

Cybersecurity in Motor Control Systems: Insights and Approaches with Infineon Products

Infineon Technologies

5 March 2025

public

Table of contents

1 Introduction to Cybersecurity & ISO21434 overview 3

2 Infineon acclerating your cybersecurity developement 7

3 Security features in Infineon Motor Control products 11

4 Infineon Microcontroller TRAVEO™ family to be ISO21434 compliant 17

5 Key take aways 19

Copyright © Infineon Technologies AG 2025. All rights reserved.

Table of contents

1 **Introduction to Cybersecurity & ISO21434 overview** **3**

2 Infineon acclerating your cybersecurity developement 7

3 Security features in Infineon Motor Control products 11

4 Infineon Microcontroller TRAVEO™ family to be ISO21434 compliant 17

5 Key take aways 19

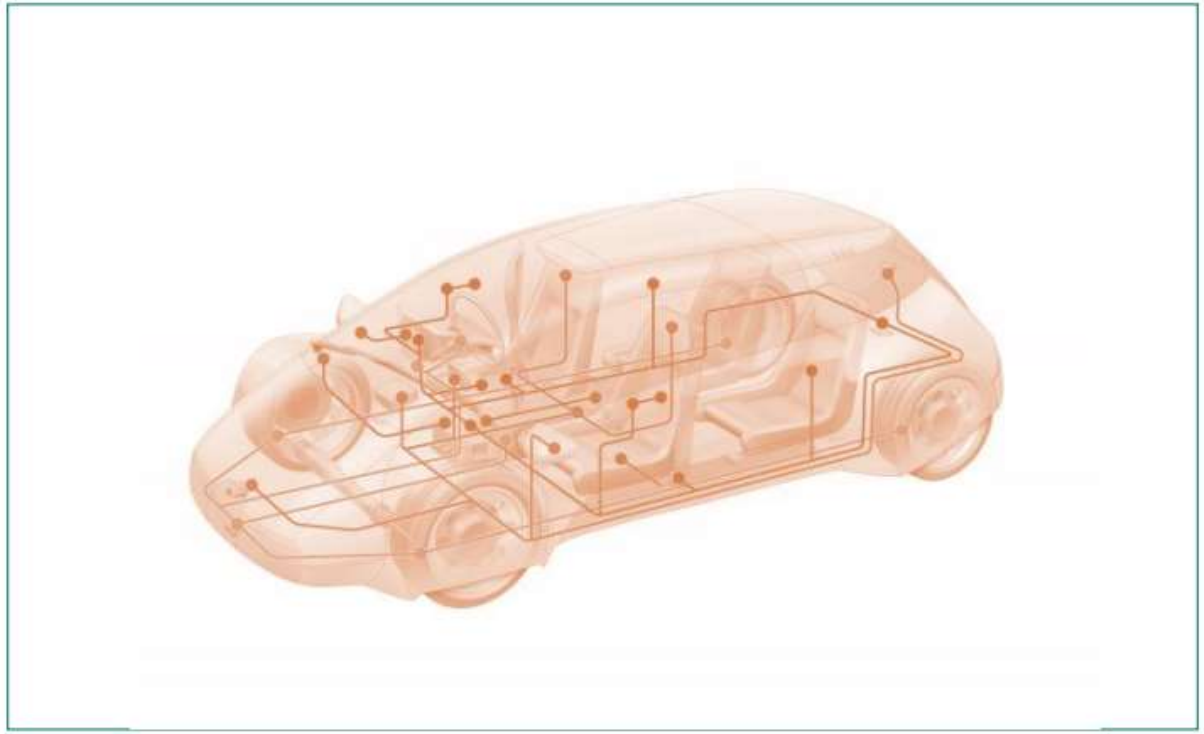
Copyright © Infineon Technologies AG 2025. All rights reserved.

Automotive Security

New standards and regulations require security for automotive applications.

