Author(s): Rathod, Paresh; Kämppi, Pasi; Hämäläinen, Timo

Title: Leveraging National Auditing Criteria to Implement Cybersecurity Safeguards for the Automotive Emergency Response Vehicles : A case study from Finland

Year: 2017

Version:

Please cite the original version:

Rathod, P., Kämppi, P., & Hämäläinen, T. (2017). Leveraging National Auditing Criteria to Implement Cybersecurity Safeguards for the Automotive Emergency Response Vehicles : A case study from Finland. International Journal of Digital Content Technology and its Applications, 11(4), 15-26. http://www.globalcis.org/jdcta/ppl/JDCTA3806PPL.pdf

Leveraging National Auditing Criteria to Implement Cybersecurity Safeguards for the Automotive Emergency Response Vehicles: A case study from Finland

[*1] Paresh Rathod, [2]Pasi Kämppi, [3]Timo Hämäläinen
[1, 2,] *Laurea University of Applied Sciences, Vanha maantie 9, FI-02650 Espoo, Finland, {paresh.rathod, pasi.kämppi}@laurea.fi*
[3,] *Department of Mathematical Information Technology, University of Jyväskylä, Finland, timo.t.hamalainen@jyu.fi*

Abstract

A modern Emergency Response Vehicle (ERV) is a combination of emergency services and functional mobile office on the wheels. The mobile office is aiming to leverage the benefits of fixed office while moving on the wheels. Researchers have observed that emergency response personnel including Law Enforcement Authorities (LEAs), Police and border guards, could be on the duty while having possibility to use same services compared to fixed office. On the one hand, demand of mobile office has significantly improved the emergency response services. On the other hand, emergency vehicle designers should rethink the demand of users. This resulted into modern standard emergency response vehicle with three compartments including cabin, office space and transport space. During our research study, users have registered special demand for mobile office, to meet this demand, designers and engineers have combined a modern vehicle platform with computers, monitors, wireless connectivity and many other devices needed in everyday activities. A set of standards has been released by local and global organisations to help building standard vehicle for emergency responses. However, there is continue challenge, the standards are not covering information and cyber security properly. This research paper fulfils that gap by applying the Finnish National Security Auditing Criteria version 2 (KATAKRI II) on top of eight asset classes that have recognised in Mobile Object Bus Integration (MOBI) project. The outcome is a pragmatic proposal that provides set of safeguards for guaranteeing ERV information and cyber security. This paper presents the information and cyber security safeguards utilising standards presented in Finnish National Auditing Criteria and applying in emergency response vehicles.

Keywords: *Cyber Security, Safeguard, Cross-border collaboration, Information Security, Emergency Response Vehicles, KATAKRI, Secure Technology*

1. Introduction

Law enforcement authorities (LEA), like police officers and border guards, are spending significant of their day-to-day service time on the road. This situation is demanding various infrastructure and resourcing plan. For example, their vehicles need to offer same facilities compared to be working in the office. To meet this requirement, a modern emergency response vehicle (ERV) is converted as an office on the wheels, technically known as mobile office. The emergency vehicles are also wired with many Information and Communication Systems. These ICT systems carries various databases and sensitive information. In addition, the law enforcement authorities are handling sensitive data including personal and sensitive data. It is evident that the mobile office has to meet high requirements for data confidentially, integrity and availability (CIA).

Currently, majority of commercial vehicles are converted to ERVs. Therefore, a common approach to reach CIA requirement is to modify a commercial vehicle according to LEA needs (Rajamäki, 2013). The vehicles are equipped with computers, monitors and many other additional electronic devices. Many researchers have reported that the standardization of ERVs is very fragmented and many associations have released the standards of their own (Rajamäki, 2013; NFPA, 2016; FAMA, 2016). The standards are focused to cover safety, performance and testing but information and cyber security is usually out of the scope, mainly because of new demands of ICT systems and evolving threat vectors. This research paper is also raising a question - how information and cyber security is covered when commercial vehicles are converted to ERVs?

A few research studies are proposing partial solutions, mainly covering secure wireless communication (Rajamäki, Rathod & Holmstrom, 2013; Rajamäki, Rathod & Kämppi, 2013; Fallah & Sengupta, 2012). In addition, we have also observed during our literature review and study that many researchers have shown their interest for general information and cyber security in vehicles and released many interesting papers to cover this topic (Larson & Nilsson, 2008; Madden, McMillen & Sinha, 2010). As a summary, there is no systematic approach on how to guarantee basic level of information and cyber security for emergency response vehicles. This research paper is aiming to fill the gap. Our approach is to propose a solution using Finnish national standard as a case.

The main purpose of this study is to create proposal for ERV information and cyber security by applying Finnish National Security Auditing Criteria known as the KATAKRI (an acronym in Finnish language). The study is an organic and natural continuum for our previous research study and Mobile Object Bus Integration (MOBI) project (Rajamäki, 2013). This research paper is also applying previous research results in innovative way.

