VTT Technical Research Centre of Finland

Cybersecurity in Autonomous Machine Systems Development

Pentikäinen, Heimo; Malm, Timo; Heikkilä, Eetu

Published: 14/11/2019

Document Version
Publisher's final version

RESEARCH REPORT

VTT-R-01087-19

Cybersecurity in Autonomous Machine Systems Development

Authors: Heimo Pentikäinen, Timo Malm, Eetu Heikkilä (editor)

Confidentiality: Public

Report's title Cybersecurity in Autonomous Machine Systems Development	
Customer, contact person, address N/A	**Order reference**
Project name Digital Development Practices for Safe & Secure Autonomous Systems	**Project number/Short name** X-BA DiDePAS
Author(s) Heimo Pentikäinen, Timo Malm, Eetu Heikkilä (editor)	**Pages** 15/
Keywords autonomous machine systems, cybersecurity, safety	**Report identification code** VTT-R-01087-19

Summary

Autonomous machine systems (AMS) are typically software-intensive and highly connected systems. Thus, cybersecurity is one of the key aspects to be considered in their development. This report provides an overview of the cybersecurity related issues, some proposed solutions, as well as future development needs. It combines views from a technical cybersecurity perspective with a machinery safety perspective. The report is structured so that we first briefly discuss the relations of cybersecurity and machinery related risks. This is followed by an overview of standards, guidelines and best practices applicable in AMS design. Finally, cybersecurity in AMS design is discussed and recommendations are provided for defining relevant cybersecurity requirements.

Confidentiality	Public

Tampere 14.11.2019

Written by	**Reviewed by**	**Accepted by**
Eetu Heikkilä Research scientist	Timo Malm Senior scientist	Päivi Kivikytö-Reponen Research team leader

VTT's contact address
VTT, PL 1300, 33101 Tampere

Distribution (customer and VTT)
VTT + internet

Contents

1. Introduction

Autonomous machine systems (AMS) are typically software-intensive and highly connected systems. While there is no one and agreed definition available for cybersecurity, it is widely considered as one of the key aspects to be addressed in development of AMS.

First, and perhaps the most important issue for cybersecurity in this context is that cybersecurity must be an essential part of entire system design from the starting point. This approach is called **Secure by design**. A way to reach secure by design approach is to emphasize requirements of cybersecurity.

In addition to the actual machine system being developed, system developers need to consider the entire software development environment, e.g. secure software compiling and proper version management. This issue is also relevant with hardware development. In this report, focus will be on software development.

This report provides an overview of the cybersecurity related issues, some proposed solutions, as well as future development needs. It combines views from a technical cybersecurity perspective with a machinery safety perspective. The report is structured so that we first discuss the relations of cybersecurity and machinery related risks. This is followed by an overview of standards and guidelines applicable in AMS design, after which the cybersecurity for AMS is further elaborated. Appendix 1 contains selected abbreviations and definitions, and Appendix 2 provides examples of cybersecurity related incidents reported recently.

While this report focuses on technical issues of cybersecurity in machine systems, cybersecurity is always also a human issue. Even the most autonomous systems interact with humans over their life cycle.

2. Relations of cybersecurity risks and machinery risks

In safety engineering, risk is typically defined as a function of probability and consequence, e.g. risk = probability * consequence. However, with cybersecurity issues it is problematic to estimate both probability and consequence. This is because usually we do not have enough data for these estimations. Additionally, safety risk is usually related to random events, whereas security risk is based on actions done on purpose. This means that probability of vulnerability associated to random events can be low, but if the vulnerability is searched on purpose, the probability becomes meaningless. Another characteristic of cybersecurity is that the cyber world is dynamic, that trends of cybersecurity attacks vary temporally or occasionally and consequences can vary case by case. Security risk may change as technologies or circumstances change, but it does not wear out and a long use history does not necessarily guarantee a secure system (see ISO/TR 22100-4).

