Volume XXVII 2024
ISSUE no.1
MBNA Publishing House Constanta 2024

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Cybersecurity analysis of IoT. A case studies.

To cite this article: Marius Rogobete, Marius I. Mihailescu, Stefania L. Nita, Valentina Marascu and Mara Rogobete, Scientific Bulletin of Naval Academy, Vol. XXVII 2024, pg. 80 - 86.

Submitted: 03.05.2024
Revised: 28.06.2024
Accepted: 01.08.2024

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-24-I1-011

Cybersecurity analysis of IoT. A case studies.

Marius Rogobete[1], Marius I. Mihailescu[2], Stefania L. Nita[3], Valentina Marascu[2], Mara Rogobete[4]

[1] Harman International Romania
[2] Spiru Haret University, Faculty of Informatics
[3] Military Technical Academy, Faculty of Computer Science, Romania
[4] Babes-Bolyai University, Faculty of Economic Informatics
marius.rogobete@yahoo.com

Abstract. Cyber security analysis is nowadays one of the main requests for any IoT apart from functional demands. Our research describes the procedure by which, given an item, for example the Traffic Surveillance System (TSS), it defines the assets that are distinguished by Cyber Security Properties (C.I.A.) and, going through different scenarios (Attack Path, Damage and Threat Scenarios) is completed with the cyber security risk analysis. This paper presents each step of the TSS thread analysis sequence with a practical case study example.

1. Introduction

A network of objects connected to the Internet is a network (IoT) and can be viewed as a social network, only instead of people, the connected elements are IoT devices. By the end of 2025, it is estimated that 40 billion devices will be on the Internet of Things. Of course, as the number of connected devices increases, so does the attack surface for cybersecurity vulnerabilities.

When we talk about IoT we mean the network of physical objects embedded with sensors, software and other technologies, including communication, that can exchange data with other devices and systems via the Internet or other communication technologies. These can range from smart household items such as refrigerators and clocks to sophisticated industrial or military hardware and tools.

Functionally, data collection through sensors specific to the monitored environment plays a key role, ranging from temperature and pressure sensors to motion detection. They are connected to a central unit that processes and interprets the data.

In order to transmit data, IoT devices are equipped with communication interfaces (such as Wi-Fi or Bluetooth) to finally obtain an Internet connection that allows a device to connect to cloud servers or other devices.

A simple example of the use of sensors in stores is the detection of the time spent by customers in different areas of the room, namely which products are visited more often and what is the most usual route of customers in the store. This data is processed and customer trends are established, problems are identified and suggestions are made.

The embedded software provides the necessary functionality for IoT use and includes security features to protect the device.

Some IoT devices possess an actuation component to perform actions or control a system based on the processed data. In this way IoT devices can collect data, process it and act autonomously.

2. IoT Security

Generally, in a complex ecosystem, IoT-based solutions are responsible for collecting, transmitting, and storing essential data. But with the interconnection of these devices that provide convenience to users, significant risks are also introduced, such as IoT security breaches.

As a result, comprehensive cybersecurity measures must lead to the protection of data, networks, and devices against ever-evolving digital threats.

The security measures themselves must be applied in tandem with strict cybersecurity procedures and IoT security standards. In this way, ensuring that IoT systems are protected against cyber-attacks with effective security solutions.

IoT security threats exploit various factors that bring security breaches, for example, having a software with many open code sources, hackers know the peculiarities of the code and can exploit it.

Among the most common weaknesses are the use of default passwords set by companies that provide gadgets, especially on security cameras, or home routers and even lighting control systems. This IoT security risk is major because default passwords are known.

When we refer to communication, we must know that the messages exchanged in the network between IoT devices are not always encrypted, which creates major security problems. Using standards such as Transport Layer Security (TLS) and transport encryption is a good way to significantly improve connection security. On the other hand, the introduction of multiple networks that isolate devices improves communication, making it secure and private, and maintaining the confidentiality of the data sent.

Personal data is often targeted by skilled data thieves or adversarial government entities, who can do significant harm even by simply recording the IP addresses of out-of-date IoT devices, as these can be used to determine location and residential address a user's exact For this reason, most security professionals recommend using a virtual private network (VPN) that hides your IP address and protects your IoT connection.

