Steering clear of automotive industry cyber threats

NAVIGATING INDUSTRY TRENDS, CHALLENGES, CYBERSECURITY AND HOW WE CAN HELP

White paper

SGS.COM

Navigating industry trends

The automotive industry is experiencing unprecedented digital and technological trends. From autonomous, self-driving and software-defined vehicles to connectivity, artificial intelligence (AI) and smart factories, companies have a lot to understand and navigate to produce the best vehicles and driver experience. All while cyber threats from nefarious actors threaten the progress, trust and sales gained from technological mobility masterpieces.

Automotive AI market

According to Global Market Insights, this market is expected to reach about USD 186.4 billion by 2034.

Internal vehicle technologies include advanced sensors, virtual assistants, intuitive interactions with in-car infotainment, vehicle safety and the relationship between vehicles and the environment.

External vehicle technologies include visualizing car configurations in seconds, dynamic pricing tools, improved supply chain management and more efficient production.

For example, Stellantis and Mercedes-Benz have integrated ChatGPT so passengers can interact with their vehicles. These systems are like virtual travel companions, providing insights on destinations and local attractions.

AI will be crucial to:

1. Autonomous driving
2. Electrification
3. Connectivity and software-defined vehicles (SDVs)
4. Changing customer preferences
5. Resilient supply chains and smart manufacturing
6. Servitization
7. Sustainability
8. Smart factories and cities

USD 186.4B

The automotive AI market is expected to reach about USD 186.4 billion by 2034.
– Global Market Insights