Standard family IEC/ISA 62443 suggest that there should be target security levels (SL 1 – SL 4), which specify the general risk level and the target to quantify countermeasures against cyber-security risks. There is some similarity to Safety Integrity Levels (SIL according to IEC 61508 and IEC 62061) and to Performance Levels (PL according to ISO 13849-1[1]), which are applied to measure safety risk and related protective measures of machinery safety functions.

[1] ISO 13849-1:2015. Safety of machinery. Safety-related parts of control systems. Part 1: General principles for design. 86 p.

According to Machinery Directive[2], the machine builder (or authorized representative) must consider in risk assessment “intended use and any reasonably foreseeable misuse thereof”. Some cyber-security risks could be associated to “reasonably foreseeable misuse”, but usually it is not the case. Machinery Directive is related to safety, but if cyber-security issue can affect safety, it should be considered.

The different approaches for machinery and cyber risk assessment are comprehensively discussed in VTT report “Risk assessment of machinery system with respect to safety and cyber-security” available online[3].

3. Standards, guidelines and certification for cybersecurity

3.1 Secure by design – standards and guidelines

Secure by design approach can be implemented following various standards and guidelines. This chapter provides an overview of selected key standards, which can be applied in the development of AMS.

3.1.1 ISO 2700x standard series

A basic standard for information security ISO 27000 (SFS-EN ISO/IEC 27001:2017) defines information security as follow: information security preservation of confidentiality (2.12), integrity (2.40) and availability (2.9) of information Note 1 to entry: In addition, other properties, such as authenticity (2.8), accountability, non-repudiation (2.54), and reliability (2.62) can also be involved. ISO 27001 standard (SFS-EN ISO/IEC 27000:2017) states management and risk issues for information security as follow: The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed. ‘Confidentiality, Integrity, Availability’ is also called as CIA-triad.

3.1.2 IEC 62443 standard series

One of the main standard of industrial control system is IEC 62443 series. The IEC 62443-1-1 standard defines the following seven foundational requirements for cybersecurity:

- Identification and authentication control (IAC),
- Use control (UC)
- System integrity (SI)
- Data confidentiality (DC)
- Restricted data flow (RDF)
- Timely response to events (TRE)
- Resource availability (RA).

[2] Machinery Directive 2006/42/EC. DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast). 63 p. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0042

[3] https://www.vtt.fi/sites/tecnetwork/PublishingImages/results/Safety_and_security_assessmentReportSgn19.3.2018%20(002).pdf

3.1.3 ISO/TR 22100-4

Technical report (intention to be published as a standard) ISO/TR 22100-4 (Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects) is published at December 2018.

Smart machines require more connections to devices, machines and infrastructures and furthermore there is a need for fast, robust and secure communication networks. From this point of view, the technical report address aspects on safety of machinery that might be affected by cybersecurity attacks related to the direct or remote access to, and manipulation of, a safety-related control system(s) by persons for intentional abuse (unintended uses). The intentional abuse falls outside the scope of ISO 12100, which represents principles of general machine design, risk assessment and risk reduction, but it is reasonable also for machinery manufacturers to consider such threats. The technical report compares safety of machinery and cyber security from risk, objective and dynamics point of view.

3.1.4 IoT standardization

It seems that cybersecurity of IoT-standardization has at the moment common understanding that standards are needed, this after about five years of IoT large launch. It is assumed that it will take another five years before the standards will be in use[4].

It is also assumed that coming cybersecurity certification regulation by EU will have three assurance levels: Basic, Substantial and High. It could be clear that autonomous systems shall meet the High level, if regulation in question covers autonomous systems. This High level includes at least the following requirements; 1. Minimisation risks of cyberattacks carried out by actors with significant skills and resources, 2. Testing towards known vulnerabilities, 3. Verification that security functionals are correctly implemented, and 4. Penetration testing. Certification will be issued by national cybersecurity authority or accredited organisation.

