CYBERSECURITY

Cybersecurity White Paper

INTRODUCTION

Digitalisation is bringing substantial benefits in transportation operational efficiency (availability, capacity, punctuality and maintainability), as well as better passenger experience and comfort. It also inevitably increases the vulnerability to cyberthreats. These trends expose mobility operators and the public to unprecedented levels of cybersecurity risks.

With these risks, the transportation system Quality of Service (QoS) could be affected (transportation system reliability), passengers' safety and more generally operators reputational damages. Cyberthreats could also affect passengers' computers and mobiles.

Cybersecurity approach must provide for the in-depth protection needed to defend against security threats, while ensuring that transportation operators are prepared to meet their compliance obligations.

An additional challenge is the trend to integrate more and more IT technology and standard telecommunications (TCP/IP, 4 & 5G, WiFi) within a transportation vital system. This will not only have an impact on the architecture design of the transportation system, but also in the maintenance phase to consider new threats during the whole lifetime of the system.

CAF: A LONG-TERM RELIABLE PARTNER FOR SAFETY AND CUSTOMER OPERATIONAL EFFICIENCY

Digital technology (artificial intelligence, IIoTs, big data, telecommunications, blockchain, etc.) and standard products such as COTS will be instrumental in helping mobility operators to face their new challenges i.e.:

- To increase the quality of service (availability, reliability),
- To increase the capacity of transportation systems, minimizing the investment level,
- To reduce operation costs under the pressure of more and more open competition.

This major technological evolution must be implemented keeping the major characteristics of the transportation vital system and with special attention put on safety.

CAF is present in the mobility business thanks to a comprehensive transportation portfolio, including: 1) railways, which are the backbone of the mobility systems, 2) road, as the European leader in the bus business. In terms of value chain, CAF is also present in activities including financing, global turnkey projects, rolling stock, signalling, components and services like traditional or predictive maintenance.

CAF's priority objective has always been to provide safe systems in respect to operators' operational efficiency. Facing these new threats, CAF decided at an early stage to launch an initiative with the objective to have the right level of maturity of CAF internal team skills and cybersecured by design products and systems portfolio for both railways and road operators.

CAF CYBERSECURITY CAPABILITY AND PORTFOLIO

Cybersecurity has an impact on telecommunications, products, cybersecurity risks management, including safety, operation security, maintenance during the whole lifetime of transportation systems and last but not least awareness and training of customers' and suppliers' staff. CAF cybersecurity program has been structured in several axis to cover all aspects needed including CAF partners and subcontractors.

- One key axis of the cybersecurity program is related to the awareness and training of CAF key employees. The objective is not only to ensure CAF's cultural maturity level, but also to support customers in all phases of a project from commercial to project delivery and maintenance.

- A second axis objective is to ensure the delivery of "cybersecured by design" solutions. A decision was made in addition to national standards to follow well-established industry standards such as IEC 62443 and CENELEC TS-50701 for railways and UNECE R155/156 for buses.

  CAF cybersecurity supports customers all along the transportation systems deployment and during the multiple decades operation phases including maintenance and security supervision: during the systems deployment phase, by identifying in partnership with customer's main cybersecurity risks and implement proper design mitigation using CAF's "cybersecured by design" products,

- In addition to project delivery, there is a need to support customers thanks to threats & the vulnerability watch and management, patch management, Security Operation Centre (SOC) to continuously monitor and improve a security posture while preventing, detecting, analysing, and responding to cybersecurity incidents. CAF has defined a roadmap to develop tools to implement these activities. Next steps will take into account return of experience of first deliveries and will anticipate customers' new needs due to the maturity increase of the transportation industry.

- One axis is dedicated to cybersecurity innovation. Cybersecurity has been included in the global CAF innovation process. Keeping CAF cybersecurity offer on the leading edge of the technology will allow CAF customers to ensure passenger safety, transportation systems operational efficiency and passenger comfort.

Railways as vital systems shall be able to operate safely when they are under attack, something that cannot be avoided, protecting critical systems developed under the concept of cybersecurity design. It is not just a question of quality of services or attacks of passengers' electronic equipment or economical losses, it is also a matter of safety for passengers.

In line with best practices and cybersecurity standards, CAF is committed to support operators with the proper skills and cybersecured by design solutions for transportation systems implementation, maintenance, and security supervision activities.

QUESTIONS & ANSWERS

Is the transportation industry facing many cyberattacks?
Compared to the cybersecurity IT area, transportation industry is facing a rather low number of attacks. However, transportation systems are systems of vital importance. The consequences could be disastrous and detrimental to operator's reputation. In term of attackers, advanced persistent threats (APTs) are the most dangerous for our industry. They have important financial means and under the control of states. Recent events like the Ukraine war have pointed out the urgent need to reinforce cyber-protection. The trend of digitalization and standardized telecommunications will increase the number of attacks.

Which are operators' needs and requirements?
The level of cybersecurity maturity is still very different from an operator to the other. CAF has some projects in countries where the level of requirements is high. The minimum for these countries is to deliver "cybersecured by design" products and systems. In addition, during the lifetime of the transportation vital system, frequent updates must be implemented to face evolving threats.

Which is the impact of cybersecurity on driverless systems?
Driverless train technology is used in metro, but will be integrated tomorrow in mainline, buses, trams. This is a major trend of the industry due to the need to increase capacity and quality of service of transportation systems. It will generate a need for an additional area of risk analysis. This is due to the fact that no human will control the decision process and automatisation level will be based on more standard telecommunication between trains/buses on-board products and trackside.

Which is the impact of cybersecurity in the day-to-day activity of CAF projects?
It is of outmost importance that cybersecurity is integrated in the whole project lifecycle from requirements analysis to system certification at the end of the project. It is very similar to the safety activity. One major difference specific to cybersecurity is the importance to ensure at the design stage that maintainability of the system will be taken into account, as cybersecurity will imply frequent patches in order to mitigate new threats.