



SGS automotive safety and cybersecurity services

DELIVERING SAFE AND CYBERSECURE AUTOMOTIVE COMPONENTS TO GLOBAL MARKETS



Automotive regulatory landscape for safety and cybersecurity

Software-defined vehicles (SDVs) are the next evolution of the automotive industry, serving as the foundation for many other advancements, including self-driving and connected cars. With vehicles becoming increasingly interconnected and reliant on complex electronic systems, ensuring the safety and security of automotive components has become crucial. Manufacturers and developers must therefore prioritize testing their products against recognized cybersecurity standards and industry safety requirements. This will mitigate risks and reduce liability while delivering competitive advantage in fast-growing global markets. SGS offers comprehensive pre-evaluation, testing and certification solutions to help you successfully access target markets with compliant and cybersecure automobiles, devices and components.



AUTOMOTIVE REGULATORY LANDSCAPE

<ul style="list-style-type: none">• ISO/SAE 21434• TISAX• IATF 16949• ISO 9001• ISO 26262	<ul style="list-style-type: none">• ISO/IEC 42001• ISO/IEC 27001• UNECE WP.29 (155 and 156)• CCC Digital Key• FIPS 140	<ul style="list-style-type: none">• Common Criteria• EMVCo• GSMA• PSA Certified• SESIP
---	--	--

TRUSTED INFORMATION SECURITY ASSESSMENT EXCHANGE (TISAX®)

TISAX® is the leading automotive industry information security initiative. It helps to protect information and data by ensuring integrity and availability in automotive business processes, including manufacturing. TISAX® utilizes the Information Security Assessment (ISA), developed by the German Association of the Automotive Industry (VDA) and Volkswagen. The catalog includes criteria for assessing the information security of automotive supply chain organizations based on ISO/IEC 27001 (information security management systems).

ISO/IEC 27001 – INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION

ISO/IEC 27001 certification demonstrates the integrity of your data and systems, and commitment to information security, cybersecurity and privacy protection. ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) for safety and security.

IATF 16949 – AUTOMOTIVE QUALITY MANAGEMENT SYSTEMS

The International Automotive Task Force (IATF) released the IATF 16949:2016 standard which aligns with and refers to ISO 9001. The IATF 16949 standard defines quality management system (QMS) requirements for automotive industry organizations, including those involved in production, service or accessory parts.

ISO 9001 – QUALITY MANAGEMENT SYSTEMS

ISO 9001 specifies the requirements for establishing a quality management system (QMS) to achieve quality policies and objectives.

The international standard defines how you must operate to meet customer and stakeholder requirements. Improve performance and demonstrate consistently high-quality products and services with an ISO 9001 audit from SGS.

ISO 26262 – ROAD VEHICLES FUNCTIONAL SAFETY

ISO 26262 was adapted for the automotive industry from IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems. It applies to each stage of the product's life cycle, including the specifications for design, as well as the implementation, integration, verification, validation, product release and decommissioning stages.

ISO/SAE 21434 – ROAD VEHICLES CYBERSECURITY ENGINEERING

ISO/SAE 21434 is the world's first international standard for cybersecurity in the automotive industry. It aims to reduce the risk of cyberattacks by embedding cybersecurity into automotive products throughout their lifetimes. The global standard specifies engineering requirements for cybersecurity risk management. These cover the concept, product development, production, operation,

maintenance and decommissioning of series production electrical and electronic (E/E) systems in road vehicles, whose development or modification began after the standard was published in 2021. This includes their components and interfaces.

ISO/IEC 42001 – ARTIFICIAL INTELLIGENCE (AI) MANAGEMENT SYSTEM

In response to the rise of AI and the challenges it creates, the ISO and IEC have created the ISO/IEC 42001 standard. It provides a certifiable AI management system (AIMS) framework in which AI systems can be developed and deployed as part of an AI assurance ecosystem.

UNECE REGULATION 155 AND 156

The United Nations Economic Commission for Europe (UNECE) World Forum for Harmonization of Vehicle Regulations (WP.29) is the UN World Forum dedicated to technical regulations applied to the broad automotive sector, addressing the safety and environmental performance of wheeled vehicles, their subsystems and parts. Two UN regulations have been published regarding cybersecurity – 155 and 156. UNECE R155 requires the original equipment manufacturers

(OEMs) to establish a cybersecurity management system (CSMS) covering the whole life cycle of the vehicle and services. UNECE R156 focuses on software updates and the associated software update management systems for vehicles.