The paper is structured in 7 sections, after an introduction, section 2 recognizes the research gap, missing cybersecurity guidelines for ERVs, and makes review for existing ERV standards, automotive standards and research activities. In section 3 we present our research approach and methodologies. The section 4 introduces a case study; how a van sized ERV be protectable asset. In section 5 we propose a practical solution that fulfils the research gap; we propose a set cybersecurity safeguards for ERVs. The last section, discusses about strengths, weaknesses and scalability of proposed solution.

2. Overview – Emergency Response Vehicles

The study started with literature review to find-out how current ERVs and automobile industry are addressing the information and cyber security related standardization? The current-state-of-the-art also reveals other aspects of ERVs; how researchers are seeing modern automobile as protectable asset? For example, the interior space of emergency vehicle can be modified and tailored according to customer need. In general, the ERV interior space divided in three compartments; (1) Vehicle Control (or) Driver's Space (or) Cabin (2) Mobile Office Space, and (3) Transport Space as shown in following figure. Following subsections explains research and innovation activities for standardisation of ERV.

2.1. Standardisation of ERVs

There are few forefront European and International standards on building emergency vehicles. The series of European Standards EN 1846-x focuses on three areas of firefighting and rescue service vehicle: (1) Nomenclature and designation, (2) Common requirements - safety and performance, and (3) Permanently installed equipment – safety and performance (EC Cen EN 1846-2, 2009; EC Cen EN 1846-3, 2008; EC Cen EN 1846-1, 2011). On the contrary, the US ambulance manufacturing division (AMD) of the National Truck Equipment Association released Ambulance Standards in year 2007.

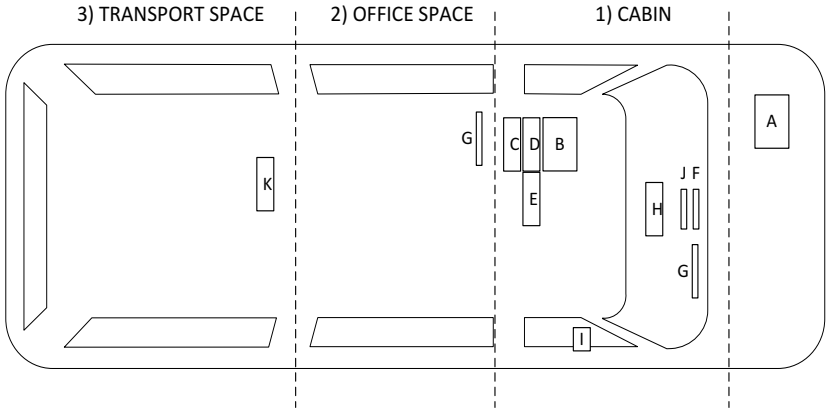

Figure 1. ERV compartments and equipment integration.

In 2014, the American Society of Automotive Engineers also released updated and more advance set of recommendations for ambulances and its safety standards. These recommendation is cumulative iteration and updates on KKK-A1822 document by General Service Administration. Researchers have often argued and questioned the KKK-A1822 for its outdated recommendation not meeting modern requirements. Our study demonstrated – European and American ERV standards are lacking structured recommendation for information and cyber security.

The most widely accepted and admired standards for building emergency vehicles came from an international non-profit organization, namely The National Fire Protection Association (NFPA). NFPA have released a set of standards on fire and rescue services, products and solutions. NFPA 414: Standard for Aircraft Rescue and Fire-Fighting Vehicles and NFPA 1917: Standard for Automotive Ambulances is closely related to the Emergency Response Vehicle. NFPA 414 revolves around the design, performance and acceptance criteria for rescue and fire-fighting vehicles. NFPA 1917 defines the design, performance and testing requirements for ambulances. These standards have specified targets such as aircraft vehicles and medical emergency ambulances.

There are two more NFPA standards which address education and training requirements for Emergency Vehicles: NFPA 1071: Standard for Emergency Vehicle Technician Professional Qualifications and NFPA 1451: Standard for a Fire and Emergency Services Vehicle Operations Training Program. NFPA has considered international and US Federal Specifications when developing these standards. However, NFPA does not offer any guidelines how to cover information and cyber security when designing or testing ERV's.

The Fire Apparatus Manufacturers' Association (FAMA) is another non-profit trade association which provides some guidelines for emergency response vehicles. However, FAMA has not released any public guidelines on how to build an emergency response vehicle. Another similar work found in the literature is from the Ministry of Health and Long-term Care of Ontario, Canada. They have released standards for the minimum acceptance requirements for land ambulances. A diverse range of studies have been done on various specific areas of emergency vehicles including the dispatching system (Han-tao, Jun-qiang & Guo-sheng, 2009) the intelligent navigation system (Salehinejad, Pouladi & Talehi, 2011) the vehicle location finder (Alsalloum & Rand, 2006), the safety and security of onboard personnel and customers (Perry & Lindell, 2003), communication systems (Chen, 2010) and others.

