Tuija Kuparinen-Koho

RISKS IN USER INTERACTION OF ALARM FUNCTIONALITY IN SITUATION AWARENESS SYSTEMS

Master's thesis

Master of Engineering, Cybersecurity

2020

South-Eastern Finland
University of Applied Sciences

South-Eastern Finland University of Applied Sciences

Author (authors)	Degree	Time
Tuija Kuparinen-Koho	Master of Engineering	May 2020

Thesis title

Risks in the user interaction of alarm functionality in situation awareness systems

113 pages
1 appendix page

Commissioned by

South-Eastern Finland University of Applied Sciences

Supervisor

Vesa Kankare

Abstract

This study aimed to identify how the perception of user alerts is supported by design instructions and standards, examine possible and realized risks associated with losing situational awareness regarding alerts, and report cybersecurity issues related to user interaction and poor design in situations requiring special attention in the cyber physical environment.

This thesis was a qualitative study combining empirical and theoretical research strategies. The empirical part was carried out by examining investigation reports published by traffic management authorities in the context of deficient situation awareness. The theoretical part was accomplished by a literature review focused on situation awareness, risks related to it and means to foster it.

The results show that in a single accident, multiple errors in situation awareness and at different system interfaces can occur simultaneously. Situational awareness was found to be often weakened by the problems in perception. Human-software interactions, as well as human-to-human interactions are vulnerable to multitudinous errors. Furthermore, it was found that the risk of vulnerability increases with the complex and inter-connected ICT systems being as targets for cyberattacks.

Keywords

situation awareness, alert, alarm, user interaction, situation awareness systems, cybersecurity, risk

CONTENTS

1 INTRODUCTION

The loss of situational awareness might lead to severe accidents. On 24th July 2013, the derailment of a high-speed train caused 80 deaths and 152 injuries in Spain. The accident was a result of a loss of situation awareness of the engine driver, caused by misinformation of the speed due to configuration and compatibility problems on the information and management systems. (Fernandez et al. 2017.)

As shown above, there can be multiple factors contributing to the loss of situation awareness. In this study, a multi-disciplinary approach to situation awareness and alarm functionalities is applied in order to highlight issues related to human computer interaction (HCI) and cybersecurity in the fields of communication and information system sciences and information engineering (IE). Thus, based on this framework, the loss of situation awareness is reviewed from a system perspective that emphasizes interactions between the system components. The SHELL-model, developed by Edwards in 1972 and depicted in Figure 1 below, demonstrates the overall interactions in the cyber world. The model was originally designed for aviation and it implies that there is not necessarily a sole cause for accidents (Perry and Perezgonzales 2010).

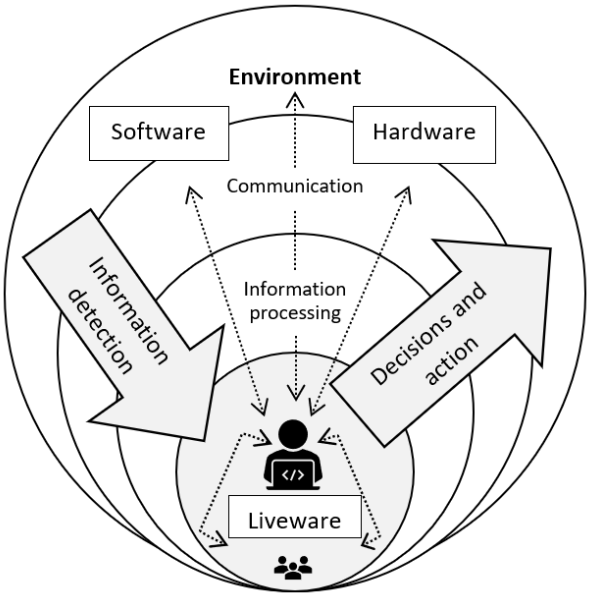


Figure 1. Interaction model (paraphrased SHELL-model from Aviation Knowledge 2010, 2013 and Skybrary 2019.)

The SHELL model represents human factors (Perezgonzales 2009) which as a multi-disciplinary approach views people in working situations, their relationship with machines (software and hardware) and surrounding environment, as well as their relationships with other people (liveware). The re-engineering of physical and social environments is essential in human factors approach to respond properly to functional requirements and to acknowledge the capabilities and limitations of the human operators. Thus, the practices concerning the implementation of human-technical interfaces and technical designs are emphasized in the discipline of human factors through the concept of ergonomics. (Perezgonzales 2013.)

The SHELL model can be used as a basic aid to understand human errors in interactions between system components. Errors can take form at the liveware-software interface as misinterpretations if symbols, checklists or documents are considered confusing, ambiguous or irrational. An example of this mismatch is the death of passengers and crew in 1980 in a flight cargo fire when it took too long to find and follow the instructions on how to respond to a smoke alarm. Similarly, liveware-hardware interface can suffer from deficit equipment design or defectively coded control devices such as warning systems that fail to alert. This was a factor in 1974, when a flight crew ignored a terrain warning alarm, which caused the plane

to crash. The alarm was simply regarded as a nuisance. In the case of liveware-environment interface, errors can occur in human perception or be caused by biased decision making. As an example of the former is a plane crash in 1985 caused by communication difficulties due to high ambient noise levels in the cockpit. Finally, liveware-liveware errors concern communication between human individuals and can take form as communication breakdowns, for example, between the flight crew and the air traffic controller. (Perry 2010.)

Regarding the aforementioned system perspective, the socio-technical system approach includes people, equipment, technology, hardware, software, data, and procedures as system components and focuses on their interactions (Charitoudi and Blyth 2012). This system approach is applicable for understanding the impact of the loss of situation awareness on organizations. Complexity increases as the world becomes more connected with the cyber environment evolution exposing new system vulnerabilities, so cybersecurity needs to be viewed holistically from the lens of systems thinking (Salim and Madnick 2016). The holistic approach considers security problems as simultaneous errors in the interrelationships between users and technologies and the social and technical components (Mujinga et al. 2017).

According to the Cyber Security Glossary published by the Security Committee 2018, cybersecurity refers to the security of a digital and networked society or organization and its impact on their operations. Cybersecurity is a target state of the cyber environment where it can be trusted and protected, and where security risks are under control. Cyber environments are, for example, ICT-based transportation and logistics systems, traffic control systems, and plant control systems. In the cyber environment, vulnerabilities that enable or can be used to cause harm, malfunction or danger can exist in information systems, processes, and human activities. (Vocabulary Center TSK, 2018.)

The loss of situation awareness can be viewed as implications or appearances of human factors and cybersecurity. The objectives, research method and research questions of this study are introduced in the following chapters. This introduction part introduced the nature of situation awareness as a research subject,

emphasized its significance and described the scientific framework. The concept and model of situation awareness, as well as ergonomic, environmental and information system aspects are introduced in Chapter 2. Chapter 3 describes issues in the design of situation awareness systems. Chapter 4 presents a concept of false alarms and examines risks that potentially compromise situation awareness related to human factors and cybersecurity. Situation awareness in different domains is reviewed in Chapter 5 which presents the survey results based on a content analysis of incident reports. Finally, conclusions are made in Chapter 6, and the reliability, validity and effectiveness of this study is estimated. Topics for further research are recommended in Chapter 6 as well.

1.1 Objectives of the study

The aim of this study is to investigate how situational awareness systems can implement situational awareness through visual usability in user informing taking into consideration the risks associated with the reliability, integrity and availability of situation information by means of an user interface and impact of this information on user decision making. Here, situation information focuses on alarms, which are signals of abnormal or dangerous events. A parallel term is alerts, which includes warnings, cautions, instructions, messages and communications requiring immediate attention and action by the user (Yeh et al. 2016). A derived theoretical research assumption is that a malicious attacker, by triggering unnecessary or false alarms, or otherwise influencing to alarm data, causes alert fatigue, which leads to loss of situational awareness.

This study does not discuss the relationship between situation awareness and situation assessment, nor does it review the functions of orientation, decision making or action, beyond observation roughly (“OODA” loop). Out of the scope is also examination of various user interfaces (such as graphical, voice control, haptic, and multimodal) or detailed design guidance for them. Furthermore, this thesis does not describe in any detail the anatomy of the human senses (such as touch, taste, smell) in the perception of alerts, or knowledge management or alarm

management. Situation awareness models and related cognitive processes are not compared. Here, unraveling or analysing exact attack techniques and vulnerabilities is not included because identifying them and their impact is considered to be sufficient. The means to rectify and improve defective systems, solutions, circumstances or working conditions (e.g. control rooms) are not studied, but proposals are made in this respect for further research. This study particularly aims to determine whether false alarms compromise situation awareness, and therefore, validation would be best done in a study using a possible practical case.

As the system environments become more diverse, and the amount of information available increases, the use and number of integrated situation awareness systems will increase. In this context, it is important to bring up the debate on the risks of use and design tools that can reduce the cognitive burden on the user from the perspective of information flooding, detection and decision making. This study aims to provide more information and understanding, because serious defects in situation awareness can literally cause planes to drop from the sky, or trains to derail, or plants to malfunction, or even patients to die. The following Figure attempts to explain some main elements of the entity of this study.

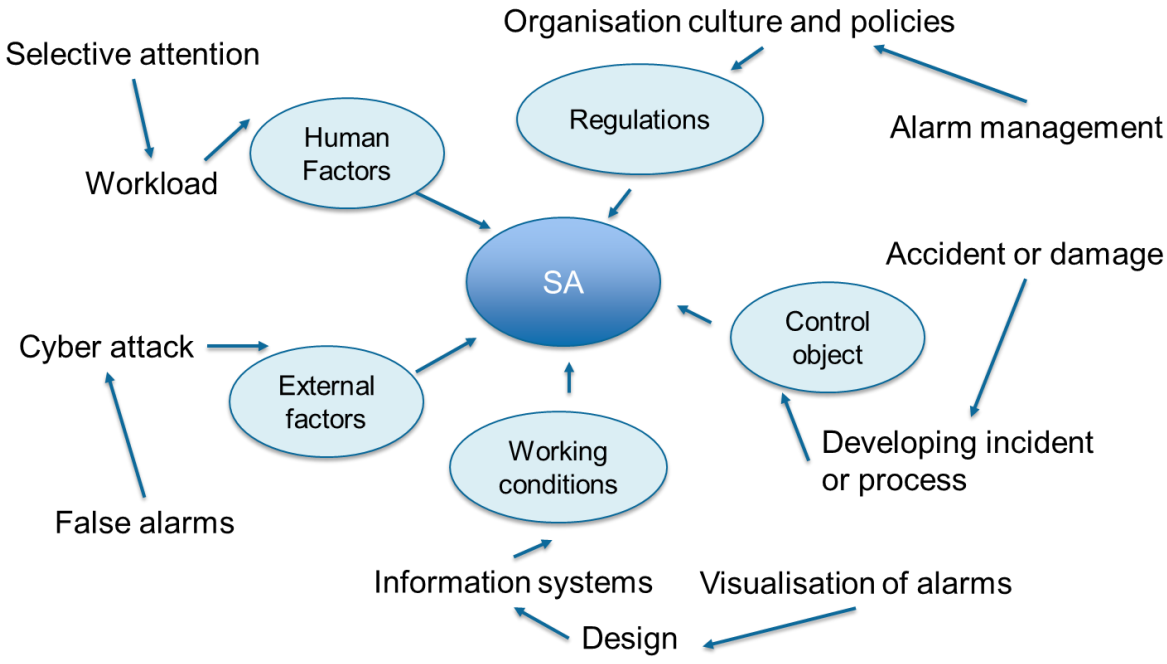


Figure 2. The elements describing the scope of the study

Based on a literature review, previous studies and the research text samples, this study seeks to determine what principles, standards, and guidelines can be used to ensure a user-friendly and safe interface, and what abnormalities or incidents, such as information security events or alert fatigue, occur in socio-technical systems including situation awareness systems that compromise cybersecurity in the context of alarm functionalities.

1.2 Research method

This study applies qualitative research methods combining empirical and theoretical research strategies. The aim of empirical research is to study the characteristics, types and themes of an existing phenomenon by directly examining the phenomenon or by using related material (Koppa 2010). Theoretical research, on the other hand, does not immediately observe the research objects, but seeks to outline conceptual models, explanations and structures based on earlier research literature (Koppa 2010).

In this study, the focus of the empirical part was on examining the investigation reports published by traffic management authorities in the context of deficient situation awareness. The theoretical part was accomplished by the means of literature review focused on situation awareness, risks related to it and means to foster it. This aimed to provide comprehensive information on the quality, properties and aspects of situation awareness and form a conception of the whole, as defined by the principles of qualitative research (Koppa 2015).

Herein, the hermeneutical method, being typical for qualitative research (Koppa 2018), is fruitful in producing interpretations of situation awareness, as well as means and risks related to it. Results of this study were produced by reviewing relationships between subjects around situation awareness in order to gain expanding understanding of it.

In the framework of this study, it is considered important that one must first understand situation awareness as a phenomenon, and then determine how the perception of alerts is supported by design instructions and standards in general. After that, the possible and realized risks associated with losing situational awareness can be examined. Finally, conclusions can be made to summarize the findings.

However, while presenting subjective interpretations, as is typical of hermeneutical research, new interpretations can emerge. This may, in turn, produce opposite interpretations, novel applications, and new research themes to gain a better understanding of the original phenomenon. Definitive results are not necessarily produced, as they depend on momentary interpretations of the researcher. (The Helsinki Term Bank for the Arts and Sciences 2016.)

What follows from what is described above, is that the results of one study can diverge from the results of another, when survey and conclusions are made by another researcher. Thereby, this study represents only one kind of viewpoint on situation awareness loss.

1.2.1 Information retrieval

The objective of the study required that information about safety incidents in transportation and communication was collected and analysed, and literature of situation awareness as a phenomenon was studied. The support available for users on the perception of alerts and cybersecurity issues related to user interaction was studied by reviewing design instructions and standards.

The material selected for analysis was already collected and published material related to the research subject, the so-called secondary data. In this thesis, the qualitative analysis of the connections between phenomena was based on a hermeneutic analysis and on a close reading (Koppa, 2009). The contents of the research material were summarized, structured, integrated and assembled in order to answer the research questions (Saaranen-Kauppinen and Puusniekka 2006).

Such material, that was current, actual, and relevant, openly accessible, and thus no more than ten years old, was selected for this study. However, it must be noticed that substantive theories of situation awareness by Mica Endsley date from the late 1980s onwards, and some safety related models date back to the 1970s. The source material for the theoretical background consisted of literature and previous publications that discuss the concept of situation awareness, influencing human factors and risks related to perception. The study material included interface design standards, style guides and guidelines for alarm functionalities, as well as investigation reports and vulnerability findings on alert functionality related incidents. In particular, the Public Transport Agency's public reports on rail and fairway safety incident reports, the Maritime Accident Analysis, Traficom’s published aviation accident statistics, investigation reports by Accident Investigation Board Norway and the US National Transportation Safety Board's Accident Reports on Aviation, Marine and Railroads are used.

As presented in Table 1 below, reports of serious accidents were searched from various databases with such keywords as "situation awareness", "situational awareness", "false alerts", "false alarms", "failure to monitor", "monitor problem", “warn” and “wrong al”. Fault categories such as “the human-machine interaction” were used if possible. This was done in order to gain an understanding of the effects of the loss of situational awareness and factors that had led to an erroneous view of a situation. Relevant reports were selected if they were published between 2010 and 2020.

Database	Information product	Traffic mode	Accepted	Search words	Search method	Limitations
Safety Investigation Authority Finland; https://turvallisuustutkinta.fi/en/index/tutkintaselostukset/ilmailuonnettomuuksientutkinta/tutkintaselostuksetvuosittain.html	Investigation reports	Aviation	14	"situation awareness"; "situational awareness"; "false alert(s)"; "false alarm(s)"; "failure to monitor"; "monitor problem"; "warn*"; "wrong al*"	extraction of single reports year by year	Situation awareness not related to or not in context of alarm functionalities or vice versa. Reports published only in finnish or english.
Accident Investigation Board Norway; https://www.aibn.no/Luftfart/Published-reports	Investigation reports	Aviation	3		text search with search words and time	
Accident Investigation Board Norway; https://www.aibn.no/Jernbane/Published-reports	Investigation reports	Railroad	1		text search with search words and time	
Accident Investigation Board Norway; https://www.aibn.no/Sjofart/Published-reports	Investigation reports	Marine	3		text search with search words and time	
National Transportation Safety Board U.S.; https://ntsb.gov/investigations/AccidentReports/Pages/aviation.aspx	Investigation reports	Aviation	4		text search with search words and time	

Table 1. Information search

1.3 Research questions

The main research question was “What are the risks in the user interaction of situation awareness systems with relation to alarm functionalities?” Further, the main question was divided to sub-questions as follows:

1. What aspects of cybersecurity are present in user interaction in the operating environments of situation awareness systems with relation to alarm functionalities?
    a. What information can be found in literature about situation awareness and supporting it in situational awareness systems?
    b. How are alarm functionalities supported and implemented as a part of situation awareness in situation awareness systems by design guidelines?
2. What are the effects of losing situational awareness?
    a. Are safety incidents or accidents related to the loss of situation awareness appropriately reported?
    b. Based on the accident reports, what are the main reasons for losing situation awareness in relation to alarm functionalities?
3. What factors can potentially compromise situational information in the context of alarm functionalities?
    a. What human factors can influence situation awareness?
    b. What kinds of cyber threats can compromise situation awareness?

The first task in this study was to gather information on the aspects of cybersecurity related to user interaction in the operating environments of situation awareness systems. The purpose was to examine the audio-visual language that provides user information in alarm functionalities of situation awareness systems and its effect on the cognitive load experienced by the user in perception based on guidelines, standards, and style guides. Also, the learning objective was to determine how user perception is supported through user interface design in situations requiring special attention and consider the likelihood for misrepresentation or misinterpretation of information.

The second task was to investigate the effects of the loss of situational awareness by examining reports and statistics on air, sea, and rail accidents. The information was obtained from public sources by utilizing investigation reports from Finland, Norway, and U.S. The result content of selected reports was classified by type of deviation, cause (creator) and consequence (effect) through interpretation.

The third task was to explore factors that may compromise situational information. The availability of accurate situational information is considered necessary to gain a correct understanding of a particular situation in a cyber environment. This exploration was accomplished by reviewing security incident and vulnerability reports and previous studies of human perception.

