Swedish Civil
Contingencies
Agency

GUIDELINES

Cybersecurity in Heavy Rescue Vehicles

Cybersecurity in Heavy Rescue Vehicles

Fire and Rescue Section

Cover photo: Johnér
Text: MSB in cooperation with FOI

Publ no.: MSB2181 - April 2023
ISBN: 978-91-7927-373-6

Swedish edition: Cybersäkerhet i tunga räddningsfordon MSB2122 - January 2023

Foreword

Developments in technology and digitalisation are progressing rapidly. The work with cybersecurity has not kept up at the same pace. This means that both individual organisations and society as a whole are vulnerable to various types of cyber threats. To achieve the best cybersecurity level possible, it is important to work both proactively and reactively.

The number of computer systems in a typical modern heavy vehicle is already considerable, and the number of radio connections installed is on the rise, which also increases the vulnerability of vehicles to remote cyberattacks. The vehicles used by the fire and rescue service are customised special-purpose vehicles with superstructures and extra equipment that are specific to the operational demands of the fire and rescue service. These superstructures are often third-party systems, i.e., systems that are installed in vehicles by a supplier that is not the original manufacturer. These installations expand potential attack surfaces and increase the risk of successful cyberattacks in the future. This, in combination with the long service lives of vehicles for the fire and rescue service, leads to the risk of security deficiencies persisting for a prolonged period of time, makes it urgent to increase the competence of procurers and users in the area of cybersecurity.

The purpose of these guidelines is to provide support concerning cybersecurity in the procurement of vehicles for the municipal fire and rescue services, and increase awareness of what needs to be taken into account when converting, operating and maintaining this type of vehicle.

The guidelines were prepared in collaboration between MSB and the Swedish Defence Research Agency (FOI) and are based on standards, research articles and industry-specific guidelines. A number of interviews and study visits to municipal fire and rescue services have also been carried out, as well as interviews with superstructure suppliers and with vehicle manufactures.

Karlstad, 30 December 2022

Patrik Perbeck

Deputy Head of Civil Protection Department, MSB

Content

Introduction

Vehicles, like many other things in society today, are increasingly connected to networks. Vehicles are no longer just a collection of mechanical parts, but now also contain electronic components and computers. This increases the risk of something going wrong, for example during software updates. The focus of these guidelines, however, is on antagonistic threats. Cyberattacks on vehicles can have serious repercussions because they can affect vehicles while driving. Such an event could have major consequences not only for the driver and passengers, but also for other road users. In the case of heavy trucks, it could also have societal affects, such as an accident involving the transport of hazardous goods. Serious societal impact would also occur if the cyberattack put a rescue vehicle or its special functions out of operation. This is especially true for heavy fire vehicles, as the availability of vehicles with fire-fighting and life-saving functions is critical for the fire and rescue service to be able to intervene effectively.

Heavy rescue vehicles are customised special-purpose vehicles with superstructures and extra equipment that are specific to the operational demands of the fire and rescue service. However, they contain the same technology as other types of heavy trucks. This means that heavy rescue vehicles have many of the vulnerabilities that exist in other heavy trucks. The fact that many fire and rescue services use vehicles from a small number of suppliers also means that many vehicles can be assumed to share the same vulnerabilities. A cyberattack (targeted or not) can thus affect many rescue vehicles at the same time.

When updating software, it is important to follow the municipality's policy for information security to ensure, among other things, that malicious code is not spread from one vehicle to another, for example when using a USB flash drive.

In order to minimise the number of vulnerabilities, information security and cybersecurity must permeate the development, production, use and maintenance of heavy rescue vehicles. This will make it possible to prevent cyberattacks from affecting availability.

Purpose and target audience

The purpose of these guidelines is to provide support in cybersecurity to municipal fire and rescue services in their work when defining requirements, purchasing and converting heavy rescue vehicles. This support may also be relevant for other types of emergency vehicles. The guidelines are primarily directed at municipal fire and rescue services, but also anyone who procures or uses rescue vehicles.

Explanation of terms

Table 1. Definitions of terms used.

Term	Definition
Cybersecurity	All activities necessary to protect network and information systems, users of these systems and other affected persons against possible actions, circumstances, or events that adversely impact the network, information systems and people. Cybersecurity is primarily about addressing antagonistic threats.
Extra equipment	Everything that is installed, apart from superstructures. This includes communication systems, emergency lights, generators and pumps.
Basic vehicle	Different types of vehicles with chassis, drivelines, cabs and similar, on which different superstructures can then be built.
Limp-home mode	Limp-home mode is an engine function that enables the vehicle to be moved with limited capacity in the event of certain problems that would otherwise mean a complete shutdown.
Information security	Protecting information so that it is always there when we need it (availability) that we can trust that it has not been tampered with or destroyed (accuracy), and that only authorised persons can access it (confidentiality). Information security is about protecting the information itself, regardless of the medium through which it is conveyed. Information security is achieved by taking administrative, organisational, technical and physical measures.
Infotainment system	Infotainment systems in vehicles refer to the equipment that is mainly associated with entertainment in the vehicle. In modern vehicles, this usually means some sort of integrated touchscreen, but in some cases it may also refer to a digital instrument display or dashboard.
Truck	A vehicle that is primarily designed to transport goods or a vehicle that cannot be defined as a passenger car or bus.
Superstructure	Something large and mainly mechanical that is permanently mounted on the vehicle’s chassis, such as tanks, cabinets and hooklifts. Superstructures are normally mounted where the bed would be on a regular flatbed truck.
Heavy truck	A truck with a total weight over 3.5 tonnes.
Heavy rescue vehicle	Heavy rescue vehicles are basically heavy trucks that have been modified. The fire and rescue services’ heavy vehicles can be broken down into three main types: 1. fire engine 2. water tender 3. aerial apparatus. There are also other types of specialised vehicles, such as rescue vehicles for chemical accidents or for emergencies requiring water diving.

Scope

These guidelines comprise support for protecting heavy rescue vehicles from cyberattacks. The primary focus is on protection against antagonistic threats, but following the recommendations will also greatly reduce the risk of other incidents, such as those caused by operator errors. All types of vehicles that fall outside the definition of heavy trucks, such as passenger cars, buses, off-road vehicles, trailers, towed machines/equipment and heavy machinery, fall outside the scope of these guidelines. There are points of contact with other vehicles, however, such as command and control vehicles and smaller rescue vehicles, where parts of these guidelines may be useful.

There are also other risks and vulnerabilities related to vehicles that do not directly relate to cybersecurity, such as physical sabotage and electromagnetic interference. These are not covered by these guidelines.

Background

Digitalisation and developments in the automotive sector have led to the fact that vehicles are now complex systems with large amounts of code[1]. Inside vehicles, various information systems communicate with each other to control basic functions and provide advanced functionality, among other things, to support the driver (driver assistance). Headlamps can, for example, be controlled through data communication instead of a mechanical switch.

This chapter provides an introduction to heavy rescue vehicles and how they differ from other types of vehicles. It also describes how vehicles are ordered and how service and maintenance are performed after a vehicle is taken into service. Finally, it provides an introduction to cybersecurity basics in relation to vehicles, as well as a discussion on the threats and risks that apply for heavy rescue vehicles.