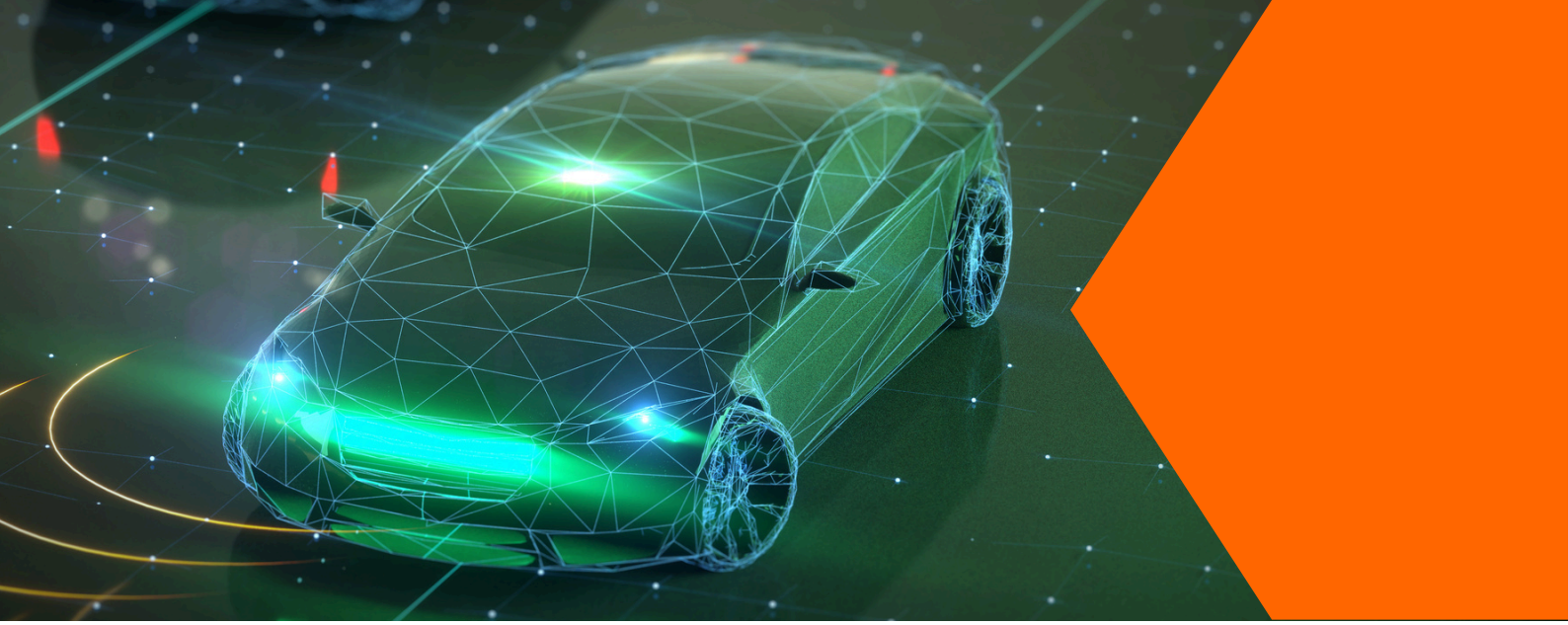
Autonomous driving

Developing and deploying autonomous vehicles/driverless cars has been slower than originally anticipated, but recent technological advances are speeding things up. The autonomous vehicle market is projected to reach USD 980.7 billion by 2040, with a 22.3% compound annual growth rate (CAGR) from 2031 to 2040.

However, the automotive industry must remove the barriers to widespread acceptance, as most people have mixed feelings about this trend. A Pew Research Study found that 44% of Americans believe self-driving cars are bad for society. However, those under 50 years old were more open to riding in one compared to those over 50 (47% versus 25%). Building customer confidence in autonomous vehicle safety and reliability through demonstrations, transparency about the technology and increased safety will be essential for earning public acceptance and achieving growth.

USD 980.7B

The autonomous vehicle market is projected to reach USD 980.7 billion by 2040.
– Allied Market Research



A shift to self-driving taxis

Self-driving taxis are here, as companies try to reimagine the automotive and taxi-hailing industry. Uber and GM Cruise have been allowing Uber ride-hailing platform users to book fully self-driving vehicles through the app in selected US cities. Apollo Go, Baidu's self-driving robotaxi service in Wuhan, has been targeting profitability, following successful operations in one of China's largest cities.

However, robotaxi vehicle sales remain low, as safety concerns, legislative obstacles and high operational costs inhibit growth. On the SAE Level 0 to 5 scale (where the higher levels have greater autonomy), most vehicles sold in 2025 adhere to SAE Level 2 autonomy. Vehicles increasingly incorporate advanced driver assistance systems (ADAS), such as braking support, but a human driver is ultimately in control.

Meanwhile, SAE Level 3 vehicles, offering conditional automation, will also grow. However, they are slowed by regulations, as numerous countries have yet to introduce legislation for their public use.

USD 121B

The connected car market is expected to reach USD 121 billion in 2025.
– Statista

Connectivity and software-defined vehicles

Incorporating vehicles into the Internet of Things (IoT) ecosystem, using data to aid an extremely personalized journey, is set to make the driving experience more efficient and enjoyable.

Vehicles can suggest errands optimized by location and recommend a break when it senses the driver's fatigue, among other advancements.

The software-defined vehicle (SDV) goes one step further, utilizing software updates, not hardware, to maintain performance. Present vehicles require mechanics to perform maintenance and face delays due to parts shortages. But SDVs can be regularly enhanced and customized via over-the-air (OTA) updates, which offer new features, performance enhancements and bug fixes directly to the vehicle.

According to Statista, the global connected car market is set to grow significantly, from USD 56 billion in 2020 to USD 121 billion in 2025.

Adapting to customer preferences

Companies must understand their customers to deliver optimal services and experiences. The uptake of connected vehicles and customized driving experiences is prompting automobile manufacturers to focus on customers more than ever. Connected vehicles provide real-time insights into customers, vehicles and usage.

Companies can digitize, automate and use AI to facilitate consistent experiences across all sales channels.
They are partnering with technology companies to develop smart features, integrating vehicles with IoT and offering services like infrastructure connectivity, remote updates and safety enhancements.