In this study, the alarm functionality is seen as illustrated in Figure 3:

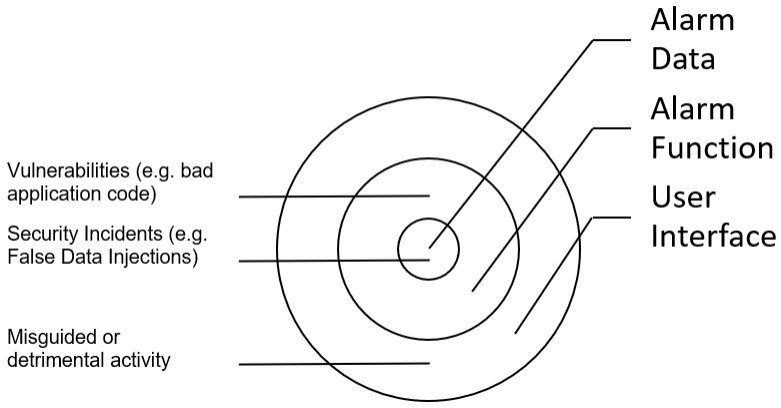


Figure 3. Alarm Functionality in a Situation Awareness System (Lal 2013, paraphrased.)

2 SITUATION AWARENESS

Situation awareness is a description or understanding of the current situation, its underlying factors, and possible alternatives to its development (General Finnish Ontology YSO 2020), and is formed by the perception of environmental elements (Crane and French in Stanford Encyclopedia of Philosophy 2017). According to much citated Endsley's (1999) model presented in Figure 4 below, situation awareness involves three levels: perception as an awareness of environmental factors, comprehension as an understanding of the meaning of what was perceived (recognizing, interpreting and evaluating the significance) and projection as an ability to predict the situation in the near future (based on perceiving and understanding the dynamic elements of the environment).

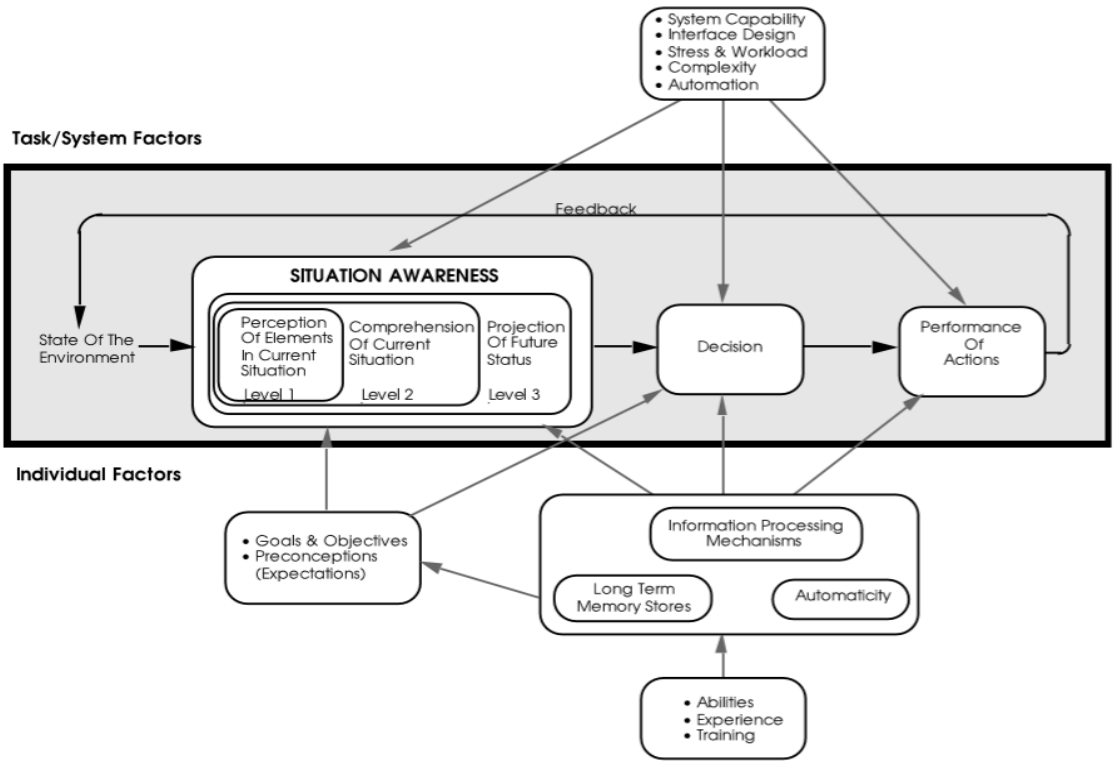


Figure 4. Situation awareness (Endsley 1999, originally 1995)

The relevant human cognitive functions for situational awareness must be recognised in order to perform a specific task or job required, as well as ensure

that the working environment is suitable for the task´s requirements. To achieve situation awareness, the abilities of sensation and perception must be facilitated so that one can, for example, hear (auditory perception) and see (visual perception) warning signals or discern alert symbols on the monitor or display. An ability of attention must be realized to focus on the perceived information, for example, in a control room where a supervisor monitors changes in the situation. Working in the environments, such as control or command centers, is complex and dynamic by nature due to constant changes in the perceptual environment. People must react rapidly and make decisions under the pressure of time, as e.g. air traffic controllers are required to do. Situation awareness will have to be complete and accurate. (Kalakoski 2016.)

The aforementioned human cognitive functions are parts of the cognitive processes which can be categorised from lower order thinking skills to higher order thinking skills (Revised Bloom's Taxonomy by Iowa State University of Science and Technology). The lowest skill is recollection which comprises remembering, recognizing and recalling and can be concretized in situation awareness e.g. by recognizing the current state of matters. The next skill in the hierarchy is understanding which comprises interpreting and classifying and can be concretized, for example, as in necessity to understand the alert priority in a situation awareness system. The skill of understanding is followed by application comprising execution and implementation, for instance when carrying out an immediate remedial action triggered by an alert. Proceeding further on the hierarchy, analyzation encompasses focusing and organizing and refers to e.g. selecting the most suitable procedures in a given situation. The next skill is evaluation which comprises checking and critiquing and refers to, for example, judgment made on the basis of action results and efficiency in an alert situation. The highest skill in this hierarchy is creation which encompasses generating and planning and refers to e.g. hypothesizing and constructing an updated mental model of the current situation as a whole. (Iowa State University of Science and Technology 2020.)

As a human cognitive process, processing of information when adjusting orientation to a situation proceeds from observation and direction of attention to structuring of information, and further to direction of activities, and finally to motivation (Timonen 2013). Figure 5 describes the cycle of information processing and the factors, objects, properties, starting points and conditions of related sub-processes.

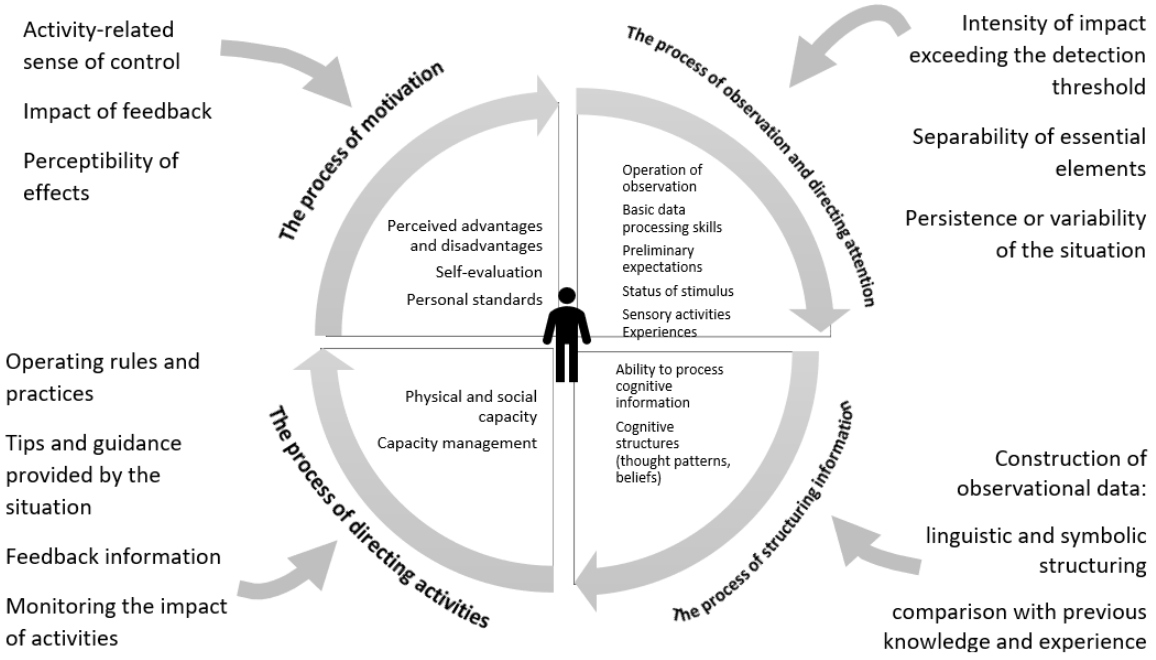


Figure 5. Information processing on situation orientation (Timonen 2013, paraphrased)

In the cognitive processes, according to semiotician C.S. Pierce, there are three levels of reality experience e.g. phenomenological categories (Figure 6), firstness, secondness and thirdness. Firstness refers to immediate experience without interpretation. Secondness relates to experience that arises when a perception is reacted to or interpreted in the light of previous experience. Thirdness signifies experience formed through logical reasoning and analysis. (Koponen et al. 2016.)

A German philosopher Edmund Husserl described time as a tripartite structure consisting of protention, the now-point, and retention. Protention is the anticipation

of the future constraining the various expectations constituting and conditioning of which is coming. Retention refers to the chain formed of the past and the reflections of previous phenomena kept in consciousness. Husserl stated that time-consciousness provides the organizing basis for all other activities of consciousness. (Dainton in Stanford Encyclopaedia of Philosophy 2017.)

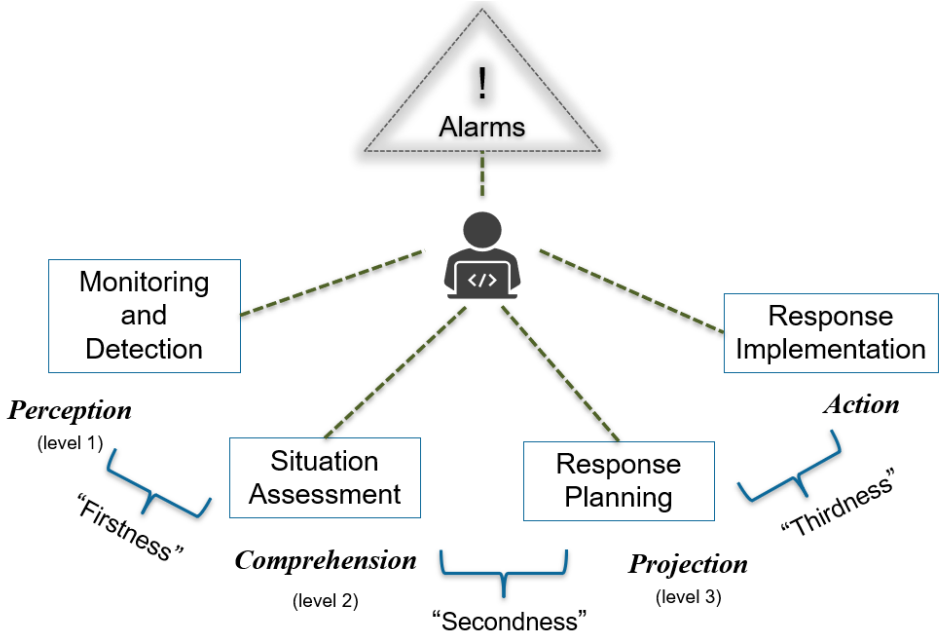


Figure 6. Combined depiction of situation awareness (Endsley, Kalakoski and Pierce, paraphrased)

As described above, Pierce's model offers a theoretical basis for sign functioning. It represents a triadic relationship between a sign or representamen (a first), an object (a second) and an interpretant (a third) (Everaert-Desmedt 2013). Based on this, an alarm message is an indexical spatio-temporal sign of something being not right, presented usually as a symbol (legisign), and demanding understanding, interpretation and action from the observer.

Perception involves sensing and filtering stimuli by directing attention. Stimuli received by sensory organs and successfully filtered by the brain are subject to interpretation so that their significance in each situation can be assessed. An individual light, sound signal, or symbol acquires its operational content through

interpretation. The interpretation is based on the models in memory about the corresponding stimuli and their meaning. Through successful interpretation, insight arises. (Safety Investigation Authority 2004.)

Symbols as signs are visual elements that describe their object in the simplest way through the "this is X" relation. The symbol can be merely figurative, i.e. iconic, or contractual, i.e. symbolic, and tells only what it is and to which category this object belongs. Information can also be conveyed as glyphs, which means a pattern that describes, in addition to its classifying or qualitative meaning, quantitative or other information related to an object in some form. Thus, the glyph is multidimensional, but a symbol can also be considered as such if it represents (encodes) quantitative or other information whose meaning consists in the interrelationships of its parts. (Koponen et al. 2016.)

Regarding visuality, it has been estimated that the visual sense transmits information eight times more to the brain than all other senses combined, i.e. circa 10 Mb/s. Although the exact amount of information cannot be directly measured, it has been found that the fastest way to acquire new information is to have it in visual form. Visual perception is particularly pronounced in the interpretation of glyphic features (such as higher bar, larger sphere). In this visual reading, at the elementary level the value of a single data point is read (e.g., the length of a single bar), at the general level the whole pattern is read (e.g., the bar graph trend), and at the intermediate level answers to specific questions are searched (e.g., a comparison of trends for selected time periods described in the time series). (Koponen et al. 2016.)

This chapter has provided a brief summary of the theoretical background relating to situation awareness through the aspect of cognitive processes. In the following sub-chapters, the concepts of cognitive and information ergonomics are introduced, as well as the applications of situation awareness.

2.1 Cognitive ergonomics

Cognitive ergonomics focuses on the interaction between a human and a technological system. It applies scientifical principles of human cognitive functions, e.g. perception, attention, data processing, decision making, and motivation. The areas of application include the design and evaluation of equipment, work processes, systems and environments. Methods in the field of cognitive ergonomics are also applied in accident investigation. The aim of cognitive ergonomics is to promote fluency and safety by reducing operational risks. (Haavisto 2006.)

Haavisto (2006) argues that for some reason, when designing systems, there is a tendency to assume that human errors can be eliminated by adding technical systems and automating functions. However, it is natural for a human to make mistakes - this can never be fully eliminated. Nevertheless, the number of mistakes and the severity of their consequences can be reduced by adding safeguards between the operator and the system. The knowledge of a person´s natural behaviour can prevent accidents caused merely by one touch of a button. Second, the tasks can be designed in such a way that the technology supports the person in performing the work, i.e. by providing sufficient information in a suitable form that allows a formation of an understanding of the work process. The mere exterior design of a user interface with a fancy appearance is not sufficient, but one must also need to know how a person forms an understanding based on knowledge. (Haavisto 2006.)

Particularly in security-critical environments, where operations are controlled on the basis of large amounts of complex data, overly automated systems have been found to degrade the quality of human decisions. However, individual warning systems and the automation of sub-functions when the load is high facilitates human activities. Still, if the job includes solely the control of an automatic process where devices instruct the person on what should be done next, decision-making is impaired. A person cannot use the accumulated knowledge gained through work and education to make complex decisions, instead, an automation system guides him to an overly straightforward decision. Thus, excessive job automation can

cause ignorance on what is going on in the work process. Many systems do not even operate according to human logic of thinking, but according to computational principles, in which case they actually entice a person to make mistakes. (Haavisto 2006.)

For example, an air traffic controller must be constantly provided with sufficient and easily understandable information on aircraft speeds, altitudes and directions in order to be able to form an overall picture of the situation and to anticipate future situations. The actions should not be directed by user interfaces, but the person. (Haavisto 2006.)

The field of cognitive ergonomics has generally developed rapidly, and methods of the field have been used in the design of nuclear power plant work processes and interfaces, in research and development of military environments, in aeronautics research and development, and in health care, especially in anaesthesia and safety. In Finland, the utilization of cognitive ergonomics expertise in increasing fluency and safety has so far been limited. (Haavisto 2006.)

Visual usability is an important element of cognitive ergonomics. The productivity of work is reduced if data are presented in an inappropriate form or have to be extracted from a varying or vague field of observation. When attention is paid to visual usability, performance and effectiveness of a worker is accelerated. The speed of data reception and processing can be multiplied by the clear display and correct layout of information. Also, in terms of visual usability, the placement of the information, i.e. layout, display and lighting, resolution, font size, colour and darkness variations is an important factor. The visualization of datasets helps to better understand the data and its significance, especially if the datasets are large and complex. (Lähdeniemi 2013.)

2.2 Work and information ergonomics

Franssila et al. (2014) define work ergonomics as a field of specialization that studies the phenomena and processes related to processing and management of

information and in complete information work environments. Information ergonomics aims at balancing an employee's cognitive abilities with the demands of the information environment. Above all, information ergonomics develops and adjusts everyday work practices and the overall information environment of work. Information ergonomics seeks to maintain and increase performance through information workload management practices, tools, and development techniques, while maintaining the information workload at a manageable level. (Franssila et al. 2014.)

Information ergonomics is reflected through information design i.e. the structuring of information into a format that is best suited for human use. Information should be presented in a clear way and it should follow two key principles: the comparison and simplification of content. The comparison concerns the interrelationships of matters and situations (e.g., normal mode vs. exceptional mode) and presupposes a consistent use of symbols, scales, and colours. The simplification of content means that only the information with the greatest significance is described. The physical design should aim to improve the discoverability of information, while the cognitive design should ensure the understandability of information and, finally, the affective design should allow for the emotional aspect of information. The latter ensures what emotions are triggered, for example, by an alarm signal and how it directs a person to correctly position oneself and act on them. (Koponen et al. 2017.)

