CASE STUDY

Automotive Industry sets High Security Standards

macmon secure helps JOYSONQUIN to achieve certification

JOYSONQUIN Automotive Systems, a joint venture between SENSSUN and JOYSON Electronics, is a global automotive supplier with approximately 4,200 employees. JOYSONQUIN is currently one of the three leading suppliers of luxury interior fittings worldwide, delivering products to renowned OEMs such as Mercedes-Benz, BMW, Porsche, VW/Audi, Tesla and GM.

„Introducing the macmon Premium Bundle was quick and easy and provided immediate added value to our IT security. We were able to achieve implementation within only a few weeks from first contact."

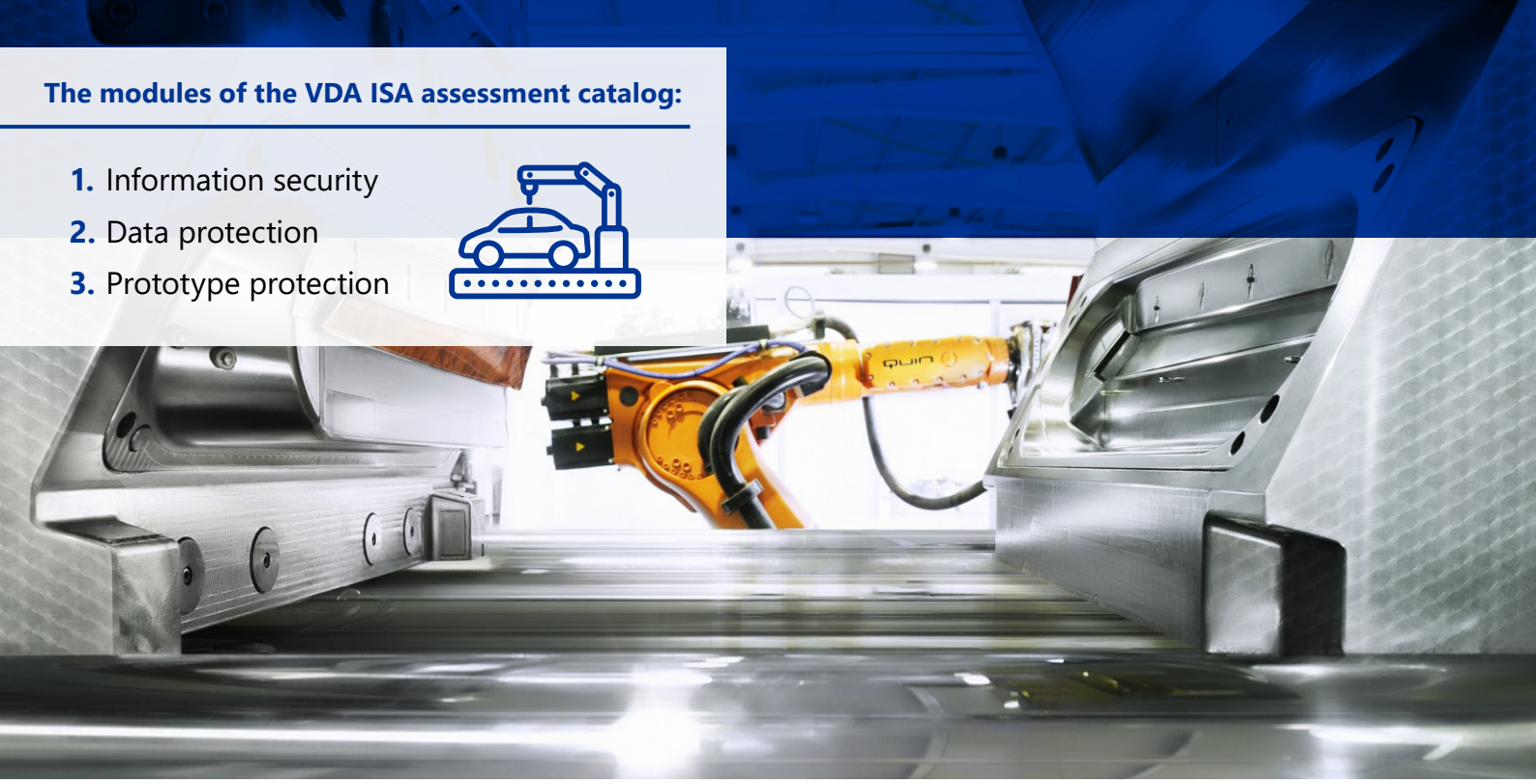
Adriano Vasile | Team Leader IT Infrastructure | JOYSONQUIN