From the point of view of the code that is the basis of automation and AI, we know that just a single programming error or even the faulty implementation of an algorithm can irreversibly affect the entire AI network and even the respective infrastructure.

2.1. IoT Cyberattacks Examples

Attacks launched on IoT or ECU (Electronic Control Unit) aim to enter thousands or even millions of unprotected interconnected devices, thus managing to destroy infrastructure or networks or access confidential data. below we present some cyber-attacks that relied on IoT vulnerabilities.

Mirai Botnet

An IoT botnet is a network of computers, running bots, and was used to carry out the worst DDoS attack against an Internet service provider Dyn back in October 2016. Following the attack, several websites have fallen, including CNN, Netflix, and Twitter.

The attack occurred through the Mirai malware infecting computers and allowing it to continuously search the web for susceptible IoT devices to infect, logging in using well-known default usernames and passwords, including various digital cameras but also DVR players.

Verkada Hack

The attack on the Verkada cloud video surveillance service, from March 2021, allowed the attackers to access private information belonging to Verkada customers and even access the live streams of over 150,000 cameras installed in various companies, prisons, hospitals, schools, etc. The security analysis has revealed that more than 100 employees had "super admin" privileges, thus revealing the risks associated with users with excessive privileges.

Attack in Finland

Hackers shut down the heating in two buildings in the Finnish city of Lappeenranta in November 2016, then launched another DDoS attack, which forced the heating controllers to repeatedly restart the heating system and thus prevented the premises from being heated.

The attack was particularly severe, due to the extremely low temperatures at that time of the year.

The Jeep Hack

A group of security researchers tested the Jeep SUV in July 2015 and took control of the car using the Sprint cellular network and taking advantage of a vulnerability offered by the firmware update mechanism, controlling the vehicle's speed and even managing to steer it in off the road.

Stuxnet

One of the most famous attacks is Stuxnet which targeted a uranium enrichment plant in Natanz, Iran. The attack compromised Siemens Step7 software running on Windows, allowing the worms access to Siemens controllers and industrial software. This allowed the worm developers to control various machines in the industrial locations and thereby obtain vital industrial information regarding uranium processing. Indications of a problem with the nuclear facility's computer system emerged when IAEA inspectors visited the plant in 2010. They noted that too high a percentage of uranium enrichment centrifuges fail beyond repair and thus several malicious files were discovered on Iranian computer systems, these files containing the Stuxnet worm. Although Iran has not provided detailed information, the Stuxnet virus is believed to have damaged more than 984 uranium enrichment centrifuges, resulting in a 30% reduction in enrichment efficiency.

Fob Attack

In 2022, in the first three quarters alone, the UK's National Insurance Crime Bureau reported that car thefts reached a record high of over 745,000 cars, a 24% increase over the same period in 2019. And in March 2022, police in London, UK launched a public appeal to find five keyless cars from a British manufacturer that were stolen using relay attack devices that could be bought online, a discovery made by French police that was a widely available modified Bluetooth speaker. sold on the dark web for €5,000, which could be used to steal vehicles from multiple manufacturers. This device was based on a "quick start key" contained in the speakers that allowed the vehicles to be started. [www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things]

3. Cybersecurity Analysis

In order to achieve a threat analysis and ultimately a risk assessment, several action items are required which will be briefly described below. Following this assessment, cyber security threats will be identified, as well as the risk associated with each identified threat. Analysis of the results will enable the extraction of additional cybersecurity requirements for identified high-risk threats, as well as their elimination or mitigation based on relevant cybersecurity best practices.

The early identification of threats is based on threat analysis methodologies and tools, to detect possible vulnerabilities on the analysed device and to determine its compliance with the cyber security processes defined in various security standards that will ultimately lead to the correct assessment of risks.

3.1. Threat and Risk Analysis

The security analysis has two purposes, one (which is the focus of this paper) refers to the determination of the cyber security risk for the analysed product and the second refers to the activities necessary to reduce the existing risk to an acceptable level.

Logical sequence for threat and risk analysis is presented in figure 1, where:

Item: is a subsystem or a combination of subsystems that implements an output function (feature) at the level of the main system, and to which cyber security activities are applied. Any item is defined based on its operational environment where the information required for cyber security engineering is collected.