Situational information must also be authentic, non-repudiable, intact and available so that to it can be trusted. It also should be timely, comprehensive and complete (Blasch 2012). Another requirement for situational information is the distinctiveness of information i.e. the observability of a message stimulus which affects human performance as the first factor in perception (Lähdeniemi 2013). Thus, receiving a stimulus is the first critical step in data processing (Lähdeniemi 2013). When the stimulus intensity is sufficient, the actual perceptual experience begins to take shape (Lähdeniemi 2013).

2.3 Control rooms

Work and information ergonomics are essential in control rooms. A control room represents a cyber-physical environment requiring special attention in order to ensure situation awareness. A control room can serve as a command center for controlling e.g. processes, operations, systems, equipment or networks.

Information security operations centre (ISOC) is an example of a control room and a command center. The Vocabulary of Cyber Security defines ISOC as an organization or part of an organization that creates, monitors and analyses the information security situation and status, prevents, identifies and analyses security breaches, documents them and responds to them in accordance with the guidelines. (Vocabulary Center TSK 2018.)

For example, the design of an air traffic controller's work station is substantial to the safe and efficient operation of the control room. Factors that affect safety include sound vs. noise, lightning and illumination, equipment, software design, readability of radar screens, ease of use of controls and efficiency of communications equipment. Successful controller working position constrains the integration of operational, technical and human factors expertise. (Skybrary 2018.)

A common room space can promote team-level situational awareness. When spaces are carefully planned, the productivity of operations can be improved, for example, by facilitating the sharing of situation information, and ideas and communication in general by placing actors and operators close together, which speeds up the exchange of information (Lähdeniemi 2013). Also, considering the significance of the sense of sight in the acquisition of new knowledge (Koponen et al. 2016), it is easy to understand the positioning and layout of the wide display screens in control rooms.

3 SITUATION AWARENESS INFORMATION SYSTEMS

A situation awareness system can be considered as any system that supports its user's situational awareness by visualizing relevant situational information for user perception and action. Nowadays, situation awareness systems can be equipped with real-time information fusion from different sources, enable basic data analysis and recognition, and allow for the presentation of the corresponding data using augmented reality principles (Fernandez et al. 2017). Extensive situation awareness systems can offer advanced decision support and analytics capabilities in addition to providing observation data. While situation awareness is a mental state, does situation assessment support it with the help of information fusion. Such applications are especially used in the military, medical, aviation, security, and environmental domains in order to synthesize manifold data into a single operating picture (Blasch et al. 2006). The situation awareness system should support all three levels of situational awareness, i.e. perception (detection), comprehension (understanding) and projection (predicting) (Koistinen 2011).

The aspect of this study regarding information systems is described with some examples in Figure 7. A situation awareness information system is viewed from the perspective of a user interface and an implementation of visualisation where interaction and information design have an impact on user interaction. User interaction is considered through the situational and user factors associated with perception, which expose operations to errors and may cause hazards. The cyber environment is viewed from the perspective of information and operational security events that have significance or consequences for the information displayed and the sources of alarms. These events may include security incidents, such as those caused by incorrect configuration of alarm sources and display errors, and may present a risk or hazard of use.

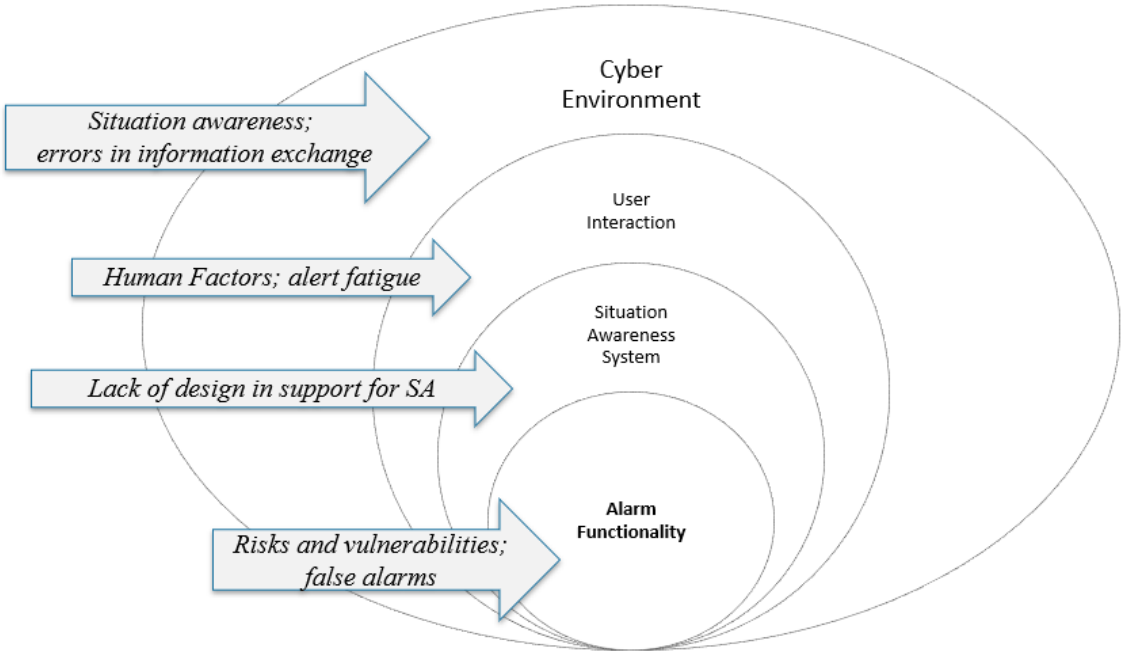


Figure 7. Sub-systems

This study aims to provide understanding how the safe use of a situation awareness system in the context of alarm functionality is supported through system design in a cyber environment. The cyber environment refers to the parallel concept of the cyber world, which refers to the totality of information networks and devices, information systems and their users, platforms and operating processes for processing information in digital form (Lehto 2019).

Based on the Open Systems Interconnection Reference Model (OSI), the structure of the cyber world can be described as a five-tier network model in which the semantic layer consists of information and data content in user and operator systems and management of user-controlled functions. The cognitive layer of this network model describes the problem-solving and interpreting environment of decision-maker, operator, and individual user information, a world in which information is interpreted and personal situational awareness is formed. (Lehto 2019.)

Each situation awareness system must have a balance between security, functionality, and user experience as shown in Figure 8. Inappropriate system

implementations weaken this balance and create an operating environment vulnerability. (Lehto 2019, paraphrased.)

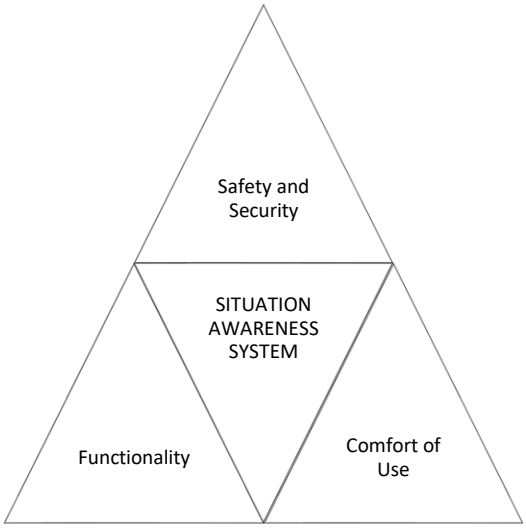


Figure 8. System Solution Priorities (Lehto 2019, paraphrased.)

Alarm functionality is implemented in graphical user interfaces according to the principles, standards and guidelines of alarm management. According to user experience architect Raj Lal (2013), user interaction implementation answers three questions: what does the user interface look like (visuality), how it is understood (cognition) and how it works (interaction). In case of deficiency in cybersecurity, a user can receive false information or operate in an impolitic manner based on information visualized in user interface. Malicious security breaches can per se lead to unsafe and dangerous actions.

The user interface design of information systems utilizes style guides, guidance from authorities and community operators, as well as standards, to ensure that the system functions appropriately for its intended use and is safe to use. Previous research has shown that a poor user interface design of systems and devices has led to serious incidents. This study highlights the risks associated with user-driven system alarm functionality.

User interaction design must address the needs of multiple user groups in a variety of environments, such as a protective clothing user with multiple display technologies in isolation mode. As systems and devices utilizing sensor technology

increase, more alarm functionality is produced, which can make the user tired of repetitive alarms (Gaba et al. 2013). Noise levels may be high, for example, in a hospital setting and may exceed the permitted guidelines.

As previously described, generic primary tasks of situation awareness consist of cognitive tasks, such as monitoring and detection, situation assessment, response planning and response implementation. Monitoring and detection, in turn, consists of activities involved in extracting information from the environment. For example, in current process systems these tasks are supported through various heterogeneous sensors and appropriate signal-processing methods, that are used to extract as much information as possible about the dynamic environment. (Naderpour et al. 2015, referring to O'Hara et al. 2011.)

Regarding the information extraction from environment, mentioned last in the previous paragraph, data fusion techniques are utilized. Data fusion refers to combining information (physical, informational or perceptual) to estimate or predict the status or mode of certain aspect of the environment (Steinberg et al. 1999). This information is presented in terms of attributive and relational states in these multi-source information systems, which provide data processing and control functions, several interfaces and associated data bases (Steinberg et al. 1999). Furthermore, to clarify the difference between data fusion and data mining, the first one aims to real-time detection of known patterns, whereas the latter concentrates on off-line discovery of new patterns (Llinas et al. 2004.).

Multi-source information systems cannot provide complete information solely by fused data from sensors or computer models, but there is a need for information originated by human expertise and knowledge also. Unobserved aspects cannot either be processed by a computer, so user knowledge and reasoning is necessary to be enabled. Thus, information systems should have properties of a reasoning system and enable control and review procedures, so that it could respond to user demands by the following features:

- knowledge acquisition procedures
- explicit representation of multi-sensor knowledge
- quantitative indicators of properties of fusion results

- intuitive, understandable displays of properties
- interactive techniques to improve the quality of fusion results
- logical rules to facilitate the acquisition and explicit representation of knowledge
- calculus of evidence to provide a mechanism to model sensor evidence and uncertain knowledge
- explanations about the fusion processes to permit quantification of the relevance of various knowledge items and the detection and identification of contradictions while enabling consideration of alternative hypotheses
- graphical displays to facilitate understanding of inferential chains and their conclusions
- interactive control and review mechanisms to permit humans to correct arguments to increase the utility of conclusion and fusion results. (Blasch et al. 2006)

Fusion models can be used for evaluation and deployment of a multi-source sensor fusion system, as Figure 9 depicts. The User Fusion model (in the left) can be applied together with the Data Fusion Information Group's model (in the right). The user carries out an assessment of the situation by a mental model, which is a representation of the world as aggregated through the data gathering, information fusion design, and the user's perception of the situation. Situation assessment in level 2 includes tacit functions which are inferred from level 1 explicit representations of object assessment. (Blasch et al. 2006.)

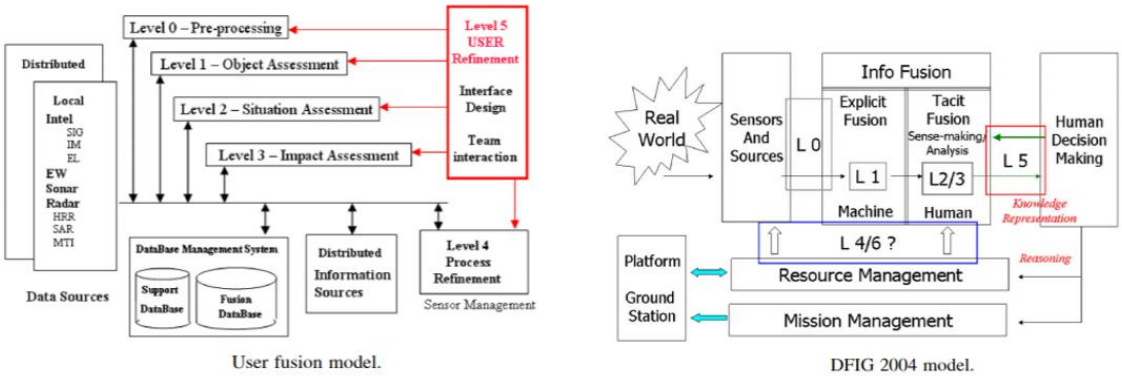


Figure 9. Fusion models for sensor fusion systems (Blasch et al. 2006)

In Figure 9, the level zero represents data estimation and prediction in object state observation on the basis of a signal or pixel. At the first level object assessment is done by estimating and predicting the entity states from associated data. The second level concerns estimation and prediction of relations among entities. At the third level estimation and prediction of effects on situations of planned or estimated actions is executed, including performance evaluation. The fourth level is about adaptive data acquisition and processing to support sensing objectives (e.g. sensor management, information systems dissemination). At the fifth level adaptive data retrieval, visualisation and display to support cognitive decision making and actions in the human computer interface is carried out. Finally, adaptive determination of spatial-temporal control of assets, route planning and goal determination is put into practice to support team decision making and actions. (Blasch et al. 2006.)

Fernandez et al. (2017) argue, that in the fields of situation awareness and alarm management, there is a growing need for integrated goal-oriented supervisory systems, platforms and frameworks, as described above. Prevention of accidents, like in Spain 2013 mentioned in the introduction, demands higher-level semantic cognitive activities, integration of both context and historical knowledge, learning capabilities and solid decision support from systems. In order to function correctly and fulfil the requirements of safety, security and emergency monitoring, integrated timestamped data fusion techniques, data semantic analysis, alarms and events statistics, and expert rules knowledge have to be applied in system solutions. System solutions must also be aware of context and content, meaning and relevance. Fernandez et al. (2017) faced a challenge to develop an advanced supervisory system supporting higher-level cognitive activities by presenting a novel cognitive architecture for Critical Situation Awareness Systems. In this particular situation awareness architecture, the Associated Reality as a new cognitive layer is significant in improving the perception, understanding and prediction. The role of the Associated Reality as a co-pilot or a personal assistant is emphasized, when modelling related information of the system and its environment for enhancing the alarms and events management. In this situation awareness system architecture for railway safety, depicted in Figure 10, has the Data Fusion Information Model been applied. (Fernandez et al. 2017.)

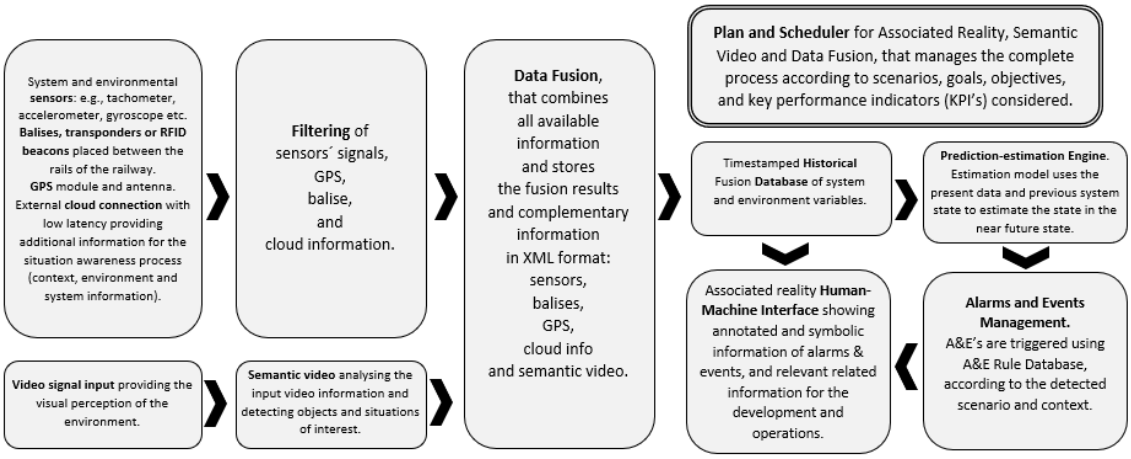


Figure 10. System architecture for railway safety (Fernandez et al. 2017)

The Figure represents an example of a train safety application, where the corresponding historical Associated Reality cognitive layer and the involved timestamped database consists of sensors (e.g. thermometer, GPS, odometer, tachometer, gyroscope, Doppler radar) and information related to them (e.g. GSM and GPRS data, command and control information, railway incidents information, and 4G LTE external cloud information or extended 5G connections and associated cloud services). Alarms and events management consists of the rules database, which can be modified by the corresponding command and control cloud service. Triggered alarms are timestamped and stored in the historical alarms and events database. The speed constraints are defined by this database based on weather conditions and distance intervals, and a simplified alarm rule to for registration could be like the following one:

Register = (Train : 00151; Rule : 8.1;
Weather : normal;
Begin : 143 Km; End : 147 Km;
Type : Alarm;
Variable : Speed; M in : 0 Km/h, Max : 90 Km/h;
Alert Message : Reduce speed)

Picture 1 Alarm rule (Fernandez et al. 2017)

As an advantage in this kind of associative situation awareness architecture is that e.g. train speed and position can be estimated in multiple direct or indirect ways

which improves reliability of the alarm system. This provides robustness and capability to response to various scenarios, even then when a sensor system is partially damaged or degraded. (Fernandez et al. 2017.)

To summarize this, in situation awareness information systems a goal-oriented associated reality cognitive layer performs tasks of a co-pilot with the help of modelized, combined and stored information from multiples sources. Information contains system characteristics, state, mode and context, semantic information and historical data, models, and simulation and estimation methods. This kind of systems are based on extracting relevant data and drawing inferences and conclusions, when perceived, analysed and associated information about the system and its environment improves constantly the knowledge and decision making. This leads to better observability, controllability and situation awareness. (Fernandez et al. 2017.)

3.1 Supporting situation awareness by standards, style guides and design instructions

This sub-chapter of the study aims to some extent bring out the features of appropriate and safe implementation of the alarm functionality in information systems. Here, the main design principle is consistency, which concerns beyond a single visualisation a greater number of Figures, colours, pictograms, symbols and other elements. All elements belonging to the same entity should be used consistently in visualizations, and presentation itself should be consistent across the screen. Finally, all forms presented should convey relevant information. (Koponen et al. 2016.)

There are three factors that affect to object findability through visual search: (1) the occurrence of the object, i.e. the visual features that our visual observation specializes in recognizing, (2) attention focusing, i.e. sensitizing our visual perception to specific targets, and (3) familiarity with the core features of the view (scene gist), i.e., ease of identification compared to strangers. These factors are utilized in alarm functionalities. For example, a flashing light, or a triangular warning sign with strong colours and colour contrast (red, black-yellow) makes a person to

notice it when appearing to the field of vision, even though this person is not actively looking for such a stimulus. (Koponen et al. 2016.)