Secondly, ETSI has created a standard 'Cyber Security for Consumer Internet of Things, ETSI TS 103 645' current version is: V1.1.1 (2019-02). This standard defines the following 13 provisions (requirements) for consumer IoT: 1. No universal default passwords, 2. Implement a means to manage reports of vulnerabilities, 3. Keep software updated, 4. Securely store credentials and security-sensitive data, 5. Communicate securely, 6. Minimize exposed attack surfaces, 7. Ensure software integrity, 8. Ensure that personal data is protected, 9. Make systems resilient to outages, 10. Examine system telemetry data, 11. Make it easy for consumers to delete personal data, 12. Make installation and maintenance of devices easy, and 13. Validate input data.[5]

NIST has published a draft 'Considerations fora Core IoT Cybersecurity Capabilities Baseline'.[6] This paper proposes following 12 items for cybersecurity capabilities (requirements, if 'can' changed into 'shall' or 'must'); 1. The IoT device can be identified both logically and physically, 2. The IoT device's software and firmware can be updated using a secure, controlled, and configurable mechanism, 3. Authorized users can securely change the IoT device's configuration, including restoration to a secure “default.” Unauthorized changes to the IoT device's configuration can be prevented, 4. Local and remote access to the IoT device and its interfaces can be controlled, 5. The IoT device can use cryptography to secure its stored and transmitted data, 6. The IoT device can use industry-accepted, standardized protocols for all layers of the device's transmissions, 7. The IoT device can log

[4] http://etn.fi/images/a/19/5/Etteplan-IoT-device-cyber-security-is-becoming-regulated---are-you-ready-May-2019.pdf

[5] https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

[6] https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf

the pertinent details of its cybersecurity events and make them accessible to authorized users and systems, 8. The IoT device can be reset by authorized users so all data-at-rest on the device is securely removed from all internal data storage, 9. Information confirming the sources of all of the IoT device's software, firmware, hardware, and services is disclosed and accessible, 10. An inventory of the IoT device's current internal software and firmware, including versions and patch status, is disclosed and accessible, 11. The IoT device can enforce the principle of least functionality through its design and configuration and 12. The IoT device is designed to allow physical access to it to be controlled.

Regardless of the status of standardization by ETSI, EU and NIST, the aforementioned requirements should be valid already now for autonomous systems.

3.1.5 Secure Development: Towards Approval

The guide 'Secure Development: Towards Approval'[7] describes secure architecture and design principles as follows: "Product security is enhanced by using established architecture and design principles: minimal attack surface, safe defaults, input sanitation, minimal privileges, defence in depth, failing safely, not trusting external services, and avoiding security by obscurity. Adopting and documenting design principles facilitates both secure implementation and security assessment." The security requirements and threat modelling by this guide are: 1. Injection, 2. Broken authentication, 3. Sensitive data exposure, 4. XML external entities (XXE), 5. Broken access control, 6. Security misconfiguration, 7. Cross-site scripting (XSS), 8. Insecure deserialisation, 9. Using components with known vulnerabilities, and 10. Insufficient logging & monitoring.

The guide emphasizes also testing, verification and audit of products.

3.1.6 Further guidelines and best practices

In addition to standards, a set of guidelines and best practices have been defined for cybersecurity. Best practices are typically based on both standards and commonly accepted cybersecurity mechanisms. Some examples are listed below:

- Guidelines / Special Publications by NIST (The National Institute of Standards and Technology. NIST was founded in 1901 and is now part of the U.S. Department of Commerce [8]).
- Security policies by SANS, https://www.sans.org/security-resources/policies/
- Publications by VTT (in Finnish):
  - KYBER-TEO project public report (in Finnish)[9]
  - Finnish Society of Automation publication Teollisuusautomaation tietoturva (in Finnish, currently not available online)
- 'Secure Development: Towards Approval' is a guide to improve the security of products in their development phase. This valuable guide is created by National Cyber Security Centre Finland (Kyberturvallisuuskeskus), and it is available online.[5]

[7] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Secure%20development%20%20towards%20approval%20003_2018J.pdf

[8] https://www.nist.gov/

[9] http://www.vtt.fi/inf/pdf/technology/2017/T298.pdf

3.2 Certification of cybersecurity aspects

Certification is a rapidly developing area of cybersecurity. There are certifications for many purposes: people, organizations and products for example. In this context, the focus is on the certification of products.