Heavy rescue vehicle

Heavy rescue vehicles are heavy trucks modified for the fire and rescue service. A cement truck and a heavy rescue vehicle could be built on the same basic vehicle, but their respective areas of operation and appearances are very different. The basic vehicle is equipped with superstructures and extra equipment that give the vehicle the functions that the fire and rescue service require. A fire engine, water tender, turntable ladder or other special-purpose vehicle can be created from the same basic vehicle. However, different types of basic vehicles may be required for different types of special-purpose vehicles.

A vehicle of the fire engine type is equipped with various extinguishing tanks, pumps and hoses; see Figure 1. It also has life-saving tools and equipment in roll-front cabinets. The cab of the vehicle contains communication equipment, including the Rakel communication system (TETRA), and in some cases also screens with command and control information.

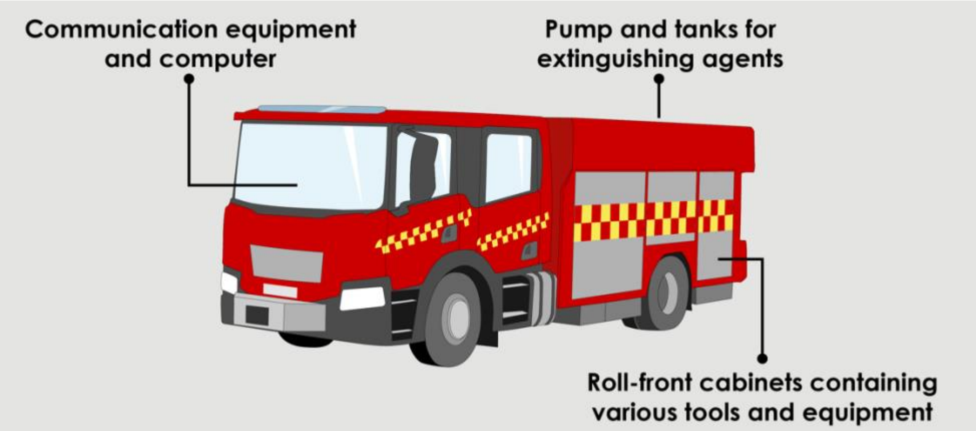
Communication equipment and computer
Pump and tanks for extinguishing agents
Roll-front cabinets containing various tools and equipment

Figure 1. Rescue vehicle with superstructures.

[1] According to a study by Vard Antinyan (2020), a vehicle from Volvo had about 100 million lines of code.

Heavy rescue vehicles generally have a long service life in comparison with other types of heavy trucks. This is mainly due to the fact that they are not used as frequently, and mileage and wear and tear on the vehicles are therefore low. Because it is a big investment for municipalities to acquire these types of vehicles, they also need to last for a long time and be well-maintained. It is of great importance for the municipality that the vehicle and associated rescue-related equipment have a high level of performance and availability, which means that they must be able to be used and function properly when they are needed.

Ordering process

As previously described, the manufacture of a heavy rescue vehicle begins with a basic vehicle. The basic vehicle is manufactured in its entirety by a truck manufacturer (such as Scania or Volvo). The basic vehicle is then sent to a superstructure supplier, which builds and installs superstructures and extra equipment on the vehicle. The fire and rescue service can also install extra equipment in the rescue vehicle, such as communication equipment.

A typical, but simplified, ordering process is shown in Figure 2.

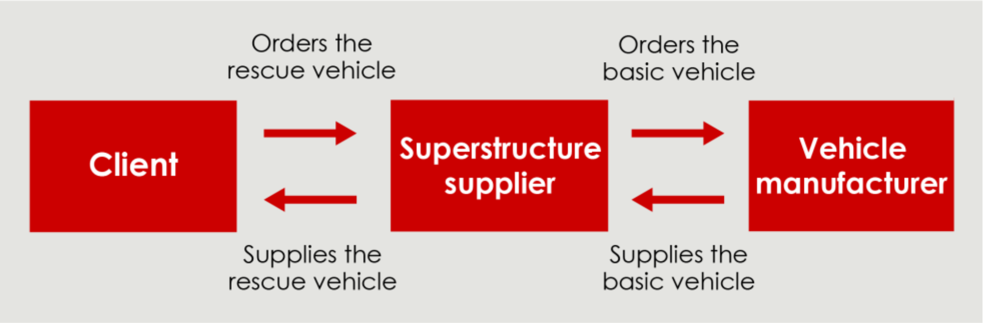
Orders the rescue vehicle
Orders the basic vehicle
Client
Superstructure supplier
Vehicle manufacturer
Supplies the rescue vehicle
Supplies the basic vehicle

Figure 2. Ordering process.

Many superstructures need to be integrated with units in the basic vehicle. Pumps for extinguishing agents, for example, need to be integrated with the vehicle's engine in order to run. To minimise the risks with integration, vehicle manufacturers generally implement superstructure interfaces, also called gateways, in the basic vehicle. These types of interfaces simplify the superstructure supplier's work by ensuring that the way the supplier's equipment communicates with the basic vehicle's equipment is clearly specified.

Vehicle manufacturers give instructions that must be followed when the basic vehicle is rebuilt or modified. If the instructions are not followed, the factory warranty for the vehicle becomes invalid.

Example: Scania’s instructions

Scania has instructions for superstructures and conversions that superstructure suppliers must follow. An authorised representative at a Scania dealer must approve superstructures and conversions that are not described in Scania’s superstructure instructions. After each superstructure or conversion, the superstructure supplier must certify that the superstructure and the work on the superstructure have been performed according to Scania’s instructions.

The superstructure supplier’s responsibilities also include ensuring:

- that the original function and quality of the chassis components remain after superstructure is completed
- the characteristics of the complete vehicle, to the extent the characteristics are affected by the superstructure
- that the superstructure meets legal, safety and suitability requirements
- that necessary instructions and information about the functioning and care of the superstructure are supplied with the vehicle upon delivery to the client
- that parts the superstructure supplier has put on the chassis are clearly marked with the supplier’s name and part number.

Both Scania’s dealers and the superstructure supplier are responsible for ensuring that requisite instructions and information are included with the vehicle at delivery to the client.

Service and maintenance

After a vehicle is taken into service, the vehicle continues to receive hardware and software updates through service and maintenance. Figure 3 shows the different actors that interact with a fire and rescue service vehicle after it has been taken into service.

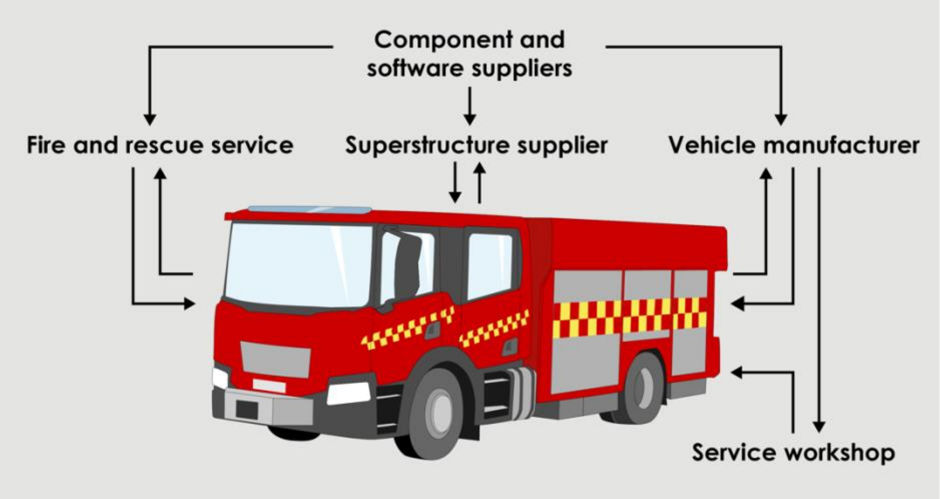

Figure 3. The rescue vehicle’s interactions with other actors.