Connected car at security risk

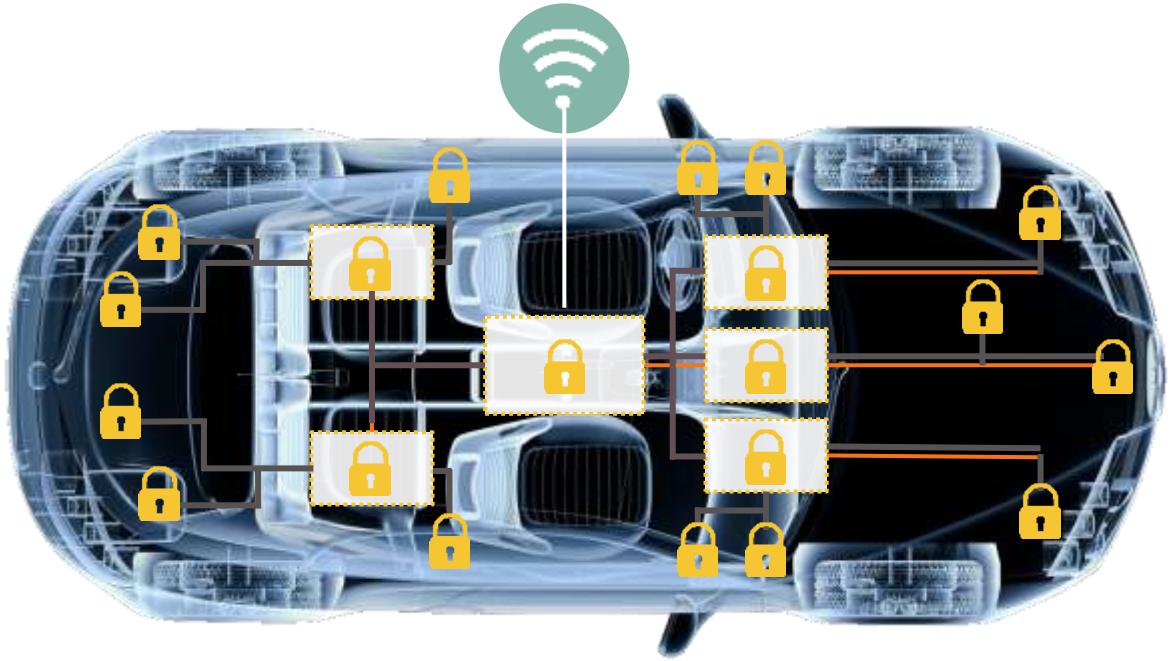
- Wiretapping
- Disguised identity
- Privacy/identity theft
- Unauthorized feature activation
- Unauthorized tuning
- Unlocking speed limit
- Forgery of driving record
- Hardware/property theft
- Manipulation of safety mechanism



Infineon’s motor control products support to secure connected cars.

Copyright © Infineon Technologies AG 2025. All rights reserved.

Principles of Cybersecurity



There's no silver bullet solution with Cybersecurity; a layered defence is the only viable defence – James Scott

Secured platform

Secured onboard communication

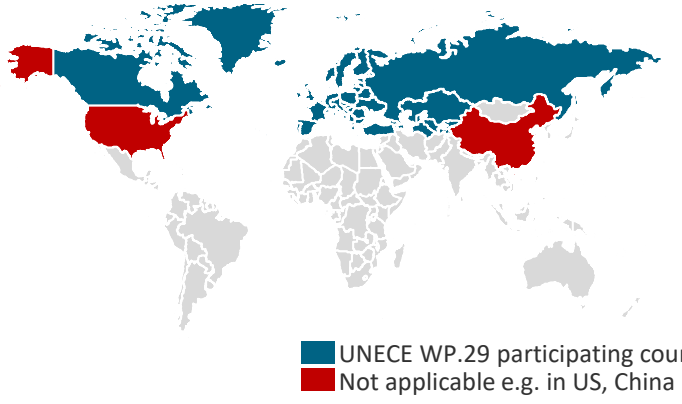
Secured network separation

Secured external communication

Copyright © Infineon Technologies AG 2025. All rights reserved.

Background: UNECE R155 and R156 regulations

- The UN Economic Commission for Europe (UNECE) regulations concerning the approval of road vehicles with regards to cyber security and cyber security management system is already in effect since 2022. This comprises of:
  - **UNECE R155 regulation for Cyber Security Management System (CSMS)**
  - **UNECE R156 regulation for Software Updates Management Systems (SUMS)**
- To get access to markets, OEMs need “Type Approval” certificate. OEMs cannot on their own get such certification. Tier-2s need to support OEMs/Tier-1s by being compliant to respective standards such as ISO21434:2021.



