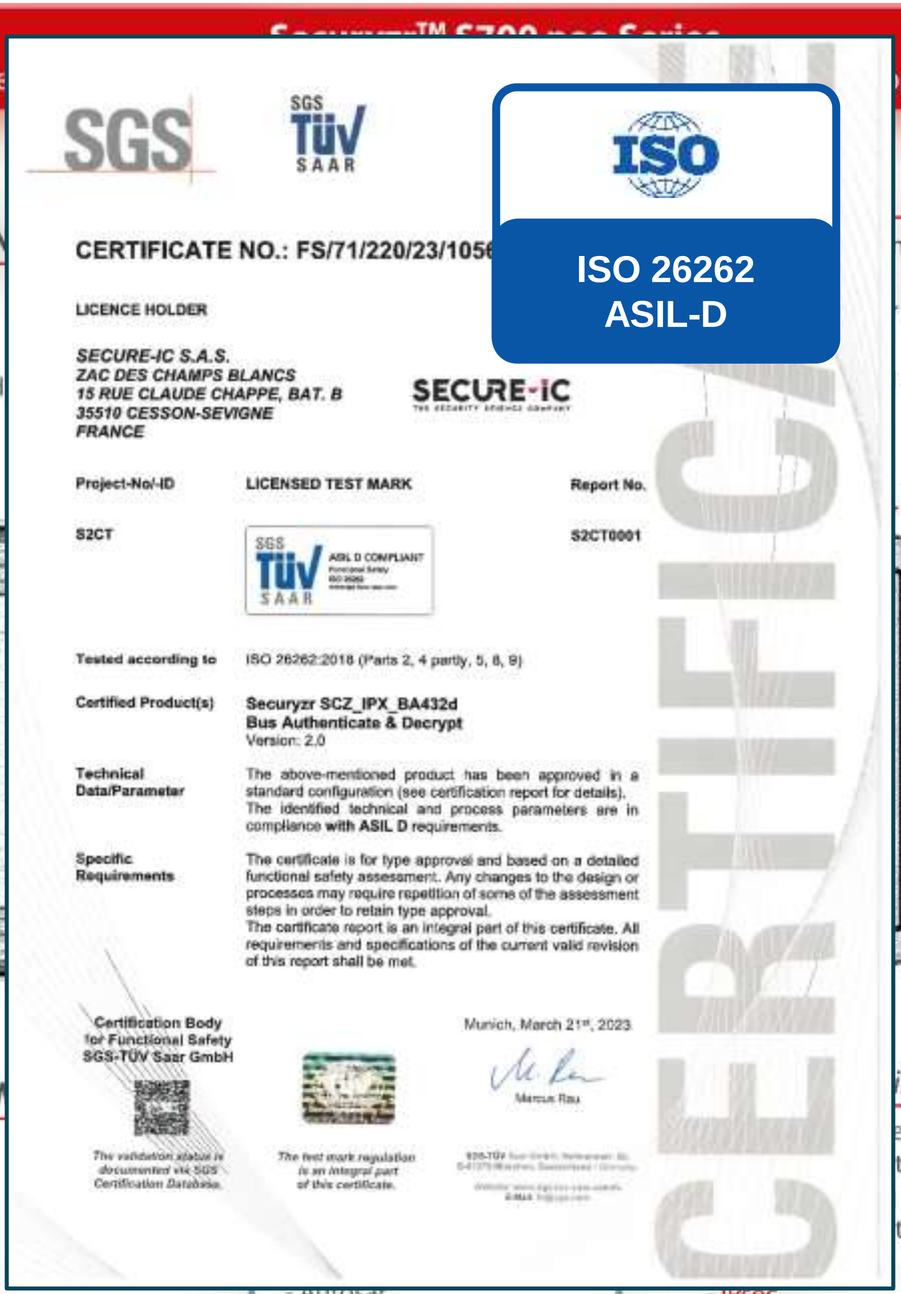
Lightweight	AI & Connect	Safe & Secure	Performance	High Security	FPGA
IoT & Connectivity	FA/AI/OT	Automotive	Cloud / Datacenter	Mobile	FPGA

Benefit From Secure-IC's Rich Legacy while Embracing Cutting-edge Technologies

SECURE-iC
THE SECURITY SCIENCE COMPANY

SECURYZR™
neo CORE PLATFORM

Securyzr™ S700 neo Series
inte… …plications



SGS TÜV SAAR

ISO

ISO 26262 ASIL-D

CERTIFICATE NO.: FS/71/220/23/1056

LICENCE HOLDER

SECURE-IC S.A.S.
ZAC DES CHAMPS BLANCS
15 RUE CLAUDE CHAPPE, BAT. B
35510 CESSON-SEVIGNE
FRANCE

Project-No/-ID	LICENSED TEST MARK	Report No.
S2CT	SGS TÜV SAAR ASIL D COMPLIANT	S2CT0001