Updates to hardware or software in the vehicle are installed by different parties depending on the type of update and which components are affected. If it is a basic vehicle, it is the vehicle manufacturer's responsibility to supply updates. These updates are normally installed at service workshops, which also perform regular service. If wireless updates are enabled, some types of software updates are installed directly by the vehicle manufacturer. Superstructures and extra equipment may also need updates because they can contain software and components that may need to be replaced. These updates are performed by the superstructure supplier. If the fire and rescue service have installed extra equipment, they are usually the ones who update these components.

Not all software and hardware are designed by the vehicle manufacturer or the superstructure supplier, however, but may also come from sub-suppliers. Sub-suppliers may supply updates that are then installed by vehicle manufacturers, superstructure suppliers or service workshops. It is therefore important that the contract specifies when the supplier's service contract expires and when security updates will no longer be provided. There should be a plan for how to deal with risks that could then arise, for example ensuring that the vehicle is able to be used offline.

To monitor that the vehicles are performing well, the vehicles may be equipped with a Fleet Management System (FMS). Information collected may include sensor data, position, distance driven, and route. The vehicle manufacturer may have an internal fleet management system integrated in the basic vehicle. Sometimes superstructure suppliers or fire and rescue services install their own fleet management systems. These fleet management systems may have their own wireless connections.

Cybersecurity in the vehicle

Information security

Information security is a prerequisite for cybersecurity and is often defined by the three aspects of confidentiality, accuracy, and availability. Availability is the most important aspect for rescue vehicles because the vehicles are necessary for life-saving activities. Accuracy is important to consider in relation to the vehicle's software and electrical systems, which are important components for the vehicle's functionality. Accuracy and confidentiality are also important to consider in relation to the information that is handled in connection with the vehicles. This might include objects to be rescued, individuals and personnel. Information that may need to be protected includes:

- location of facilities classified as needing protection
- information that the fire and rescue services need in their work, such as information about water mains and pumping stations
- call-out, departure and arrival times
- drawings of facilities to be protected

- information about firefighters
- vehicle location
- speed during call-outs
- other information that can give an idea of the fire and rescue service's collective capacity and actions.

Aspects of information security

- **Confidentiality** – that information is not disclosed to unauthorised parties.
- **Accuracy** – that information or functionality is not altered or destroyed by unauthorised parties.
- **Availability** – that information and functionality are available when they are needed.

Cybersecurity

Cybersecurity encompasses all activities necessary to protect network and information systems, users of these systems and other affected persons against possible actions, circumstances, or events that adversely impact the network and information systems and people.

Previously, devices used in vehicles had limited functionality and, above all, vehicles did not have the same possibilities of communicating with the outside world. Automotive developments over the past 10–15 years, however, have brought increasingly broader functionality, while communication possibilities have also increased. This, in turn, entails an increased risk that vehicles can be influenced by attackers. This increased risk has made cybersecurity an important aspect to take into account and set requirements on in terms of vehicle development, use and management.

Security functions that are normally used in traditional computer systems and networks can be difficult to use in vehicles. This is due in part to limitations in the technology used in the vehicles, but also to the fact that there are functions with high demands for real-time communication. Security functions that are introduced therefore need to be adapted to the purpose.

Threats to fire and rescue service

There are two general types of threats: intentional and unintentional. Intentional threats involve an actor with an active desire to cause damage. Unintentional threats involve mistakes or operator errors that can lead to serious vulnerabilities, which in turn can be exploited by an attacker.

The threat actor – the person carrying out the attack – can be categorised in various ways. It is usual to classify threat actors by technical or financial ability and motivation. They can be categorised into four different levels, according to how great the threat is:

- script kiddies
- hacktivists
- criminal groups
- state actors.

Script kiddies are opportunistic attackers, with relatively low skills and financial assets. The motivation of these attackers varies and can include financial gain or the desire to test something that they have learned.

Hacktivists have varying degrees of skills and financial means. What chiefly distinguishes this type of threat actor from script kiddies is motivation. Hacktivists are generally politically or ideologically motivated and are rarely driven by aspects such as financial gain.

Criminal groups in this context are almost exclusively motivated by financial gain and also often have the competence required to pose a relatively large threat.

State actors are those who have the largest budget and skills to carry out cyber-attacks, which makes them the most dangerous threat actor. The motivation for state actors can vary, but generally consists of some sort of desire to undermine the party being attacked.

The fire and rescue service are often spared from attacks, as the activities carried out by the fire and rescue service are generally perceived as good and important, even by individuals who do not always value society's rules and laws. However, there are threat actors who are motivated to direct attacks against the fire and rescue service. For criminal organisations, it can be very lucrative to use extortion, through so-called ransomware, to get at money from vital societal functions. State actors can be motivated by the desire to undermine the function of the service, indirectly affect another essential service, or to collect confidential information.

Attacks that are not specifically aimed at the fire and rescue service can also present problems. Criminal organisations can use various types of broad attacks (such as with Trojans or other malicious code) to gain access to different systems. This access can then be sold onwards to a third party that is specifically interested in the fire and rescue service. The threat actor can also intend to use the hijacked devices to attack someone else, for example in denial of service (DoS) attacks on the internet.

The fire and rescue service can also be indirectly affected by attacks aimed at a supplier in their supplier chain. Such attacks can spread through software updates, remote logins, etc. in which the supplier has access to users' systems.

Potential attack surfaces

Vehicles are exposed to their surroundings through their functions and the interfaces that exist to the outside world. Cyberattacks can either be carried out remotely or via physical access to the vehicle. If the vehicle is connected to the internet via wireless links, an attacker can attempt to affect the vehicle remotely. Various physical interfaces can be used to insert malicious code. This malicious code can be inserted directly by the attacker or indirectly, e.g. via software that a service technician installs.

This section provides an introduction to the different interfaces that exist in a vehicle that an attacker can attempt to exploit.

Physical interfaces

Interfaces that allow data transfer provide attack surfaces for an attacker who wants to transfer malicious code. If they are connected to the internal communication network, malicious code that comes in via the interface can have a great impact on the vehicle's critical functions. The basic vehicle has several types of physical interfaces for data communication. There may also be physical interfaces on superstructures and extra equipment, for example for updates.

Vehicles have a diagnostic socket (OBD-II/EOBD[2]), which is primarily used to read fault codes and messages from the vehicle's control units. The socket can also be used to update software. This type of socket enables communication directly to the vehicle's internal critical control units. The vehicle can then be fully exposed to connected equipment, but this is often supplemented with some type of authorisation check. There are also OBD-II adapters for monitoring and management of the vehicle fleet that communicate over the internet, which further increases exposure. When a vehicle undergoes regular vehicle service, various software updates are often included. These are usually done by connecting a computer to the vehicle via the OBD-II port. It is conceivable that the service station's or workshop's IT systems could be exposed to attacks in which an attacker is seeking access to service computers.