Asset: means an object or anything that can cause the item's cybersecurity to deteriorate when its cybersecurity properties are compromised. Cybersecurity properties refer to attributes for an asset that include confidentiality, integrity, and availability (CIA). Damage scenario describes an undesired outcome as a result of a cyber security property of an asset or group of assets being compromised.

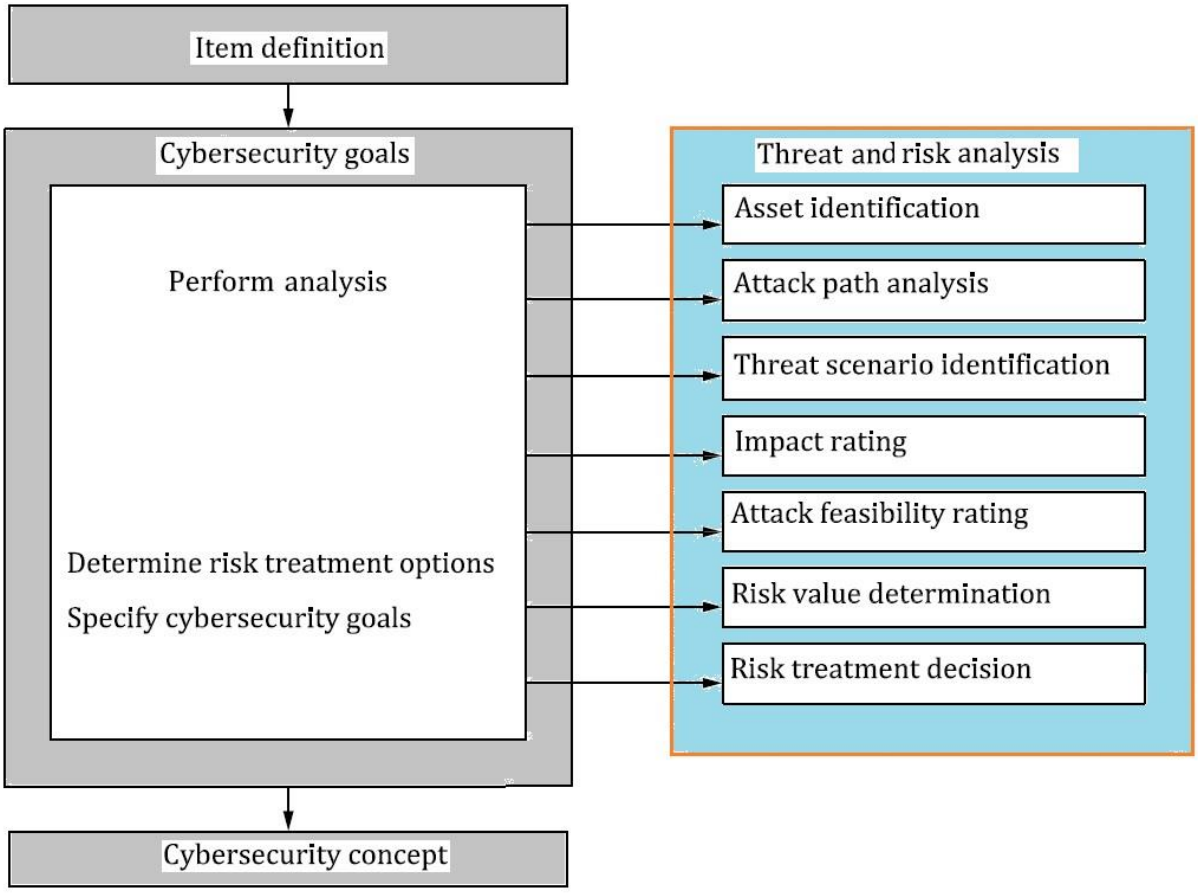

Figure 1 Threat and Risk Analysis Sequence

Attack path: a set of actions that lead to the realization of the threat scenario and it is on the basis of the attack feasibility assessment.

Threat scenario: describes the statement of potential negative actions that correspond to a damage scenario. Its objective is to identify scenarios that may compromise the cybersecurity properties of identified assets.

Impact rating: refers to the impact categories associated with the damage scenarios and their level (serious, major, moderate or negligible). Evaluation of damage scenarios will be evaluated for at least the following impact categories: Safety, Financial, Operational and Privacy (S, F, O, P).

