VICCON

CONSULTING

Automotive Security Management

An innovative approach for the further development of security management in the automotive industry

IMPRINT

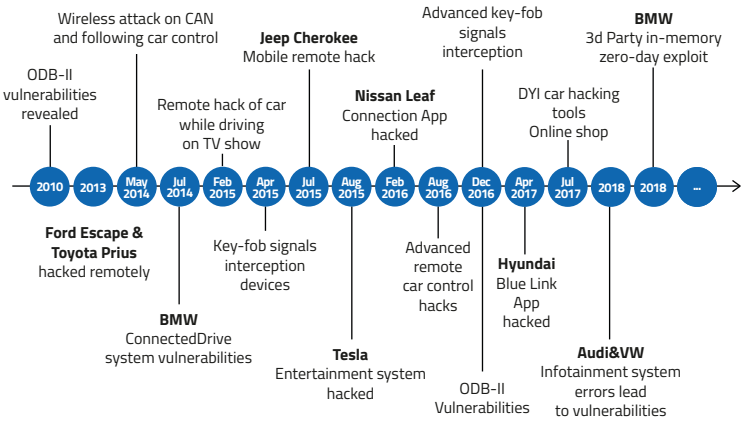
Brochure Automotive Security Management - An innovative approach for the further development of security management in the automotive industry

The different incidents of the hacking timeline show that there is a threat potential for automotive in cyberspace

The transformation of the automotive industry is progressing rapidly. The four main trends in Mobility are: Electrified, Connected, Automated, Shared. The industry must find answers to these challenges. This is only possible with digitized and communicating automobiles, the so-called connected cars. Connected cars also mean the connection between systems that do not trust each other. This requires a sufficient level of cyber security, because through stronger networking, additional interfaces and functionalities drastically increase the attractiveness of an attack on vehicles and the connected infrastructure by hackers.

The various incidents of the hacking timeline show that there is a threat potential for the automotive industry in cyberspace. This threat potential may only be given today through specific components, yet it will grow rapidly as a result of digitalization and networking. According to experts, hacker groups such as Group123, Dark Hotel or Mofang are active in the automotive sector. Thus, highly developed hacker groups face an industry that is now merely starting to use digitalization, communication and networking in full breadth and depth.

And connectivity means not only connecting vehicles to the Internet or to other vehicles, but also, under certain circumstances, to the electricity network. In the future, electric vehicles could also become part of the power network and communicate with this technology. Controlled by hackers, they could themselves become an attack vector on the power grid. Considerations of this type exist.



Connected Cars will thus provide rapid growth to such threat situations. The attack vectors can no longer be assigned to a single corporate or IT domain with regard to the effects on vehicle or component production. Looking at the development process in the enterprise, an attack on the software development environment for vehicle components that is operated in the office communications environment can later lead to malfunctions of a component in the vehicle. Protection requirements that are only defined in one department, domain or production unit and that are not subject to a global consideration and control, will not be effective in the long run and will fail.

This does not look any different at the level of a vehicle. A vehicle consists of various digital domains such as chassis control, body control, assistance systems or infotainment, some of which are safety-relevant, some not. All systems consume or generate data. To control and manage these digital functions, typical automobiles of the current decade have over 100 microprocessors, several dozen electronic control units, several kilometers of cable and about 100 million lines of software code. Undetected weak points are therefore unavoidable. A comprehensive threat and vulnerability management system must exist, as must an incident handling process.

Furthermore, security-relevant system developments are becoming increasingly complex, leading to ever greater demands upon the manufacturers and their suppliers. In order to gain the necessary product safety, it is necessary to develop according to the state of the art, in order to be able to prevent possible product liability claims. The aim is to ensure the functional safety of the corresponding products, systems and processes. Security contributes to this.

Security-relevant system developments are becoming increasingly complex

VEHICLE SECURITY

Vehicle Security includes the elements necessary for the safe operation of a vehicle

Safety means the protection of people and the environment. Security means the protection against malicious actions. Data protection or user data privacy protects personal data from misuse. If one considers the functionality of vehicles, the functional safety of vehicles, vehicle parts, products and services must also be guaranteed when using digital components. Security protects the operational and safety-relevant functions of a vehicle as well as the privacy of the users of the vehicle.

Vehicle security comprises the elements that are necessary for the safe operation of a vehicle, in particular for automated or autonomous vehicles. Added to this are purchased components or services from a supplier and parts of the supply chain that relate to digital elements. These components, services or parts are also subject to numerous cyber risks that are unknown to a manufacturer or an integrator and must therefore also be controlled by a Cyber Security Management System (CSMS). Maintenance and operation of components, services or vehicles that may produce personal data must also be considered and must be specially protected. Examples include Internet-related devices and apps (IoT devices) that communicate or interact with vehicles or products.