Pictograms and ideograms are used to visualize alerts, alarms and warnings. The former is a stylized image of a material object (e.g., a device or room) and its state of affairs (status: not working), while the latter describes a set of values, prompt, or other functional aspect (e.g., leak alarm, take the following actions). A symbol is an ideogram when it connects two or more things together. Symbols can be (1) locative, i.e. indicating the place of occurrence, (2) instrumental, i.e. indicating the activity or event by an instrument used therein (e.g. indication of a maintenance claim with an image of a wrench), or (3) objects, i.e. referring to content (e.g. logo, ID). Standards - such as e.g. ISO7000 and IEC60417 - guide the use of these marks in hardware and software. (Koponen et al. 2016.)

In the domain of nuclear plant safety, Human-System Interface Design Review Guidelines (NUREG-0700, Revision 3) provides guidance for evaluation of the physical and functional characteristics of human-system interfaces. These guidelines address the basic elements – such as information displays – i.e. building blocks to develop HSI systems to serve specific functions. The guidelines also consider reviewing of the sub-systems - like alarm system, safety parameter display system, group-view display system, computer-based procedure system, automation system, and communication system. NUREG-0700 document presents high-level human-system interface design review principles, which support the operating personnel's primary task of monitoring, controlling, recognition, tolerance and recovery from human errors. These principles are divided into four categories: general principles, primary task design, secondary task control, and task support. General principles (1) aim to verify, among other things, that the design is compatible with the general cognitive and physiological capabilities, such as support for visual and auditory perception. Primary Task Design principles (2) seek to ensure the operator's primary task of process monitoring, decision making and control to maintain safe operation. This includes maintaining of situation awareness, as the information presented to the users should be correct, recognizable in an instant, and easily understood (e.g., "direct perception" or "status-at-a-glance" displays) and support the higher level goal of user awareness

of the status of the system. Secondary Task Control principles (3) target to minimize secondary tasks, such as activities associated with navigation through displays or accessing data, which can detract personnel from performing the primary tasks. This has much to do with cognitive workload management by minimizing e.g. making of mental calculations, transformations or use of recall memory. For example, recalling lengthy lists of codes, complex command strings, information from one display to another, or lengthy action sequences should be avoided. Information presented by the system should be rapidly recognized and understood, and therefore, raw data should be processed and presented in directly usable and accessible form. Task Support principles (4) strive to, among other things, mitigation of errors by the fail-safe design. Error tolerance and control should be refined so, that it covers the situation of a failure damaging equipment, injuring personnel or operating inadvertently critical equipment. A user error should not have serious consequences, thus, the negative effects of errors should be controlled and minimized. The system should offer simple, comprehensible notification of the error and simple, effective methods for recovery. (U.S. Nuclear Regulatory Commission 2012.)

In aviation, there are guidance such as the Minimum Operational Performance Standards for Aircraft Surveillance Applications System (RTCA DO-317B 2014) and Airworthiness Approval for Systems and Applications (FAA AC 20-172B).

Designing safe system solutions, it is also recommendable to take into consideration accessibility issues and user disabilities, if possible. For example, Web Content Accessibility Guidelines (WCAG) 2.0 and the user-oriented design system Color Universal Design (CUD) can be utilized in this.

In interactive system design, it is desirable to be aware of common expectations about colour codes. According to western colour conventions, red signifies danger, yellow caution, green safety, whereas grey or white or blue neutrality. Warm colours represent action or response required, whilst cool colours represent status or background information. Colours are used for achieving greater information density and colour alterations can be applied to indicate status changes. Visibility, observability and familiarity contributes to attention drawing to alarms, alerts and

warnings. Ensuring visibility and observability of elements helps users to perceive what functions are available and what the system is currently doing. Familiarity is realized through known terms and recognizable symbols. (Benyon 2011.)

3.1.1 Alerts and alarms

An alert is attentive by nature, i.e. it exists for notifying of something. It serves as an indication of change and thus, a status annunciator. A typical example of an alert is a warning or an error message. An alarm, in turn, can be characterized as summoning, when urging to do something (e.g. requiring operator action) to the abnormal situation. According to U.S. Nuclear Regulatory Commission's (2012) definition, alarms are generated, when conditions or events are expected to occur but do not, or when an alarm is expected but it does not occur. However, the terms are used often interchangeably for each other. In the following paragraphs, some common design instructions for alerts and alarms are presented.

Standards, such as ANSI/ISA-18.2-2009, EEMUA 191, and NAMUR NA 102 are for the improvement of alarm management, claiming that an effective alarm system delivers the right alarm to the operator at the right time with the right importance and the right information. Basic principles are the following: (1) every alarm should have a defined response, (2) each alarm should alert, inform, and guide, and (3) each alarm presented to the operator should be useful and relevant. There are multiple advanced alarming techniques e.g. for managing of alarm rates, for modifying alarm behaviour and shelving or suppressing alarms. (Fialkowki 2012.)

There are commercial software products on the market for alarm management with features like dynamic alarming. Dynamic alarming refers to techniques for modifying alarm attributes and eliminating alarms floods in planned and in unplanned events, aiming to provide an optimum alarm configuration in plant environments. An alarm flood is defined as such condition, that during which alarm rate exceeds the rate the operator can effectively manage. If the rate is more than 10 alarms per 10 minutes, the risk of missing a critical alarm increases. As a feature, dynamic alarming with automatic modification or suppression, will come in

handy in multiple alarms situations resulting from an equipment malfunction or process abnormality. (Emerson 2019.)

Considering the message visualisation in systems, Jakob Nielsen (2001), the famous usability expert, instructs design of error messages by pointing out the following issues:

- message visibility and high noticeability (both of the message itself and how it indicates which dialogue element users must repair)
- multiple encoding mechanisms and redundant cues, instead of e.g. using only a colour to indicate an error
- explicit and comprehensive indication of all error situations (relates to alarm management)
- human-readable language, instead of obscure codes or abbreviations (e.g. "an error of type 0987 has occurred")
- precise description of the exact problem, instead of vague generalities (e.g. "syntax error")
- congruous and constructive advice on how to solve the problem or situation, instead of leaving user and activity as blank.

The issues Nielsen pointed out are taken into account in these following recommendations for alert design in user interfaces as well (Zlatkus 2019):

- producing the minimum content for an alert with a title, a description, and a primary and a secondary action button
- placing the alert in the middle of the screen or display to ensure maximum attention
- placing the messages near where problem arose. However, placed in a consistent position on the bottom of a screen is sufficient near to and not obscuring relevant information.
- background dimming as for highlighting an alert modal to put emotional weight and significance to it
- avoiding the generic – and confusing – naming of the buttons, but using a button name following the message title (i.e. descripting the function)

- putting weight to primary buttons by positive colours (negative are red, yellow and orange), and colouring secondary buttons in grey (a “ghost” button). Except, when the alert is confirming a high-impact deletion, the primary button colour can be red.
- including the exit and cancel functions
- describing shortly (up to approximately six words) with the title, why user’s attention was captured or why user was halted, by explaining what will happen (in case of confirmation) or what has happened (in case of an error alert)
- not forcing a user to answer merely “yes” or “no” by a title question
- avoiding repetition in the description, i.e. not using the title as the first sentence again or not ending the description in a question (repetitive information)
- providing the results or repercussions of what just happened or what will happen if a user proceed in description
- using centered phrasing
- using uppercase-only messages for serious warnings
- avoiding code numbers, but if required, including them at the end as additional information
- applying audio signals with discretion by enabling user control in this.

It has to be taken into consideration, that some of these recommendations and guidance for design can be exploited and thus having a counter-effect in the form of risks. This aspect will be discussed in more detail in a later chapter.

In situation awareness and assessment, determination of an alarm’s priority is essential. Priority is static or dynamic by type. Statically determined priority is based on static values, that are analysed, typed and assigned to alarms prior to system implementation. Dynamically determined priority is based on change management and depends on the required immediacy level of an operator actor and the significance of the conditions to operation, process or plant safety. (U.S. Nuclear Regulatory Commission 2012.)

In addition to multiple guidance for alarm design, OASIS Standard Common Alerting Protocol can be used as general format for exchanging all-hazard emergency alerts and public warnings over various types of networks and for consistent warning message dissemination simultaneously over many different warning systems (OASIS 2010).

3.1.2 Secure by design

The principle of “Secure by design” promotes security being as first and foundational in software engineering, and as guidance for designers and developers (Santos et al. 2017). There are numerous standards, guides and instructions published by national, global and public organizations and societies, best known of them being International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), The European Union Agency for Cybersecurity (ENISA), The National Institute of Standards and Technology (NIST) and the International Society of Automation (ISA). The most significant of these publications are the ISO/IEC 27000-series of information security, ENISA’s regulations, NIST Cybersecurity Framework and the ISA-62443-series of system security (i.a. Security for Industrial Automation and Control Systems, System Security Requirements and Security Levels).

In addition, designers and developers should seek guidance from the sites of Common Architectural Weakness Enumerations (CAWE) and Common Software Weaknesses (CWE), maintained by The National Cyber Security Division at U.S. Department of Homeland Security (DHS) and MITRE Corporation. The former, CAWE, describes an architectural flaw in a software system resulting in a security vulnerability. Tactics and weaknesses are categorized by type as follows: audit, authenticate actors, authorize actors, cross cutting, encrypt data, identify actors, limit access, limit exposure, lock computer, manage user sessions, validate inputs, and verify message integrity. For example, by “Validate input” tactic any externally provided inputs are sanitized, neutralized and validated to minimize malformed data from entering the system and preventing code injection in the input data. Under this tactic is 39 weaknesses listed. (Santos et al. 2017.)

In the question of secure coding, developers should turn into The Open Web Application Security Project (OWASP) providing tools, resources, community, networking, education and training for improvement the security of software. OWASP publishes “The OWASP Top 10” awareness document of the most critical security risks to web applications, lists vulnerabilities, and offers application security principles. Concerning the latter, among other things, it urges to minimize attack surface area, to apply layered security mechanisms as they increase security of the system as a whole, and to use positive security model (“whitelists”). (The Open Web Application Security Project 2017.)

Continuing on secure coding, the Software Engineering Institute (SEI 2020) and the CERT Division have published Coding Standards for commonly used programming languages such as C, C++, Java, and Perl, and the Android™ platform (Carnegie Mellon University 2020). Software Engineering Institute SEI has developed a reference architecture for the classification and advanced prioritization of flaws in code, that enables automatic, accurate and adaptive classifying and prioritizing of alerts ensued on these flaws (Flynn 2018).

In software development various different quality assurance methods can be used to evaluate the safety of systems and to prevent errors, especially in safety critical industries, such as aerospace or nuclear power. These methods include, for example, numerous risk analysis tools, fault tree analysis, fault and impact analysis tools, as well as deviation analysis methods and cause-elimination techniques for bug detecting and failure analysis. (Kotkansalo et al. 2017.)

Besides this, there are some domain specific publications, such as guidances for Supervisory Control and Data Acquisition Systems (SCADA) in energy sector. The OPC interoperability standard for the secure and reliable exchange of data in the industrial automation space and in other industries, published by the Open Platform Communication Foundation, also directs in implementation of alarms and events. The specification (available for paid members only) describes the behaviour of an OPC Server monitoring areas and notifying clients about alarm conditions. This publication covers an overview and purpose of Alarms & Events technology; an overview of general architecture and methodology of alarms, events,

acknowledgments, queries, and areas; detailed descriptions of interfaces, methods, parameters, and expected behaviours; detailed descriptions of data types and structures; and sample code containing interface definitions and error codes. (OPC Foundation 2017.)

Finally, the Safety Boards and Investigation Authorities provide safety recommendations based on the issues identified during a safety investigation. These public recommendations are based on a systematic analysis performed during the investigation, and often published along safety incident and accident reports.

4 RISKS OF PERCEPTION IN SITUATION AWARENESS

In a cyber environment, information can be used to influence one or more levels of activity. As the situational awareness required for decision-making at different levels of activity differs in content, thus, at different levels of activity, situational awareness is also affected by different information. (Kuusisto 2014.)

As mentioned in the introduction regarding the SHELL-model, risks can arise in every system component (Liveware, Software, Hardware, Environment) and in the interfaces between them. Considering the first level of situation awareness being about perception of elements, information handling and communication capability is crucial there. Endsley (2000) states that, for example, pilots, control officers, operators, and medical staff must perceive and comprehend masses of fast changing and constantly flowing data. The lack of information is not the problem, rather accessing relevant and authentic data at each necessary moment is, which brings forth an information gap (Endsley 2000). The information gap occurs, when data overload becomes problematic and data must be processed before the required information is received (Koskinen-Kannisto 2013). Data and information related elements affecting to situation awareness are information sharing enablers (such as data and information types, amount of information, communication channels, information access), information sharing functions (such as information pull and push, information initiation), and information sharing products (such as information processing, information management and information analysis) (Koskinen-Kannisto 2013).

As previously stated, the loss of situation awareness is based on information related deficits. Systems may not be able to receive or produce necessary information for human decision, action and assessment. This information can be foreknowledge, deterrent or cautionary by nature, and possibly inaccurate, false or otherwise inapplicable, or not generated at all. The amount of information can be so excessive, that it cannot be processed and a state of paralysation occurs, or so low, that interpretation becomes difficult. Some information may hide or override other kind of information, which distorts perception and interpretation. Prejudice and bias affect to perception and comprehension by directing focus on

misinformation and making it difficult to deal with surprises, such as unexpected events or non-occurring expected events. (Kari 2018, paraphrased.)

These are further discussed in the following chapters.

4.1 Risks related to Human Factors

According to Benyon (2011), failures in attention are often defined as a reason for accidents. A multitasking user with divided attention can have difficulties in reacting and decision making when the tasks require simultaneously attention. A control room operator might be overwhelmed and tired of the multiplicity of notices requiring attention. A supervisor can end up assuming situations beforehand and by this bias becomes selective on sensory information awareness. (Benyon 2011.)

However, a prerequisite for the formation of a high-level situational awareness is that a person is able to perceive several different things simultaneously. The attachment of attention to only single factor causes the tunneling of attention. This tunnel-like attention prevents the transfer of attention between different sources of information. A person is able to deal with five to nine things at a time. (Nikkinen 2018.)

Things that a person would not want to pay attention to can also be the subject of observation. If a person does not control his own attention, many outside things will attract him. Attentiveness has been studied by testing the perception and remembering of two overlapping messages (either heard or seen) in which the task has been to follow one message and ignore the other. As a result, the monitored message is remembered, but the one left in the background is not. Attention thus has its limitations in terms of selective, focused and shared attention. In demanding and rapidly changing circumstances, it is important to select the appropriate stimuli to deal with, as wrong choices can lead to dangerous situations. Demanding situational awareness tasks require the successful selection of information, the person's ability to direct attention to the chosen object and to maintain attention in this object. (Lähdeniemi 2013.)

A mental model is a significant factor in the formation and development of situational awareness, when a person interprets the information received. With the help of mental models, a person combines the most important information and forms a projection of the course of events. The wrong mental model leads to a situation where a person continues to projection of future and decision making on the basis of wrongly interpreted information. This can occur when, for example, an automatic system is assumed to report any possible disturbances or deviations and the person no longer actively perceives possible deviations. Thereby, the level of situational awareness decreases. (Nikkinen 2018.)

A state, where a person tends to look for information that supports one's beliefs, is called cognitive dissonance. Cognitive dissonance is experiencing mutually conflicting and contradictive phenomena of the mind, and it arises when a person's knowledge and attitudes conflict. It explains why a person receives and accepts information that supports one's perception more easily than information that contradicts one's perception. Reduction of cognitive dissonance is realized by behavioural change. Cognitive dissonance creates a base for other individual-level psychological barriers and limitations, such as confirmation bias and heuristic evaluation. The first occurs when a person favours information that supports one's own prejudices and ignores or underestimates the information that opposes them. Relevant information is collected selectively, and this further distorts interpretation, or ambiguous material is interpreted only to reinforce one's own view. Skewed interpretations cause permanent beliefs and ostensible correlation. A person's own view (i.e., belief) remains valid even if there are sufficiently facts to refute it to make the belief false. In the latter, heuristic evaluation, rules of thumb, academic conjectures and intuitive conclusions are used, i.e. ready-made, pre-conceived or acquired solutions are applied to problem solving. It aims to get close enough to the best possible outcome quickly, but the disadvantage is that it focuses on only one subset in a complex problem. (Kari 2018.)

The previously described is recognized also in investigation reports, one of which states the following (AIBN 2012):

> *“In order to assess whether a situation has been correctly understood, one looks for information confirming one's own point of view. As a result, one can easily fail to register valuable information from the surroundings. In such cases it is essential to seek information that disapproves one's own perception of the situation, i.e. to ask oneself whether one could in fact be wrong. Excessive focus on information that confirms our own understanding of a situation means that we focus less on information that raises doubts about the correctness of our understanding.”*

Other causes for risks are disorders of situational awareness including time pressure, fatigue, restlessness, workload, and other stressors. For example, prevailing conditions (e.g., heat, cold, poor lighting) or a dangerous operating environment increase the experienced stress and make it difficult to pay attention. Also, an excessive amount of information can overload a person’s sensory and cognitive systems. A person’s ability to manage larger amounts of information cannot be increased beyond natural boundaries, but the amount of information and load should be considered already in the design of situation awareness information systems. Besides this, a misplaced source of information can distract the formation of situational awareness. Flashing lights or sound from the wrong direction may unnecessarily strain a person during situation. (Nikkinen 2018.)

Franssila et al. (2014) refer in their study to Eppler and Mengis (2004) who showed that information (over)loading may be due to personal factors (e.g., lack of individual information processing ability), nature of information (e.g., ambiguity of information), nature of task (e.g. the urgency of the task) or information technology (e.g. sharing the same information content across multiple channels). The user should be able to customize one’s entire work environment, for example, with a profile that requires a "focused workflow" with minimal effort, and be able to revert to a real-time interruption profile when necessary and desired. The cognitive load in work environments can be breakdowned by the source types being (1) information overload, (2) continuous multi-tasking and interruptions, and (3) workflow complexity. Receiving large amount of information will burden one, as each message, document or update requires decision of how it will be processed and evaluation whether it is useful now, in the near future, or later or not at all. A large amount of incoming information arriving at an unpredictable rate will be

burdened if the information worker does not have effective procedures in place for managing the incoming information stream, and if the message stream is always processed ad hoc. (Franssila et al. 2014.)