Attack feasibility rating: evaluating the feasibility of attacks based on ease of exploitation and assigning an item a qualifier that describes the ease of successfully performing a particular attack.

Risk value: for any TS, the impact of its associated damage scenario and the feasibility of its associated attack paths will determine this value.

Risk treatment: an activity of evaluating and treating and managing unacceptable risks through an analysis of treatment options.

3.2. Case Study

We consider a traffic surveillance system with a system block diagram as in figure 2.
Simplifying, our item (Traffic Surveillance System) has three assets that can impact security: Debug Interfaces, Ethernet Interface and GSM Cellular Connection.

The Impact analysis is presented in table 1

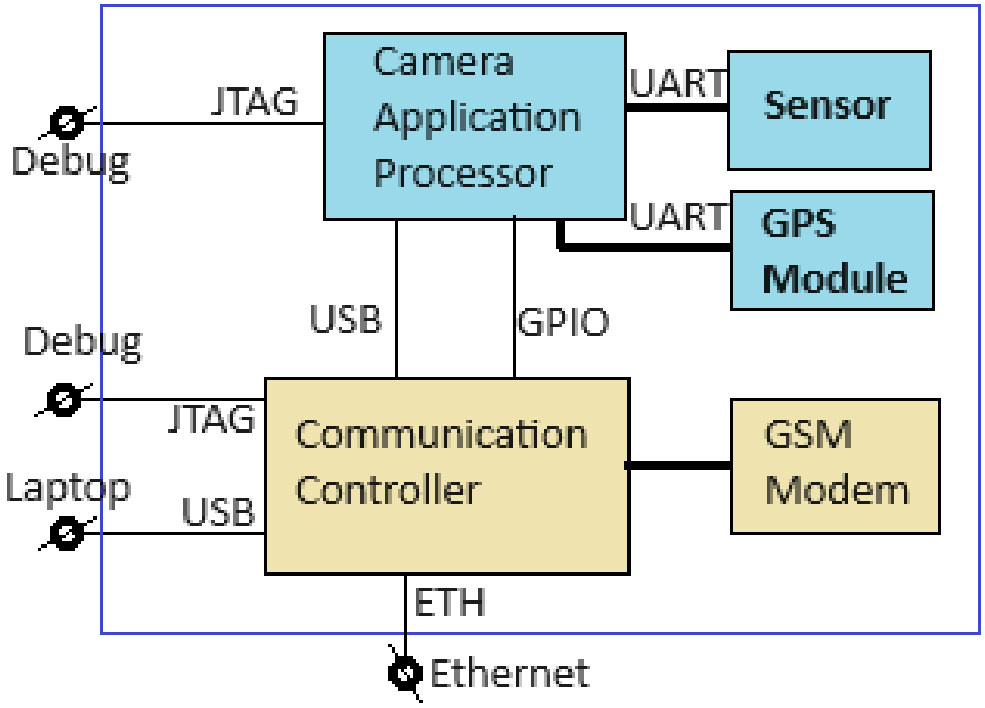

Figure 2 Traffic surveillance system block diagram

Asset	Sec Prop	Damage Scenario	Stakeholder: Road User/ driver				Stakeholder: Road User			
			Criteria for Safety Impact rating	Criteria for Financial Impact rating	Criteria for Operational Impact	Criteria for Privacy Impact rating	S	F	O	P
Camera Application Processor Debugging Interface	*Integrity*	Abuse on false traffic events or even wrong license plate number	S2: Severe and life-threatening injuries (survival probable)	F0: The financial damage leads to no effect, negligible consequences or is irrelevant to the road user.	O0: The operational damage leads to no impairment or non-perceivable impairment of a function.	P0: The privacy damage leads to no effect or can create few inconveniencies to the road user. In this case, the information regarding the	2	0	0	0
	Confidentiality	Extract traffic confidential information	S0: No injuries	F0: The financial damage leads to no effect, negligible consequences or is irrelevant to the road user.	O0: The operational damage leads to no impairment or non-perceivable impairment of a function.	P2: The privacy damage leads to serious impact to the road user. In this case, the information regarding the road user is: a) highly sensitive and	0	0	0	2
	Availability	Block official access to traffic system	S0: No injuries	F1: The financial damage leads to inconvenient consequences which the affected road user will be able to overcome with limited resources	O2:The operational damage leads to the loss or impairment of an important function.	P0: The privacy damage leads to no effect or can create few inconveniencies to the road user. In this case, the information regarding the	0	1	2	0
Comunication Channel to the Internet	*Integrity*	Render PDUs and extract data to control functionalities using malware software.	S3: Life-threatening injuries (survival uncertain), fatal injuries	F0: The financial damage leads to no effect, negligible consequences or is irrelevant to the road user.	O3: The operational damage leads to a vehicle not working, from non-intended operation up to the vehicle being non-operational.	P0: The privacy damage leads to no effect or can create few inconveniencies to the road user. In this case, the information regarding the	3	0	3	0
	Availability	Render PDUs and extract data to block functionalities using malware software.	S0: No injuries	F0: The financial damage leads to no effect, negligible consequences or is irrelevant to the road user.	O2:The operational damage leads to the loss or impairment of an important function.	P0: The privacy damage leads to no effect or can create few inconveniencies to the road user. In this case, the information regarding the	0	0	2	0
GSM Connection	*Integrity*	Exploit the cellular connection (Base Station) to tamper data or to set up a fake Global System for Mobile Communications (GSM) base station	S0: No injuries	F0: The financial damage leads to no effect, negligible consequences or is irrelevant to the road user.	O0: The operational damage leads to no impairment or non-perceivable impairment of a function.	P2: The privacy damage leads to serious impact to the road user. In this case, the information regarding the road user is: a) highly sensitive and	0	0	0	2