CAR CONNECTIVITY CONSORTIUM (CCC) DIGITAL KEY

The CCC Digital Key is a standardized ecosystem that enables mobile devices on any operating system to securely store, authenticate and share digital keys for smart vehicles.

GSMA EUICC SECURITY ASSURANCE (ESA)

The Global System for Mobile Communications (GSMA) Embedded Universal Integrated Circuit Card (eUICC) Security Assurance (eSA) scheme is a dynamic set of procedures for eUICC security evaluation. While based on the Common Criteria approach to security assurance, it is more condensed, making the process fast and efficient. The installation of eSIMs in newer automobiles is a big contributing factor in the growth of the GSMA eSA scheme.



OUR SERVICES

We provide comprehensive solutions to support manufacturers and developers in the delivery of compliant automotive components and products to regulated markets. Our services include training, pre-assessment, evaluations, certification(s) and post-evaluation maintenance. Through our global network, we can assess all products against a wide variety of internationally recognized standards. We evaluate automotive components for any type of vehicle: software-defined vehicles (SDVs) or more traditional vehicles (electronic control units (ECUs), software, hardware, automotive integrated circuits (ICs), hypervisors, advanced driver assistance systems (ADAS) components, digital keys for smart vehicles, etc.)

TRAINING

- TISAX introduction training course – to understand TISAX requirements and elements, the differences between the initiative and ISO/IEC 27001 and how to execute a TISAX project
- ISO/IEC 27001
- IATF 16949/ISO 9001
- ISO 26262
- ISO/IEC 42001
- Basic awareness workshop – covers all relevant cybersecurity requirements for the automotive industry
- Advanced awareness – tailored to the targeted product; focuses on common threats and evaluation procedures

- Threat analysis and risk assessment (TARA) customized workshop – to understand the potential threats to your product and the required level of security, you should have an initial TARA document. The workshop usually takes place in the timeframe of about one and a half months, with the client providing work products for review by SGS staff
- Secure coding – to understand best practice when writing code to protect your product

PRE-EVALUATION

- Evidence readiness – pre-assessment preparation, including gap analysis, maturity assessment, product and procedure readiness, etc.
- Pre-evaluation of core SDV components before tape-out and mass production
- Technical system development life cycle (SDLC) advice
- Developer advisory support
- Gap assessment – to assess readiness for certification
 - ISO 9001
 - ISO/IEC 42001
- IATF 16949 pre-audits
- Guidance through TISAX process – including registration, assessment provider selection, document review and/or on-site assessment and exchange of results

SECURITY EVALUATION

- Penetration testing
- TARA
- IATF 16949 corporate audit scheme certification – multiple manufacturing sites can be audited collectively. A corporate audit scheme enables a QMS to be centrally structured and managed via regular internal audits at all sites
- ISO 9001 integrated management systems certification – audit solutions against bespoke quality performance criteria
- Test report for UNECE Regulation 155 and 156 – the OEM can use the report to claim conformance
- Certification audit – our audit can include a gap assessment and benchmarking. We will determine your level of information security competence and provide advice on how to achieve ongoing improvement
 - ISO/IEC 27001
 - ISO 9001

- ISO 26262
- ISO/IEC 42001
- ISO/SAE 21434
- TISAX assessment
- Car Connectivity Consortium (CCC) – Digital Key
- Target of evaluation (TOE) certification (hardware/software/device)
 - Common Criteria (various international schemes) – IC, SoC (System on Chip), Hypervisors, OS's, ADAS, HSM, etc.
 - GSMA eUICC
 - SESIP and PSA – mid assurance sensors, entertainment systems, etc.
 - EMVCo
 - FIPS 140

POST-EVALUATION

- Re-testing
- Re-certification

WHY SGS?

We are SGS – the world’s leading testing, inspection and certification company. We are recognized as the global benchmark for sustainability, quality and integrity.

With an unrivaled network of experts and state-of-the-art laboratories, we provide market-enabling solutions to help you operate more effectively in global markets. With specialists in all market segments, including financial, medical, automotive, industrial and consumer, we have the capabilities in place to help you deliver products that achieve competitive advantage while demonstrating your commitment to functional safety and cybersecurity.

CONTACT US

+31 (0)15 269 2500

brs.automotive@sgs.com

www.sgsbrightsight.com

<https://www.linkedin.com/company/sgsbrightsight>

When you need to be sure

SGS Headquarters
1 Place des Alpes
P.O. Box 2152
1211 Geneva 1
Switzerland

sgs.com