Tested according to	ISO 26262:2018 (Parts 2, 4 partly, 5, 8, 9)
Certified Product(s)	**Securyzr SCZ_IPX_BA432d** **Bus Authenticate & Decrypt** Version: 2.0
Technical Data/Parameter	The above-mentioned product has been approved in a standard configuration (see certification report for details). The identified technical and process parameters are in compliance **with ASIL D** requirements.
Specific Requirements	The certificate is for type approval and based on a detailed functional safety assesament. Any changes to the design or processes may require repetition of some of the assessment steps in order to retain type approval. The certificate report is an integral part of this certificate. All requirements and specifications of the current valid revision of this report shall be met.

Certification Body
for Functional Safety
SGS-TÜV Saar GmbH

The validation status is documented via SGS Certification Database.

The test mark regulation is an integral part of this certificate.

Munich, March 21st, 2023

Marcus Rau

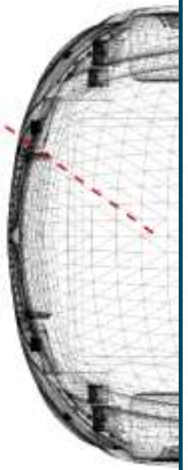
CERTIFICATE

IN VEHICLE EXPERIENCE / INFOTAINMEN

- MACsec for Ethernet
- Memory Protection ASIL-D compliant
- Anti-Tampering IPs
- Intrusion Detection System (IDS) - Edge AI-Powered
- Open SSL

V2X *(Vehicle to Everything)*

- Anti-Tampering IPs
- Intrusion Detection System (IDS) - Edge AI-Powered
- IPsec, TLS/DTLS, 3GPP IP Core
- Public Key Engine



COMPLIANT STANDARDS

- CC EAL4/5+ *(PP0114 V2X)*
- ISO 21434 *(CAL 1 up to 4)*
- ISO 26262 *(ASIL-B up to D)*

Common Criteria ISO

GATEWAY, CONTROL UNITS, ENGINE, POW

- MACsec for Ethernet
- Memory Protection ASIL-D compliant
- Anti-Tampering IPs
- Intrusion Detection System (IDS) - Edge AI-Powered

- Autosar

evita AUTOSAR

nt

The Air

on IDS

TELEMATICS & CONNECTIVITY

- Anti-Tampering IPs
- Intrusion Detection System (IDS) - Edge AI-Powered
- FIPS ready SW Crypto Library
- IPsec, TLS/DTLS, 3GPP IP Core

SERVICES

- HW & SW Penetration Testing (Pentest)
- Security Evaluation as a Service
  - White / Grey / Black Box Analysis
- SCARE & FIRE (SCA & FIA reverse engineering)
- Security Certification as a Service
  - End-to-End readiness support
- TARA analysis, security trainings
- Automotive attacks/countermeasures reports
- PSIRT (Product Security Incident Response Team)

ing LIDAR & RADAR)