2.2. Automotive Standards

Research study also suggests that automotive standards are not widely covering information and cyber security. Society of Automotive Engineers (SAE) has released a few standards for covering electric vehicles and diagnostics interface; SAE J2186_200506: E/E Data Link Security, J1939/73_20130: Application Layer – Diagnostics and SAE J2931/1_201412: Digital Communications for Plug-in Electric Vehicles. In nutshell, current situation is not able to define automotive information and cyber security systematically. Again, the practices are very fragmented and seeks more targeted solution.

Recently, Society of Automotive Engineers (SAE) has put their effort and work towards information and cyber security. They released their guidelines, SAE J3061: Cybersecurity Guidebook for Cyber-Physical Automotive Systems, in 2016. Their approach is to find out if the existing concepts and methods could be applied in automotive industry. The demand to cover holistic automotive cyber security created an opportunity for the Alliance of Automobile Manufacturers and the Association of Global Automakers to found Automotive Information and Sharing Center (Auto-ISAC). Auto-ISAC combines work forces of auto manufacturers, standardization, other industry and academia to find out the best possible solution regarding automotive cyber security (Auto alliance, 2015).

2.3. Research and Innovation Activities

Academic researchers have also put significant effort for automotive cyber security. Their focus is to handle the combination of the vehicles and ICT as cyber physical systems (Fallah & Sengupta, 2012; McMillen & Sinha, 2010). Their research target is to find out possible physical threats caused via ICT instead of applying existing information and cyber security frameworks in automotive ecosystem. Petit et al. (2015) are presenting analysis for potential risks for automated vehicles without any standardised

safeguards against potential threats. They are using Failure Modes and Effects Analysis (FMEA) to find out the most remarkable risks regarding automated vehicles. Their research work reveals many unseen trends. According to their research the Global Navigation Satellite System (GNSS) will be the most vulnerable part of the automated vehicle ecosystem, the observation previously omitted by researchers. Famous hacking conferences, like Def Con and Black Hat, are also interested to share the latest findings regarding automobiles and especially trendy cars. In 2013, Hackers revealed the first vulnerabilities in Def Con 21 when they could control the car remotely (Rosenblath, 2013). After Def Con 21 car hacking has been permanently in the conference schedule.

3. Research Approach and Methodologies

This study focuses on developing a pragmatic information and cyber security solutions for ERVs. The research approach and methodologies are also reflecting the solution oriented target. This research study is aiming to develop a systematic information and cyber security framework for ERVs using inductive reasoning scientific method considering specific analytic reasoning process. The method is strongly based on providing solutions. The analytic reasoning method draws the premises from unknown to known with iterative process that develops confidence in achieved solutions and hence ensures the trust. In this method, the goal of analyst is to reach a judgement about an issue or problem. The outcome of analyses presents the tangible results in the form of a product (Cook & Thomas, 2005).

The process starts with planning of proving solutions to given issues. The planning phase includes resource usage and timeline plan. The second step in the process includes gathering and familiarizing with available information on top of the already gathered information. Next, the analyst hypotheses and outlines multiple candidates with explanations. Indeed, analyst aiming to reach a judgement by evaluating alternative explanations. The whole process allows to expand and broaden understanding of analyst's previous thinking. The final step allows analyst to summarize the judgement with creation of reports, documents and products. The inductive reasoning method starts with the specific observations and measures that allows to detect patterns and regularities, and resulting into formulate some tentative hypotheses to explore. Finally, the explorations of hypothesis end with broader generalizations, developing conclusions or drawing model. In general, this research method is an ongoing-iterative and highly collaborative process where people, process and technology synchronously scale to support cyber security reasoning, assessment and actions to implement safeguards in ERVs.

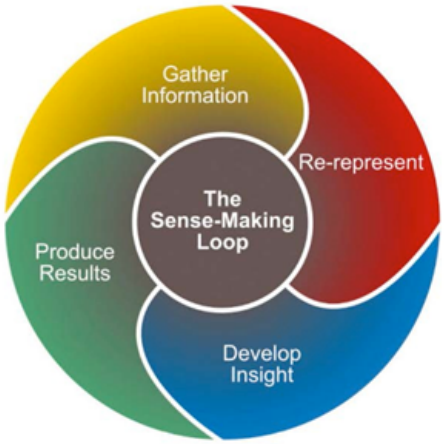

Figure 2. The Analytical Reasoning Process. Source: Illuminating the Path: The Research and Development Agenda for Visual Analytics. IEEE computer society

4. A Case Study – Van Sized Emergency Response Vehicles

Typically, ERVs are built on the top of the commercial vehicle platforms (Rajamäki, 2013). The type or model of the platform is selected according to purpose and need. There are several options

available on the market including sedan, wagon, van or truck. In this study, we have taken a case of a van sized ERVs. The interior space of the van sized vehicle can be modified and tailored according to customer need. In our previous studies, we have piloted new approach with Finnish Police (Rajamäki, 2013; Rajamäki & Rathod, 2013). The Finnish Police has divided interior space in three compartments; (1) Vehicle Control (or) Driver's Space (or) Cabin (2) Mobile Office Space, and (3) Transport Space.