- To support OEMs/Tier-1s in achieving compliance Infineon provides dedicated **compliance roadmap** that includes process and product compliance for microcontroller products.
- **Process compliance**: Infineon CSMS certified by TÜV NORD & SGS to fulfill requirements of ISO21434:2021.
- **Product compliance**: Infineon microcontrollers categorized as QM and ISO21434-compliant.

Copyright © Infineon Technologies AG 2025. All rights reserved.

Table of contents

1 Introduction to Cybersecurity & ISO21434 overview 3

2 **Infineon acclerating your cybersecurity developement** **7**

3 Security features in Infineon Motor Control products 11

4 Infineon Microcontroller TRAVEO™ family to be ISO21434 compliant 17

5 Key take aways 19

Copyright © Infineon Technologies AG 2025. All rights reserved.

Infineon’s product development process is certified according to ISO/SAE 21434 by SGS-TÜV Saar





The certification includes:

- Cybersecurity Management Continuous Cybersecurity Activities (e.g., monitoring, risk assessment, vulnerability analysis)
- Risk Assessment Methods (e.g., threat identification)
- Concept Phase (e.g., cybersecurity goals)
- Product Development Phase (e.g., integration and verification)
- Post Development Phase (e.g., cybersecurity incident response)

Infineon’s position as a trusted partner in automotive security has been proven by an external party

Copyright © Infineon Technologies AG 2025. All rights reserved.

Infineon offers dedicated support to OEMs and Tier1s to achieve ISO/SAE 21434 compliance with off-the-shelf-components



ISO/SAE 21434 Process Certificate

- Implementation of a global cyber security management system (CSMS)
- Certified by TÜV Mobility



Cyber Security Monitoring and Incident Response

- Monitoring for vulnerabilities or attacks in the clear and dark web, as well as other sources performed by Infineon‘s Cyber Defense Center
- PSIRM process by dedicated Product Security Incident Response Team



Cyber Security Product Documentation

- Dedicated product specific documentation, such as: User manuals, datasheets, appnotes, erratas or the Infineon Cyber Security Compendium

Infineon may offer additional customized support as a service on individual agreement

Copyright © Infineon Technologies AG 2025. All rights reserved.

Compliance categories

Infineon Label	QM	ISO 21434-compliant
Documentation	Use case specific	Cybersecurity Manual
Developed acc. to ISO/SAE 21434	**No**	**Yes**
Customer Document description	› Nominal description of features (data sheet, user manual) › Off-the-shelf component (section 6.4.6)	› Cybersecurity Manual incl. cybersecurity claims & features, threats, known weaknesses & limitations, top-level cybersecurity requirements, etc › Cybersecurity case › Cybersecurity assessment report
Post-M9 / Continuous Activities	› Monitoring and Incident Response	› Monitoring and Incident Response
MCUs	› **TRAVEO™ T1G** › **MOTIX™ TLE988x/9x**	› **TRAVEO™ T2G, T2G_EXT**

Copyright © Infineon Technologies AG 2025. All rights reserved.

Table of contents

1 Introduction to Cybersecurity & ISO21434 overview 3

2 Infineon acclerating your cybersecurity developement 7

3 **Security features in Infineon Motor Control products** **11**

4 Infineon Microcontroller TRAVEO™ family to be ISO21434 compliant 17

5 Key take aways 19

Copyright © Infineon Technologies AG 2025. All rights reserved.

MOTIX™ TLE988x/9x
Security features



Feature Overview

Cryptographic support	MOTIX™ TLE 989x/988x
Cryptographic algorithms	
Symmetric encryption/decryption	✓ AES
Hashing	✓ CMAC
Security features	
Secure boot mechanism	✓
Key storage with key management support	✓
Layered access right management	✓
Secured Software Container	✓

Cryptographic support in software:

- AES-ECB and -CBC for encryption and decryption
- AES-CMAC for authenticity check