Common Criteria[10] is an international standard (ISO/IEC 15408) for computer security certification. Common Criteria (CC) has seven Evaluation Assurance Levels (EAL), of which EAL 1 is the lowest level and EAL 7 is the highest level. Naturally, the EAL 7 is also the most expensive, and overall comment for Common Criteria is that the certification is a costly process.

The Common Criteria certification for autonomous systems could be a candidate; at least CC should be analysed deeper with a proposal of EAL level. The target EAL level can be varied by domain and the role of autonomous system.

The European Union Agency for Network and Information Security (ENISA) has created a study in 2018, which identifies and analyses the current landscape of ICT security certification laboratories in EU.[11] The study describes standards as follows: Standards used in the evaluation process include mainly ISO/IEC 15408-3 and ISO/IEC TR 18045. The main use of ISO/IEC 15408 is to assess the security of IT products. There are direct relationships between ISO/IEC 15408-3 assurance structure and the structure of evaluation process as described in ISO/IEC TR 18045. The ISO/IEC TR 18045 provides a description of evaluation process in terms of roles and responsibilities, and general evaluation model. Thus, the ENISA's study emphasizes also Common Criteria, although CC has also been criticised.

In 2017, EU views on certification were described as follows[12]: Certification plays a critical role in increasing trust and security in products and services that are crucial for the digital single market. Currently, a number of different security certification schemes for ICT products exist in the EU. Without a common framework for EU-wide valid cybersecurity certificates, there is an increasing risk of fragmentation and barriers in the single market. EU has an ongoing process to improve cybersecurity of consumer products as follows: The cybersecurity certification scheme will cover products, processes and services, providing a standardised guarantee for consumers of enhanced security across their devices and services.[13] In summary, it can be concluded that cybersecurity certification of products on EU level is not ready, but it is under development.

In Finland, the National Cyber Security Centre (Kyberturvallisuuskeskus) published a news on 2018 that it will start cybersecurity verification process for some consumer products on in 2019, but at the time of writing (May 2019) there is no further information to be found on the current situation of this verification process.

It is possible to verify a single part of product, e.g. a cybersecurity data traffic protocol. This kind of tasks have been performed also in VTT's WarRoom, but it shall be noted that specification of protocols is not always unambiguous. Therefore, real requirements of the protocol are not clear in all cases. Naturally, when verification covers a part or some parts of product only, we cannot speak of product verification.

[10] https://www.commoncriteriaportal.org/

[11] https://www.enisa.europa.eu/publications/ove rview-of-the-practices-of-ict-certification-laboratories-in-europe

[12] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

[13] https://www.governmenteuropa.eu/eu-cybersecurity-act-security-europe/91464/

4. Cybersecurity for autonomous machine systems

This chapter focuses on the cybersecurity issues of autonomous machine systems. First, the differences of office and automation networks are discussed, after which system examples are presented.

4.1 Differences of office networks and automation networks

There are some differences between office and industrial automation networks (Industrial Control System, ICS). In office networks, basic cyber requirements are (in this order): 1) Confidentiality, 2) Integrity, and 3) Availability. In automation network, the order is as follows: 1) Availability (including real-time requirements), 2) Integrity, and 3) Confidentiality.

As an example: robotic arm must be moved very quickly (let's say in 100 ms) with certain length in certain angle →requirements are ordered so that resource availability (real-time) is the first. The second is integrity, i.e. movement of arm is as planned (not more or not wrong direction). Availability and integrity are on the same level of importance in practice, but in this case, these commands are not confidentiality matters.

Above, the differences in importance of requirements between office networks and automation networks were discussed. In future, importance of all cybersecurity requirements could be at same level. This because business models are changing; for example, a single device can have valuable data from several owners. Therefore, confidentiality is necessary, but at the same time, integrity and availability cannot be put below of confidentiality.

4.2 Case example: one system

The following presents a simple case example of a machine system related cybersecurity issues. Basic idea is to set cybersecurity requirements in all instances when data is transferred, stored or handled. Figure 1 represents a simplified software (SW) system.