The driver space is reserved for the driver and his pair. It contains all vehicle control related features like steering, gear control and break control. Additionally, there could be installed equipment that is used in everyday activities; onboard computer, touch screen display, keyboard, mouse, voice communications equipment and extra batteries for mission critical systems. The second compartment, mobile office space, acts like an office and it is designed to offer facilities for bigger operations when the vehicle is parked and stabilized. It contains seats, table, storage for equipment, printer and touch screen display. The third compartment, transport space, is reserved for prison or equipment transportation. It has bench and locker. Above Figure-1 presents ERV's integrated system components: For example, Figure 1 demonstrates (A) dedicated start-up battery, (B) dedicated battery for equipment, (C) inverter/charger with possibility for external charging, (D) standby main unit for manual equipment control & intelligent power management, (E) on-board computer, (F) standby control panel/ display and (G) touch screen display, (H) keyboard, (I) mouse, (J) voice communication equipment and (K) data connection equipment.

4.1. Research and Innovation Activities

The ERV design process is highly demanding. The rigorous process should be able to cover required aspects, including information and cyber security. Our previous study focused on user-centric research and it produced user requirements specification based on the real needs of the Finnish police officers (Rathod & Kämppi, 2013). The outcomes of the research study have recognized eight main categories within ERV assets to be protected, as presented in Figure 3, including Emergency Response Preparedness, Vehicle Features, Vehicle Equipment, Interior Space and Cabin Design, ICT Systems, Data Communications, Voice Communications and Power Supply Systems. The scope of previous study did not cover information and cyber security including recognized processes, features, systems and devices. The risk and threat vectors have been significantly increased since our previous studies. In this study, we will use recognized processes, features, systems and devices as assets and functional requirements (FR) with information and cyber security safeguards.

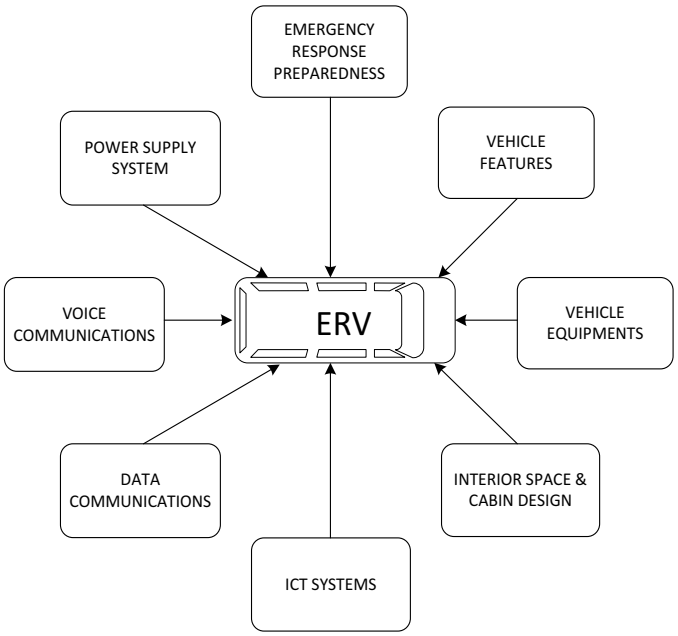

Figure 3. ERV protectable assets categories.

5. Solution – Applying Cybersecurity Safeguards with Security Auditing Criteria

In the second phase of the study, we have identified appropriate standard for applying cyber security safeguards using Finnish National Security Auditing Criteria (KATAKRI) for ERVs (Finnish Ministry of Defense, 2011). The KATAKRI provides significant standardized way to implement cyber security auditing criteria and apply relevant safeguards. The secure ERVs demands protections of different asset classes and components. Following subsection explains our proposed solution and outcome of pilot case.

5.1. Applying KATAKRI Auditing Criteria

A regular risk assessment process includes five phases including risk assessment preparation, identifying threats, risk determination, risk significance determination and risk control strategy (VAHTI, 7/2003). The use of the process is justified when there is identified that assessed target will contain unusual risks. The process may also require significant resource depending on used risk assessment method. When there is a need to define basic level for cyber security other approaches are more useful and effective, in addition to risk management. The Finnish National Security Auditing Criteria version 2 (KATAKRI II) offers feasible, scalable and adaptive alternative for defining information and cyber security. KATAKRI II is divided in four subdivisions and includes four levels for information and cyber security. The subdivisions of the KATAKRI II are administrative security (A), personnel security (P), physical security (F) and information assurance (I). KATAKRI includes information and cyber security levels, these are recommendations for the industry, base level (restricted), increased level (confidential) and high level (secret).

In this study, we have included KATAKRI II the base level of the subdivision I (information assurance) and integrated with the previous research results of the MOBI research project (Rajamäki, 2013). The MOBI project delivered very first user-centric the requirement specification for the emergency vehicles (Rathod & Kämppi, 2013). The results are used as protectable assets for cyber security point of view. KATAKRI II subdivision I define required safeguards for selected assets.