Perception is affected also by degree of activation, such as sleep, observation or panic. There is a connection between activation, behavioural states and performance. This is evident in solving complex tasks requiring attentiveness and monitoring when the level of activation should not be too high, nor too low. Thus, activation is perceived value (what a person expects to happen) minus actual value (what actually happens), i.e. it increases as the gap between perceived value and actual value widens. In other words, for example, in perceiving an alarm and making decision for proceeding, the actual value must increase sufficiently to exceed the perceived value. Correspondingly, too low degree of activation means low and delayed responsiveness, as, for example, happens when a person is in a state of tiredness or drowsiness. Reasons for this activation decrease can be due to performing monotonous tasks, being in darkness, standing still, feeling too comfortable, hearing monotonous sound of low frequency, or automation (i.e. not mastering self the tasks or relying too much on the technology). All of these reduce attentiveness. (AIBN 2012.)

The previously described is essential especially in bridge work or in working in control rooms and command centers. With technology aimed at improving safety, the nature of this kind of work has changed from task-oriented to control-oriented. This, in turn, has led to the ergonomic design of workstations, the typical features of which are comfort of the workplace seat, good reliability of the technical equipment, monotonous sound world and exhausting uniformity of the air conditioning. These factors together with the working time poorly suitable for the human wakefulness rhythm contributes to an environment impairing the state of alertness. A tired person ignores stimuli or does not always manage to think about their meaning sufficiently, hence suffering from a deterioration in memory performance. The reaction rate can also be slowed down in an operationally significant manner, which creates a lack of situational awareness critical to the required decision-making. In a complex situation where there are too many or too

few stimuli, a remarkably vigilant readiness is required to process the information, for which the tired brain has no capacity within the time available. (Safety Investigation Authority 2004.)

When a user (such as an operator, a supervisor) becomes tired of alarm stimuli and develops a tolerance to it, it is a question of alarm or alert fatigue, causing sensory load and leading to delay or absence of an alert response (West et al. 2018). Alert fatigue results when a person is exposed to an excessive number of alerts leading to desensitization, ignoring, overlooking or overriding even relevant alerts (Kane-Gill et al. 2017). It is possible to meter alert fatigue, as Figure 11 depicts below.

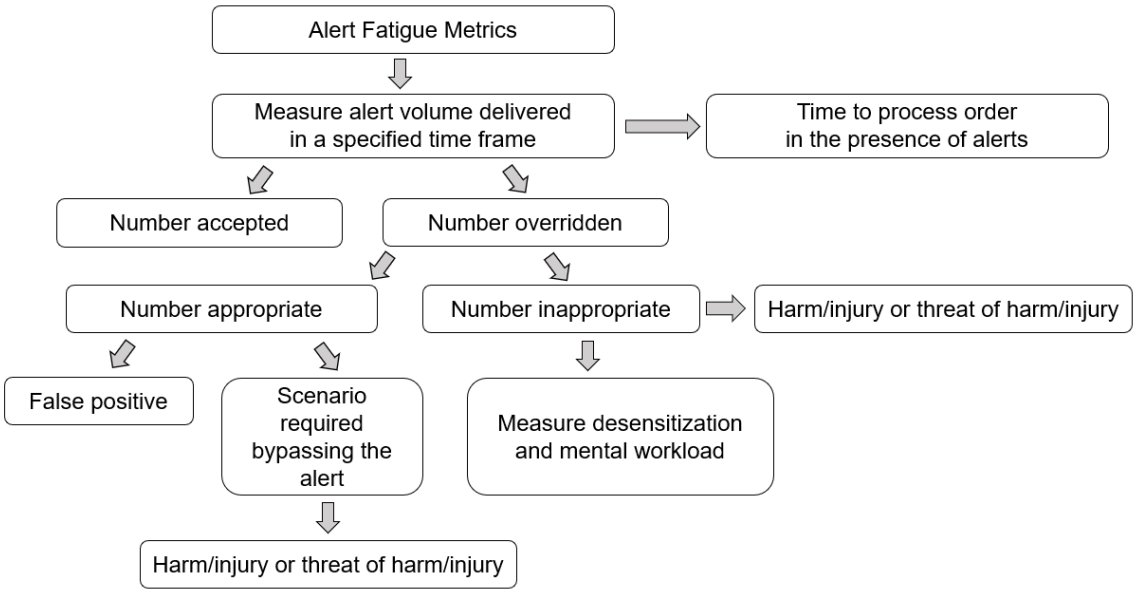


Figure 11. Alert Fatigue Metrics (Kane-Gill et al. 2017)

In Figure 11 above, alert fatigue is presented as a proportion of inappropriate overrides to total alert quantity in the presence of desensitization or high level of mental workload. Delayed processing time is a negative consequence of alert volume. A correlation between alert volume and processing time is a valuable information that can also be useful to evaluate for appropriate and inappropriate overrides separately. Accepted alerts indicate justified reaction and action. Here the alert value is a sum of appropriate alerts delivered in a timely manner including alerts that are accepted, added to alerts with appropriate overrides warranted

because of the response scenario, added to alerts with overrides that were inappropriate. Inappropriate alerts are true positive that are overlooked and not warranted by work scenario. Harm/injury or threat of harm/injury is a negative consequence of alert fatigue and a major outcome to measure. Here it is noticeable, that an alert override may be appropriate due to poor alert design, but there is always the possibility of resultant adverse events. Alert quantity and appropriate overrides provide information about opportunities to improve alert performance. (Kane-Gill et al. 2017.)

The negative effects of alert fatigue are frustration and annoyance, decline in memory recall about alert, inappropriate override response and delay in processing orders. However, if the total number of alerts is reduced, it may produce unacceptable impacts and compromise the sensitivity of alert system, resulting to decreased safety and situation awareness, and missed opportunities to avoid adverse outcomes. (Kane-Gill et al. 2017.)

According to brain researcher Mona Moisala, the already more common concentration disorder called Attention Deficit Trait (ADT) is making people overloaded and anxious. Moisala states, that the risk of developing ADT is increased by work that is difficult to regulate and requires long-term concentration and new information adoption, with the requirement of continuous availability of the employee and constant interruptions of work. (STT 26.10.2019.)

Already in the 1990s, American doctor Edward M. Hallowell recognized ADT and described people who had been living too busy for too long, doing many things at once, not taking breaks, jumping from one job to another, neglecting to sleep, and creating these behaviours, where the brain no longer functions normally (Koho, 2018). He states that ADT springs from the environment demanding our time and attention and is an artefact of modern life. When human mind fills with constant noise and events, the brain will lose its capacity to attend fully and thoroughly to anything (Hallowell 2004).

Although the default is that human-system interfaces should not impose an excessive workload for the user, but on the contrary should support the usability by, for example, window manipulation, display selection, or navigation (NUREG

2013), it may well be that the systems and devices themselves can be disruptive (Lähdeniemi 2013). Studies show that the addition of technological equipment can potentially lead to a decrease in productivity due to the overload of information, or the overload of communication, or the overload of multifarious system features, caused by the equipment to its users, especially to information workers. If technological devices are not designed with human cognitive capacity in mind, their use can cause undesirable effects. Excessive cognitive workload can be to blame for reduced performance if it results in information being overlooked and in errors. This is especially important to consider in situations where safety is a critical factor, such as air traffic control and process control. However, there are situations where a person is unable to perceive the necessary information, even if it is in the field of observation. Reasons for this can be, for example, the state of alertness of the body, the difficulty of selecting or finding essential information from a large amount of information, the difficulty of concentrating on the essentials, or the information processing requirements that are too one-sided or too large. Auditory and visual noise or movement can distract, in which case tasks may be interrupted and cognitive overload may arise. In this case, the quality of the work deteriorates, and e.g. in decision-making situations, the quality of decisions deteriorates and the time spent on them increases. After a distraction, it takes time to reach the same point as it was before the interruption. If there are numerous interruptions during the day, it affects work productivity through experienced time pressure and information overload, producing capacity disruption. Structural disruption is caused when a person receives two signals that require the same psychological mechanisms to process. These can be, for example, two visual signals, such as an alarm generated by a monitoring system and a simultaneous other event in the work environment, or several alarms at the same time. Interruptions in the task, attention-grabbing movements, flashes of light, and sounds strain memory, cause stress, and can increase the number of errors. (Lähdeniemi 2013.)

In numerous investigations of rail, aviation, marine and road traffic accidents it has been stated, that operational personnel overlook easily visible information. This inattentional blindness due to limited capacity of perception occurs through filtering subconsciously the information of surroundings. An insufficient mental workload,

i.e. reduced alertness and ability to react due to a feeling of control in the situation, are often related to tasks that require monitoring. Also, low level of activation can result in misinterpretation of the environment. (AIBN 2012; AIBN 2013.)

To conclude this chapter, The Human Factors Analysis and Classification System (HFACS) is introduced. HFACS (in Figure 12) serves as a human error framework, originally used by the US Air Force to investigate and analyse human factors aspects of aviation. The HFACS framework can be applied as a tool for investigations to understand the underlying causal factors having led to an accident. It can also be used for training purposes as well as for preventive action and development purposes. (SKYbrary 2019.)

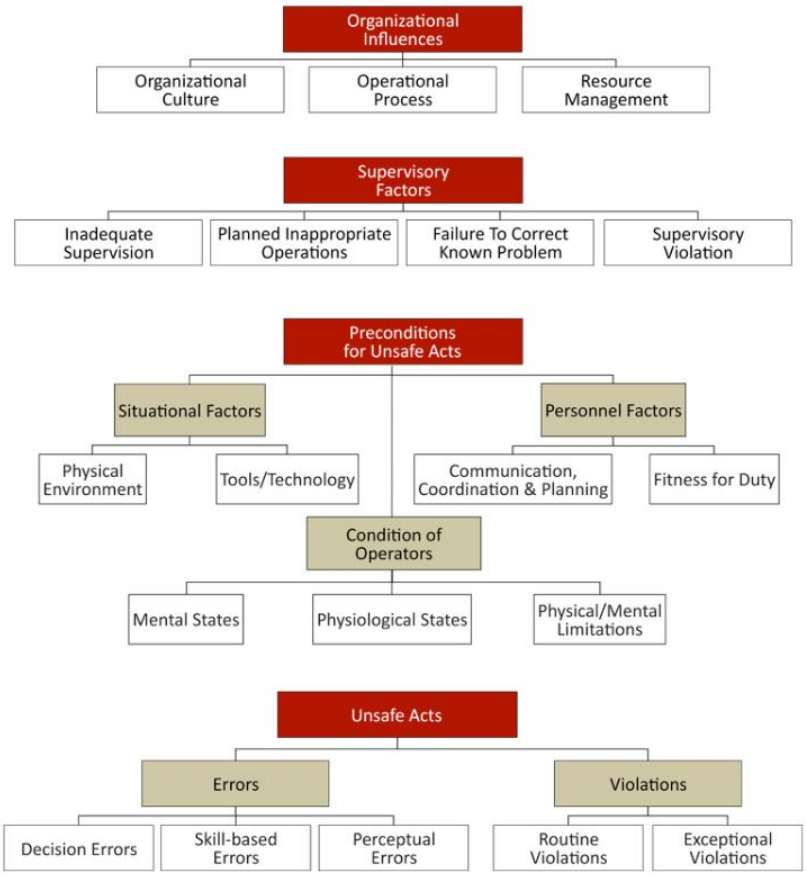


Figure 12. HFACS framework (HFACS Inc. 2014)

4.2 Cybersecurity risks

Levels of cyber threats include cyber vandalism, cybercrime, cyber intelligence, cyberterrorism, cybersabotage and cyber warfare. Selected attack methods can be targeted to different layers of the cyber world, such as component corruption to the physical layer, SQL injection to the syntactic layer, data contamination to the semantic layer, denial of service attack to the service layer, and identity theft to the cognitive layer. (Lehto 2019.)

According to Europol's definition, cyber-dependent crime is any crime that can only be committed using computers, computer networks or other forms of information communication technology. This criminal activity includes creation and spread of malware, hacking to steal sensitive personal or industry data and denial of service attacks to cause financial or reputational damage. European cybercrime investigators have identified attacks on critical infrastructure as a significant cyber threat. The attacks disrupt or subvert the internal functions of critical infrastructures, such as energy, transport, water supply, and health sectors, by implementing techniques such as Distributed Denial of Service (DDoS), malware, cryptoware and ransomware. These cause denial of access for an organisation to its own data and denial of access for others to that organisation's data or services. Various malware types, such as botnets, rootkits, worms, trojans, file infectors, backdoor or remote access trojans, and their combinations are used for DDoS, data theft, gaining access, spying, deleting or manipulating data, disabling files, monitoring, or installing additional malware. (Europol 2020.)

The Internet Organised Crime Threat assessment (IOCTA) for 2019, published by European Union Agency for Law Enforcement Cooperation and European Cybercrime Centre, states, that attacks to the infrastructure itself is a primary motive, but a financial motivation is not so much. This is said so far to be due to an increased risk for criminals of getting caught by drawing massive attention to the attack. Thus, considering the attacks to the infrastructure, these are estimated to be performed likely by script kiddies (on the contrary of smart attackers) and nation states. Crime As A Service concept available all over contributes to execution of these attacks. Cybercrime as a whole is evolving and concentrating even more on

financially profitable targets, but data will further play a significant role in it. (IOCTA 2019.)

One of the most serious security threats in the near future is cyberterrorism (Lehto 2019). Cyberterrorism seeks physical destruction using information technology and can target, for example, air navigation systems, railroad traffic control systems, or production and control systems in water and electricity grid (Lehto 2019). The ability of technological adaptability of terrorist groups is often high and they can adopt early new technologies. This ability is put into practise as, for example, in in exploiting emerging platforms for the dissemination of propaganda. Thus, this sets requirements for law enforcement practitioners to anticipate, understand and project new and emerging technologies better than before. (IOCTA 2019.)

As the Director of National Intelligence James R. Clapper has stated, cyberthreats have long been at the top of threats listed by the National Intelligence Worldwide Threat Assessment. However, a massive Armageddon-scale attack against the entire infrastructure remains more unlikely to encounter, but instead low or moderate level cyberattacks and cyberoperations from various sources for manipulating data will increase. (Homeland Security News Wire 2.10.2015.)

As for an example of significant control system requiring situation awareness, Global Navigation Satellite System (GNSS) technology is used as a sensor for several safety-critical applications, such as for guided landing approach of airplanes and for timing and synchronization of reference stations for telecommunications, electrical power supplies and the financial sector. Rügamer and Kowalewski (2015) have studied deliberate interference of GNSS signals and stated, that jamming and spoofing of GNSS signals have become an underestimated risk. Jamming means intentional interference targeting the unavailability of the system and spoofing is faking of a false position/time towards a target GNSS receiver. Jammers are used for denial-of-service attacks and spoofers can cause a receiver to estimate a fake position and/or time without recognizing it – the latter posing a greater threat (Rügamer and Kowalewski 2015). Northern Finland encountered GPS interference on 6th of November 2018 and

according to Yle News (Leisti 9 November and 13 November 2018) the warning issued by ANS Finland was the first of its kind in Finland.

In the field of aviation there has been a debate regarding Boeing's poor information security practices that have been alleged to threaten aviation safety and national security of U.S. Boeing test development networks are claimed to be publicly exposed to the internet, and email servers said to be infected with multiple strains of malware. Since, evidence showed that Boeing's systems were compromised. The worrying matter here is, that Boeing serves also as a supplier for military. Apparently, it had been a while before the company took action on the basis of the findings publicly announced. Besides this, Department of Homeland Security (DHS) announced, that none of the issues identified are unique to aviation. Also, the Federal Aviation Administration (FAA) is working with airplane manufacturers to ensure that critical airplane systems are protected from intentional unauthorized electronic interference, which encompasses cybersecurity vulnerabilities. (Porup 2019.)

On the other hand, according to an estimation (Disso 2016) for the last decade, of which 99.9% of the exploited vulnerabilities were compromised still more than a year after the Common Vulnerabilities and Exposure (CVE) was published, and majority of malware being unique to a single organization, the speed and means of acting must be questioned. The pressure for solving cybersecurity risks by the stakeholders and environment could possibly be more tenacious.

As a part of Industrial Networks, Industrial PC and Supervisory Control And Data Acquisition (IPC, SCADA) systems have also faced serious cyberattacks, one of them being the famous Stuxnet, the 2010 uncovered computer worm. The systems were originally designed to automate, monitor and control in such environments and networks of critical infrastructure that are isolated and air gapped. Nowadays these facilities cover vast geographical areas, involve numerous proprietary and legacy devices and protocols, contain multiple data sources by type and in number, and are interconnected within manifold of networks, and communicating via Internet. Even more, considering a fact, that there is a lack of security mechanisms in SCADA protocols, and in availability of guidance or methodologies for data

acquisition at the control level, these systems offer a significant threat vector. (Blyth 2018.)

Vulnerabilities can occur anywhere on the assembly. For example, a floating production storage and offloading (FPSO) vessel and its production control system, used by the offshore oil and gas industry for the production and processing of hydrocarbons and for the storage of oil, was reviewed and identified defects and vulnerabilities. These were, among other things, unauthorised bidirectional transfer of data and binaries, unauthorised access & privilege escalation, vulnerability to the Man in the Middle Attack, Windows services reconfiguration by non-admin users, insecure permissions on program files and services, unnecessary open ports, multiple transport layer encryption Weaknesses (Gorkowienko 2018). Thus, an attacker can use several techniques in various of targets in order to reach one's aim, whatever it may be (illustrated in Figure 13).