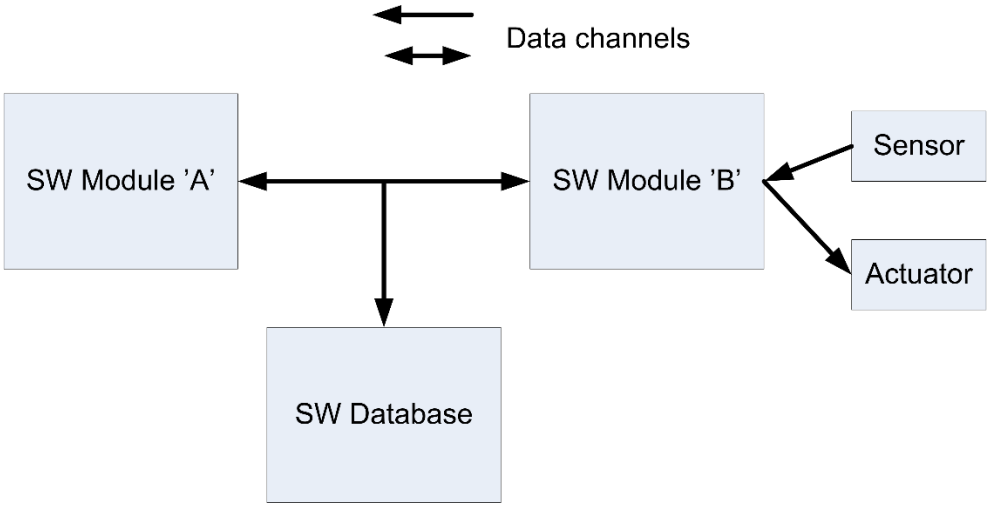

Figure 1: Software modules in a single system.

Data channel can be wireless, wireline or fibre (optical). Usually the data channel is digital. Data flow in the channel can be unidirectional or bidirectional (tele terms are: simplex, duplex).

Data channels use very many protocols or data communication mechanisms. However, cybersecurity requirements shall be independent on the technology of data channel. Below is an example of the situation presented in Figure 1:

- Sensor is connected to SW module B with analogue current loop 4-20mA.
- Actuator is connected with (digital) Profibus, which is a standard for fieldbus communication in automation technology.
- SW B is a part of automation system and it is handling peripheral devices (sensor and actuator).
- SW database, i.e. it stores in long term certain data from SW modules.
- SW Module A manages whole system.

4.3 Case example: two connected systems

Figure 2 represents a simple configuration of two autonomous systems. A data channel between systems can traverse public internet without guaranteed security and data can ow in non-friendly environment. Figure x has two systems, there can be also more than two systems, but cybersecurity requirements are similar with two or more systems.