This is happening while purchasing preferences continue to evolve. Younger generations, particularly Gen Z, increasingly prefer eco-friendly, technology-driven options.

Resilient supply chains

The automotive industry is strengthening its supply chain through diversifying suppliers, adopting advanced technologies and prioritizing sustainable practices. This helps manufacturers prevent supply chain disruptions and better meet consumer demands.

Automobile manufacturers are diversifying their supplier base to decrease reliance on single sources. Utilizing AI and IoT in the supply chain allows real-time monitoring and faster responses to disruptions. According to a SAP survey, almost 42% of automotive executives say improving or expanding supplier and partner networks is a priority in their growth plans.

Sustainable sourcing sees renewable materials reduce risks. Sustainable practices, flexibility and technology are helping the industry create a robust supply chain that withstands issues, such as global pandemics and natural disasters.

About 42%

Almost 42% of automotive executives say improving or expanding supplier and partner networks is a priority in their growth plans.
– SAP survey

AI and smart factories

AI and smart factory technologies are more crucial to automotive manufacturing. For example, Stellantis has shown how AI transforms production efficiency. The company has reduced production costs, accelerated vehicle launch timelines and improved flexibility across global operations, ensuring faster responses to changing market demands, thanks to AI.

Up to 40%

Autonomous mobility could account for up to 40% of a smart city's traffic.
– PwC

Smart cities

Smart cities, urban areas that leverage technology, data and connectivity to improve sustainability, efficiency and quality of life, are expected to reshape automotive industry business models and consumer behavior.

Greater connectivity will make vehicles part of the city infrastructure, enabling real-time data-sharing to improve aspects like traffic flow and safety. Beijing and San Francisco were some of the first cities to incorporate driverless or robotaxis, using sensors and AI to detect surroundings and analyze the environment before choosing and implementing an action.

PwC estimates that, by 2030, more than one in three kilometers driven could involve sharing concepts, and autonomous mobility accounting for up to 40% of a smart city's traffic.

Technology breeds risk

These trends naturally have positive and negative aspects. While they enhance and simplify the user experience, new technologies are prone to cyber threats.

Factors, including vehicle connectivity, automated vehicles and more complex automotive components, have heightened the risk of cyberattacks – unauthorized access, remote hacking, data privacy breaches and malware or virus infection.

Enhanced cybersecurity is essential to maintaining product quality and customer trust.

Key automotive industry challenges

1. Evolving threat landscape: as technologies like AI, SDVs and electric vehicles (EVs) alter the industry, cyber threats are evolving and require new strategies.
2. Rising cyber threats: modern vehicles are targets for cyberattacks because of their connectivity and software reliance.
3. Cyberattack surge: the number of cyberattacks greatly increased in 2024, from 296 in 2023 to 409, chiefly driven by ransomware. Notorious ransomware groups, such as LockBit, are specifically targeting the industry.
4. Supply chain weaknesses: the industry's complex supply chain increases the risk of exploitation by threat actors.