	Availability	Exploit the cellular connection (Base Station) to block the GSM communication	S0: No injuries	F0: The financial damage leads to no effect, negligible consequences or is irrelevant to the road user.	O2:The operational damage leads to the loss or impairment of an important function.	P0: The privacy damage leads to no effect or can create few inconveniencies to the road user. In this case, the information regarding the	0	0	2	0

Table 1 Impact analysis

Asset	Sec Prop	Damage Scenario	Threat Scenario	Attack Path Analysis	Elapsed Time	Specialist Expertise	Knowledge of the item	Window of opportunity	IT hardware/ software of other
Camera Application Processor Debugging Interface	*I*	Abuse on false traffic events or even wrong license plate number	Physical access on debugging interface to install malware and then to abuse specific decision (e.g., traffic lights) or tamper collected data	*- access JTAG interface of AP* *- download malicious software* *- take control on traffic camera* *- report wrong data as original to Communication Controller*	≤ 1 week	Proficient	Confidential information	Easy	Specialised
	C	Extract traffic confidential information	Physical access on debugging interface to install malware and to extract confidential data	*- access JTAG interface of AP* *- download malicious software* *- take control on traffic camera* *- extract confidential data and report it over debugging interface*	≤ 1 week	Proficient	Confidential information	Easy	Specialised
	A	Block official access to traffic system	Physical access on debugging interface to install malware and to block the system	*- access JTAG interface of AP* *- download malicious software* *- take control on traffic camera* *- block the traffic system*	≤ 1 week	Expert	Confidential information	Easy	Specialised
Comunication Channel to the Internet	*I*	Render PDUs and extract data to control functionalities using malware software.	Access physical Ethernet interface using a custom cable to communicate with the system, then render PDU and extract data (communication or bridge) to control functionalities using malware software already	*- exploit Ethernet communication channel* *- intercept message flow* *- performs a MITM attack to tamper the communication*	≤ 1 week	Proficient	Restricted information	Moderate	Bespoke
	A	Render PDUs and extract data to block functionalities using malware software.	Access physical Ethernet interface using a custom cable to communicate with the system, then render PDU and extract data (communication or bridge) to block system functionalities using malware software already	*- exploit Ethernet communication channel* *- jamm message flow to block the communication*	≤ 1 week	Proficient	Restricted information	Moderate	Bespoke
GSM Connection	*I*	Exploit the cellular connection (Base Station) to tamper data or to set up a fake Global System for Mobile Communications	An attacker exploits the cellular connection in a vehicle to: - Access the subscriber identity module (SIM) through the system unit - Eavesdrop on cellular communications or	*- gets acces to the GSM SIM* *- install new SIM* *- get all information via new comm channel*	≤ 1 day	Layman	Restricted information	Unlimited	Standard
	A	Exploit the cellular connection (Base Station) to block the GSM communication	An attacker exploits the cellular connection in a vehicle to: - Access the subscriber identity module (SIM) through the system unit - Eavesdrop on cellular communications or rogue cellular base transceiver station	*- gets acces to the GSM SIM* *- remove the SIM* *- block the comm channel*	≤ 1 day	Layman	Restricted information	Unlimited	Standard