There are also other physical interfaces in a vehicle. One example is the USB ports that are available for the driver to charge their mobile phone or to connect to the infotainment system.

It is conceivable that an attacker could take over a mobile telephone and install customised malicious code in it. When the mobile phone is then connected to the vehicle via, e.g., USB, the malicious code could then attack the vehicle's infotainment system. Another example of a socket that could be used is the SD card reader that is used for the infotainment system. It is easy to think that threats to the infotainment system wouldn't lead to any serious consequences for the vehicle as a whole, but the infotainment system could be connected to the internal communication network. This means that it could be possible to access the vehicle's more critical control units via the infotainment system.

[2] EOBD is the European variant of OBD-II. They are basically identical and the terms are often used synonymously. However, the most commonly used term is OBD-II.

Any accessible network sockets could be used to carry out attacks against the vehicle's devices that are using the network. Some vehicle manufacturers have begun using Ethernet for faster information transfer in the vehicle, which facilitates attacks as this is a common standard.

Wireless communication

Vehicles may have devices for wireless communication, such as Bluetooth and mobile networks. Bluetooth can, for example, be used to pair a mobile telephone with the infotainment system. Mobile networks can be used for remote over-the-air (OTA) updates or to send diagnostics information. Some superstructure functions and extra equipment have a wireless communication link. These communication links can, for example, be used by suppliers to see status, update and investigate problems in the function, or even to control the function.

Attackers may want to exploit wireless communication to affect vehicles remotely. If there is a link to the vehicle's critical control units, this can pose great risks as an attacker can, for example, attempt to transfer malicious code that disables critical functions.

Sensors

Sensors for, e.g., tyre inflation pressure, Global Positioning System (GPS), cameras and radar can be connected to the internal communication network. Attacks against sensors thus also constitute an attack surface against the internal communication network.

Receivers for Global Navigation Satellite Systems (GNSS) (e.g. American GPS or European Galileo) receive radio signals with very low output from satellites in orbit around the Earth and can therefore relatively easily be jammed. It is now fairly easy, albeit illegal, for private individuals to acquire jammers that can interfere with GNSS signals. In conjunction with military exercises in the vicinity of Sweden, large geographic areas have been affected by GNSS disturbances, particularly in the north. The fire and rescue service should therefore have well-practised routines in their continuity planning for how they will conduct operations when positioning support is not available.

Superstructures and extra equipment

Superstructures and extra equipment must be protected against attack and can even constitute attack paths against the vehicle's critical functions or other critical superstructures or extra equipment. The attack path is more direct if it does not go via the superstructure interface, but instead goes via the vehicle's internal communication network. Connections should therefore always be made according to the vehicle manufacturer's instructions.

Because the vehicle may contain functionality from various providers, it is important to ensure that one component or function does not adversely affect another. At installation, a superstructure may be isolated, not accessible with an external communication solution, and thereby protected from attack. If a new component with external communication is then connected, this isolation is broken and cybersecurity can be weakened. In the long run, this can affect the function of the vehicle as a whole.

It is therefore important to ensure both that individual components and vehicle functions are working correctly and securely from a cybersecurity standpoint, and that implementation and interaction between components and systems do not adversely affect one another when retrofitting components. In addition to this, it is also important to ensure that issues with a supplier's own IT systems for service and maintenance cannot lead to an impact on the vehicle, or that any potential influence is minimised. This applies throughout the system's service life.

Secure components with secure interaction

The following are important to ensure:

- Each individual component or function must function correctly and be secure from a cybersecurity standpoint.
- No undesired influence should be possible in interaction with other components and functions. This is particularly important to consider when retrofitting components.

For heavy trucks, the year of manufacture is relevant in relation to cybersecurity. This is because many heavy trucks, regardless of manufacturer, have the same subcomponents from the same sub-suppliers. This means that a vulnerability in a specific model also presumably exists in other manufacturers' models from the same year. A cybersecurity vulnerability in a heavy vehicle can therefore have a very large spread and impact.

Year of manufacture and cybersecurity

Heavy trucks manufactured in the same year, regardless of make, often use subcomponents from the same supplier. The same vulnerabilities can therefore exist in several different truck models from different manufacturers.[3]

[3] Wiemerskirch, Becker & Hass 2017; Jonson 2018; Tollefson 2019; and Valassi, C and Karressand, M. (2020). Cyberfysiska sårbarheter i tunga fordon – Med inriktning mot tunga fordon av vikt för civilförsvaret (Cyber-physical vulnerabilities in heavy vehicles – Focus on heavy vehicles of importance for civil defence). FOI-R--5067—SE.

Organisational recommendations

This chapter presents the guidelines' organisational recommendations to increase cybersecurity in heavy rescue vehicles. Seven areas are described, with recommendations and examples for handling related risks. The recommendations are based on material from the ISO 21434:2021 and ISO 27000 series standards and from interviews with vehicle manufacturers, superstructure suppliers and the fire and rescue service.

The chapter contains organisational recommendations within the following areas:

- planning, requirements and design based on a life-cycle perspective
- governance and contracts for cooperation
- audits and quality assurance
- system updates
- configuration management
- secure supply chain
- training.

Planning, requirements and design based on a life-cycle perspective

A rescue vehicle has a long service life and can be exposed to a number of different situations that need to be addressed from a cybersecurity perspective. Cybersecurity must be taken into account right from the planning stage, before the acquisition of new rescue vehicles. This enables a more cost-efficient and optimised design than if security is added on later. Cybersecurity must also be included from the start when acquiring new peripheral systems, i.e., the computers that interact with the vehicles for updates, data communication, etc.

A challenge for systems with long service lives is that the software they use is no longer maintained after a few years, or that the systems they are dependent on are no longer available. One example is if the vehicle or component manufacturer goes bankrupt, so that the manufacturer's FMS is no longer available. This must be addressed, and can be resolved in various ways.

The battle between attackers and defenders is ongoing and new risks and vulnerabilities will arise even after the vehicles are put into service. There must therefore be processes in place for identifying new risks and vulnerabilities and for maintaining security during the vehicle's service life. When the vehicles are decommissioned, equipment containing sensitive information must be removed to ensure that it does not end up in the wrong hands.

By considering cybersecurity throughout the entire life cycle, the organisation can identify measures that address the challenges that can arise throughout the lifetime of the vehicle, including during decommissioning.