The automotive industry cybersecurity market

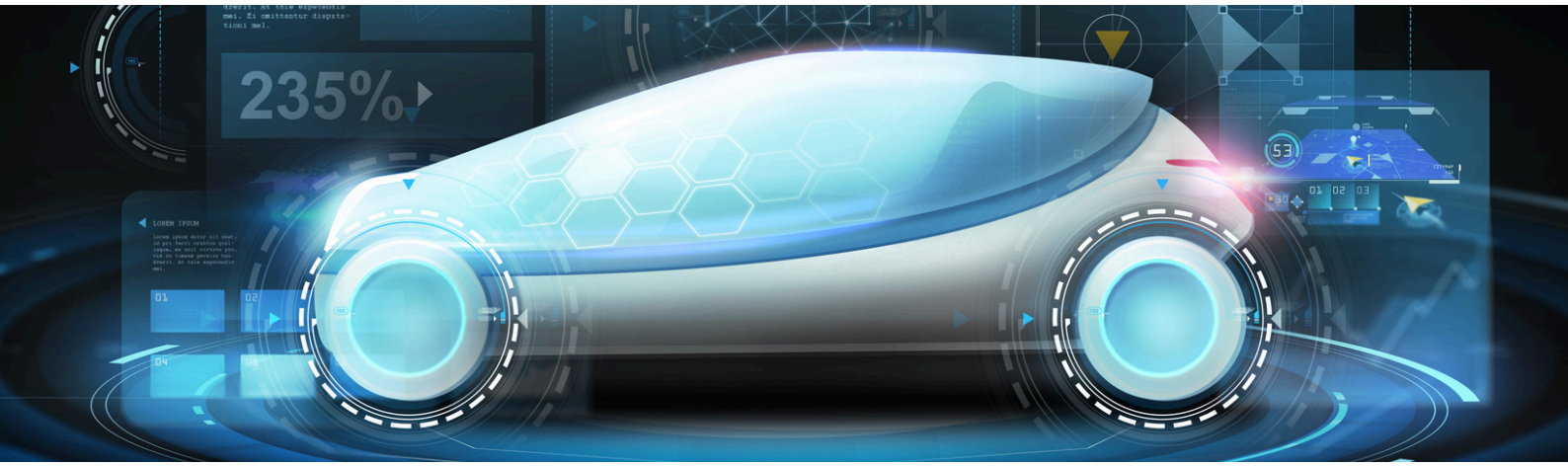
The industry's cybersecurity market will experience significant growth over the coming years, with an estimated 22% CAGR. This indicates cybersecurity's increasing significance in the industry.

Here are some key statistics:

- The automotive cybersecurity market generated USD 3.2 billion in revenue in 2022. This is expected to rise to USD 22.2 billion by 2032
- In 2022, 97% of the industry's cyberattacks were remote, while the remaining 3% were physical
- Suppliers bore the brunt of cyber incidents, accounting for 67.3%

Key solutions

1. Protective measures: the automotive industry can utilize end-to-end encryption, multi-factor authentication and third-party security providers to enhance data protection.
2. Regulatory landscape: organizations, such as ISO, SAE International and the ENX Association, are addressing the challenges and mitigating safety risks.
3. Future growth: the automotive cybersecurity market is growing exponentially, highlighting the importance of safeguards.



SGS's safe and secure services

As the world's leading testing, inspection and certification company, with decades of experience in the automotive, digital trust and cybersecurity arenas, we can get you to your destination – safe and secure systems and situations.

ISO/SAE 21434 – the first international standard for automotive cybersecurity

The shift toward vehicle connectivity and automated vehicles, coupled with increasing numbers of complex automotive components, has heightened the risk of cyberattacks. Integrating electronic systems, connectivity and automation into vehicles increases the chances of hacking, data breaches and virus or malware infection, among other threats.

ISO/SAE 21434 is the automotive industry's first international standard for automobile cybersecurity. It aims to reduce the risk of cyberattacks by embedding best cybersecurity practice into automotive products throughout their lifetime.

The 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/SAE 21434's framework covers processes for risk assessment, treatment, monitoring and review, as well as requirements for cybersecurity processes and a common language for communicating and managing cybersecurity risks.

Automotive manufacturers must also demand that their suppliers comply with relevant cybersecurity standards, such as ISO/SAE 21434.

The standard does not prescribe specific cybersecurity technologies or solutions.

WHAT ARE THE BENEFITS?

ISO/SAE 21434 certification gives you a competitive advantage and helps ensure customer trust. Certification follows successful completion of an audit and enables you to:

- Ensure that products and services are developed and maintained in a secure and trustworthy management process
- Better identify and mitigate potential threats and vulnerabilities
- Indicate that you have conducted a security assessment with the greatest possible independence
- Demonstrate your level of embedded cybersecurity to customers
- Improve operational efficiency
- Reduce costs
- Contribute to the UN Sustainable Development Goal (SDG) 9 – Industry, Innovation and Infrastructure

Certification can also help you comply with relevant standards and regulations, such as the UN Regulation No. 155 (UN R-155) – cybersecurity and cybersecurity management system – and the General Data Protection Regulation (GDPR).