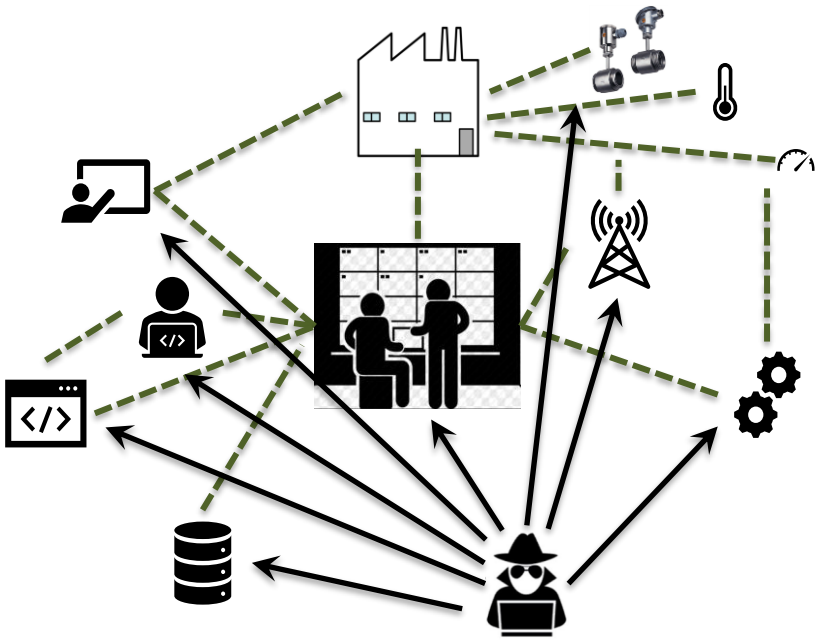


Figure 13. Attack routes

Nevertheless, cybersecurity is a social challenge as well, besides the technical one. This has come to light in the form of attacks that use social engineering and other tactics aimed at human weaknesses. With respect to the fact, that there still exists systems with serious design flaws leaving users vulnerable to sophisticated

attacks, should more and more attention be paid to secure by design principle for systems to meet the basic requirements. If most users cannot even correctly interpret SSL security error and warning messages generated by the web browser during the authentication process for a secure connection, it is not a solution to offer them a possibility to bypass or ignore security mechanisms. The whole chain of security must be watertight. (Mujinga et al. 2017.)

For example, a critical data repository (including certain core registries) is considered contaminated and integrity collapsed if 6% of its data has been rendered unreliable by an integrity attack, either over a long period of time or as a one-off attack (Kuusisto 2014). In industrial plants, the contamination of even one sensor or processor can cripple the entire plant's operation due to a deficient application and network architecture.

The Royal Institute of International Affairs published a comprehensive report of Cyber Security at Civil Nuclear Facilities with threat summary and recommendations, where it is suggested that nuclear plants may lack preparedness for a large-scale cybersecurity emergency, particularly if one were to occur outside normal working hours. At that time, the latest publicly known incident at a nuclear facility was the hacking of Korea Hydro and Nuclear Power Co. commercial network in December 2014, where the hackers infiltrated and stole data from the commercial network. They gained access by sending phishing emails to the employees, resulting to clicked links and downloaded malware. The purpose of the hack was to obtain the blueprints and manuals of two reactors, and to use them for extortion. This kind of incidents are estimated to be relatively frequent in the domain. The report states, that greatest cybersecurity issue facing the nuclear industry is about actors not entirely understanding the risks. Furthermore, a cultural challenge manifests itself by difficulties in communication between nuclear plant personnel (i.e. operational technology engineers) and cybersecurity personnel (information technology engineers). It has also been found that this challenge is aggravated when the cybersecurity personnel operates from the off-site location. In summary, it has been found that thee risk of a serious cyberattack on civil nuclear infrastructure is growing. (Baylon et al. 2015.)

Since then, the E & E News (Sobczak and Behr 2017) and other media reported in June 2017 of unidentified hackers having breached at least one US nuclear power plant. The attack was named as The Nuclear 17, and it was speculated that it could have been a part of a simultaneous global cyberattack. On October 2019, The Hacker News (Kumar 2019) brought out the sequence of events of the cyberattack at Kudankulam Nuclear Power Plant in Tamil Nadu, India. This attack was limited to an Internet-connected computer used for administrative purposes, which was isolated from mission-critical systems at the nuclear facility. Based on all this, it can be assumed that cyberattacks continue to increase and that the majority of them will never come public knowledge.

4.3 False alarms

As indicated above, an attacker can use several techniques for various targets attacking on a facility, installation or a plant. These techniques include operating system attacks, misconfiguration attacks, application level attacks and default code attacks, physical attacks or signal attacks. An attacker can perform denial of service, spoofing or jamming. Operating systems, applications, configurations, devices, databases and telecommunication can all be vulnerable. The aim of an attacker is to impact on data and information, and therefore to perception and situation awareness, for example, by altering data (adding, deleting or changing the content), by prohibiting information exchange (prevention/inhibition, delay), or by generating false (nuisance) warnings, alerts and alarms. This will cause the trust in the situation awareness system to weaken and the usability and effectiveness will no longer be at required level.

Giraldo et al. published 2018 a survey of physics-based attack detection in cyber-physical systems. The research question was how to detect false sensor or false control attacks. They expressed their interest being in false sensor measurements, false control signals manipulating vehicle platoons or manipulating demand-response systems, and the sabotage Stuxnet manipulating the rotation frequency of centrifuges. The survey aimed to build indicators of attacks using real-time measurements of physical world. Before Giraldo’s et al. survey Mo et Sinopoli

studied 2010 two possible classes of attacks, which are Denial of Service (DoS) attacks and deception attacks (i.e. false data injection attacks). They describe that a DoS attack prevents the exchange of information, usually either sensor readings or control inputs between sub-systems, while false data injection attack affects the data integrity of packets by modifying their payloads.

According to Zhao et al. (2018) a false data injection attack (FDIA) is by type a perfect interaction and a conform of inferior data. The researchers presented various types of attacks all being part of a class of false-data injection attacks (FDIAs), where an attacker accesses real-time measurements (for example electricity consumption in a power plant) and changes them before the measurements are utilized for state estimation in a control center. They refer to Liu et al. (2011), who demonstrated the existence of three types of FDIAs that are state attacks, topology attacks and load redistribution attacks. These attacks are accomplished by random, targeted or generalized false data injection. In a random false data injection attack an attacker aims to find any attack vector as long as it can lead to a wrong estimation of state variables. In a targeted false data injection attack an attacker aims to find an attack vector that can inject arbitrary errors into certain state variables i.e. that can inject a specific error into certain state variables. In a generalized false data injection attacks an attacker can utilize the small measurement errors typically tolerated by state estimation algorithms so that the impact of false data injection attacks can be further increased without being detected. It is possible, that an attacker remains undetected if she/he is able to determine a current configuration of a target system while injecting malicious measurements that will compromise the whole state estimation process of a plant or vehicle.

Giraldo et al. state (2018), that the control systems are usually designed to be observable so that the only way to fool them into thinking it is at a false state, is by compromising the sensors and sending false sensor readings. However, Zero-dynamics attacks are carried out injecting fake signals in sensors and modifying hidden or unobservable states. The attacker can also perform a physical attack (for example a theft of a device or physical tampering of meters) and at the same time launch a cyber-attack by compromising sensors to send false data masking the

physical attack. This is called a combined use of cyber- and physical attack or a covert attack. Fake signals can also be transmitted as in Global Positioning System spoofing attacks, where a spoofer generates a counterfeit GPS signal and sends it to a GPS antenna replacing a real reading with a fake position, or in attacks on other control signal systems where an incorrect signal can cause disconnections or blackouts.

Neither healthcare domain is immune to hacking. In the 2019 list of Top 10 Health Technology Hazards published by the ECRI Institute, ranked as first is remotely hacking systems, allowing malicious software to be installed, data stealing or conversion, or other means to attack the target system. An attacker can render a device or a system inoperative or compromise device or system, which leads to degraded performance, puts patient at risk and hinders patient care.

According to the National Institute of Standards and Technology NIST of the U.S. Department of Commerce, wireless infusion pumps with weak cybersecurity can expose a health care enterprise to system breaches that pose serious operational and safety risks, e.g. access by malicious actors, breach of protected health information, loss or disruption of health care services or damage to productivity. Healthcare Information and Management Systems Society, Inc. HIMSS is a global advisor and thought leader supporting the transformation of the health ecosystem through information and technology, and publishes Healthcare IT News. In the article on 5 March 2018 by Bill Siwicki it is said, that 71% of IoT medical device ransomware infections caused by user practice issues, such as using embedded browsers on medical workstations to surf the web, conduct online chat or download content. This makes the attack vector enlarge.

Though alarm-related events happen in all health care environments, they are estimated to be underreported (Joint Commission 2013). In the U.S. Food and Drug Administration’s (FDA) Manufacturer and User Facility Device Experience (MAUDE) database there are 566 alarm-related patient deaths reported between January 2005 and June 2010. In the Joint Commission’s Sentinel Event database there are reports of 98 alarm-related events between January 2009 and June 2012, of which 80 resulted in death, 13 in permanent loss of function, and five in

unexpected additional care or extended stay. The Joint Commission states, that common injuries or deaths related to alarms included those from falls, delays in treatment, ventilator use and medication errors, and all of these events were traced back to alarm system issues. The major contributing factors in the reported events were absent or inadequate alarm system, improper alarm settings, non-audible alarm signals in all areas or inappropriately turned off alarm signals. The other contributing factors were alarm fatigue, uncustomized and non-individual alarm settings (i.e. default settings are not adjusted for the individual patient or for the patient population), inadequate staffing to support or respond to alarm signals, alarm conditions and settings that are not integrated with other medical devices, and equipment malfunctions and failures. (Joint Commission 2013.)

Every day several hundred up to tens of thousands alarm signals are generated each day from monitoring a single patient to monitoring function in the whole hospital (Joint Commission 2013). If it turns out so, that most alarm signals would not always require clinical intervention, will clinicians become more and more desensitized or immune to the sounds and become overwhelmed by information, suffering from alarm fatigue. As a result, the volume of the alarm may be turned down, turned off, or the alarm settings adjusted outside the safe and appropriate limits. This can have serious and fatal consequences. Medical personnel throughout the world have tried to solve this challenge of reacting to true positive alarms, false positive and false negative alarms, as in the Summit of Medical Device Alarm 2011. Attempts to form a policy on nuisance alarm problem have been made. So far, the preferred response to alarms has been to question what is wrong, check out the circumstances and fix the cause. If clinicians are overwhelmed by false alarms, there will not be sufficiently time fix all alarms issues. The solution takes form in providing clinical context to alarms and by saving all alarm information for analysis and judgement. (Joint Commission 2013.)

However, suppressing alarms cannot be the only solution to process and manage false or nuisance alarms. It is true, that so far alarm functionalities in most situation awareness systems have based on users' respond to every single alarm. This creates more requirements for human operators' ability to monitor and will increase their cognitive workload. A difficult dilemma is faced, because on the other hand

automation can mask relevant information and diminishes that way situational awareness.

In the domain of aviation, the integrity of the alerting system should be examined due to its effect to the flight crew's trust and response when assessing an alert, it says in publication "Human Factors Considerations in the Design and Evaluation of Flight Deck Displays and Controls" (Yeh et al. 2016) by Human Factors Division of Federal Aviation Administration of U.S.. Concerning false and nuisance alerts, the impact of them as frequently occurring event increases flight crew's workload, reduces flight crew's confidence in the alerting system (generates distrust), and affects their reaction in case of a real alert (slower response to real and high-urgency alerts or suppressing an alert before determining whether a hazardous condition exists). This may lead to ignoring and disabling real alerts when they are presented. That is why the alert function must be designed to minimize the effects of false and nuisance alerts by preventing the presentation of an inappropriate or unnecessary alert and by providing a means to suppress an attention-getting component of an alert caused by a failure of the alerting function that interferes with the flight crew's ability to safely operate the airplane. Shortly said, the alerting functions or system should be designed to avoid false alerts and nuisance alerts, while providing reliable alerts to the flight crew when needed.

Thus, systems that have a high incidence of false alarms contributes to monitoring problems due to lack of trust in automation (Endsley 1996). Since the 1980'ies it has been reported of several aviation accidents related to heeding of automatic alarms based on the lack into the system due to its high false alarm rate. Flight crew have ignored or disabled alarms or neglected to monitor the automation and its parameters or not comprehended the significance of alarms. On the other hand, automation can mask failures and degraded conditions when compensating for them (U.S. Nuclear Regulatory Commission NRC 2012). This may prohibit a user to determine causes of degraded conditions and failures and leads to the operator's loss of situation awareness, which makes difficult for personnel to take over the situation in circumstances where automation does not compensate any more. A user may have a diminished understanding and appreciation for the overall

situation as a result from automation due to processing less information or processing information at less depth.

In addition to false alarms and FDIAs, the non-desirable effects and risks will cumulate with false predictions as base or source information (Huovila et al. 2010) or with problems related to working environment and information ergonomic design in operator's control rooms (U.S. Nuclear Regulatory Commission 2012). This is to be seen, for example, in using prediction information, when the real-time risk assessment and subsequent warning decision is based on the forecast alone, the risk area is large and false alarms are possible. But when the real-time risk assessment and warning is based both on the observation and forecast of the development of the situation, the risk area can be precisely delimited, and the likelihood of false alarms is low. Furthermore, this combined with portioned information visibility as in limited viewing areas of information display screens or other factors and design solutions that may narrow attention only to local and one-timely problems instead of overall awareness.

Based on previously described (U.S. Nuclear Regulatory Commission, 2012), an attacker can generate too many or too few alarms (positive, false negative, false positive) by utilizing following alarm characteristics and system features during development, implementation or use:

- in alarm definition: altering or creating false definitions, for example, on alarm categories or their parameters. Operators will eventually become less likely to respond to alarms, especially performing cognitively demanding tasks, when established setpoints produce many false alarms. Frequent false indications contributes to failure to recognize a serious condition.
- in alarm signal, signal condition or alarm generation processing: influencing on signals or sensors or parameters by falsifying or otherwise manipulating (deletion, addition) selection, automatic evaluation, analysing or validation on setpoint exceeding
- in alarm prioritization: affecting on determination of the relative importance of alarms for the operating crew

- in alarm message availability: affecting to selection of alarms to be presented for user based on alarm priority and alarm condition priority. This can lead to emphasizing the minor or less important messages instead of emphasizing the important ones and will result to focusing operator's attention on the messages with the least operational significance.
- in alarm routing: mixing or changing transmission to appropriate recipient. All alarms should not be addressed to control room operators, as, for example, diagnostic alarms used by maintenance personnel.

In addition, an attacker can interfere with user's perception by manipulating the visualization of alarms, for example, by changing (reconfiguring) alarm symbols, or distorting colours or notification messages, which affects the interpretation of their importance. An attacker could also try to mislead by interfering with the number or timing of alerts. Furthermore, an attacker can also affect on user-system interaction by altering factors in working environment, for example, tampering and changing inputs or modes on display devices, which leads to uncoordinated visualization and problems in perception. The following Figure brings forth one point of view of this risk situation.

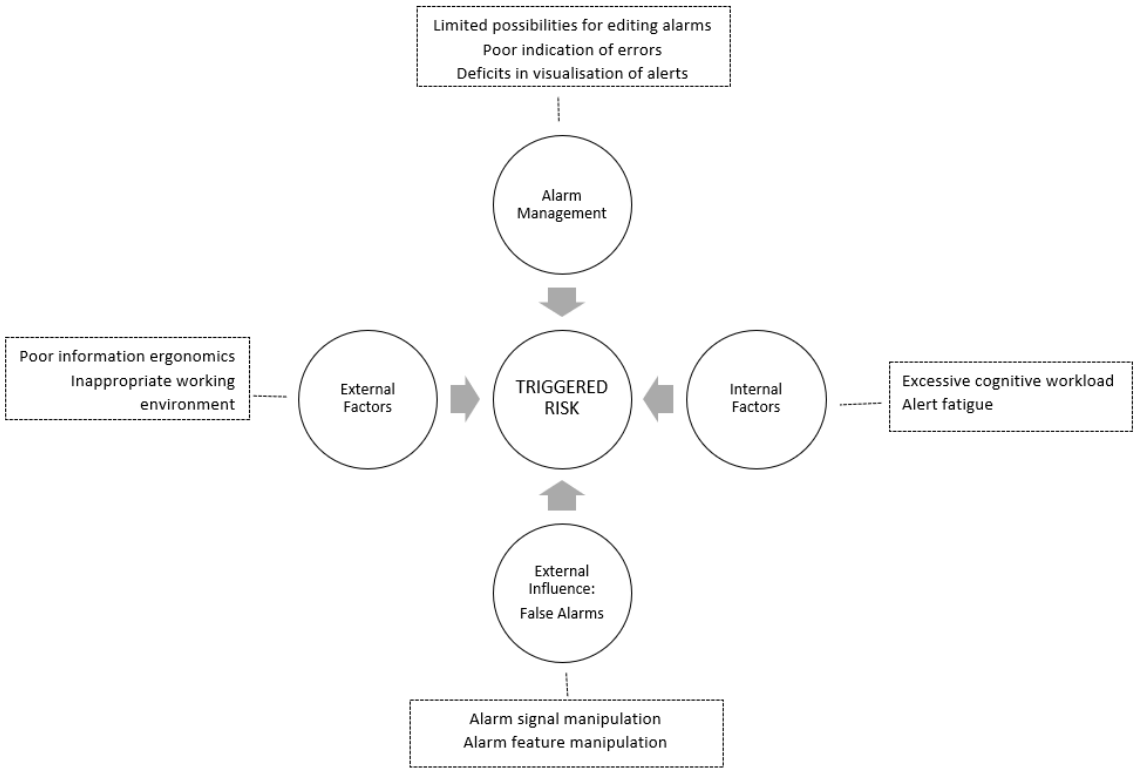
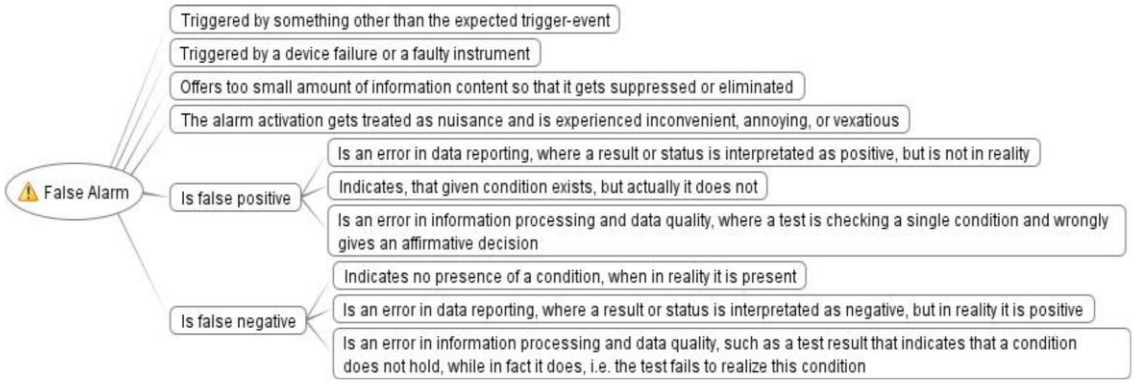


Figure 14. Example of a risk entity

To return to the concept of false alarm, Wikipedia (Wikipedia 2020a; Wikipedia 2020b) gives a concrete example of it: it is the deceptive or erroneous report of an emergency, causing unnecessary panic and bringing resources, such as emergency services, to a place where they are not needed. However, there is a semantic problem considering the sensor operation being false due to its true indication of the present state by nature. This does not take a position on a chance of a feint yet. The advisory circular 25.13222-1 by Federal Aviation Administration defines a false alert as an incorrect or spurious alert caused by a failure of the alerting system including the sensor. As it has previously turned out, "nuisance alert" as a parallel term of "false alert" has been also used in some context in other domains. The possible definitions of a false alarm are outlined in the following picture.



