Case Study

Implementing a Cyber Security Management System for UNECE-155 Compliance in Vehicle Manufacturing

Our client pioneered the world's first double-decker hydrogen fuel cell bus. Today, they stand as a trailblazer in constructing zero-emission vehicles, propelling the transportation industry into a new era of energy efficiency with their fuel cell technology.

In response to the ever-evolving landscape of cyber security threats, it is imperative for our client to proactively evaluate and fortify cyber security across its vehicles' infrastructure and components. To withstand cyber attacks, vehicle manufacturers need to establish detection and response protocols to address security incidents across the entire lifespan of their vehicles

> As vehicles become increasingly connected and autonomous, they become more vulnerable to attacks. As a result, cyber security needs to be considered at the earliest stages of vehicle development

Methods were commissioned to deliver and implement a Cyber Security Management System (CSMS), that enabled our client to demonstrate compliance with automotive regulation UNECE-155 and obtain vehicle type approval for a vehicle delivered into Germany.

The UNECE Regulation No.155 is a legally binding regulation that establishes requirements for the cyber security of vehicles and associated systems. It applies to all new types of vehicles approved for use in countries that are members of the United Nations Economic Commission for Europe (UNECE). UN-155 was developed to address the growing risk of cyber attacks on vehicles.

Why is UNECE-155 important?

UNECE-155 compliance is a pivotal component of regulatory adherence crucial for our client. It serves as the cornerstone of their operational framework, ensuring that their vehicles meet the necessary standards and requirements for sale in relevant markets. Without adhering to UNECE-155, our client would face significant barriers in commercialising their vehicles, potentially leading to market exclusion and hampering their ability to compete effectively. Therefore, implementing UNECE-155 is not just a procedural requirement but a strategic imperative for our client to maintain its market presence and uphold its reputation for quality and compliance within the transportation industry.

Methods covered all areas of a CSMS implementation including the creation and delivery of:

- A vehicle Threat Assessment and Remediation Analysis (TARA), and methodology to support the identification and assessment of cyber security risks
- Technical remediation analysis to implement security controls to mitigate risks
- A suite of documents including but not limited to policies and procedures that aligned with best practice and support the organisation in establishing the CSMS
- Process establishment for assessment and assurance across the supply chain
- Supporting documentation and process improvements across incident response and supply chain assurance to be integrated with existing processes

Outcomes

We developed and delivered several key components/processes to support the implementation of an effective CSMS that would meet client requirements. The implementation of industry best practice (ISO21434) supports our client in meeting regulatory (UNECE-155) requirements. We delivered the following activities:

Gap Analysis
Performance of gap analysis against industry standards ISO21434 to assess the current cyber posture across the organisation, position the scope of delivery, and provide recommendations to ensure best practice guidance to meet UNECE-155.

Statement of Applicability
Established a Statement of Applicability (SoA) to create a central document used by both the security auditors and organisation to improve understanding and provide clear direction through the CSMS process controls. The SoA supported and explained succinctly the cyber security controls that are relevant to the vehicle and the business.

Risk Management

Delivered a Threat Assessment and Remediation Analysis (TARA) document that assessed the cyber risk across the vehicle. The TARA enabled our client to remediate identified cyber risks, establish ongoing continuous risk management processes, and support informed risk decision-making.

We helped deliver a risk framework and methodology to support risk assessment and risk management activities. These deliverables enable the client to ensure that best practice is adopted, assessing vehicle components for vulnerabilities and understanding emerging cyber security threats and risks posed to a vehicle and their associated systems.

Ongoing knowledge transfer will further enable the client to be able to not only establish effective risk management as a repeatable framework, but also to consume risk assessment in-house as part of transition activities.

Supply Chain

We developed a supplier assurance process to assess compliance of third-party suppliers and a self-assessment questionnaire delivered across the supply chain of the vehicle to assess the security posture of the supplier. A dashboard was created to support reporting, and a supplier risk register to enable management of risk, together with action plans for our client to support continuous remediation activities.

Incident Response/DR&BC

We created procedures for incident response, clear policies, processes, and tools to be integrated into existing incident management processes and support the manufacturers' ability to respond to a cyber incident. In addition, we will ensure that as part of continuous improvement, a capability for detection and analysis of cyber security threats and vulnerabilities is defined. Effective threat monitoring will ensure that our client can:

a) detect and prevent cyber attacks against vehicles of the vehicle type
b) support the monitoring capability of the vehicle manufacture to detect threats, vulnerabilities, and cyber attacks relevant to the vehicle type.

Understanding UNECE-155 and implementing a CSMS is essential for vehicle manufacturers striving to adapt to the swift digital evolution and safeguard their customers against cyber threats. By establishing resilient cyber security measures and effective software update management systems, manufacturers can guarantee the safety and security of their vehicles, enabling consumer confidence in their vehicles.

Methods' Added Value

As a manufacturing organisation in the automotive sector, cyber security regulations, good practice, and standards are relatively new, and cyber security was not fully embedded across the organisation. As well as supporting delivery to meet audit requirements and obtaining of UNECE-155, we have been integral in educating and raising awareness of cyber security risks and vulnerabilities which may compromise the vehicles and have a detrimental effect on the organisation. Our tailored approach has provided our client with direction on how they embed cyber security, as well as raise the significance of adopting cyber security best practice as part of the engineering lifecycle.

Implementation of the Methods CSMS will enable knowledge transfer across the organisation and ensure a top-down approach to driving continuous improvement.

> To meet the requirements for an audit by the Vehicle Commissioning Agency (VCA) and enable our client to fulfill their order in Germany, we had to work within challenging timescales. We successfully delivered CSMS deliverables and a Vehicle Threat and Remediation Analysis (TARA) document, aiding our client in achieving compliance with industry regulations.

Next Steps

We continue to work collaboratively with Alten and our client to further embed cyber security, including threat intelligence monitoring and incident response, general cyber security training and awareness, supply chain, and risk management, across key functional areas

We undertook support improvement activities following the audit, establishing cyber security specific roles and responsibilities and engaging with senior stakeholders and management across the organisation to support the transition into an in-house capability through effective knowledge transfer and tailored training.