ŠKODA CYBERSECURITY

WHITE PAPER

ŠKODA | Škoda Group

ALL MOBILITY OPERATORS ARE IMPLEMENTING A CYBERSECURITY STRATEGY.

Cyber-attacks are growing and create a threat to mission critical systems including mobility. In the USA, cybersecurity in transport is seen as a national threat. In Europe, the Cybersecurity Act unifies the EU's cybersecurity into a single framework, with ENISA as its main core. All mobility operators are implementing a cybersecurity strategy. There are 2 major trends that triggered this evolution: 1. digitalisation, 2. new regulation.

MAJOR DIGITAL TECHNOLOGICAL EVOLUTION

Due to increased competition and needs for better service, operators and infrastructure managers must drastically improve the transportation system operational efficiency (availability, capacity, punctuality) as well as provide better passenger experience and comfort. There is also a second trend, namely the mobility revolution and more generally Smart Cities. A holistic approach of the multimodal mobility system is the answer providing passengers a global door to door proposal.

Recent new technology (5G, cloud-based systems, artificial intelligence, IOTs, etc.) and development methodology (lean start-up) offer the proper foundations to build these new mobility systems. Connectivity inevitably increases the vulnerability to cyber-threats. Increasingly more digital systems also expand the attack surface and the number of vulnerabilities.

These trends expose mobility operators and the public to unprecedented levels of cybersecurity risk. Advanced Persistent Threats (APT) are the main danger for the mobility sector. Depending on the geopolitical situation, these APTs may have the support of some major countries.

With these risks the transportation system Quality of Service (QoS) could be affected (transportation system reliability), as would passenger safety and, more generally, operator and supplier reputational damage.

MAJOR REGULATION EVOLUTION

An additional challenge is the new cybersecurity regulation, e.g., in the USA and EU. EU member states will have to adopt a national strategy to transpose the NIS2 and CER directives into national law. EU members will also have to conduct regular risk assessments to identify those deemed critical or essential to society and the economy, During this time, member states will adopt and publish the measures necessary for their implementation.

THE FIRST REGULATION IN EUROPEAN COMMUNITY IS BASED ON:

- The 2019 Cybersecurity Act introduced, which strengthens the role of ENISA by giving the agency a permanent mandate and more financial and human resources.
- Directive of 6 July 2016, on measures for a high common level of security for networks and information systems within the EU (NIS Directive).

At the end of 2022, two key directives on critical and digital infrastructure entered into force, strengthening the EU's resilience to criminal threats from cyber-attack, public health threats or natural disasters. These adopted directives are:

- Directive on measures for a high common level of cyber security across the EU (NIS Directive 2).
- Directive on Critical Entity Resilience (CER).
- Cyber Resilience Act (CRA) prepared by the EU.

NIS2 strengthens the cyber risk management requirements that companies are required to comply with, and will streamline incident reporting obligations with, among other things, more precise provisions on reporting procedures, information scope and time limits for reporting.

Faced with an increasingly complex risk landscape, the new CER directive replaces the 2008 European Critical Infrastructure Directive. The new rules will strengthen infrastructure resilience to a range of threats including natural hazards, terrorist attacks, insider threats and sabotage. Eleven sectors will be covered, including transportation.

ŠKODA IS COMMITTED TO DELIVER SOLUTIONS FOR MODERN AND SUSTAINABLE MOBILITY

Modern mobility operations will have an increased efficiency thanks to digitalisation. Digital technology (big data, artificial intelligence, IIoTs, telecommunications, etc.) is instrumental in helping mobility operators face their new challenges i.e.:

1. to increase the quality of service (availability, reliability),
2. to reduce operation costs under the pressure of increasingly more open competition.

This major technological evolution must be implemented while maintaining the major characteristics of the transportation vital system, especially its safety.

ŠKODA IS PRESENT IN THE MOBILITY BUSINESS THANKS TO A COMPREHENSIVE MOBILITY PORTFOLIO INCLUDING:

1. railways, which is the backbone of the mobility system, including urban use with trams or mainlines with regional trains,
2. road with bus transport including battery bus, trolley bus, fuel cell hydrogen solutions including ECUs, converters and chargers including diagnostics tools,
3. services including the Premis/Astrid predictive maintenance tool,
4. future autonomous driving including smart depot and obstacle detection,
5. MACS multimedia system for passenger information and comfort,
6. other embedded SW and HW products.

Škoda's main objective is to propose secure systems for its complete offer. In order to respond to technological trends and EU regulations, Škoda management launched a programme with the following objectives:

1. implement certified CSMS,
2. 'cybersecure by design' product portfolio for both railways and road operators,
3. vulnerability management, which consists of monitoring vulnerability information, identifying system vulnerability, assessing risks and updating systems or applying other mitigation measures,
4. building a mature CySe team.

ŠKODA IS COMMITTED TO DELIVER SOLUTIONS FOR MODERN AND SUSTAINABLE MOBILITY.

CYBERSECURITY HAS IMPACT ON MAJOR COMPONENTS OF MOBILITY SOLUTION.

ŠKODA CYBERSECURITY PROGRAMME

Cybersecurity has an impact on major components of a mobility solution: telecommunications, vehicle, maintenance systems. It has also an impact on all the mobility system life cycle from requirement definition to after sales activities. The Škoda cybersecurity programme has been structured in several axis. This programme also includes Škoda partners and subcontractors.

One key element of the cybersecurity programme is related to awareness of the whole organisation and training of Škoda employees. The objective is to support customers in all phases of a project from commerce to project delivery and maintenance.

A second key programme element is to develop “cybersecured by design” solutions. In order to comply with EU regulations and with customer cybersecurity requirements, a decision was made to use well established industry standards such as IEC 62443 and CENELEC TS-50701 for railways and ISO/SAE 21434 / UNECE R155, UNECE R156 for buses. In parallel, Škoda is a member of European standardisation groups like IEC 63 452 to anticipate future customer requirements.

Even with these sets of standards, Škoda will implement a single strategy for bus and railway solutions. This will help to speed up the implementation, but also will implement all conservative/necessary measures to migrate to autonomous vehicle with high A-SIL level.

During the project deployment phase, Škoda teams are identifying the main cybersecurity risks and design solutions to mitigate the primary vehicle risks or complete systems integrating vehicle and wayside products within customer partnerships. Solutions are based on the Škoda “cybersecured by design” products.

Škoda cybersecurity is also involved in after sales activities. This is a long-term activity. To support its customers, Škoda plans to offer a set of services including cybersecurity maintenance, vulnerability/ patch management, auditing, etc., for safety and non-safety systems. It will also include a Security Operation Centre (SOC) to continuously monitor and improve security while preventing, detecting, analysing and responding to cybersecurity incidents. Some rail specific functions will also provide recovery decision support to operators.

Škoda vehicle and way side products as vital systems can’t afford to be affected by cyberattack. This is not just a question of service quality or economic loss. It is also a matter of passenger safety.

In line with best practices and cybersecurity standards, Škoda is committed to support operators with the proper skills and cybersecured by design solutions for transportation system implementation, maintenance and security supervision activities with rail specific detection and recovery functions.

Škoda Group
skodagroup.com