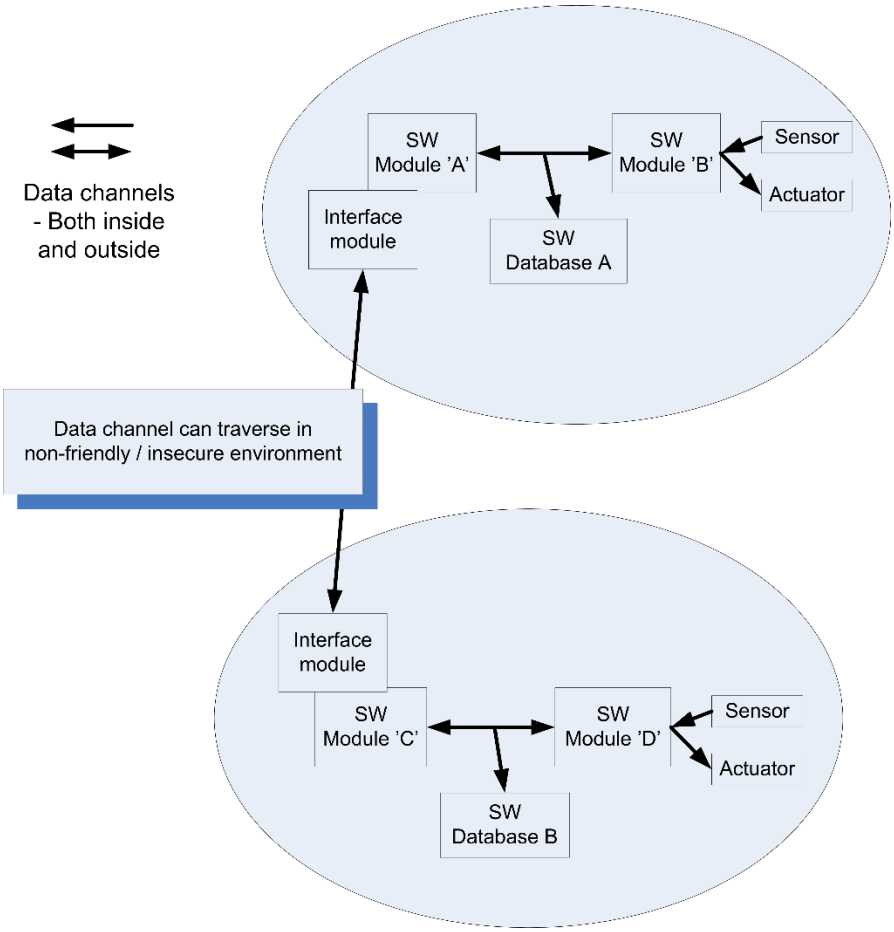

Figure 2: Software modules in two systems.

Confidentiality and integrity are the most important requirements when data is running in non-friendly or insecure environment. Availability is a more speculative requirement. With service level agreement (SLA) a certain level of guaranteed availability can be reached. In the case of single internet operator, SLA is a single agreement, but with multi operators SLAs are more complex completeness.

VPN (virtual private network) is a method for data flow in non-friendly environment, basically VPN encrypts data and checks integrity, but not guarantees availability. There are several methods and products for VPN, e.g. a simple solution is SSH[14] and LAN-to-LAN is more complex. Offices in different cities are typically connected by a LAN-to-LAN VPN and a single device can be connected by SSH.

4.4 Cybersecurity requirements for autonomous machine systems

Based on the standard IEC 62443, seven requirements are proposed for supporting AMS related cybersecurity development. However, other requirement sets can also be used. For example, standards IEEE 802.11p or Intelligent transportation System (ITS) could be valuable to analyse further for the requirement set.

All places where data is stored, transferred or handled should be analysed using these seven requirements. Table 1 can be used to document the analysis, including also consideration for whether each of the requirements is relevant for the case at hand.

Table 1: Seven requirements for autonomous systems cybersecurity

Requirement	**Valid (yes,no)**	**Note for valid**	**Other notes**
Identification and authentication control (IAC)	.	.	.
Use control (UC)	.	.	.
System integrity (SI)	.	.	.
Data confidentiality (DC)	.	.	.
Restricted data flow (RDF)	.	.	.
Timely response to events (TRE)	.	.	.
Resource availability (RA)	.	.	.

4.4.1 Data flow actors

Table 1 above includes 'Identification and authentication control' requirement, which could cover also data flow actors (sensors, actuators, SW and databases). It is very important to secure that it is working with a guaranteed party. This requirement protects against man-in-the-middle attacks, which can be a very severe threat and problem. This can be seen as a mandatory requirement in the cases where data is flowing between different physical machines. With a single machine, this requirement shall be at least analysed.

4.4.2 White and black channels

The IEC 61508 standard defines that following issues shall be taken into account in data communication: transmission errors, repetitions, deletion, insertion, re-sequencing,

[14] Referring to the Finnish SSH company offering SSH solutions

corruption, delay, and masquerade. If a channel meets IEC 61508 requirements it is called as 'white channel', otherwise the channel is 'black channel'.

It should be noted that VPN is a tunnel in the channel. Even if the channel is a black channel, with tunnel mechanism (like VPN) the black channel can meet most of the requirements set by IEC 61508. As discussed, availability could be difficult, other difficult thing is delay with VPN (in some views availability and delay has relation with each other).