Recommendations

- Describe vehicle functions and their interactions with the outside world throughout the life cycle, which includes commissioning, maintenance and service updates. Interaction refers in this context to communication to and from the vehicle, both physically and remotely. Identify which functions and components in the rescue vehicle and support systems require cybersecurity and thereby need special protection and handling.
- Specify overall goals for cybersecurity for the rescue vehicle and its interacting systems for, e.g., updates and other data communication.
- Conduct risk analyses to identify risks associated with the vehicle and the support systems it interacts with. Evaluate and assess the consequences of the risks, identify mitigating measures and appoint personnel to be in charge of managing the risks. Risk analyses should be conducted at the start of the acquisition process and at every system change that could have an effect on cybersecurity. Risk analyses must also be performed on the vehicle as a whole based on the vehicle's impact on the capacities of the fire and rescue service. To support this work, ongoing strategic intelligence can be gathered to determine which risks and threats exist to the vehicle and to the operation of the fire and rescue service.
- Manage identified cybersecurity risks through appropriate measures. Depending on the nature of the risks, measures may include changes in requirements, technical changes or changes in processes and procedures. In many cases, there are several different ways to manage a risk. The organisation must therefore take a position on which measures are most appropriate for its operations.
- Specify requirements based on the organisation's needs. The requirements may concern the technology, how the organisation should work with the rescue vehicle and its integrated systems, and cooperation with suppliers. Then ensure that the requirements address the needs and that all risks are managed.
- Remove the vehicle's information-bearing equipment when the vehicle is decommissioned so that confidential information does not fall into the wrong hands and the equipment cannot be used to access fire and rescue service systems.

Governance and contracts for cooperation

A rescue vehicle and its support systems consist of many different sub-components. The responsibility for cybersecurity is spread over several different actors. The vehicle manufacturer is responsible for the basic vehicle itself and for the basic vehicle functions. The superstructure supplier is responsible for the superstructures and the external equipment they have installed. The fire and rescue service are responsible for the extra equipment they install themselves. The responsibility for setting requirements and ensuring that every actor lives up to their obligations for cybersecurity lies with the client ordering the vehicle.

It is important to determine who is responsible for what and to regulate expectations and responsibility surrounding the cooperation in contracts with the suppliers. Without a client ensuring that everyone involved understands their responsibilities, important work can fall through the cracks. It is also important to appoint people in the organisation to be responsible for cybersecurity, to ensure that they have a budget enabling cybersecurity-related activities, and to maintain the necessary relationships for communication between actors. All relevant actors need to work together for effective cybersecurity.

Recommendations

- Appoint staff who coordinate and are responsible for cybersecurity in the organisation.
- Enable activities related to cybersecurity by, for example, allocating funds for this.
- Clarify both the organisation and role which are responsible for each activity in the work with cybersecurity. When the work includes multiple organisations, the parties should also identify relevant dependencies and define how the interaction between the parties should take place.
- Enlist the help of your own organisation’s experts in procurement and cybersecurity to get advice on how to formulate requirements that provide sufficient security.

Audits and quality assurance

There are directives and regulations that vehicle manufacturers and superstructure suppliers need to follow. Clients should also ensure that the superstructure suppliers follow the vehicle manufacturer’s instructions for superstructures. If regulations and contracts are not complied with, there is a risk that superstructures and extra equipment are installed in a way that causes cybersecurity risks to be introduced in the vehicle. Such risks can then be exploited by an attacker to affect the vehicle. Basically, what this means is that vehicle and chassis manufacturers must have processes in their software design ensuring cybersecurity in the vehicle and minimising cybersecurity risks from external interfaces. It is in the interest of the vehicle or chassis manufacturer to maintain a dialogue with superstructure suppliers about this, and to ensure in contracts that legally stipulated functionality is not affected during conversion or superstructure bodybuilding.

The UN regulations mentioned under 'Recommendations' apply for certain types of vehicles depending on which components are included in them. For vehicles that are EU-approved, the requirements of Regulation (EU) 2022/545 apply for manufacturers of new vehicle types from July 2022, and to all vehicles produced from July 2024.

All vehicles, regardless of type, are reviewed in some way or another from traffic safety and personal safety standpoints, such as through registration and motor vehicle inspections. Reviews also need to be performed from a cybersecurity perspective. Such cybersecurity audits are aimed at ensuring that the rescue vehicle's superstructures and extra equipment do not pose cybersecurity risks. This also includes peripheral systems that interact with the vehicle and the interfaces that the vehicle's systems use to communicate with the outside world. These types of reviews do not take place routinely. It is the client who has the responsibility for ensuring that they are performed.

Recommendations

- The vehicle manufacturer and/or the superstructure supplier should be able to document that:
    - The vehicle manufacturer meets cybersecurity-relevant regulations and standards, including ISO 21434 and the UNECE regulations UN Regulation No. 155 and UN Regulation No. 156, in the manufacturing of the vehicle.
    - The superstructure supplier meets cybersecurity-relevant regulations and standards, including ISO 21434 and the UNECE regulations UN Regulation No. 155 and UN Regulation No. 156, in the modification and customisation of the vehicle.
    - The superstructure supplier follows the manufacturer's instructions and guidelines for cybersecurity in conversions or superstructure bodybuilding.
    - The superstructure supplier ensures that legally stipulated functionality in the vehicle is not affected in conversions or superstructure bodybuilding.
    - The vehicle manufacturer and superstructure supplier have regulated in contracts which modification may take place and how it may be carried out.
    - Superstructures meet the fire and rescue service's cybersecurity requirements.

- The function responsible for cybersecurity in the municipality or in the municipal fire and rescue service must ensure that:
    - A cybersecurity audit is performed of extra equipment that the fire and rescue service have themselves installed in the vehicle. This can be done using internal expertise or with the help of an external auditor.
    - A cybersecurity audit is performed of software and commercial off-the-shelf products (COTS) before the products are used in the vehicle or in peripheral systems. This also applies to software used for the operation and updating of vehicles.
    - An audit is performed of updates and changes in the vehicle's hardware and software to discover changes that could adversely affect cybersecurity. Responsibility for this can also be transferred to the supplier/superstructure supplier/administrator and is then done through requirements-setting during procurement by the responsible function. The responsible function also needs to carry out checks to ensure that this is done.

Examples of risks

A disgruntled employee at a supplier agrees, in return for payment, to insert malicious code in an update that will be installed by the fire and rescue service. Because there is no review process, the update is installed. This results in a function in the rescue vehicle being unusable at a time chosen by the attacker.

System updates

Updates are necessary both to improve functionality and to increase security for the system. Security updates must take place regularly and quickly when they concern serious vulnerabilities, so that attackers do not have time to exploit the vulnerabilities. In the event of a cybersecurity incident, it is also important to get updates out quickly in order to patch vulnerabilities so that no further damage can occur.

An update can be manipulated by an attacker so that it causes unwanted altered functionality or contains malicious code. It is therefore important to check that the update comes from a reliable source and that it was not tampered with during delivery. It is also important that trusted staff perform the updates.

In the same way that spare parts are stored for mechanical systems, or that it is ensured that the systems can be replaced with newly manufactured systems, a life-cycle perspective must also be adopted for software updates, preferably over the vehicle's entire planned lifetime. The tools needed for updates must also be administered throughout the time the vehicle will be used.

Recommendations

- Update the vehicle and support systems continuously and promptly when there are new versions of software or security updates. However, there must be a process in place for identifying and prioritising updates. Just updating immediately is not recommended in critical operations; each update must be handled correctly. Ensure that functionality is not adversely affected by the update. Once the updates have been made, they must undergo functional testing.

- Ensure in particular that only dedicated service computers, with good basic protection and procedures for use, are used to introduce updates into the vehicle. If the service computers are also used for other purposes, such as for private browsing, the risk of malicious code infecting the computer is increased.