MOTIX™ TLE988x/9x security products

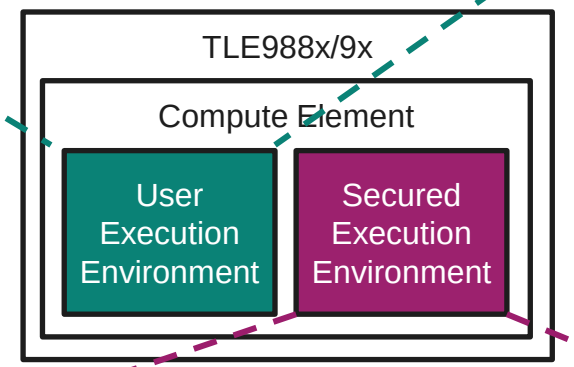
S = with crypto library; supports secured FW update, secured key storage

TLE9893-2QKW62S
TLE9893QKW62S
TLE9893-2QTW62S
TLE9893-2QTA62S
TLE9883-2QTW62S

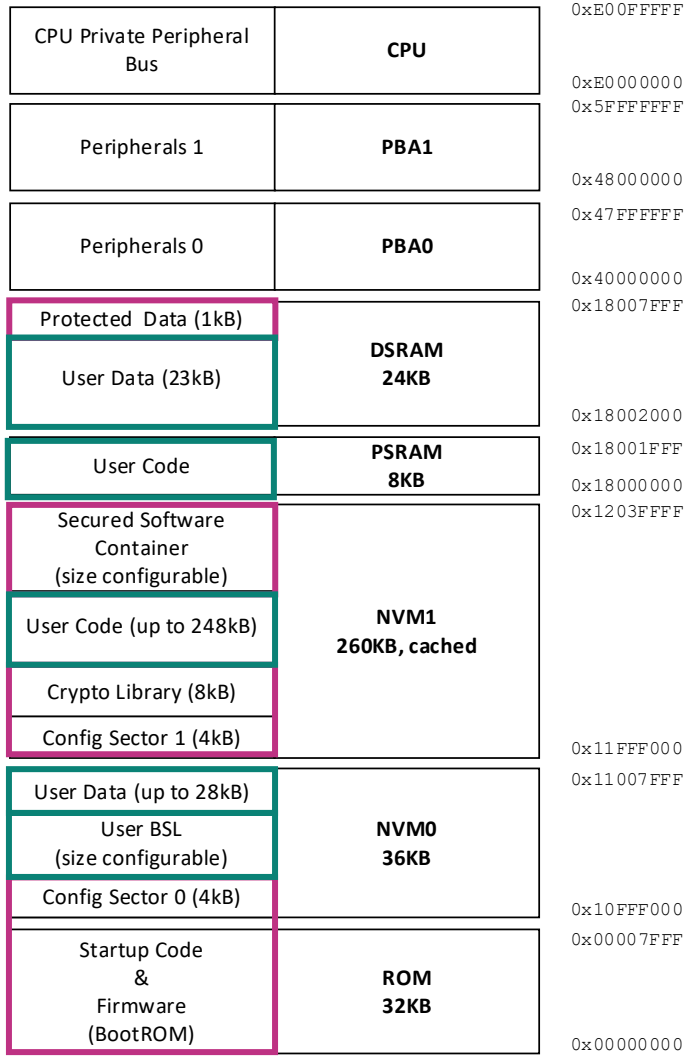
Copyright © Infineon Technologies AG 2025. All rights reserved.

MOTIX™ TLE988x/9x
Security – privileged memory access management

- Application Data (RAM) ➔ User data
- Application Software ➔ User code
- BootROM ➔ Utility APIs



- Protected Data (RAM) ➔ secured data
- Secured Software Container ➔ secured code
- Crypto Library ➔ crypto APIs
- Config Sector ➔ crypto keys
- BootROM ➔ access managment APIs