Picture 2. False alarm definitions

False alarms pose a significant challenge also in Security Information and Event Management (SIEM) and Intrusion Detection Systems (IDS) systems providing real-time analysis of security alerts generated by applications and network hardware. There have been incidents on massive data breaches with no action taken because alerts about the breach were treated as likely false alerts, or with even some of the network infiltration alerting system turned off due to too many false positive alerts. It has been found out, that large global enterprises can receive more than 10 000 alerts each month, of those about half being false positives and over two thirds being redundant. However, security operations managers have been reported to see even 5000 security alerts in one day. Near 40 % of the enterprises reviews manually each alert, thus, requiring a human analyst resource to verify the threat between a bona-fide, or clear but not applicable, or too minor. These human analysts encounter information overload due to incapability of a system to filter out anomalies prior to alert generation. It has also been found out, that enterprises can investigate only a little over half of the alerts received in a day, half of which is justified, and half of those justified leads to action. (Francis 2017.)

However, SIEM and IDS systems have their own requirements in terms of alarm functionality compared to industrial control systems, so they are not discussed further here. Their potentiality of development, as well as the alarm philosophy and management differ from the subject of this study. There are also numerous studies about management of nuisance alarms in industrial domain. These nuisance alarms can result from the inconsistency between the alarm design and operating

states. The solution can be an implementation of a dynamic alarm system. Still, it is possible, that a clear majority of alarms in systems can actually be false.

The following Figure 15 illustrates a chain of event of false alarms with influencing factors and elements to situation.

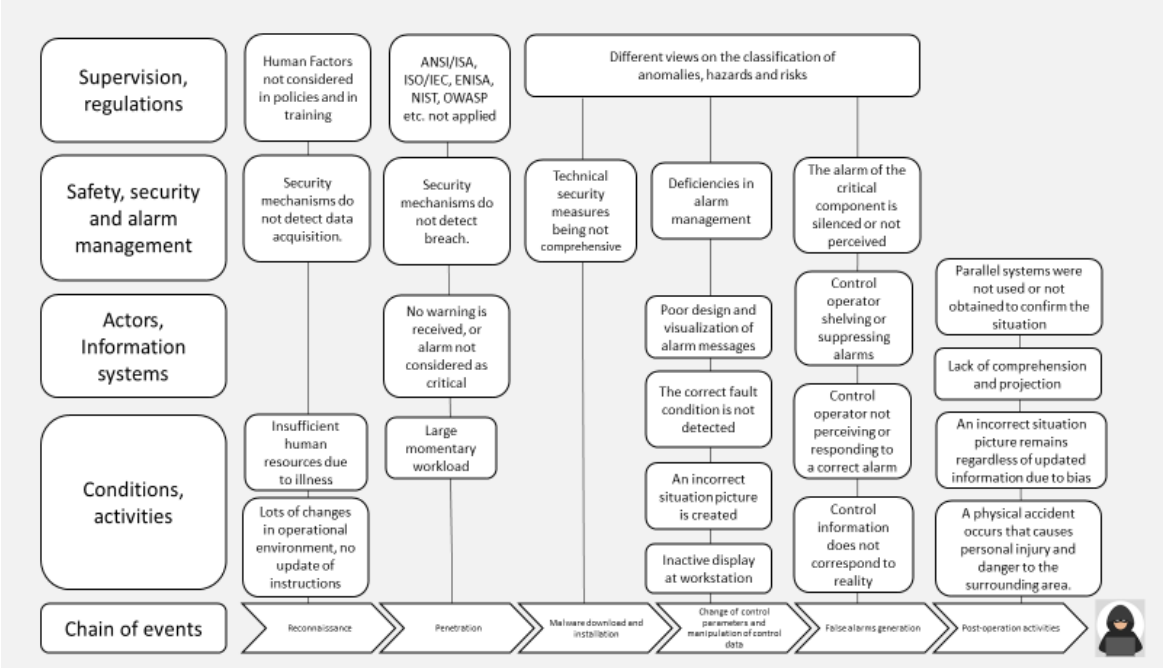


Figure 15. Chain of events

The Figure 15 above (also as appendix 1) represents a situation, where an attacker executes a false alarm attack and where the controls of operational security and cybersecurity are insufficient. The challenge of the situation increases with false alarms multiplied and being possibly used as a feint. The actual alarm of a critical component, to which the operator should immediately respond to, can remain hidden that the risk of an accident gets triggered, or by the time it takes to detect or process it. Or, due to the increased workload, there is no time to deal with it, until the accident already occurs. Also, the time elapsed between reconnaissance and attack execution can be long, such as weeks or months, although in this illustration it is presumed to be up to one day.

4.3.1 Design issues for mitigation of vulnerabilities

The National Institute of Standards and Technology (NIST), a physical sciences laboratory and an agency of the U.S. Department of Commerce, maintains the National Vulnerability Database (NVD). NVD is the U.S. government repository of standards-based vulnerability management data containing a dictionary of publicly known information security vulnerabilities and exposures knowns as the Common Vulnerabilities and Exposures (CVE). CVE is a list of entries of publicly known cybersecurity vulnerabilities. Common Weakness Enumeration (CWE), in turn, is a community-developed list of common software and hardware security weaknesses by type, offering a common language and serving as a baseline for weakness identification, mitigation, and prevention efforts. The CWE list is maintained by the MITRE Corporation, which is a not-for-profit organization working in the public interest across federal, state and local governments, as well as industry and academia. NVD integrates CWE into the scoring of CVE vulnerabilities by providing a cross section of the overall CWE structure. NVD is using CWE as a classification mechanism that differentiates CVEs by the type of vulnerability they represent. A vulnerability is defined as a weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability. Mitigation of the vulnerabilities can involve coding changes, specification changes or specification deprecations (e.g., removal of affected protocols or functionality in their entirety). (The National Institute of Standards and Technology NIST 2020c; MITRE 2020.)

A search done in NVD by the words “false alarm” (National Institute of Standards and Technology 2020a) or “false alert” (National Institute of Standards and Technology NIST 2020b) produced vulnerabilities listed by the period of 2015-2020, such as:

- a vulnerability allowing user inputs to be reflected as error or warning messages, misleading the victim to follow malicious instructions inserted by external attackers, and leading to Cross Site Request Forgery, severity classified as medium (CVE-2020-6206 SAP Cloud Platform Integration for Data Services; CWE-352 Cross-Site Request Forgery)

- a vulnerability allowing remote attackers to execute arbitrary SQL commands i.a. via certain parameters to d4d/alarms.php, severity classified as critical. (CVE-2012-1259 Multiple SQL injection vulnerabilities in Plixer International Scrutinizer NetFlow & sFlow Analyzer; CWE-89 Improper Neutralization of Special Elements used in an SQL Command)
- a vulnerability allowing remote attackers to trigger false alerts via crafted packets to the upload port, severity classified as medium (CVE-2012-4026 The Johnson Controls Pegasys P2000 server with software; CWE-20 Improper Input Validation)
- a vulnerability of missing encryption of sensitive data, caused by specially crafted malicious radio transmissions, allowing an attacker to remotely trigger false alarms, severity classified as low (CVE-2018-8864 ATI Systems Emergency Mass Notification Systems devices; CWE-311 Missing Encryption of Sensitive Data, CWE-287 Improper Authentication)
- a vulnerability of not using integrity protection, facilitating man-in-the-middle attackers to initiate a false alarm or deactivate an alarm by modifying the client-server data stream, severity classified as medium (CVE-2015-8254 The Frontel protocol before 3 on RSI Video Technologies Videofied devices; CWE-345 Insufficient Verification of Data Authenticity).

In addition to above mentioned, weakness types such as Missing Encryption of Sensitive Data (CWE-311) and Generation of Error Message Containing Sensitive Information (CWE-209) can contribute to false alarms. Regarding the first, omitting the use of encryption in any program which transfers data over a network of any kind should be considered as an unnecessary risk, and causes that the victims have not really any means to separate valid data from invalid. Considering the latter, programs might reveal passwords in error messages if an attacker can trigger certain database errors, which enables an attacker to use the contents of error messages for launching another more focused attack. Herein, it is noteworthy, that SCADA products use HTTP Basic Authentication, which is not encrypted. CWE offers good mitigation information in connection within each weakness type listed, but the most important piece of advice could possibly be that all input is assumed malicious. (MITRE 2020.)

5 THE LOSS OF SITUATION AWARENESS IN DIFFERENT DOMAINS

Research indicates that many of the performance and safety problems occurring in the large-scale industrial systems domain may result from deficits with operators' situational awareness. One analysis of offshore drilling accidents demonstrated that more than 40% of those accidents were related to situation awareness. In that analysis it turned out also, that the majority of situational awareness errors (67%) occurred at the perceptual level, 20% related to comprehension, and 13% were manifested during projection. (Naderpour et al. 2015.)

Naderpour et al. studied 2015 the role of situation awareness in three accidents in the process sector and analyzed situation awareness related errors. The identified errors were able to be categorized in errors due to a lack of appropriate design of operator support systems or in errors due to poor mental models. Naderpour highlights, that there is an urgent need to discover cognitive support systems in order to lower operator workload and stress and consequently human errors. Naderpour describes the explosion at Bellwood, Illinois occurred on 14 June 2006 as follows: the ignition of a vapor cloud generated by mixing and heating a flammable liquid in an open top tank located in a chemical mixing area killed one contractor and injured two employees, and caused a significant business interruption. This ignition was generated by malfunction of a temperature controller, which allowed the steam valve to remain open and heat the mixture to its boiling point, the operator without knowing the inside temperature of the tank. Besides this, due to a failure of the system design of high temperature alarm missing, the operator lacked substantive information for situation awareness. There have been speculations on infrared thermometer information being available, but not been observed for some reasons by the operator. Reasons for that might have been e.g. plain omission, attentional narrowing or external distractions due to for instance high workload or prior expectations to see assumed rather than real situation. (Naderpour et al. 2015.)

A taxonomy for classifying and describing errors in situation awareness was developed by Endsley, based on the elements of human information processing

and cognition, as well as the factors affecting situation awareness at each of its three levels (Endsley 1999). The taxonomy is illustrated in the Table 2 below.

SA level I Fail to perceive or misperception of information	
1.1	Data not available
1.2	Data hard to discriminate or difficult to detect (e.g., visual barrier)
1.3	Failure to monitor or observe data due to omission, attention narrowing, distraction or high workload
1.4	Misperception of data
1.5	Memory failure
SA level II Improper integration or comprehension of information	
2.1	Lack or incomplete mental model
2.2	Use of incorrect mental model
2.3	Over-reliance on default values in model
SA level III Incorrect projections of future trends	
3.1	Lack or incomplete mental model
3.2	Over-projection of current trends

Table 2. The taxonomy for situation awareness errors (Endsley 1999)

This taxonomy has been used in different domains, among other things in analyzing accidents in process industry, in aviation accident investigations and in health care reviews. Studies tend to show so far, that the large majority of the errors is attributed to level 1 i.e. in perception, the second most category being level 2 errors i.e. in comprehension.

5.1 Nautical

In Finland, the maritime traffic management operates on the basis of a so-called maritime traffic situation picture, which includes a combined radar image and the ship's AIS data, involving the name of the vessel, the purpose of the vessel and the position of the vessel. In addition, the maritime traffic situation picture includes VHF radio announcements that indicate which vessel is involved, the vessel’s route, where the vessel is heading, and whether the vessel is aware of other movers. Furthermore, the general maritime traffic management situation picture includes vessel schedules (port lists), weather and ice condition, as well as expected potential problems or deviations, port disturbances, fairway disturbances, broken equipment and safety equipment deviations. In maritime traffic

management, both decision-making and situation information are centralized and the predictability of situations is emphasized. Studies have demonstrated that operators face challenges in understanding a situation picture with only minor changes. In addition, personal characteristics have been found to influence the perception of things. One of the objectives is to develop a learning situation picture system, so that maritime risks could be identified and warned automatically, and for identification of normal situations, that may vary depending e.g. on the type of vessel, weather conditions or tides. (Koistinen 2011.)

According to the 2001-2005 vessel accident analysis, the most common causes of accidents were human errors and conditions outside the vessel (e.g. weather). Of all accidents, 49% were partly due to human factors, that were in 38% as the main cause. Loss of situational awareness is not recorded as a separate category, but the related categories of causes are as follows: (A) Circumstances outside the vessel, such as (A04) failure of navigation equipment, lights or other electrical equipment, or (C) Technical condition of vessels' equipment, such as (C01) navigation equipment failure; or (D) Equipment operation and type problems and human-machine problem, such as (D05) other device operating problem; or F) Routines, communication, and organization, such as (F01) deficient control routines, (F10) deficient monitoring and maintenance routines, and (F15) deficient security routines; or (G) Human errors, such as (G04) improper use of warning devices, (G08-G09) misunderstandings and (G13) special circumstances (excessive work). One of the accidents was due to navigating by a bus sign and trusting its location, even though the bus sign had moved out of place. As a result, the vessel came into contact with the ground. The shortcomings of the database and of the marine casualty reports, used as a source, have made it difficult to conduct a reliable analysis, as well as the fact that the reports did not have a similar causal field as the database. (Finnish Maritime Administration 2007.)

According to International Maritime Organization IMO (2020), maritime cyber risk refers to a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised. In the shipping industry, cyber can be

categorized into threats to ships and safe navigation, satellite communication, cargo tracking systems, marine Radar systems and automatic Identification systems (Paganini 2016). The maritime cybersecurity survey conducted in 2017 to companies revealed, that 34 percent of respondents had experienced a cyberattack in the previous 12 months, mostly suffering from ransomware and phishing (Rider 2018). Various attack techniques can be used, such as hacking the electronic chart systems ECDIS of navigation or the satellite communications (Munro 2018). The first utilizes the fact, that ECDIS are often ran by old operating systems and crew tends to rely persistently on them instead of seeking other visual information. The latter is due to that many satcom terminals on ships are available on the public internet and have default credentials, e.g. admin/1234 (Munro 2018).

Ships are said to be complex industrial systems, only floating, transporting high-value cargo with legacy systems, combined with poor processes and awareness, while the seaports they dock in often suffering from the same cybersecurity problems. The ensemble of systems includes i.a. VSAT, GSM/LTE and Wi-Fi connections, crew internet access, electronic navigation systems, ECDIS, propulsion, load management and multiple other complex customized systems. Gaining access to these systems predisposes vessels to loss of navigation, control and situation awareness offering e.g. pirates to steer the vehicle in the territory where it can be robbed (such as in incident of a vessel from Cyprus to Djibouti in 2017). Also, access provides opportunities for criminals to influence to the control of the movement of containers for smuggling illegal material (such as in the Belgian port town of Antwerp). (Magee 2018.)

In 2017 a massive GPS spoofing attack crippled navigation on over 20 vessels in the Black Sea (Goward 2017). There is no indication of the diminishing of cyberattacks in maritime industry either, therefore, development measures are needed to improve security and safety.

5.2 Aviation

According to SKYbrary - an electronic repository of safety knowledge related to flight operations - situational awareness from a pilot's perspective means having a mental picture of the existing inter-relationship of location, flight conditions, configuration and energy state of an aircraft as well as any other factors that could affect safety such as proximate terrain, obstructions, airspace reservations and weather systems. In turn, for a controller, situational awareness means acquiring and maintaining a mental picture of the traffic situation managed and maintaining an appreciation of the potential for unexpected progressions or changes. A potential consequence of inadequate situational awareness is a loss of control. (SKYbrary 2019.)

In aviation, as a pioneer in so many respects, there are multiple traffic and safety advisory systems, such as the Engine Indicating and Crew Alerting System (EICAS) and the Electronic Centralized Aircraft Monitoring (ECAM) designed to support situation awareness, and to ease pilot stress in abnormal and emergency situations and for instant assessment of the situation. These systems can monitor aircraft functions displaying and relaying them to the pilots by messages detailing failures and by listed procedures for undertaking corrections to the problem. The system limitations after failures can also be illustrated within. Caution messages and affected systems are presented on the displays with a colour-coded scheme using three-level classification on alerts. The importance and urgency of the corrective actions required defines the level of an alert. The highest priority is in level 3 relaying of an emergency and urging the crew to take immediate corrective or palliative action. Level 3 alerts are visualised as warning light flashing in red. Level 2 cautions relay to an abnormal configuration requiring immediate crew awareness, but no immediate and mandatory corrective actions. These are visualised by an amber caution light. Level 1 cautions relay to a configuration requiring crew monitoring, that are often failures leading to a loss of redundancy or degradation of a system. (SKYbrary 2017.)

Endsley conducted a study on major air carrier accidents from the years 1989-1992 in the U.S. by analysing accident investigation reports with the taxonomy of

situation awareness errors (presented in Table 2). In total 15 accidents were related to situation awareness loss, including multiple errors in single report. Altogether 32 situation awareness errors were found, of those the majority (23 pcs, 72%) being level 1 situation awareness errors i.e. failures to perceive information in the situation. 22% (7 pcs) were level 2 errors in which the data was perceived but not integrated or comprehended correctly. Finally, errors were least on level 3 i.e. in projecting the near future based on the aircrew's understanding of the situation. (Endsley 1999.)