In the case of Internet Protocol, it should be noted differences between protocols of UDP and TCP. The UDP is designed for real-time operations and it has not any reliability features, it just send data packets without checking. If the use of UDP is needed, reliability mechanisms shall be implemented at upper level than UDP. TCP provides reliable (but not secure) communication with control mechanisms for data packet flow.

The issue can be considered from the point of view of layers of OSI (Open Systems Interconnection) model, which are: 1. Physical, 2. Data link, 3. Network, 4. Transport, 5. Session, 6. Presentation, and 7. Application. Both UDP and TCP are located in layer 4. Transport in OSI model[15].

IPsec and TLS are security mechanisms, IPsec is a protocol suite for VPN solutions and TLS (formerly SSL) is mainly for sessions. In OSI model, IPsec locates on layer 3 and TLS locates on layer 6. Note: TCP and UDP are on layer 4.

The SSH, which is a secure protocol in Internet world (like as 'a simple VPN'), typically run over transport layer, as RFC 4251 defines: The Transport Layer Protocol [SSH-TRANS] provides server authentication, confidentiality, and integrity. It may optionally also provide compression. The transport layer will typically be run over a TCP/IP connection, but might also be used on top of any other reliable data stream.

4.5 Trusted Platform Module

One solution to meet cybersecurity requirements in autonomous systems is to use Trusted Platform Module (TPM)[16]: "TPM is an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys... Trusted Platform Module (TPM) was conceived by a computer industry consortium called Trusted Computing Group (TCG), and was standardized by International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) in 2009 as ISO/IEC 11889.".

The use of TPM seems to increasing, e.g. in car/vehicle industry[17][18]. TPM solution is also available in software C code, i.e. enable to use in simulations[19]. Properly designed TPM should not cause operations to become slower. TPM generally does not perform heavy cryptographic calculations, and if needed, a cryptographic accelerator can be used for heavy calculation.

[15] https://en.wikipedia.org/wiki/OSI_model

[16] https://trustedcomputinggroup.org/resource/tpm-main-specification/

[17] http://etn.fi/index.php/13-news/8990-turvapiiri-tulee-myos-auton-datalle

[18] https://www.infineon.com/cms/en/product/security-smart-card-solutions/optiga-embedded-securitysolutions/optiga-tpm/sli-9670/

[19] Markku Kylänpää, a member of VTT's cybersecurity team, is an expert of TPM.

4.6 IPR and secret data

Immaterial matters (IPR) shall be protected so that they are not easy to find out also in non-friendly environment. For example, an algorithm can be a valuable IPR.

Single computer or system can include confidential data from several operators. General requirement is that unauthorized operator or other user shall not have access to confidential data.

5. Secure development environments

In analysis of the whole system lifecycle (which consists of 1. Creation, 2. Development, 3. Operation / Use / Maintenance, and 4. Disposal / Removal), the development phase is very critical, to ensure that the end product includes only what was planned and not anything extra. Entering the development system is a very powerful method for harmful operations. There are two main questions regarding the development system:

- How to ensure that software compiler is not corrupted?
- How to remove a harmful part from the product, if the harmful part has been entered successfully during the development phase?

A fact is that different SW-compilers produce different results (executable file) from the exact same source code, which makes direct and easy comparison between results of compilers impossible. Another fact is that corrupted software compilers occur very seldom, but it is possible.

A practical way is to use commonly used SW-compiler(s) and to follow cybersecurity news and other sources, where possible corrupted SW-compiler(s) should be reported. A doctoral thesis 'Fully Countering Trusting Trust through Diverse Double-Compiling' (2009) by David A. Wheeler[20] presents a method for testing whether a SW-compiler is corrupted. This method, however, is quite complex and perhaps not suitable for daily usage.

If a corrupted SW-compiler is detected, it is costly and time-consuming work to install a clear (un-corrupted) version of SW-compiler and then re-compile all software.

Mainly software development aspects were discussed here, but nowadays also hardware development uses directly software-based tools or software-related tools. Therefore, threats of corrupted tools are valid for both software and hardware development systems. In the risk perspective, it can be assumed that the probability of using a corrupted tool is very low but the consequence is catastrophic.