ernet

tion ASIL-D compliant

IPs

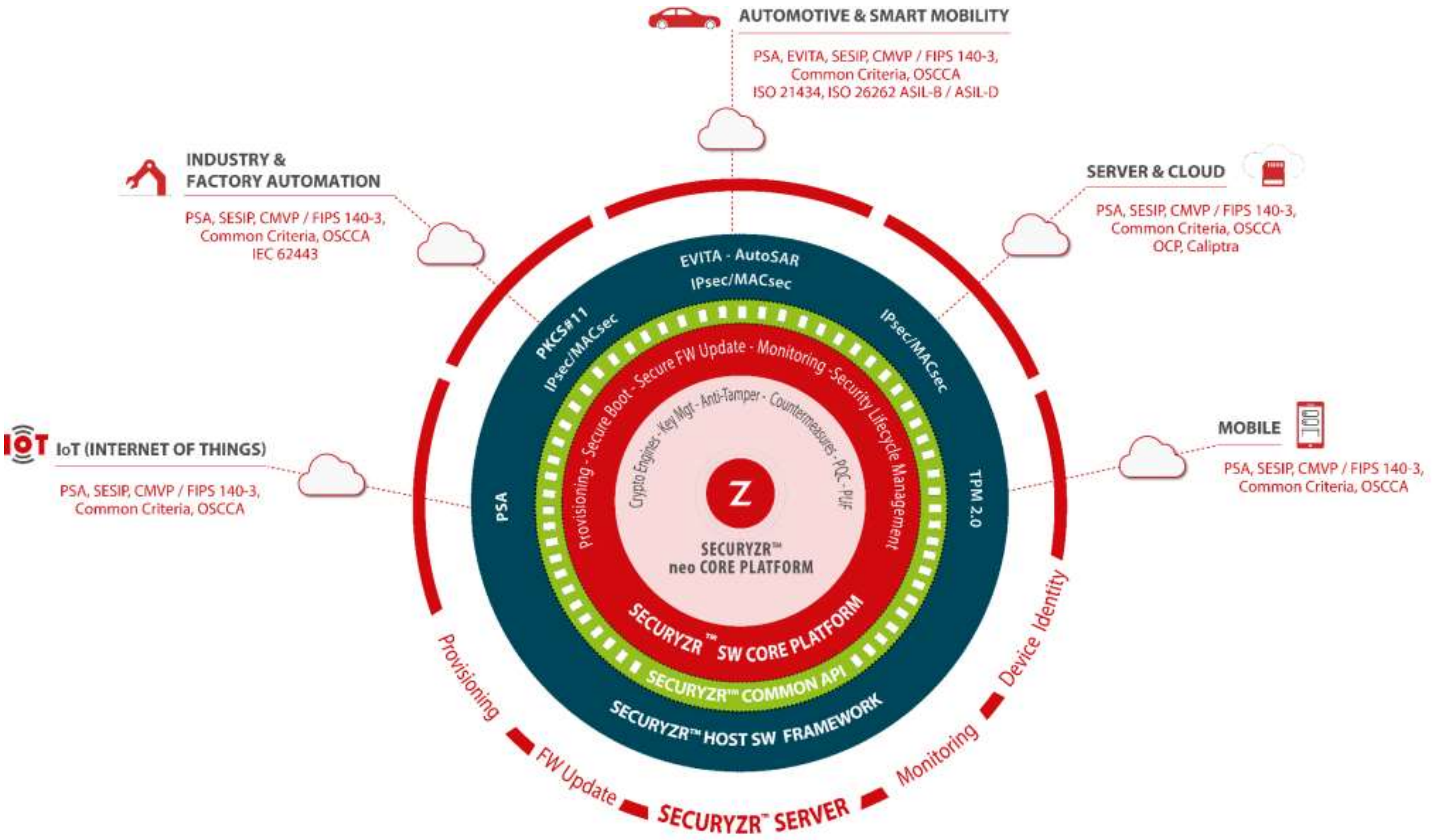
tion System (IDS) - Edge AI-

- IPsec

PQC READY

SECURYZR™ iNTEGRATED SECURE ELEMENT

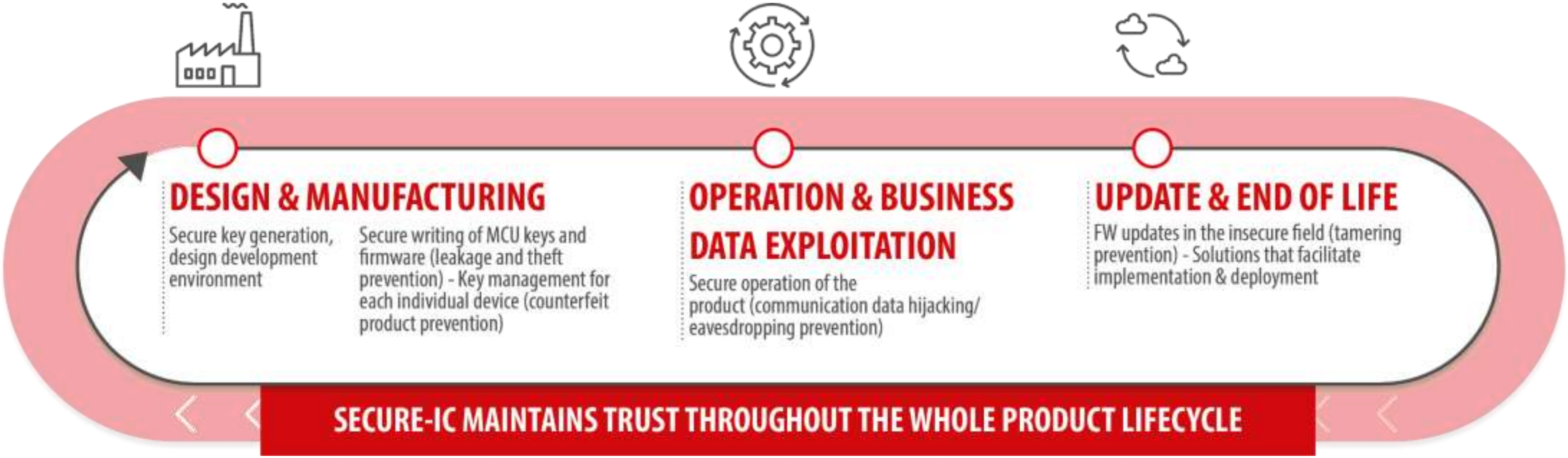
SECURITY FROM CHIP TO CLOUD – MARKET DRIVEN SW LAYERS



AUTOMOTIVE & SMART MOBILITY
PSA, EVITA, SESIP, CMVP / FIPS 140-3,
Common Criteria, OSCCA
ISO 21434, ISO 26262 ASIL-B / ASIL-D
INDUSTRY &
FACTORY AUTOMATION
PSA, SESIP, CMVP / FIPS 140-3,
Common Criteria, OSCCA
IEC 62443
SERVER & CLOUD
PSA, SESIP, CMVP / FIPS 140-3,
Common Criteria, OSCCA
OCP, Caliptra
IoT (INTERNET OF THINGS)
PSA, SESIP, CMVP / FIPS 140-3,
Common Criteria, OSCCA
MOBILE
PSA, SESIP, CMVP / FIPS 140-3,
Common Criteria, OSCCA
EVITA - AutoSAR
IPsec/MACsec
PKCS#11
IPsec/MACsec
IPsec/MACsec
PSA
TPM 2.0
Provisioning - Secure Boot - Secure FW Update - Monitoring - Security Lifecycle Management
Crypto Engines - Key Mgt - Anti-Tamper - Countermeasures - PQC - PUF
SECURYZR™
neo CORE PLATFORM
SECURYZR™ SW CORE PLATFORM
SECURYZR™ COMMON API
SECURYZR™ HOST SW FRAMEWORK
Provisioning
FW Update
SECURYZR™ SERVER
Monitoring
Device Identity

SECURE-IC THE SECURITY SCIENCE COMPANY

YOUR END-TO-END PARTNER FOR SECURITY ALL ALONG THE DEVICE LIFECYCLE



DESIGN & MANUFACTURING

Secure key generation, design development environment

Secure writing of MCU keys and firmware (leakage and theft prevention) - Key management for each individual device (counterfeit product prevention)

OPERATION & BUSINESS DATA EXPLOITATION

Secure operation of the product (communication data hijacking/ eavesdropping prevention)

UPDATE & END OF LIFE

FW updates in the insecure field (tamering prevention) - Solutions that facilitate implementation & deployment

SECURE-IC MAINTAINS TRUST THROUGHOUT THE WHOLE PRODUCT LIFECYCLE