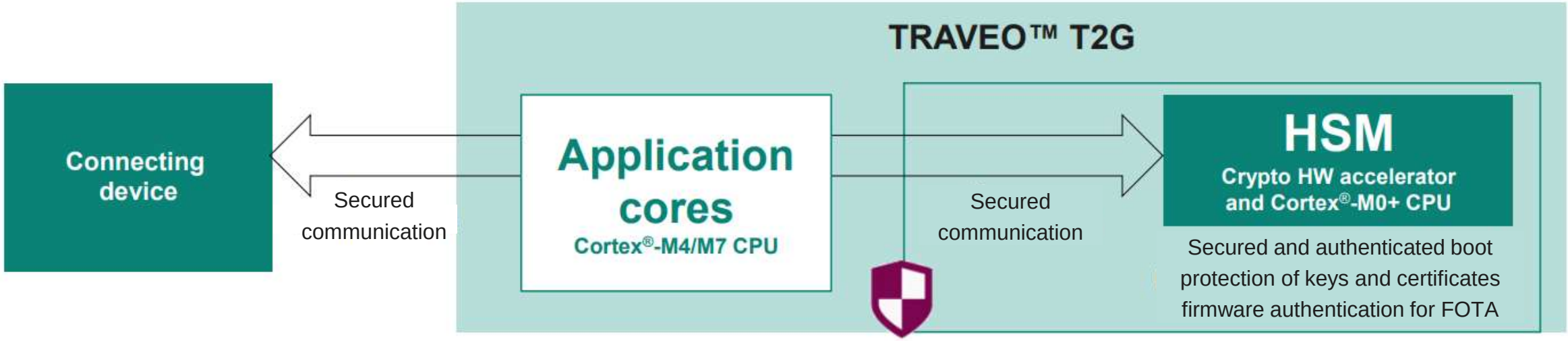


Copyright © Infineon Technologies AG 2025. All rights reserved.

TRAVEO™ T2G
HSM for security

- Root-of-trust boot ROM and chain-of-trust boot firmware
  - Establishment of hardware isolation between secured and non-secured applications
  - Enable fast authentication of ECU software during secured boot

- Flexible configuration of secured domain for efficient resource utilization
- Generation and storage of device-unique secret AES keys



Copyright © Infineon Technologies AG 2025. All rights reserved.

TRAVEO™ T2G
Security enhancement: SHE & HSM

EVITA Profile	evita Light	evita medium	evita full	TRAVEO™ T2G HIS SHE	TRAVEO™ T2G HSM
Cryptographic support	Sensor/actuator ECU	Gateway ECU	V2X ECU, center stack	Body and cluster ECUs	Body, Cluster, and gateway ECUs
Cryptographic algorithms					
Asymmetric encryption/decryption		✓	✓		✓
Symmetric encryption/decryption	✓	✓	✓	✓ AES	✓
hashing		✓	✓		✓
Hardware acceleration					Hardware accelerator
Asymmetric encryption/decryption			✓		✓ RSA, ECC
Symmetric encryption/decryption	✓	✓	✓	✓ AES	✓ AES, TDES, ChaCha
Hashing			✓		✓ SHA, SHAKE
Security features					
Secure / authenticated boot	✓/✓	✓/✓	✓/✓	✓/-	✓/✓
Key control per use / bootstrap	✓/✓	✓/✓	✓/✓	-/✓	✓/✓
PRNG with TRNG seed	✓	✓	✓	✓	✓
Monotonic counters 32 / 64 bit	✓/✓	✓/✓	✓/✓		✓/✓
Tick/UTC-synced internal clock	✓/✓	✓/✓	✓/✓		✓/✓
Internal processing					
User extendable feature set		✓	✓		✓
Internal V/NV (key) memory	✓	✓	✓	✓	✓

Full range of crypto HW accelerators enable EVITA full

Copyright © Infineon Technologies AG 2025. All rights reserved.

TRAVEO™ T2G
Security capabilities - overview

- eSHE/HSM solutions can utilize Cortex®-M0+ and crypto HW accelerator

Hardware accelerated functions

AES	128/192/256-bit keys
TDES	64-bit key
SHA1/2/3	Variable length
RSA and ECC	Vector unit (VU) for asymmetric cipher acceleration offers large integer support of up to 4096-bits
PRNG	Pseudo Random Number Generator
TRNG	True Random Number Generator BSI AIS 31 PTG.2 compliant

Memory and peripheral protection

- Memory protection unit (MPU)
- Shared memory protection unit (SMPU)
- Peripheral protection unit (PPU)
- Protection context mechanism

- Serial memory interface with integrated on-the-fly AES encryption

Lifecycle management (eFuse-based)

- Normal, secured
- Field failure analysis (RMA)

- JTAG debug and test security

Secure boot

- M0+ boots from ROM, while M4/M7 kept in reset
- ROM code provides root-of-trust
- M0+ authenticates flash image, then starts customer firmware on M0+ and M4/M7

Copyright © Infineon Technologies AG 2025. All rights reserved.