In summary, the guidance is (at least) to use commonly used SW-compiler(s) or other software based tools and to follow cybersecurity news and other sources, where possible corrupted tool(s) shall be reported.

6. Conclusions

As increasingly autonomous machine systems are developed, their sensitivity to cybersecurity threats is seen to increase. The world of cybersecurity is highly dynamic and

[20] https://dwheeler.com/trusting-trust/dissertation/wheeler-trusting-trust-ddc.pdf

constantly in change. For example, certification of cybersecurity is an area with many developments ongoing.

To succeed in this dynamic environment, cybersecurity shall be incorporated as an integral part of system design right from the early concept development phases. To support this, this report provides suggestions for cybersecurity standards and guidelines to be followed, as well as recommendations for requirements to be considered in AMS design.

Appendix 1. Abbreviations

This section provides an overview of abbreviations used in this document. Additional definitions in English, Finnish and Swedish can be found in the Vocabulary of Cyber Security by The Finnish Terminology Centre TSK.[21]

Abbreviation	Definition
AMS	Autonomous Machine System
CC	Common Criteria
ENISA	The European Union Agency for Network and Information Security
ETSI	ETSI is a European Standards Organization (ESO)
ICS	Industrial Control System
IEC	The International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet protocol
IPR	Intellectual Property Rights
IPsec	Internet Protocol Security
ISO	International Organization for Standardization
ITS	Intelligent transportation System
LAN	Local Area Network
NIST	The National Institute of Standards and Technology
OSI model	Open Systems Interconnection model
RFC	Request for Comments
SANS	SysAdmin, Audit, Network and Security
SLA	Service Level Agreement
SSH	Secure Shell
SW	Software
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
VTT	VTT Technical Research Centre of Finland Ltd.

[21] http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Appendix 2. Selected examples of cyberattacks

Several cyberattacks and potential threats in current and future technologies have recently been reported. Below, selected cases from several sectors from years 2008–2019 are listed (newest first) to give an overview of the situation. Generally, all sectors and all systems are under threats of cyberattacks.

- Hacking of a hospital device to manipulate diagnoses (in Finnish): https://www.hs.fi/teknologia/art-2000006059385.html
- A lens maker's factory was hit by a cyberattack at its key production base in Thailand: https://www.japantimes.co.jp/news/2019/04/06/business/corporate-business/hoya-hit-cyberattack-february-disrupting-thai-factory-operations/
- Cyberattack on Norsk Hydro, where manual control was forced to use: https://www.theregister.co.uk/2019/03/19/norsk_hydro_ransomware/
- A Department of Homeland Security official admitted that a team of experts remotely hacked a Boeing 757 parked at an airport (in Finnish): https://www.tekniikkatalous.fi/tekniikka/kyberturvaosaston-tyontekijat-onnistuivat-hakkeroimaan-boeing-757-lentokoneen-6687032 and (in English) https://www.csoonline.com/article/3236721/security/homeland-security-team-remotely-hacked-a-boeing-757.amp.html
- Industrial robotics related issues have also been reported: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/rogue-robots-testing-industrial-robot-security. This article includes five steps how an attack can be performed. Another article on the same issue: https://www.wired.com/2017/05/watch-hackers-sabotage-factory-robot-arm-afar/
- Cyberattack against the electric grid of Ukraine (in Finnish): https://www.hs.fi/ulkomaat/art-2000002878434.html and (in English): https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
- Cyberattack against a steel company in Germany (in Finnish): https://www.hs.fi/ulkomaat/art-2000002787644.html and (in English): https://www.bbc.com/news/technology-30575104
- Well-known harmful computer worm Stuxnet is a milestone in cyber world – even to the extent that the time before and after Stuxnet are used as definitions. Many analyses and articles have been written on Stuxnet, some of which can be accessed e.g. through the Wikipedia page: https://en.wikipedia.org/wiki/Stuxnet.
- Hacking of a tram network by a teenager in Poland: https://www.theregister.co.uk/2008/01/11/tram_hack/. This was performed using a modified TV remote control unit.