HOW CAN WE HELP?

Successfully implementing ISO/SAE 21434 is a complex and ongoing process. You must fully understand the standard, gain commitment from top management and regularly conduct comprehensive risk assessments. You must also develop and document cybersecurity policies and procedures, so cross-functional teams can respond to incidents effectively and undertake continuous improvement.

Combining our extensive automotive and digital trust experience, we can help you along the path to certification with an ISO/SAE 21434 audit. Your audit can include a gap assessment and benchmarking. We will determine your level of competence and provide advice on how to achieve ongoing improvement.

SGS Academy also offers an Introduction to ISO/SAE 21434 Training Course that introduces automotive cybersecurity, the standard, cybersecurity in product development and implementing best practices.

TISAX®– trusted automotive industry information security

Businesses wanting to remain competitive in the digital age must pay close attention to information security. This is particularly true for the automotive industry, where massive amounts of confidential data are exchanged daily.

The Trusted Information Security Assessment Exchange (TISAX) is the leading automotive industry information security initiative. The assessment helps ensure a uniform level of information security among car manufacturers, service providers and suppliers. It helps to protect data by confidently ensuring integrity and availability in automotive business processes, including manufacturing.

A dedicated online platform has been developed for the exchange of information security assessment results. After registration, companies can share their assessment results with trusted business partners.

TISAX is based on the Information Security Assessment (ISA) developed by the German Association of the Automotive Industry (VDA) and Volkswagen. The catalog includes criteria for assessing automotive supply chain organizations' information security based on ISO/IEC 27001 (information security management systems) and ISO/IEC 27002 (information security controls), but has additional requirements.

The ENX Association maintains the ISA, audit provider criteria and assessment requirements (TISAX ACAR). It also approves audit providers and monitors the quality of implementation and assessment results. ENX is supported by the TISAX Committee, comprising manufacturers, suppliers and associations.

WHAT ARE THE BENEFITS?

Successfully passing a TISAX assessment allows your organization to share the TISAX label with business partners. This helps highlight your information security status.
Key benefits include:

- Assessment results recognized by all TISAX participants
- A commonly accepted assessment standard that enables the exchange of assessment results
- Accepted by suppliers and original equipment manufacturers (OEMs)
- Saves time and money
- Creates confidence in your company
- Eliminates duplicate and multiple assessments

HOW CAN WE HELP?

Utilizing our key experience and global network of experts, we are perfectly placed to provide TISAX alongside helping you manage your supply chain, providing safe and reliable vehicles, improving quality, efficiency and safety, and reducing environmental impact.

We can guide you through the entire TISAX process, including registration, assessment provider selection, document review and/or on-site assessment and exchange of results.

SGS Academy also offers a TISAX Introduction Training Course. On completion of this face-to-face or virtual instructor-led training (VILT) course, you will understand TISAX requirements and elements, the differences between the initiative and ISO/IEC 27001, and how to execute a TISAX project.

ENX VCS – a standardized, industry-wide cybersecurity audit scheme

Recognizing the evolving need, individual automotive industry stakeholders asked ENX to create and maintain a standardized, industry-wide audit scheme for a supply chain vehicle-cybersecurity management system (V-CSMS).

The ENX Vehicle Cybersecurity (ENX VCS) audit provides the industry with a uniform road vehicle cybersecurity standard for suppliers, achieving this by leveraging the existing ENX audit framework and infrastructure.

ENX governs ENX VCS by managing an approved pool of auditors, maintaining provider criteria and assessment requirements, and monitoring audit quality. It also administers the exchange mechanism and provides a single results database.

UN R-155 requires vehicle manufacturers to manage dependencies of their V-CSMS with supplier-related risks for the security of vehicles or vehicle components. V-CSMS supplier audits can support vehicle manufacturers in managing such dependencies.