While globalized sourcing and manufacturing processes reduce costs, they **increase risks exposure**. Considering the complexity of value chains, the **challenge is to generate and manage trust in data**.

Secure-IC aims at answering this challenge relying on interoperability and open standards.

THE RISING LEADER IN THE SECURITY INDUSTRY

Down to
2nm

MULTI-CERTIFIABLE technologies for multiple markets

FULLY DIGITAL technology for all technology nodes and foundries

Management of security **ALL ALONG DEVICES' LIFECYCLE**

P C E S

ONE-STOP-SHOP for embedded security

Unique & patented technologies: **ANTI-TAMPER & CYBER-PHYSICAL** attack protection

***

PQC and **AI-POWERED SECURITY**

MATURE & WIDELY DEPLOYED solutions

10+
years

250+
patents

350+
publications

4. KEY TAKEAWAYS

KEY TAKEAWAYS

- Despite current slowdown, we are heading towards **exciting times**,
  - Connected and autonomous vehicles are the future of automotive.

- The automotive industry is aiming at '**softwarization**',
  - Software-Defined-Vehicle (SDV),
  - The Hardware to Support the Software for services and value creation,
  - From Distributed ECU to Zonal Control Unit.

- **Security** is a major enabler of **value unlocking** in the automotive market.
  - The transformation can only be achieved with trust anchors within all chipsets, easy to adopt and deploy, with the associated security lifecycle challenges in mind from the beginning.

- Secure-IC will bring the **best of security** from the ground up,
  - From anti-tampering to key management, and AutoSAR security services.
  - Down to the smallest technology node (2nm) and up to the latest trends (Chiplet).

- Thank you GSA for cimenting our industry!

THANK YOU FOR YOUR ATTENTION

CONTACTS

EMEA	sales-EMEA@secure-IC.com
APAC	sales-APAC@secure-IC.com
CHINA	sales-CHINA@secure-IC.com
JAPAN	sales-JAPAN@secure-IC.com
TAIWAN	sales-TAIWAN@secure-IC.com
AMERICAS	sales-US@secure-IC.com

FOLLOW US ON SOCIAL MEDIA