- Conduct regular security updates of the operating systems and other software, as well as updates of signatures for anti-virus programmes on peripheral systems and service computers. Update only one computer at a time. Service computers and tools can in some cases be as critical as the vehicle itself. If so, then these must also be protected.

- Consider whether wireless updates are necessary or if it is possible to install these over a wired connection or with portable storage media. If vehicle updates are performed over a wireless connection, this could result in increased exposure of the vehicle's systems that an attacker could attempt to exploit. Regardless of what is selected, updates must take place over a secure communication channel.

- Make sure that the fire and rescue service can choose a date and time for wireless updates, if these are allowed. This helps prevent vehicle updates from disturbing ongoing operations, for example during a call-out.

- Do not update several vehicles of the same model at the same time. If several vehicles of the same model are updated simultaneously, a fault in an update could lead to all the vehicles becoming unusable. After updating the first vehicle, carry out a functional check before updating other vehicles.

- Make sure it is specified in the contract when the supplier's service contract expires and when security updates will no longer be provided. The risks this entails can then be managed in time. Set requirements that the vehicle's main function must not be compromised when service contracts have expired.

- Specify in contracts that suppliers, upon discovery of vulnerabilities, promptly notify and provide updates or system changes to counteract the effects of the vulnerabilities.

- Updates to vehicles or peripheral systems should be provided so that it is possible to discover tampering. This can be done for example by comparing the hash values for software before and after delivery, and through protective sealing of hardware. Have a process in place for checking that tampering has not taken place before updates are performed.

Examples of risks

A service technician connects via a wired connection to a rescue vehicle to see the status of the vehicle and to perform service updates to the vehicle's software. In addition to the wired connection, the service computer also has a wireless internet connection. Through a vulnerability, an attacker has acquired remote control of the service computer and can thereby transfer malicious code to the vehicle when the service computer is plugged in, for example to put the vehicle or one of its functions out of operation.

Configuration management

Knowledge of which components and software that vehicles and peripheral systems consist of is required in order to understand which risks and vulnerabilities exist. Knowledge is also required of which different versions of software are used, as different software versions have different vulnerabilities.

Sometimes a vulnerability quickly becomes known and attackers begin to use it. For software providers, it becomes a race against time to provide security updates before the vulnerability is exploited. By keeping track of which versions are in use, the organisation can quickly assess which critical vulnerabilities they are exposed to and determine where they need to work to quickly install security updates, or take other measures while waiting for the updates to become available. Note, however, that even if a vulnerability is serious, it may be difficult to exploit. It may be located in a component that is not directly connected to the outside world or to another internal system and is therefore not necessarily time-critical to rectify.

The organisation needs to keep a log of what has been updated and which updates and software versions are installed. The log should also contain a list of when the update was performed, and by whom, in order to make sure that necessary updates are performed. Unauthorised changes can then also be more easily detected.

Recommendations

- Make a complete list of the rescue vehicle's hardware and software. The list should include the supplier's name, hardware model and included software, including version.
- Maintain an updated list of which versions and configurations of hardware and software are used in the vehicle or in its peripheral systems. Update the list when changes are made.

Examples of risks

A vulnerability in an old version of software in a service computer enables an attacker to introduce ransomware that encrypts all files on the computer. Unfortunately, it spreads to several of the municipality's computers, which also become encrypted.

Secure supply chain

A rescue vehicle consists of a large number of electronic components in the basic vehicle, the superstructures and the extra equipment. These components are in turn manufactured by different suppliers, which often have sub-suppliers, who themselves may have sub-suppliers. It therefore quickly becomes difficult to track which actors are part of the supplier chain. It is enough that a single person at a supplier company sneaks something malicious into a product for there to be consequences for the vehicle's operation and performance. Some alterations can of course be detected in inspections and product tests, but not all of them. One should therefore ensure that the supplier complies with relevant standards for safety and quality, e.g., ISO 9001, and that one can ensure traceability concerning the products all the way through to installation in the vehicle.

Recommendations

- Evaluate vehicle manufacturers, superstructure suppliers and suppliers of extra equipment from a suitability perspective.
- Establish contracts and rules for cooperation with suppliers. These contracts should specify, among other things, that the supplier must protect their production and development environments, how delivery checks and information exchange shall be carried out with regard to cybersecurity, and how quickly security updates shall be provided after vulnerabilities are discovered.
- Ensure that products cannot be tampered with during delivery. For example, this could be done by comparing the hash values for software before and after delivery, and by sealing hardware before delivery.
- Both during the vehicle's development and during the bodybuilding phase (for conversion into a rescue vehicle), production and development environments should have the necessary protection to prevent vulnerabilities being introduced into the vehicle.
- During software development, a methodology for secure development, such as one of the methods from CIS, NIST, SAFECode, BSA or OWASP, should be used.[4]

[4] Center for Internet Security Critical Security Controls (CIS),
National Institute of Standards and Technology Secure Software Development Framework (NIST),
Software Assurance Forum for Excellence in Code (SAFECode),
Software Alliance BSA Framework for Secure Software,
Open Web Application Security Project (OWASP)

Training

Cybersecurity for a system is dependent on the users and how they use the system and function in question. This applies to both fire and rescue service staff and to other actors who interact with the vehicle, such as for service and maintenance. It is therefore important that the staff understand cybersecurity and the consequences inadequate cybersecurity can have for the fire and rescue service. To properly accomplish this, the organisation needs to train the staff in information security and in the fire and rescue service's procedures for this. It is also relevant to train affected employees in specific procedures for cybersecurity in relation to the rescue vehicle. Training leads to increased knowledge, which in turn reduces the risk of operator errors that can compromise cybersecurity.

It is also important that the training is tailored to the staff category being trained. For example, a firefighter needs to understand how they should handle the systems and components in the vehicle, while a technician needs deeper knowledge of how the systems function and how they should be handled, as well as procedures and systems for example, for service and updates.

Recommendations

- Develop policies and routines for cybersecurity in the organisation, for users of the systems, and for the operation and maintenance of rescue vehicles and their peripheral systems.
- Train staff in procedures for cybersecurity in the use, operation and maintenance of vehicles and their peripheral systems. The training should also address the consequences which faulty or negligent use could have.
- Require suppliers of basic vehicles and installers of superstructures and extra equipment to develop training for how these should be used and maintained to uphold a high level of cybersecurity. The training should also address the consequences which faulty or negligent use could have.

Technical recommendations

The following section presents the guidelines' technical recommendations to increase cybersecurity in heavy rescue vehicles. Five areas are described, along with recommendations. A description of the area, examples of potential risks, and specific recommendations are provided for each area.

The recommendations are based on interviews conducted with vehicle manufacturers, superstructure suppliers and the municipal fire and rescue service.

The chapter contains technical recommendations within the following areas:

- limitation of function and complexity
- wireless communication
- separation of communication within the vehicle
- physical security
- emergency operation.

Limitation of function and complexity

Increased functionality does not always mean higher productivity or performance. Increased functionality often leads to increased complexity for the user, which in turn increases the risk of operator error. A greater number of functions also means that the product itself becomes more complex, which entails an increased risk for vulnerabilities, problems or faults. Note that increased use of software may prolong the start-up time for the vehicle.

Recommendations

- Only equip the rescue vehicle with functions and extra equipment that are necessary for operational needs. This limits the complexity and thereby the cybersecurity risks.