5.2. Proposed Cybersecurity Safeguards

The ERV design process is highly demanding. The rigorous process should be able to cover required aspects, including information and cyber security. Our previous study focused on user-centric research and it produced user requirements specification based on the real needs of the Finnish police officers (Rathod & Kämppi, 2013). The outcomes of the research study have recognized eight main categories within ERV assets to be protected including Emergency Response Preparedness, Vehicle Features, Vehicle Equipment, Interior Space and Cabin Design, ICT Systems, Data Communications, Voice Communications and Power Supply Systems.The scope of previous study did not cover information and cyber security including recognized processes, features, systems and devices. The risk and threat vectors have been significantly increased since our previous studies. In this study, we will use recognized processes, features, systems and devices as assets and functional requirements (FR) with information and cyber security safeguards. The following sections reports outcome of our pilot study and experiments.

5.2.1. FR1: Emergency Response Preparedness

The emergency response preparedness functional requirement is focusing on making sure the ERV is ready on a standby for operation at any time. ERV preparedness can be ensured by three different type of checks and quick functional auditing; routine check, before mission check and after mission check (Rathod & Kämppi, 2013). The routine check is based on car manufacturers' recommendation and it is made on mileage or time basis. The routine check is comparable for any vehicle maintenance program. The before mission check is made by vehicle embedded diagnosis system and ERV personnel. When the ERV is powered on, vehicle embedded diagnosis system starts and indicates immediately if something is wrong. Next, the ERV personnel will go through a checklist according to

their mission. After mission, the ERV personnel will check the vehicle again and they will report observed faults (if any) to maintenance personnel.

The regular maintenance program should contain procedures for maintaining required information and cyber security level. At first place, there should be clear policy how the system is documented and how the documentation is updated, who has rights to install new hardware and software and what criteria must be followed in system acceptance process. All devices, software and licenses should be registered to avoid situations where expired license or software could cause security vulnerabilities.

To guarantee system confidentially, integrity and availability, all new hardware and software need to be verified in testbed before integration into real ERV. It is also important that ERV configuration changes can be made only by authorized personnel. Test accounts and test data should be removed when they are not needed anymore. As there is need for frequent maintenance cycle for engine or brakes, same principle should be applied also with ERV ICT-systems. Software and security updates need to be installed in regular basis, systems need to be scanned frequently to find out possible vulnerabilities and vehicle body need to be checked for tracking or espionage devices. After maintenance work systems should be locked and vehicle is checked according clear desk policy.

5.2.2. FR2: Vehicle Features

The features of emergency response and patrol vehicles are extremely critical to provide effective and timely incident response. Some of the emergency vehicle features accelerate the performance and increase the safety of personnel (Wang & Shih, 2013). The list of required features comprises a broad range of aspects that are embedded with the vehicle platform including car size, sustainable functioning, ground clearance and performance of car, vehicle type, interior and exterior of vehicles and others. This list addresses features such as good driving condition, fatigue and stress resistance, safety features and comfort against extreme conditions, performance against constant traveling in odd conditions. But the nature of the car is changed dramatically during last decades. A modern car is like data center on the wheels and it can contain 50-70 Electronic Control Units (ECU) that are responsible for e.g. cruise control, navigation and safety systems (Larson & Nilsson, 2008). Cars are also connected to background systems and it increases possibilities for having vulnerabilities via wireless networks.

KATAKRI does not provide directly any safeguards for vehicle specific features. Anyhow, the latest research results can be used to complete KATAKRI. Larson et al states that connected vehicle enables remote software updates for ECUs, same time also the number security risks increases (Larson & Nilsson, 2008). Wang et al (2014) found that the vehicle internal communication network, Controller Area Network (CAN), does not provide message authentication mechanism. This vulnerability makes possible to control ECUs via On Board Diagnostics (OBD) interface. In practice the attacker could control ECUs via USB or Bluetooth enabled OBD-adapter. Checkoway et al (2011) raises even more potential vulnerabilities. They state that embedded CD-drive, internal Wi-Fi, embedded Bluetooth, smart phone integration possibilities, remote keyless entry and Tire Pressure Management System (TPMS) could open doors for attackers

There is no comprehensive list for vehicle features related safeguards available, we can propose some recommendations. We recommend protecting OBD service interface in a way there is no possibility to install devices for unauthorized access. We also recommend disabling Bluetooth, avoid using smart phone integration and following latest research results to get up to date information about car related information and cyber security vulnerabilities.

5.2.3. FR3: Vehicle Equipment

Police officers, firefighters, public safety officers and other personnel of emergency response carry various types of equipment in their vehicles (Rathod & Kämppi, 2013). Some of them are use specific like speed radars, explosion meters, carbon meters and thermal cameras. There are also many commercial devices used in the ERV. We can name navigators, cellular phones, voice recorders, printers and USB-sticks. As a summary, the list of the used equipment can be long and heterogeneous.

Before installing any new equipment in the ERV it should be ensured that installation process follows company policies, new device meets specified technical requirements and security controls are

protective enough without having negative effect for usability. New devices should have possibility for mass memory protection and the mass memory should be removed or erased if the device is sent for maintenance. Printers require memory encryption features. All unused Bluetooth- and WLAN-connections are disabled if they are not used and secured. As a basic principle, there must be verified that new devices do not create any new information and cyber security risks. When the new device is installed, the device hardware and software information need to be updated to vehicle specific register. Updated register makes possible to schedule needed software updates in conjunction with vehicle maintenance program.