JOYSONQUIN also controls a large share of the Chinese market for air management systems, engine air intake systems and washing systems. With development and manufacturing sites in China, the United States, Mexico, Germany, Poland and Romania, JOYSONQUIN offers global service to its customers. Thanks to the successful implementation of the **macmon Premium Bundle**, the company was able to meet its customers' certification demands in record time.

Adriano Vasile, who as team leader for IT infrastructure is responsible for IT security at JOYSONQUIN, says the following: "In collaboration with an external data protection officer and our **IT system house Luithle + Luithle GmbH**, we were able to pass 'Assessment Level 2 (AL2)' of the TISAX®certification in only a few months – and with a top score. Introducing the **macmon Premium Bundle** was quick and easy and provided immediate added value to our IT security. We were able to achieve implementation within only a few weeks from first contact."

The modules of the VDA ISA assessment catalog:

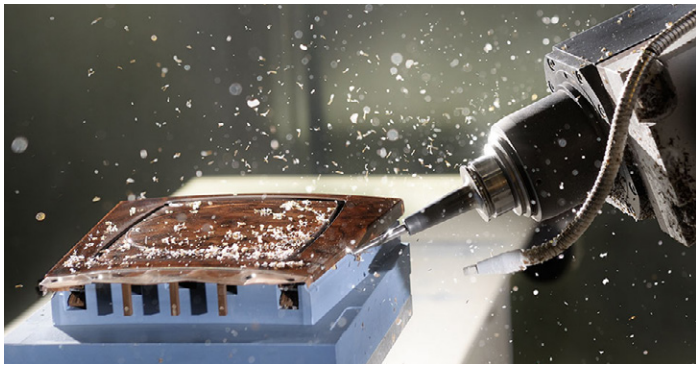
1. Information security
2. Data protection
3. Prototype protection



Product development in the automotive industry is subject to strict security requirements, as innovations need to be carefully protected

TISAX® – standardized security for the highly specialized automotive industry

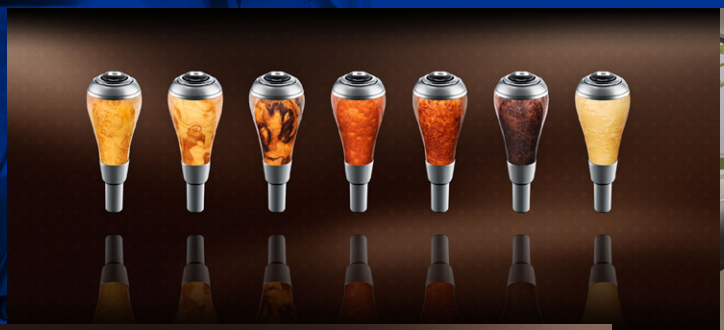
Developed by **the German Association of the Automotive Industry** (VDA), TISAX® is an information and cyber security standard that is specially tailored to the requirements of the automotive industry. Its aim is to ensure secure processing and the trusted exchange of information between suppliers and car manufacturers. With TISAX® automotive suppliers can implement an **information security certification** that is specifically geared to the needs of the industry.