WHAT ARE THE BENEFITS?

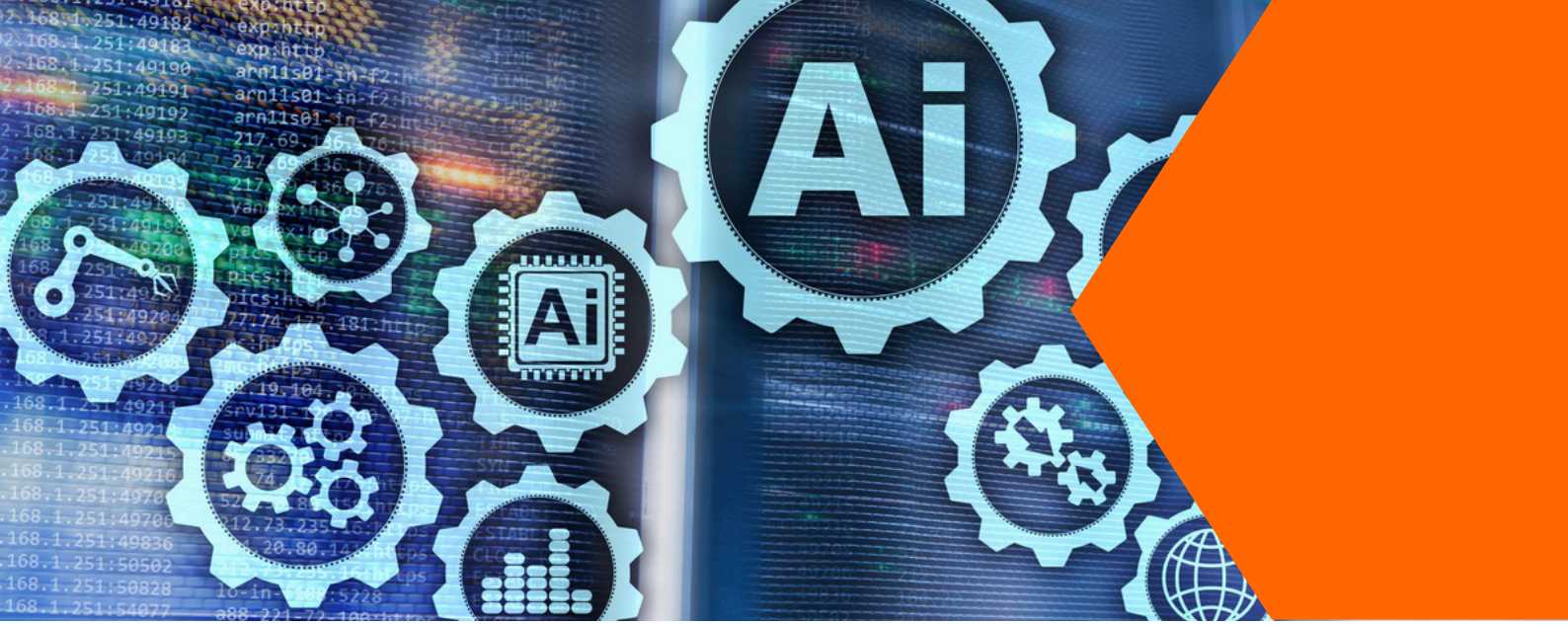
ENX VCS is the universal standard certification of an ISO/SAE 21434-compliant V-CSMS and wholly implements ISO/PAS 5112 recommendations. ENX VCS provides:

- A universal standard for third-party V-CSMS certification, avoiding the growing number of proprietary schemes
- Alignment with the proven ENX Automotive Compliance, Assurance and Risk Services (ACARS) framework used for TISAX
- A standard that adopts and works with key TISAX mechanisms
- Alignment with ENX's proven governance regime to ensure quality and comparability
- A standard developed and maintained by an international, open group of experts from leading automobile manufacturers and suppliers
- Reduced cost and effort by avoiding redundant audits and various proprietary schemes
- Relief from having to create and maintain acceptable assurances
- An approved pool of audit providers, including SGS, and audit quality monitoring

HOW CAN WE HELP?