Table of contents

1 Introduction to Cybersecurity & ISO21434 overview 3

2 Infineon acclerating your cybersecurity developement 7

3 Security features in Infineon Motor Control products 11

4 **Infineon Microcontroller TRAVEO™ family to be ISO21434 compliant** **17**

5 Key take aways 19

Copyright © Infineon Technologies AG 2025. All rights reserved.

Infineon TRAVEO™ T2G Automotive Microcontrollers to be ISO21434 compliant soon

What?

– Plan to implement product compliance for the TRAVEO T2G automotive microcontroller family with the latest automotive cybersecurity standard ISO/SAE 21434.

Why?

– Growing need of cybersecurity in the connectivity of road vehicles
– Enabling existing and new customers with compliance allowing reuse of existing software and hardware.

How?

– Necessary documentation including the Cybersecurity Manual and Cybersecurity Case Report to be provided to customers.

When?

– End of 2025



Infineon plans to implement ISO/SAE 21434 product compliance for TRAVEO™ T2G automotive microcontrollers

Dec 10, 2024 | Market News

Munich, Germany – 10 December 2024 – The increasing connectivity of road vehicles leads to a growing need for cybersecurity. The United Nations Economic Commission for Europe (UNECE) has therefore adopted the R155 and R156 regulations, which define the cybersecurity requirements for OEMs. OEMs who want to sell new vehicles in UNECE-regulated markets must hold a valid type approval certificate and implement cybersecurity practices throughout the supply chain to minimize the risk of attack throughout the vehicle's lifecycle. The TRAVEO™ T2G Automotive Microcontroller family for Body and Cluster from Infineon Technologies AG (FSE: IFX / OTCQX: IFNNY) features a Hardware Security Module (HSM) that is capable of executing secured boot and ensuring secured isolation of HSM applications and data. To further enhance this, Infineon plans to retrospectively implement product compliance for the TRAVEO T2G automotive microcontroller family with the latest automotive cybersecurity standard ISO/SAE 21434. All necessary documentation, including the Cybersecurity Manual and Cybersecurity Case Report, will be provided to customers.

"With ISO/SAE 21434 compliant TRAVEO T2G automotive microcontrollers, OEMs' effort to comply with UNECE R155 and R156 regulations will be significantly reduced. This enables faster time to the regulated markets", said Ralf Koedel, Vice President Automotive Microcontroller at Infineon. "For existing customers, compliance becomes simpler, faster and more cost-effective while allowing the reuse of existing software and hardware. New customers can also benefit from the ISO/SAE 21434 compliance."

Check here - **Infineon plans to implement ISO/SAE 21434 product compliance for TRAVEO™ T2G automotive microcontrollers**

Copyright © Infineon Technologies AG 2025. All rights reserved.

Table of contents

1 Introduction to Cybersecurity & ISO21434 overview 3

2 Infineon acclerating your cybersecurity developement 7

3 Security features in Infineon Motor Control products 11

4 Infineon Microcontroller TRAVEO™ family to be ISO21434 compliant 17

5 **Key take aways** **19**

Copyright © Infineon Technologies AG 2025. All rights reserved.

Summary



- Infineon’s product development process is certified according to ISO 21434 by SGS-TÜV Saar
- Product compliance categories: QM and ISO21434-compliant
- QM: **TRAVEO™ T1G and MOTIX™ TLE988x/9x**
- ISO21434-compliant: **TRAVEO™ T2G and T2G_EXT**
- Cybersecurity maintenance based on continuous monitoring and incident response in accordance with ISO 21434 available within Infineon
- Dedicated customized customer support based on the requirement

Copyright © Infineon Technologies AG 2025. All rights reserved.

Product Collaterals

TRAVEO™ T2G Automotive Microcontroller

- Product page
- Infineon plans to implement ISO/SAE 21434 product compliance for TRAVEO™ T2G automotive microcontrollers

MOTIX™ MCU TLE988x & TLE989x

TLE988x

- Product page
- Datasheet

TLE989x

- Product page



Copyright © Infineon Technologies AG 2025. All rights reserved.

Questions & Answers




Infineon