5.2.4. FR4: Interior Space and Cabin Design

The design principles for interior space and cabin has important role in everyday activities. Design principles focus on the interior design and build of the vehicle, considering the optimum use of available space, ergonomics, safety, material consumption and easy maintenance. International standards as well as feedback from users of ERVs suggest a need for three separate spaces: the cabin, office and customer compartments.

The recommended standard for ERV building depends on the type of vehicle. Related standards (EN 1846, CEN 1789, NFPA 414:2012, NFPA 1917:2013) are concentrating on safety, performance and testing for the ERVs. In information and cyber security point of view, we could concentrate on data confidentially and availability. Interior space should offer lockable storage space for confidential material. For data availability, there should be available suitable space for ICT-systems and cable routings.

5.2.5. FR5: ICT Systems

Although a modern vehicle is like data center on the wheels it needs more processing power to be converted as office on the wheels. The MOBI project introduced an approach where ERV is equipped with rugged on-board computer with Windows OS, touch screen displays, keyboard, mouse and printer. This approach is very flexible and it enables users to access their software applications including office, email, diary, and reporting.

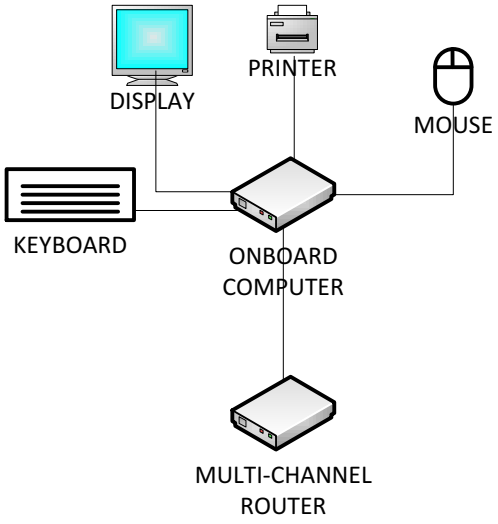

Figure 4. ICT Systems of ERVs.

The system supports also situation awareness including real-time maps, video streaming, 3D view of location, real-time communication and others. Additionally, there could be included portable devices like laptops and tablets. Figure 4 describes typical ICT-system setup in the ERV. The use of legacy operating system enables the use of legacy information and cyber security frameworks. KATAKRI

offers very comprehensive set of safeguards that can be implemented in on-board computer. The most important safeguard is properly configured host based firewall and malware protection application. KATAKRI defines that only predefined traffic is allowed and denied traffic is logged. There should be also a clear policy for firewall configuration, documentation and frequent rule base review. Operating system needs to be hardened; only needed services are activated, applications have minimal number of user rights, mass memory is encrypted, default passwords are changed and all unnecessary physical interfaces are disabled. And finally, all detected security breaches need to be logged.

5.2.6. FR6: Data Communications

As stated earlier, ERVs are more like mobile offices nowadays. A mobile office requires data communication channel that can guarantee data transmission confidentially, integrity and availability. The most economical way is to use commercial mobile networks due the fact that dedicated authority networks are optimized for voice communications (Boris & Wood, 2013). Anyhow, commercial networks are not optimized for availability in critical communications point of view. The availability requirements can be fulfilled by special devices, multi-channel routers, which are able to combine several data bearers as a single transparent data bearer. The multi-channel router offers local data connectivity for end users via both wired and wireless Wi-Fi connections. Figure 5 present the principle of the multi-channel routing.

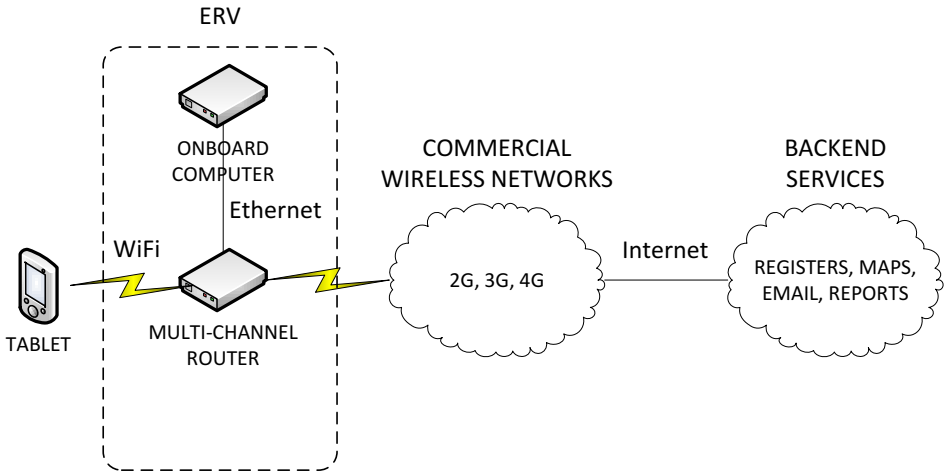

Figure 5. Data Communications System in ERVs.