As a qualified and experienced TISAX assessment provider, along with other key solutions, we support your exact ENX VCS needs and guide you through the entire process. Our ENX VCS audits, support and expertise enable you to:

- Confirm your ENX VCS compliance
- Ensure effective cybersecurity throughout your supply chain
- Provide safe and reliable vehicles
- Improve quality and efficiency
- Reduce environmental impact



ISO/IEC 42001 – the world-leading AI management systems standard

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

The global standard specifies the requirements for establishing, implementing, maintaining and continually improving an AIMS. The goal is to help organizations and society benefit the most from AI while reassuring stakeholders that systems are being developed and used responsibly.

WHAT ARE THE BENEFITS?

ISO/IEC 42001 certification follows successful completion of an audit and enables you to:

- Implement AI safely, with evidence of responsibility and accountability
- Consider security, safety, fairness, transparency and data and AI system quality throughout the life cycle
- Show that introducing AI is a strategic decision with clear objectives
- Indicate strong governance concerning AI
- Strike a balance between governance and innovation
- Ensure that AI is used responsibly, especially concerning its continuous learning
- Ensure that all relevant safeguards are in place
- Combine key frameworks with experience to implement crucial processes like risk, life cycle and data quality management

HOW CAN WE HELP?

Combining our vast digital trust expertise, we help you understand, apply and enhance AI systems safely through vital services like our accredited ISO/IEC 42001 certification.

CertX – cybersecurity, AI and functional safety certification specialists

We have acquired CertX, which specializes in cybersecurity, AI and functional safety certification. Founded in 2018 as a spin-off from the University of Fribourg, Switzerland, CertX is a certification and Notified Body (NB) for functional safety and cybersecurity, internationally accredited by the Swiss Accreditation Service (SAS). NB (CE) and technical service (car homologation). The services cover:

Functional Safety & RAMS: certification and inspection of products and processes to identify flaws before they cause hazards in field operations.

Cybersecurity: working horizontally across multiple domains to benefit from a broad expertise in best security practices, considering sector-specific constraints.

AI: systematically and independently evaluating your AI solution, performed by AI, safety, security and risk management experts.

A trunkful of trusty services

These are just some of our Digital Trust Assurance services. Contact our experts now to determine your digital needs and reinforce your protective measures.

For more information:
Digital Trust Assurance section on www.sgs.com
or https://certx.com.
Certification@sgs.com

References

Allied Market Research – https://www.alliedmarketresearch.com/

Automotive Manufacturing Solutions – https://www.automotivemanufacturingsolutions.com/

Car Buzz – https://carbuzz.com/

Cyber Insight – https://cyberinsight.co/

ENX – https://www.enx.com/en-US/

Euromonitor International – https://www.euromonitor.com/

Global Market Insights – https://www.gminsights.com/

ISO – https://www.iso.org/standard/70918.html

KELA – https://www.kelacyber.com/

Market.us Scoop – https://scoop.market.us/

McKinsey & Company – https://www.mckinsey.com/

NHTSA – https://www.nhtsa.gov/

Pew Research Center – https://www.pewresearch.org/

PwC – https://www.pwc.com/gx/en.html

rinf.tech – https://www.rinf.tech/

Safety Detectives – https://www.safetydetectives.com/

SGS – https://www.sgs.com/en

SGS Digital Trust Assurance – https://www.sgs.com/en/our-services/business-assurance/digital-trust-assurance

SOCRadar – https://socradar.io/

Statista – https://www.statista.com/

The Future of Commerce – https://www.the-future-of-commerce.com/

TISAX – https://www.enx.com/en-US/tisax/

VicOne – https://vicone.com/

When you need to be sure

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

sgs.com