AUTOMOTIVE SECURITY MANAGEMENT

ASMS is a comprehensive and promising approach

New approaches and ideas are currently being discussed in the automotive sector as to how cross-company security management can be achieved. The need arises from the necessary interaction of different corporate units, the common goal of protecting functional safety, and the connectivity and fusion of digital systems with business IT. Thus, a security management approach is searched, which connects the areas of business, production and product with one another. At the same time, there are numerous requirements for manufacturers and suppliers that can result from data protection, certifications or compliance audits, such as ISO 27001 or TISAX, for which VICCON has developed a risk analysis method. Furthermore, there are international frameworks such as that of the UN ECE, which influence vehicle security and product liability and requires a CSMS.

VICCON pursues a comprehensive approach in the form of an Automotive Security Management System® (ASMS) for automobile manufacturers and automotive suppliers that takes the supply chain into account. The production of a vehicle or a vehicle component can be divided into different phases which interact closely with business processes. A common and efficient protection across all business units and production sites should be provided in order to achieve the overall goal of a secure digitized product. To this end, existing and future standards for cyber security and information security are combined and applied.

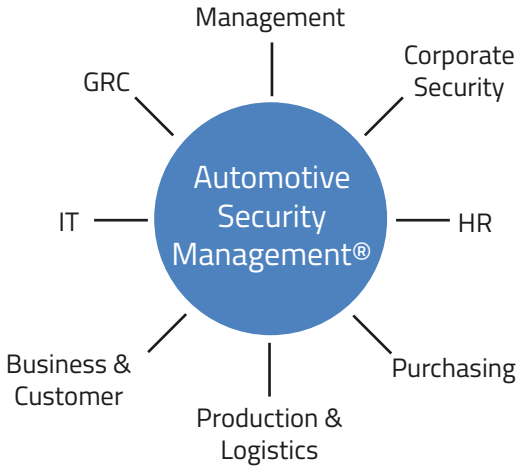
Automotive Security Management System®			
Business Process Information Security Knowledge Protection / Information Security / Data Protection			
Concept	Product Development	Production	Operation, Maintenance
Protection of Prototypes	Protection of Engineering Systems	Protection of Production Systems/Machines	Protection of Operational Systems / Maintainance Data

DIGITAL TRUST AND SECURITY STRATEGY

The production of vehicles or vehicle components is of course not limited to the purely digital aspects. Controlling globally distributed business processes at different locations, global logistics and dealing with different cultures and travelling employees requires comprehensive security management at company level, combined with the functions Governance, Risk and Compliance (GRC). The management and the specialized business interfaces must be considered and corresponding processes and instruments must be further developed and adapted to one another. Moreover, the question arises as to how awareness raising, knowledge transfer, agile work and collaboration can be meaningfully organized in the fast-moving world of trends, products and employment relationships.

The value of material goods perceived by the customer is shifting in favour of immaterial goods and services. Vehicle-related services must be available regionally and internationally, function safely and be reliably available. This requires the cooperation of many areas. New capabilities must be integrated into existing structures. The price of the modern, digital world is greater complexity, real-time reactions and a variety of wishes.

Trends and topics such as industry 4.0, digital trust, resilience, networked society and new work must be incorporated into future reflections. VICCON processes such requirements in a security strategy from which concrete measures for the future work of the security departments and the entire company are generated with a methodical approach.



Strategic proceeding considers relevant requirements, rends and developments and enables a future view on security

ADVICE - DIALOG - KNOWLEDGE TRANSFER - IMPLEMENT - EDUCATE

For about 20 years, VICCON has supported organizations in understanding security-relevant developments, building up the necessary know-how and processes for them, thus allowing them to control them securely.

With you and in dialogue with all company levels, VICCON develops ideas and seeks a suitable orientation for the security policy in the light of the different requirements.

VICCON develops strategies for secure and resilient organizations, follows the digital transformation and advises on the implementation of these strategies in the form of Next Generation Security Management.

VICCON pursues the goal of strategically anchoring security in the company according to management and business policy. Particular emphasis is placed on information security management, the management of cyber risks as well as prototype and know-how protection.

CONTACT

For further information please contact us:

VICCON GmbH

Ottostrasse 1
76275 Ettlingen
Germany

Phone: +49 7243 719734
Fax: +49 7243 719704

E-mail: info@viccon.com
www.viccon.com

VICCON

CONSULTING