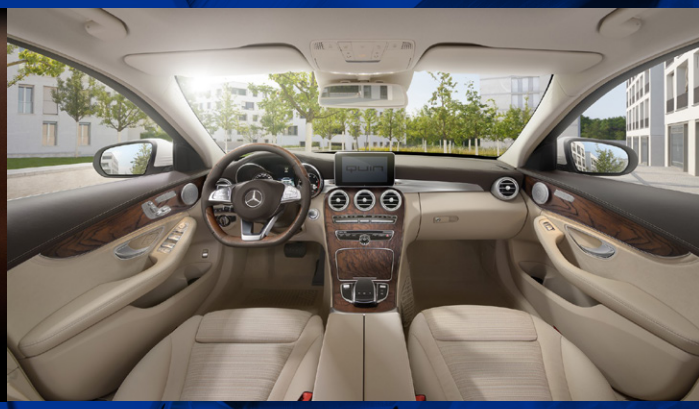


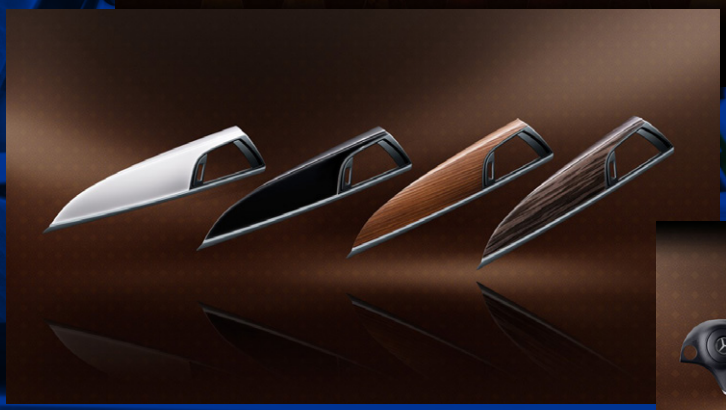
JOYSONQUIN's production is highly precise – just like macmon's security solution

The requirements catalog for TISAX®certification (VDA ISA) builds on the international industry standard ISO 27001 but goes even further. It includes requirements specific to the automotive industry, such as integration of partners into the company's own IT infrastructure, JOYSONQUIN's production is highly precise – just like macmon's security solution data protection and prototype protection. To obtain certification, companies must meet the requirements set out in the VDA ISA assessment catalog. This catalog consists of three modules: **1. information security, 2. data protection and 3. prototype protection.**

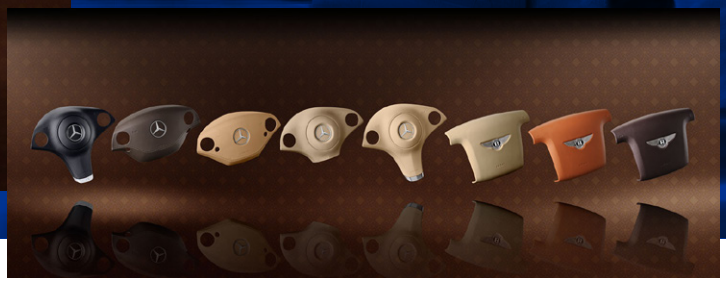
Information security is the main module, that is checked during every assessment, based on ISO 27001. The three additional modules are added to the assessment as needed. Aim of the module "information security" part of the TISAX®certification checks whether a company's IT security is planned, monitored, audited and continuously improved. To achieve this, three key things are required: standardized processes, automated workflows and audit-proof reports. This is where the **macmon Network Access Control** IT security solution steps in.







Outstanding "Made in Germany" quality – secured by macmon secure from Berlin



The fast track to full network transparency and control

The "asset management" part of the TISAX® requirements deals with both information assets (data/information) and information carriers (IT/OT systems of any kind). Under these requirements, it is essential to maintain a central directory of all existing assets and the persons who are responsible for them. By using **macmon NAC**, JOYSONQUIN ensures the complete transparency of all devices connected to the network.