The most important safeguards for external data communications is support for strong data encryption and possibility to use redundant connections. Secret keys for encryption are used only by authorized users. The session management should meet requirements; re-activation of closed session is prevented; inactive sessions are terminated and the length of the session has certain time limit. And finally, routing messages are verified and filtered. If the data connection is shared locally for the end users by Wi-Fi, the connection should be protected according best practices. The Service Set Identifier (SSID) needs to be hidden, users are authenticated and the connection is encrypted by IEEE 802.11i (WPA2) and the system uses private IP-addresses for the local communication.

5.2.7. FR7: Voice Communications

Voice communication systems include dispatching systems, telephone systems, public reporting systems, and radio systems (Welch et al., 2013). Voice communication systems provide the following functions: communication between the public and emergency response agencies, communication within the emergency response agency under given conditions and communication among emergency response agencies (Boris & Wood, 2013).

The most used technologies for voice communications are Terrestrial Trunked Radio (TETRA), TETRAPOL and Project 25 (P25). The technologies are designed to meet high security and availability requirements for critical voice communications. Anyhow, we can present a few safeguards for handheld terminals. The terminals should be protected by password if feasible and all additional connection types like Bluetooth and Wi-Fi should be disabled if they are not needed. Mass memory is encrypted and the system should support terminal remote management (locking and erasing).

5.2.8. FR8: Power Supply System

The power supply system acts very important role in any modern vehicle. It was stated earlier that modern vehicle can contain 50-70 ECUs and each of them requires power to offer maximum service capability. In case of ERV the situation is more critical. ERVs are loaded with additional equipment that requires extra power to guarantee maximum availability.

The situation could be solved by installing two separate batteries in ERV; one battery for vehicle infrastructure and one battery for additional equipment. The battery system should be designed properly and it should have enough capacity for standby missions, possibility for external charging and it should have real time indication for low charging level (Kämppi & Rathod, 2013). Researchers have worked on finding a holistic solution and finally using NFPA 110 where power systems include "power sources, transfer equipment, controls, supervisory equipment, and all related electrical and mechanical auxiliary and accessory equipment needed to supply electrical power to the load terminals of the transfer equipment" (NFPA, 2016). Researchers also suggested using alternative power systems during failures of the main power systems, for example Emergency Power Supply System (EPSS).

6. Conclusions and Future Research Work

This paper presented and discussed, the modern emergency vehicle is a very complicated combination of different technologies. An emergency vehicle can be described as an office on wheels that integrates together modern vehicle platform with ICT-technologies. The relevant and necessary standardization is very fragmented with many national and international standards. Standardization is focused to cover safety, performance and testing issues. Information and cyber security is still uncovered although ERVs has been equipped with additional equipment during many years.

In this study, we made a feasibility study how KATAKRI audit criteria could be applied with ERVs that are equipped with additional devices and ICT-technologies. We found that KATAKRI does provides large set of safeguards if we are protecting legacy systems or on-the-self products; commercial hardware and standard operating systems. We also discovered that maintenance of the additional technology, including hardware and software, should be integrated as a part of vehicle maintenance program. Continuous maintenance is the key issue for maintaining reached level of information and cyber security. It is obvious that the traditional information and cyber security standards and frameworks are not able to cover information and cyber security risks of modern vehicle platforms. Traditional information and cyber security standards and frameworks can be used as guidelines but there is needed a lot of research work to recognize vehicle related information and cyber security risks.

In summary, our study confirms that KATAKRI is usable when it is applied for legacy hardware and software. If there is any deeper integration with vehicle computing systems, we are recommending going through more comprehensive risk analysis procedure. The future research work can explore specific and comprehensive information and cyber security solutions for ERVs covering suggested eight components in this paper.

Acknowledging

The research study could not have been finished and applied without support of Finnish Emergency Response Organisation including Finnish Police, Airbus-Finland, Research Lead Rajamäki, J., and working life organisations. We also appreciate Laurea University of Applied Sciences and their students to be part of Learning by Developing RDI work. We are acknowledging and thanking your contribution.