> **Examples of risks**
>
> The fire and rescue service procure a rescue vehicle with touchscreens to control various superstructure functions. It turns out that these touchscreens have external communication for updates. An attacker takes advantage of this and manages to insert a malicious update that blocks the functionality of the touchscreen, which causes the function controlled by the touchscreen to become unavailable. Luckily, the function can be run in emergency operation mode, but this costs precious time.

Wireless communication

The rescue vehicle can use wireless communication to simplify, improve and speed up rescue work. Wireless communication can also be used for other purposes, such as to update or diagnose the vehicle or its functions remotely.

Wireless communication brings increased exposure, which attackers can take advantage of to access the vehicle's various systems. This can involve a range of consequences depending on how the vehicle's internal systems are designed. If an attacker can access critical functions in the vehicle, the attack can cause consequences for personal safety and rescue operations. Due to the risk of external attack, it is very relevant to limit the number of wireless communication links from the emergency vehicle and only include those deemed absolutely necessary.

The Swedish government can decide to put the country on a heightened state of alert if for example there is a danger of war. In such a situation, wireless connections can be used to track the rescue vehicle in order to combat it kinetically. When at heightened state of alert, war or during use in a foreign country, wireless communication is likely to have a lower degree of availability. It is therefore important to have knowledge of all communication dependencies, such as if the vehicle is at risk of going into limp-home mode if internal diagnostics do not make contact with the chassis manufacturer's FMS. Another example is that a function is switched off if the component can't make contact with a license or subscription server.

TSFS 2016:22 – exemption from quality requirements

In the Swedish Transport Agency's regulations (TSFS 2016:22) and general advice on vehicles and trailers pulled by vehicles, vehicles used by the Swedish Armed Forces, the Swedish Defence Materiel Administration and the National Defence Radio Establishment were exempted from the requirements regarding quality and condition, as an integrated tracking and communication system in the vehicles (such as e-Call), which is not under their own control or security-classified, entails a very significant limitation in the operations conducted by these authorities.[5]

Recommendations

- It shall be possible to operate the vehicle without active wireless connections, e.g., to an FMS. It shall be possible to activate this mode locally.
- Keep wireless communication links to a minimum. For each wireless communication link, write a justification describing why the connection is necessary.
- Limit wireless connections to and from the vehicle to reduce exposure. For example, ensure that only approved users and peripheral systems are permitted to connect.

[5] https://www.transportstyrelsen.se/globalassets/global/regler/remisser/vagtrafik/tsf-2022-137/remissmissiv.pdf

- Protect confidential and critical data communication over wireless links by using encryption. This protects communication from unauthorised interception and manipulation.

> **Examples of risks**
>
> A superstructure supplier has installed a superstructure system with wireless communication to send diagnostics information and for updates. An attacker exploits the external link to communicate with the superstructure system. The attacker manages to transfer malicious code that makes the superstructure system unusable.

Separation of communication within the vehicle

Separation refers to a software boundary or physical boundary between different devices or groups of devices. Separating devices in the vehicle reduces the risk of an attacked device affecting other parts of the vehicle.

Vehicle manufacturers provide instructions for how connections to the internal communication network may be made, and which physical requirements superstructures must meet. However, the instructions cannot cover every conceivable type of connection or superstructure. As an example of how manufacturers deal with this challenge, all conversions and superstructures that are not specifically described in Scania's bodybuilding instructions must be approved by an authorised representative at a Scania dealer. It is therefore important to maintain a dialogue with the basic vehicle's manufacturer regarding the superstructure's connections.

Recommendations

- Superstructures and extra equipment shall only use interfaces of basic vehicles that are type-approved for the purpose. For each superstructure or extra equipment that is connected directly to the vehicle's internal communication network, a justification shall be provided explaining why the connection is necessary and how it is made. The connection shall also be analysed so that any impact on the vehicle's cybersecurity, type approval etc. is known.

- Do not connect superstructure equipment and extra equipment that have wireless communication interfaces to other equipment unless this is necessary.

- Do not connect superstructures and equipment that have wireless communication interfaces to superstructures and extra equipment that carry confidential information. This reduces the likelihood of confidential information being leaked.

Examples of risks

A superstructure supplier has installed a superstructure system that is connected directly to the vehicle’s internal communication network. An insider or unauthorised user updates the software in the superstructure system, which in turn affects the vehicle so that the vehicle becomes unusable when an extraordinary event occurs.

Examples of risks

A firefighter connects their mobile phone to the rescue vehicle’s USB port for power supply because the phone’s battery is running low. Unfortunately, there is malicious code on the telephone that is transferred to the vehicle’s infotainment system. The infotainment system has insufficient separation from the internal communication network. This results in the malicious code being able to communicate with other devices in the vehicle, thereby affecting critical vehicle functions.

Physical security

If an attacker has physical access to the vehicle, the attacker has great opportunities to manipulate or cause damage. It is therefore also important to restrict physical access to the vehicle’s systems.

Rescue vehicles are usually equipped with roll-front cabinets that contain equipment such as tools, hoses and pumps. Due to accessibility requirements, these roll-front cabinets are unlocked, something that can be taken advantage of by an attacker. It is therefore important to not expose data communication cables or physical interfaces in these cabinets or in other easily accessible places.

Recommendations

- Protect cables and ports for data communication against unauthorised access from the outside of the vehicle, from the vehicle’s cab, and from behind the cabinet shutters. This makes access difficult for attackers.
- Ports that are accessible from the vehicle’s cab shall be equipped with one-way USB (for electrical charging) or only permit authorised equipment to be connected.
- Install burglar alarms on cabinets that contain cables for data communication. The alarms shall activate when the cab is locked. Also introduce a function that shows an indication in the cab when a cabinet shutter is open.

Examples of risks

The rescue vehicle is idling unsupervised during a rescue operation, which leads to an attacker being able to work undisturbed next to the vehicle. The attacker connects their laptop to a physical interface on one of the superstructures and transfers malicious code. When the firefighters later return to the vehicle to drive away, the superstructure functions have stopped working.

Emergency operation

Some parts of the rescue systems are critical for maintaining life-saving operations. If normal functions for controlling such system components stop working, alternative control functions are required. Such alternative ways of control are called emergency operation or emergency mode.

Recommendations

Ensure that:

- emergency mode is available for critical functions in the vehicle
- emergency mode is independent of regular systems
- instructions for emergency mode are available
- the organisation practices the use of emergency mode systems.

Examples of risks

The firefighters drive out to a fire in a residential building. Unfortunately, the extinguishing system has stopped working due to a hacker attack. The firefighters are forced to send another fire engine, which takes up valuable time, allowing the fire to develop and the building burns to the ground. Emergency operation of the extinguishing system through another method would have been helpful in this situation.

In-depth technical overview

This chapter presents an in-depth technical overview of the vehicle's internal communication networks and the protocols used in vehicles. The purpose is to provide a basic understanding of how heavy vehicles in particular are constructed. The descriptions help make it easier to understand the threats, risks and possible attacks described in these guidelines.