Devices can be grouped and managed on the network according to various criteria, such as location, network access, device type, information content and many other properties. **macmon NAC** thus creates a directory of all assets connected to the network while also providing additional information such as a device's life cycle or current location.

> *"Since the introduction of macmon NAC, we finally have full control over all endpoints [...] and with just a few clicks. This was something that really wowed us right from the beginning."*
>
> **Adriano Vasile** | Team Leader IT Infrastructure | JOYSONQUIN

Adriano Vasile adds: "Since the introduction of **macmon NAC**, we finally have full control over all endpoints. What's more, we're able to manage the switches centrally from the macmon console, and with just a few clicks. This was something that really wowed us right from the beginning."

Trust based on long-term partnerships

Adriano Vasile describes the process of selecting an NAC solution: "Once we had clearly formulated our customers' demands for TISAX® certification, we turned to our partner system house. It was a huge advantage having a competent partner by our side to help us in selecting, implementing and optimizing our hardware and software structure. **Luithle + Luithle GmbH** is **silver partner of macmon secure** and has been providing proven solutions for many years. After attending a webinar on another company's successful use of **macmon NAC**, I was able to quickly make the right decision."

Mitigate damage with event processing and situational responses

Incident management refers to the structured processing of information security events within an organization, with the goal of limiting possible damage and preventing recurrence. In addition to network access control and the associated policies, **macmon NAC** offers a separate event processing feature that can be used to respond individually to each situation. Data about endpoints and network devices is collected, processed and analyzed to generate attack events such as ARP and MAC spoofing, informal "network session started" events, and warnings such as "endpoint almost non-compliant" or "network device changed." JOYSONQUIN has defined various reactions to these events (of which there are about 50), such as isolating an endpoint to prevent damage. All environmental variables such as location, time and person responsible can be included as conditions to facilitate individualized incident management.

JOYSONQUIN's networks are protected against illegal access around the clock

Adriano Vasile is impressed by the performance of **macmon NAC**: "If an unauthorized device tries to log in to the network, the device is immediately and automatically blocked to prevent access to the network. If we want to grant access to a new device, we can configure this directly in the macmon console. In just a few seconds, we can then enable the correct network (VLAN) at the remote switch port in order to grant access with a single click. This process is very convenient and saves us valuable time and stress in the IT department."

Checking and implementing security policies for mobile endpoints

macmon NAC supports the enforcement of security policies for mobile endpoints by checking the implemented security measures – such as virus protection, Windows Firewall or patches – and by enabling organizations to take direct action. Mobile endpoints that have not logged into the JOYSONQUIN corporate network for a long time are checked in a separate quarantine network and, if necessary, updated or reconfigured. Only after passing a security check are they allowed to access the corporate network again. Security measures involving fingerprinting, WMI and SNMP are used to individually verify the integrity of these endpoints.

"If an unauthorized device tries to log in to the network, the device is immediately and automatically blocked to prevent access to the network."

Adriano Vasile | Team Leader IT Infrastructure | JOYSONQUIN

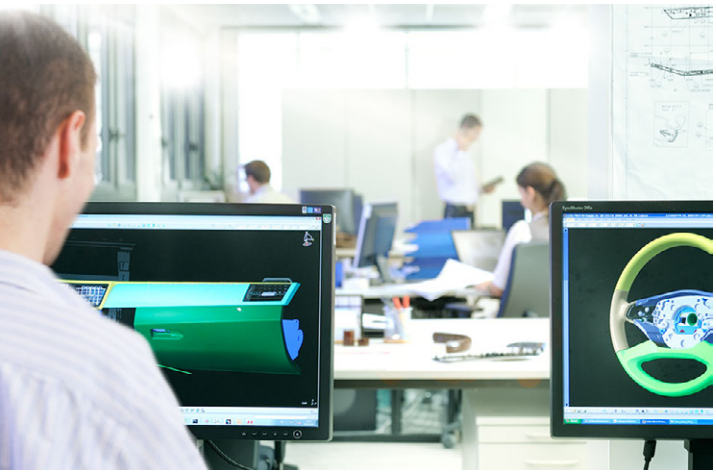
Only trusted endpoints admitted

An organization's identity management system is responsible for identifying and authenticating trusted sources with the aim of allowing only authorized persons and devices to access corporate resources. As part of JOYSONQUIN's certification, the company also defined logging measures and procedures to ensure that detected security breaches are permanently documented.