Table 2 Threat scenarios and Attack Paths

Table 2 shows threat scenarios and attacks and table 3 present its risk assessment.

Asset	Sec Prop	Attack Path Analysis	Elapsed Time	Specialist Expertise	Knowledge of the item	Window of opportunity	IT hardware/ software of other	Total Value	Attack feasibility Value	**Risk Treatment decision**	**Cybersecurity Controls/ Remarks**
Camera Application Processor Debugging Interface	*I*	*- access JTAG interface of AP* *- download malicious software* *- take control on traffic camera* *- report wrong data as original to Communication Controller*	1	3	7	1	4	16	Medium	Reducing the risk (e.g. implementation of controls)	assumption: organizational rules, monitoring of employees and controls like access rights will lead that social engineering will not succeed
	C	*- access JTAG interface of AP* *- download malicious software* *- take control on traffic camera* *- extract confidential data and report it over debugging interface*	1	3	7	1	4	16	Medium	Reducing the risk (e.g. implementation of controls)	assumption: organizational rules, monitoring of employees and controls like access rights will lead that social engineering will not succeed
	A	*- access JTAG interface of AP* *- download malicious software* *- take control on traffic camera* *- block the traffic system*	1	6	7	1	4	19	Medium	sharing or transferring the risk (e.g. through contracts, buying insurance)	assumption: organizational rules, monitoring of employees and controls like access rights will lead that social engineering will not succeed
Comunication Channel to the Internet	*I*	*- exploit Ethernet communication channel* *- intercept message flow* *- performs a MITM attack to tamper the communication*	1	3	3	4	7	18	Medium	accepting or retaining the risk	The internet communication cannot tampered because encryption and redundancy. Risk is very low, can be accepted
	A	*- exploit Ethernet communication channel* *- jamm message flow to block the communication*	1	3	3	4	7	18	Medium	accepting or retaining the risk	The internet communication cannot tampered because encryption and redundancy. Risk is very low, can be accepted
GSM Connection	*I*	*- gets acces to the GSM SIM* *- install new SIM* *- get all information via new comm channel*	0	0	3	0	0	3	High	sharing or transferring the risk (e.g. through contracts, buying insurance)	sharing with an insurance, financial impact will be only on System Manufacturer side.
	A	*- gets acces to the GSM SIM* *- remove the SIM* *- block the comm channel*	0	0	3	0	0	3	High	sharing or transferring the risk (e.g. through contracts, buying insurance)	sharing with an insurance, financial impact will be only on System Manufacturer side.

Table 3 Risk Assessment

4. Conclusion

This paper describes and presents a cyber security analysis that includes item and asset definitions and concludes with threat scenarios and countermeasure risk assessment for a traffic monitoring system. The example is analyzed by considering ISO SAE 21343 as a cyber security standard and could be applied to any type of industrial IoT or even military electronic control units.

In conclusion, for any cyber security analysis, the main demand is to understand the specifications of the system, the hardware and the software at the architecture levels to be able to derive and analyze the security requests correctly.

References

[1] ISO 31000:2018, Risk management — Guidelines

[2] ISO/IEC 33001, Information technology — Process assessment — Concepts and terminology

[3] ISO/IEC/IEEE 12207, Systems and software engineering — Software life cycle processes

[4] ROSS Ron, et al. (2018), Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems [online]. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1. Updated March 2018 [viewed 2021-02-16]. Available at: https:// doi .org/ 10 .6028/ NIST .SP .800 -160v1

[5] IEC 61508-7, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures

[6] IEC 31010, Risk management — Risk assessment techniques

[7] ISO/SAE 21434, Road vehicles — Cybersecurity engineering