Modern vehicles consist of a number of different communicating electronic control units, rather than strictly mechanical or electro-mechanical functions as they did in the past. Today's communicating electronic control units are often referred to by their abbreviation, ECU. The operating systems used for these types of units are usually very simple and designed to be reliable, but often without taking cyber-security aspects into account. The control units handle more or less the entire functionality of the vehicle, from steering and performance to entertainment and comfort. For these control units to function correctly, communication channels are required between them in the vehicle. The internal communication between control units in passenger cars often goes via a central gateway. This can simplify segmentation of the network, providing boundaries that, e.g., reduce the risk of spreading malicious code. Heavy vehicles, on the other hand, often have a flatter architecture, without central gateways for segmentation.[6] However, a gateway is usually implemented between the vehicle chassis and any superstructure interfaces. Developments are increasingly being made toward central architectures with multiple gateways in order to simply segmentation.

Vehicles use different protocols for communication between different sub-components in the internal communication network. For critical subcomponents, low-level communication is usually based on the ISO11898 standard for CAN (Controller Area Network). This standard defines how devices in the communication network communicate on the data link layer.[7] For CAN, this takes place through broadcasting, which means that all receivers see all packages and decide for themselves which they listen to and which they ignore. An alternative to CAN is FlexRay, which is also used for low-level communication between critical subsystems within the internal communication network in vehicles. FlexRay is designed to be quicker and more reliable than CAN, but is not widely used. FlexRay is currently only used as a complement in security-critical subsystems by vehicles that require real-time communication and redundancy.

To communicate over CAN, a high-level protocol is needed that establishes how the package contents shall be interpreted and how the communication is structured. On this level, heavy vehicles and passenger cars differ. Heavy vehicles usually follow the SAE J1939 standard, which defines high-level protocols over CAN. Passenger vehicles usually use manufacturer-specific high-level protocols instead.

[6] Valassi, C and Karressand, M. (2020). Cyberfysiska sårbarheter i tunga fordon – Med inriktning mot tunga fordon av vikt för civilförsvaret (Cyber-physical vulnerabilities in heavy vehicles – Focus on heavy vehicles of-importance for civil defence). FOI-R--5067—SE.

[7] See the OSI model.

Heavy vehicles can also use manufacturer-specific high-level protocols, but this is usually only done for isolated subsystems. In comparison with manufacturer-specific high-level protocols, J1939 may be more easily accessible for potential attackers because there is greater transparency regarding the protocol's function and structure. This simplifies potential attacks against equipment that follows J1939. At the same time, the greater transparency means that more people can review the standard to discover vulnerabilities.

In addition to CAN-based communication, there are also other communication protocols in the vehicle, such as local interconnect network (LIN) and media-oriented systems transport (MOST). These are primarily used for non-critical systems and have many similarities between different types of vehicles.

LIN is a serial network protocol with relatively low data transfer capacity. The protocol was developed for use in vehicle parts with lower demands on robustness and performance. LIN is therefore used in non-critical systems that do not require the transfer of large amounts of data, such as electronically controlled rear-view mirrors, seats and climate systems, as well as for various function buttons on the steering wheel.

MOST is a multi-media protocol used for video, audio and similar data signals in-the vehicle. The protocol has a relatively high transfer speed and is therefore well suited for media handling. The protocol is also customisable and has plug-and-play integration.

Vehicles are being equipped with ever more advanced driver assistance functions, which requires increased bandwidth for communication within the vehicle. Ethernet is therefore a protocol that is beginning to be used more and more in the automotive industry.

References

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Schacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., & Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. I USENIX Security Symposium, vol. 4, p. 447–462.

Gustafsson, T. and Valassi, C. (2018). NCS3 – Kartläggning av elektroniska styrsystem i tunga fordon (Survey of electronic control systems in heavy vehicles). FOI Memo 6358.

ISO 21434:2021 Road Vehicles – Cybersecurity engineering.

ISO 27000 series.

Jonson, U. (2018). Heavy Vehicle Cybersecurity Program (presentation at the Auto-ISAC Monthly Community Call 2018-04-04).

Kennedy, J., Holt, T., & Cheng, B. (2019). Automotive cybersecurity: accessing a-new platform for cybercrime and malicious hacking. In Journal of Crime and Justice, 42:5, 632-645. DOI: https://doi.org/10.1080/0735648X.2019.1692425.

Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. Black Hat USA, 2015, 91.

Mukherjee, S., Van Etten, J. C., Samyukta, N. R., Walker, J., Ray, I., and Ray, I. (2019). TruckSTM: Runtime Realization of Operational State Transitions for Medium and Heavy Duty Vehicles. I ACM Transitions on Cyber-Physical Systems Vol. 4, No. 1, Article 4. October.

Norte, J., K. (2016) Hacking industrial vehicles from the internet. http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html

Scania (2021). Användning och ansvar (Use and responsibility). https://til.scania.com/groups/bwd/documents/bwm/mdaw/mdaw/~edisp/064094.pdf [2021-12-17].

Stachowski, S., Bielawski, R., and Weimerskirch, A. (2018). Cybersecurity Research Considerations for Heavy Vehicles. DOT HS 812 636. Washington, DC: National Highway Traffic Safety Administration (NHTSA).

Swedish Code of Statutes (SFS)(2001). Act (2001:559) on road traffic definitions. (Svensk Författningssamling (SFS)(2001). Lag (2001:559) om vägtrafikdefinitioner.)

Tollefson, R. (2019). As the connectivity of trucking fleets grows, so do cyber-security risks. Infosec. https://resources.infosecinstitute.com/topic/as-the-connectivity-of-trucking-fleets-grows-so-do-cybersecurity-risks/ [2021-12-17]

Valassi, C and Karressand, M. (2020). Cyberfysiska sårbarheter i tunga fordon —Med inriktning mot tunga fordon av vikt för civilförsvaret (Cyber-physical vulnerabilities in heavy vehicles – Focus on heavy vehicles of importance for civil defence). FOI-R--5067—SE.

Vard Antinyan (2020). Revealing the complexity of automotive software. Proceedings of the 28th ACM Joint Meeting on European Software Engineering, Conference and Symposium on the Foundations of Software Engineering.

Weimerskirch, A., Becker, S., and Hass, B. (2017) Commercial Vehicle vs. Automotive Cybersecurity – Commonalities & Differences. http://www.weimerskirch.org/files/WeimerskirchBeckerHass_CommercialVehicleVsAutomotiveCybersecurity.pdf [2020-11-10].

More reading suggestions

Additional information can be found here:

- Metodstöd för LIS (Method support for LIS) – Informationssäkerhet.se (https://www.informationssakerhet.se/metodstodet/)
- Upphandla informationssäkert – en vägledning från MSB (Procuring information security – A guide from MSB) (https://rib.msb.se/filer/pdf/28742.pdf)
- The Swedish Civil Contingencies Agency (MSB), the National Defence Radio Establishment, the Swedish Armed Forces, and the Swedish Security Service have jointly established a national cybersecurity centre, within which the authorities provide advice and support regarding threats, vulnerabilities and risks. Nationellt cybersäkerhetscenter (National Cybersecurity Centre) (https://www.ncsc.se/).

A collaboration between:

Myndigheten för samhällsskydd och beredskap

FOI

© Swedish Civil Contingencies Agency (MSB)
651 81 Karlstad Tel. +46 771-240 240 **www.msb.se**
Publ.no. MSB2181 - April 2023 ISBN 978-91-7927-373-6