macmon Network Access Control is able to authenticate both endpoints and users, and it can even recognize combinations of the two. In addition to ensuring that only trusted devices that meet the security requirements are granted access to the network, the combination with user identities makes it possible to define that only certain users are authorized to operate certain devices in the network. This allows companies to define security zones based on available resources and information, and to protect these against unauthorized use with **macmon NAC**. In addition to managing access and segmentation, various third-party solutions such as firewalls or IPS systems can also be integrated. These features from macmon provide significant improvements in IT security, which is particularly important given the increasing incidence of cyber crime and industrial espionage in the automotive industry.

Control, segmentation and management of all endpoints in JOYSONQUIN's network infrastructure

Operations security refers to an organization's procedures for securing its IT network infrastructure, with the aim of considering information security aspects during any change to business processes – which is a very common occurrence in companies with global supply chains. It also aims to ensure the reliability, confidentiality and integrity of data. After all, an automotive manufacturer can invest several billion euros in the development of a new vehicle and is in constant competition with other manufacturers to come up with new innovations.



Only authorized employees can access sensitive data

> *"Network segmentation is both a fundamental feature of macmon NAC and one of its greatest benefits."*
>
> **Adriano Vasile** | Team Leader IT Infrastructure | JOYSONQUIN

The basic principle of **macmon NAC** is to enable the management and control of a network, including all the endpoints and network devices within it.

Adriano Vasile explains: "We use internal firewalls to secure highly critical network areas. Only endpoints and users that have been uniquely identified by **macmon NAC** and have the appropriate security clearance are allowed to communicate through these firewalls. Network segmentation is both a fundamental feature of **macmon NAC** and one of its greatest benefits, as it enables us to create new networks more easily and roll them out quickly, which in turn reduces the amount of administrative work." The internal IT infrastructure team can define the boundaries between segments using virtual networks (VLANs) or access control lists (ACLs) to ensure that only authorized people and devices have access to certain information services and systems.

Optimizing IT security in the automotive industry – a continuous process

JOYSONQUIN is continuously optimizing the security and performance of its IT infrastructure. After the first satisfactory implementation phase, the company gathered and evaluated its experiences of working with **macmon NAC**, in cooperation with **IT system house Luithle + Luithle GmbH**. Additional features are continually being implemented to ensure that network security is always optimized and improving. And thanks to **macmon NAC**'s useful interfaces to numerous technology partners, Adriano Vasile expects even more synergies in the future. Specifically, the IT infrastructure expert's ambitious agenda includes looking at the global network infrastructure, as well as the topics of OT network security and the strategic use of cloud services.

The macmon Premium Bundle provides automotive supplier JOYSONQUIN with transparency, compliance and access control. Thanks to its acquisition by **Belden**, **macmon secure** has extended its expertise to OT networks, which in turn will lead to further optimizations, additions and enhancements for companies in the automotive industry.

CONCLUSIO by Adriano Vasile, IT Infrastructure Team Leader, JOYSONQUIN

Information security requirements in the automotive industry are growing exponentially. Achieving IT security for this complex and global value creation process requires three things: standardized processes, automated workflows and audit-proof reports. macmon Network Access Control (NAC) was quickly and easily implemented as an IT security solution to achieve TISAX® certification.

macmon secure GmbH | Alte Jakobstraße 79 - 80 | 10179 Berlin | Phone: +49 30 23 25 777 - 0 | nac@macmon.eu | www.macmon.eu