7. References

[1] Rajamaki, J. 2013, "The MOBI Project: Designing the Future Emergency Service Vehicle", Vehicular Technology Magazine, IEEE, vol. 8, no. 2, pp. 92-99.
[2] Home | National Fire Protection Association. Available: http://www.nfpa.org/ [2015, 11/16/2015].
[3] J2186: E/E Data Link Security - SAE International. Available: http://standards.sae.org/j2186_200506/ [2015, 11/16/2015].
[4] Rajamaki, J., Rathod, P. & Holmstrom, J. 2013, "Decentralized Fully Redundant Cyber Secure Governmental Communications Concept", Intelligence and Security Informatics Conference (EISIC), 2013 European, pp. 176.
[5] Rajamaki, J., Rathod, P. & Kamppi, P. 2013, "A New Redundant Tracking System for Emergency Response", Intelligence and Security Informatics Conference (EISIC), 2013 European, pp. 218.
[6] Petnga, L. & Austin, M. 2013, "Cyber-physical architecture for modeling and enhanced operations of connected-vehicle systems", Connected Vehicles and Expo (ICCVE), 2013 International Conference on, pp. 350.
[7] Petit, J. & Shladover, S.E. 2015, "Potential Cyberattacks on Automated Vehicles", Intelligent Transportation Systems, IEEE Transactions on, vol. 16, no. 2, pp. 546-556.
[8] Onishi, H. 2014, "Approaches for vehicle cyber security", Communications and Network Security (CNS), 2014 IEEE Conference on, pp. 506.
[9] Home | Fire Apparatus Manufacturers' Assocation . Available: http://www.fama.org/ [2015, 11/17/2015].
[10] Ministry of Defence Finland 2011, KATAKRI, National Security Auditing Criteria. Version II.
[11] National Truck Equipment Association August 2007, Ambulance Manufacture Division Standards 001-025.
[12] Mission | Fire Apparatus Manufacturers' Association . Available: http://www.fama.org/about-fama/mission/ [2015, 11/18/2015].
[13] Alsalloum, O.I. & Rand, G.K. 2006, "Extensions to emergency vehicle location models ", Computers & Operations Research, vol. 33, no. 9, pp. 2725-2743.
[14] Perry, R.W. & Lindell, M.K. 2003, "Preparedness for Emergency Response: Guidelines for the Emergency Planning Process ", Disasters, vol. 27, no. 4, pp. 336-350.
[15] Chin-Ling Chen, C.C. 2010, "A secure fire truck communication protocol for VANET ", , pp. 58-63.
[16] Chen, C. & Chang, C. 2010, "A Secure Fire Truck Communication Protocol for VANET", Proceedings of the 10th WSEAS International Conference on Signal Processing, Computational Geometry and Artificial VisionWorld Scientific and Engineering Academy and
[17] Society of Automotive Engineers 2015, Application Layer -Diagnostics,J1939/73_201508, http://standards.sae.org/j1939/73_201508/ edn.
[18] Society of Automotive Engineers 2014, Digital Communications for Plug-in Electric Vehicles, J2931/1_201412.
[19] Society of Automotive Engineers 2015, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, J3061.
[20] SAE committee busy developing standards to confront the cybersecurity threat - SAE International 2015, Jan 05-last update. Available: http://articles.sae.org
[21] Automakers Announce Initiative to Further Enhance Cyber-security in Autos | Alliance of Automobile Manufacturers 2015, July 14-last update. Available: http://www.autoalliance.org/ [2015, 11/20/2015].
[22] Beene, R. 2015, August 14-last update, Automakers form alliance to bolster cybersecurity . Available: http://www.autonews.com/article/20150824/OEM06/308249985/automakers-form-alliance-to-bolster-cybersecurity [2015, 11/20/2015].
[23] Madden, J., McMillin, B. & Sinha, A. 2010, "Environmental Obfuscation of a Cyber Physical System - Vehicle Example", Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual, pp. 176.
[24] Fallah, Y.P. & Sengupta, R. 2012, "A Cyber-physical Systems Approach to the Design of Vehicle Safety Networks", Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on, pp. 324.

[25] Rosenblath, S. 2013, 2013, August 2-last update, Car hacking code released at DefCon - CNET . Available: http://www.cnet.com/news/car-hacking-code-released- at-defcon/ [2015, 11/21/2015].
[26] P. Rathod and P. Kämppi, 2013, User requirements specification: MOBI Project, Laurea Publications
[27] Hao-you Wang & Huang-Chia Shih 2013, "A robust vehicle model construction and identification system using local feature alignment", Consumer Electronics (ISCE), 2013 IEEE 17th International Symposium on, pp. 57.
[28] Larson, U.E. & Nilsson, D.K. 2008, "Securing Vehicles Against Cyber Attacks", Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges AheadACM, New York, NY, USA, pp. 30:1.
[29] Qiyan Wang & Sawhney, S. 2014, "VeCure: A practical security framework to protect the CAN bus of vehicles", Internet of Things (IOT), 2014 International Conference on the, pp. 13.
[30] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, 2011, "Comprehensive Experimental Analyses of Automotive Attack Surfaces", USENIX Security
[31] Welch, S.J., Cheung, D.S., Apker, J. & Patterson, E.S., 2013, "Strategies for Improving Communication in the Emergency Department: Mediums and Messages in a Noisy Environment", The Joint Commission Journal on Quality and Patient Safety, vol. 39, no. 6, pp. 279-286.
[32] Borislow, D.M. & Wood, G.L. 2013, Computer-related devices and techniques for facilitating an emergency call via a cellular or data network using remote communication device identifying information, Google Patents.
[33] Kamppi, P. & Rathod, P. 2013, "Smart battery system for emergency vehicles: Results from a pilot field study", Connected Vehicles and Expo (ICCVE), 2013 International Conference on, pp. 182.
[34] NFPA 110: Standard for Emergency and Standby Power Systems, NFPA 110 2013,
[35] ETSI - TETRA 2015-last update. Available: http://www.etsi.org/technologiesclusters/technologies/tetra [2015, 11/21/2015].