Studies have indicated that the frequency of situation awareness problems in operational errors ranges between 59 % and 88 % in aviation (Schulz et al. 2016). This has proved to be fact also in the investigation report of an accident and loss of control near Tallinn airport on 28.2.2018 during a training flight. There were some contributing technical factors, such as a false caution of a fault and warning messages displayed with a delay, and malfunctions of the override mechanisms inducing on message triggering. The latter were such as erratic signals coming from micro-switches caused by a non-standard displacement of an override mechanism piston, and by wrong oil type in the override mechanism clutch unit. Also, a system design flaw allowed a single event to cause the loss of pitch control. Several warning messages were generated, but there were no reaction to these warnings, and the flight continued despite of repetitive warnings. Contributing facts were, that the training instructor was performing in two roles, as a monitoring pilot and as an instructor, hence, the task sharing being different from a normal situation. The role change might have caused a delay in understanding the situation, taken into account that the performance of the student pilot compared to an experienced pilot is often lower in a stressful emergency situation. In addition, the role of the Safety Pilot being not clearly defined might have caused confusion considering the task sharing had to be improvised under a stressful situation. This all resulting to, that the training instructor and the student did not comprehend the situation and shared their lack of understanding, due to information overload and confusion from the unexpected situation. However, according to the existing recommendations concerning duties and responsibilities, the commander is responsible to monitor the level of fatigue of all the crew members, and during the

flight the commander can decide to stop the flight activity anytime due to the level of fatigue of the crew members and the occurrence of technical faults. (Estonian Safety Investigation Bureau 2019.)

In turn, key factors for runway safety include radio phraseology, communication format, equipment, airport lighting and markings, aerodrome maps, operational factors, as well as situational awareness and human factors. Situations in which pilots do not follow air traffic control instructions are often the result of a loss of communication or loss of situational awareness. These situation are such, that pilots may think they are at a different point in the airport than they actually are, or they may think they have been allowed to taxi on the runway. Other factors that predispose to pilots' errors are deficient signs and markings at the airport. Air traffic control can give instructions exactly as the aircraft is taxiing after landing, making it difficult to hear air traffic control in the cockpit. Pilots can lose situational awareness by focusing on tasks where the gaze is kept low and performing complex tasks can result in pilots rushing too much. The complex design of the airport area, especially for runway crossings, can also expose pilots to mistakes. Incomplete taxiing instructions are a risk, as are last-minute changes to taxiing routines. One of the commonly identified reasons for the loss of situational awareness is paying attention or channeling of interest to only one activity or event. (Safety Investigation Authority 2018a.)

Although the general automation of systems, many of them require manual control by operators e.g. in situation where parameters exceed specified set points and operators need to act. Manual control and automation should be appropriately combined in system design, so that accidents like the 2009 Air France 447 crash into the Atlantic Ocean due to erroneous information of airspeed sensors for primary flight instruments and autopilot would not happen again, and so that real-time operators would correctly adapt to situation when the automation is suddenly not functioning properly. (Gaba et al. 2013.)

As for the cybersecurity in aviation, the International Civil Aviation Organization (ICAO), the European Centre for Cybersecurity in Aviation (ECCSA) and the International Air Transport Association (IATA) each are developing cybersecurity

by strategies, toolkits and guidance material, such as the Security Management System Manual or Aviation Cyber Security Toolkit. These are increasingly needed for the growing amount of cyber threats encountered.

Connectivity of aircraft systems provides a vast attack surface. Aircrafts' complex data networks cannot be monitored as effectively as the comparable ground-based networks, thus, lacking the ability to avoid and respond to potential cybersecurity incidents. Modern digitalisation with advanced technologies, such as Global Positioning Systems (GPS) and Automatic Dependent Surveillance Broadcast (ADS-B) can be susceptible to manipulation by hostile actors. There is some indications of the link between the Aircraft Communication Addressing and Reporting System (ACARS) and Flight Management System (FMS) being a potential access point (i.e. an attack pathway) into aircraft systems. This link may compromise navigation functions, some authorities disclaiming it and asserting that it would not work in real world. Another system, the Airborne Collision Avoidance System X (ACAS-X) utilizes probabilistic modelling and dynamic programming to determine the best course of action with the help of multiple data sources (including ADS-B), and in generating avoidance warnings and commands. The increasing amount of integrations and data sources causes the appearance of risks. The threat scenario is, that adversaries attempt to cause ACAS to take avoiding action on false ADS-B signals, which may result to loss of situation awareness and control. One of the vulnerable systems can also be the In-Flight Entertainment (IFE), due to multiple versions of this software being freely available online. Utilizing this provides possibilities e.g. for tampering of lighting or manipulation of displayed information. Also, airports arise adversary interest due to their nature of being as federated management systems with multiple interdependent service providers. Deficiencies in airport cybersecurity contribute to allowing bypass, subversion, and eventual breaches of physical security. Finally, the human element cannot be omitted. In practise, employees having legitimate access to large amounts of sensitive data that attracts cyber criminals, fraudsters, and terrorists, are vulnerable to attack. (Cooper 2017.)

There have been some news reports (Murdock 2018) on vulnerabilities and security weaknesses in satellite communication (SATCOM) technology that allows in-flight aircraft hacking from the ground. Also, the cyber experts of U.S. Department of Homeland Security (DHS) are known for having remotely breached the defenses of a Boeing 757 commercial plane (Biesecker 2017). The vanishing of the Malaysia Airlines Flight MH370 in 2014 has also been a subject of speculations of a cyberattack (Infosec 2014).

Jamming attacks consist of an intentional emission of radio frequency signals to interfere with the operation of a radar. The principal types are mechanical jamming (i.e. reflecting or re-reflecting the radar energy back to the source to produce false target returns on the operator's scope) and electronic jamming (i.e. specific device jammers generating signals to interfere with target's radar, as blocking the receiver with highly concentrated energy signals by noise or repeater techniques and repeater techniques). Jamming causes losses and deletion of messages, resulting in adoption of less efficient or less accurate surveillance and control methods. This is significant especially in high density areas, such as in the environments of major international airports, where disorders of surveillance or collision avoidance could result in human failure with fatal consequences. In an experiment a continuous white noise jamming waveform was emitted. This waveform caused complete deletion of all messages. This kind of an attack can also produce fake alarms, such as those an aircraft might transmit during an emergency or terrorist attack. (Infosec 2014.)

The final approach and landing are the most stressful stages of the flight for the flight crew. Resolving a fault in an airplane system during these phases of flight may set the crew to the limits of their cognitive capacity. To provide an overall picture of the dangers of the situation and the consequences of the incidents, a large amount of additional information processing capacity is required, in which pilots have limited availability during stressful flight phases. As a result of the workload, the action may become reactive, i.e. react to oncoming events as they occur. It is no longer possible to look at the situation holistically and to anticipate or plan future events. In this case, in the decision-making situation, it is easy to

resort to different rules of thumb created by previous experiences and be exposed to hallucinations. Under stress, crews do not have the resources to actively challenge erroneous assumptions created by biases. (Safety Investigation Authority 2013a.)

Safety Investigation Authority of Finland (2013b) states, that aviation training programs must be developed in such a way that the limitations of human perception and decision-making ability are addressed more in teaching than at present.

Considering different flight categories, such as instrument or visual meteorological conditions (IMC, VMC), each are covered by their own rules (e.g. instrument or visual flight rules). Some warning systems are configured to protect a certain condition and rule and to be suppressed in the other. The warning system can be activated also in the other condition and rule, but it may produce numerous false alarms for aircraft operating in certain circumstances. Thus, the risk for accidents increases. (National Transportation Safety Board 2015.)

5.3 Railways

The operational field of railway traffic is wide and disruptions are very complex in Finland. Situational information is decentralized between several different actors. In incident management, the challenge is that decisions are decentralized between different parties and actors are often dependent on each other's decisions. Situational information and decisions do not always meet, i.e. some actors can have all the information about a particular situation, but no decision-making power or vice versa. This contributes to making difficult to form an overall picture. All these challenges set requirements for situation awareness system, such as enabling all actors to have access to the same situational information at the same time. (Koistinen 2011.)

The Safety Investigation Authority conducted a theme Investigation on wrong routings in train traffic in 2015 and found out, that some traffic control systems and

interlocking devices have functions that could be used to technically protect track work. However, the traffic control systems used are different and some systems completely lack security-related functions. The systems used for traffic management have undergone a constant change affecting users. This is partly due to the development phase of the systems, the improvements to be made to them and the new features to be introduced at different stages. Traffic management systems are being developed centrally for the use of various traffic control centers under the leadership of the Finnish Transport Infrastructure Agency. The Finnish Transport Agency defines, acquires and owns traffic control tools, but Finrail Oy, which implements traffic control, is responsible for their use. According to the investigation and the survey of traffic controllers, the basic features and operating methods of the systems have not been sufficiently understood. Traffic controllers are not familiar with the operation of different systems. Some of the graphical user interfaces of the traffic control systems were such that the possibility of a slip or error of a traffic controller is increased. This is affected by the monitor symbols in the older user interfaces and their small size as well as unclear colouring. Even newer interfaces may lack a marking of the location of passenger platforms at traffic locations. In some cases, small symbols and small text on traffic controller graphics screens have been affecting the incorrectly set path. Especially when the control areas are wide, the views of the traffic control system should be easy to interpret and understand. The systems should be similar for the control area entities. Many operating systems with different logic, even in the same workspace, increase the risk of errors. The characteristics of systems directly related to traffic control are different in traffic control centers operating in different locations and also in different workstations. This is due to the system vendors selected for each site and the investments made in different eras. The diversity of the systems has also been and continues to be influenced by the special features of the suppliers' own products and the customer's requirements related to the traffic control systems in each procurement. Since its introduction, changes and improvements to the systems have proved to be rigid in practice. Traffic controllers feel that individual faults in the systems are rectified quickly, but suggestions for system development and improvement are not taken into account. The feedback collected in the user experience feedback system does not progress to development measures.

Underlying the problem is that the development of systems often requires large financial resources. It also seems to be that the infrastructure manager and the user are different parties. (Safety Investigation Authority 2016.)

In the short term, many other changes have also taken place, including in the organizational structure, regulations and guidelines. The investigation revealed that traffic controllers experience constant changes as stressors in their work. For individual workers, the whole set of changes is not necessarily outlined, but can be seen as fragmented and merely hampering work. Motivation to learn new instructions and regulations decreases. There have been delays in the completion of the guidelines by the Finnish Transport Agency, which means that the short time between the completion of the guidelines and their introduction has created problems in the training of traffic controllers. There have even been situations where the regulations in force and the regulations in use are not the same, leading to ambiguity as to which regulations must be complied with in practice. This also undermines public confidence in regulations and those who issue them. In addition, during the investigation, the railway traffic control manual published by the Finnish Transport Agency was still a confidential document. In practice, this made it difficult to use the handbook in a variety of ways and, for example, for self-study opportunities for traffic controllers. (Safety Investigation Authority 2016.)

Within the shift, the workload is increased by track work, when the traffic controller is hardly able to take advantage of the automation in use, but has to work on many things with memory. The workload of traffic controllers is not measured very systematically. According to the study, automation errors are rare. The investigation revealed only one case where an automation error was suspected. This happened during the commissioning phase of the new program, when the automation worked unexpectedly due to a programming error. (Safety Investigation Authority 2016.)

In rail transport, research on human factors has traditionally been less than in aviation domain. Studies show that about half of the errors are typically human attention errors, decreased alertness, and fatigue. However, even attention errors

are often caused by poor equipment design or other organizational factors. (Safety Investigation Authority 2016.)

Safety incidents are recorded by several different safety authorities, but the Finnish Transport Infrastructure Agency is responsible for the safety of transport networks and statistics on safety incident data (Safety Investigation Authority 2016). However, deviation and incident data are not collected from an information system perspective, i.e. incidents related to the information system entity are not recorded and no public classification or taxonomy has been created for them (Safety Investigation Authority 2016). Deviations in information systems are equally possible and significant in relation to other classified anomalies, and therefore knowledge of them is needed to provide the most complete security picture possible.

Based on the 2015 thematic study, Safety Investigation Authority ended up issuing a safety recommendation on reporting and classification. It is noteworthy that the status of the Recommendation is still “partially implemented”, so apparently this is a difficult and complex issue that requires a long time to implement practical solutions. (Safety Investigation Authority 2016.)

The classification criteria are the EU-level common safety indicators defined in the Railway Safety Directive 1 and the complementary national safety indicators (VNa 864/2010), as well as the Finnish Transport Safety Agency's (Trafi) railway safety indicators, which were revised in 2013 (Finnish Transport Infrastructure Agency 2019b). In addition, the Association of Accident Insurance Institutions (TVL) classification of accidents at work (ESAW European Statistics on Accidents at Work) and the classification methods for accidents at work developed by Eurostat, the EU's statistical office, are used (Finnish Transport Agency 2014).

Safety deviation data are compiled from several sources, such as the Finnish Transport Agency's safety and risk management information system, Finnish Rail Traffic Centre's incident reports, VR-Yhtymä Oy's railway safety reports and technical systems data (hot running, overload and wheel fault information). Safety incident reports come from one spesicif system on two different notification templates, incident reports as e-mails and safety reports as pdfs. The template

used by traffic control has taken into account the investigation of the underlying causes of the cases, but in the other template the identification of the underlying factors is challenging. However, the ultimate purpose of incident reports and railway safety reports is not to serve as background material for the classification and analysis of safety incidents, but to inform stakeholders closely. It is difficult to use concise and, to some extent, header-level information to identify the causes of deviations and to devise corrective measures. There is no separate field in the project template of the safety and risk management information system for recording culprits. The wider use of the underlying causes of safety deviations and development measures must take into account all the input data, as system changes only to the current safety and risk management information system alone do not cover all data. (Finnish Transport Infrastructure Agency 2019b.)

Multiple incident reports are made for the same deviation and only one incident report is selected to describe that deviation. This choice affects the information available in the analysis when deviations are treated by category and some of the information is thus lost. The challenge also arises with deviations from different sources. (Finnish Transport Infrastructure Agency 2019b.)

The classification criteria do not include a category for the loss of situational awareness, but the information related to it can be obtained from the categories of the safety control system issuing a false signal for the train (e.g. a clearance or an authorization of speed higher than allowed), of grade crossing accidents equipped with automatic audio or visual warning system, and of incidents caused by the third party for the rail system. Incorrect operation of the safety device system has not been reported at all in 2018 (Finnish Transport Infrastructure Agency 2019b). 302 incidents caused by the third party were reported in 2017, but they comprise physical damage for the equipment, structures or equipment, not influencing attempts (e.g. malicious activity) to systems (Finnish Transport Infrastructure Agency 2019a). There is no separate category for cyber threats or similar hazards. Regarding the unnecessary or false alarms, for example, in 2017, of the alarms of hot running and wheel power 508 pieces were confirmed as valid alarms and 80 pieces (16%) were confirmed as unjustified alarms (Finnish Transport Infrastructure Agency 2019a).

As for hacking, the with new digital railway systems are estimated to expose the railway network to cyberattack (Khandelwal 2015), this being due to i.a. the European Rail Traffic Management System ERTMS and the European Train Control System ETCS replacing traditional signalling and offering automatic train protection across Europe, using wireless technology and computerised in-cab signals (Railway Technology 2017). In Finland, the digitalisation of rail traffic is progressing when the service life of train access control equipment expires at the end of the 2020s and EU regulations oblige to equip lines with ERTMS (Digirail 2020). The new radio-based system is said to speed up the setting of traffic restrictions and promote traffic safety (Digirail 2020). The European Electricity Standardization Organization CENELEC is developing a cyber safety standard for ERTMS. Cybersecurity is being developed in cooperation with the European Cyber Security Agency ENISA, that together with national authorities, such as Traficom in Finland, will perform the system certification. (Ministry of Transport and Communications 2020). According to the UK Department for Transport, railway systems are becoming vulnerable to cyber-attack due to the shift from legacy and bespoke stand-alone systems to open-platform, standardised equipment built using commercial off the shelf components, and increasing use of networked control and automation systems that can be accessed remotely via public and private networks (Railway Technologies 2017).

There are numerous news published of cyberattacks to railways, such as the one (Railway Technologies 2017) claiming that the UK rail network had been hit by at least four major cyber-attacks over a 12-month period in 2016. Before this, hackers, that estimated to be overseas, attacked computers at an unidentified railway company in U.S. disrupting railway signals for two days in 2012 and causing rail schedules to be delayed (Zetter 2012).

In 2016 a team of researchers evaluated the level of cybersecurity implemented in modern railroad systems and discovered several vulnerabilities i.a. in the train protection system SIBAS widely adopted in Europe. The SIBAS uses the Siemens SIMATIC components, e.g. the WinAC RTX controller, which was affected by several security vulnerabilities. The team was said to be impressed by a large number of vulnerabilities, such as the lack of authentication protections, poor

maintenance, operating systems and software components not updated, and of hard-coded passwords. (Paganini 2016.)

Thus, these so called traditional air-gap protected systems, such as in railways have been, are not immune to attacks. It remains to be seen, whether any progress has been made since the days of 2008, when a 14-year old teenager used a modified TV remote control to interfere with the tram track and point system, causing derailment of four vehicles and injure of 12 people (Fachot 2018).

5.4 Healthcare

Situation awareness can be promoted with new technology. Patient monitoring comprises an interface between the physical quantities measured in the patient and the sensorium and cognition of the human decision making. The interface design of patient monitors does not traditionally support the human sensory perception, neither enabling time-effectively comprehension of the patient's condition, as humans are better in recognizing shapes, colours, and movements, than in reading numbers. This craves high cognitive effort to integrate the presented information into a mental model of a patient's current status and expected progression. Synthetic vision technology originates from aeronautics and military aviation, and is newly applied to healthcare domain. This technology supports situation awareness by converting numerical vital sign values and waveform monitoring data into a real-time virtual image as a patient avatar, and is expected to be useful in environments with high cognitive demand and immediate decision making. (Tscholl et al. 2020.)

Technology related threats have to be considered while adapting new technologies. For example, regarding wireless infusion pumps, the present-time threats comprises targeted attacks attempting to compromise the pump and system components directly affecting pump operations, and advanced persistent threats with malware enabling a threat actor to perform unauthorized actions (NIST 2018). In Finland, according to the National Supervisory Authority for Welfare and Health (Valvira), the majority (38%) of serious incidents related to medical devices were defects in the manufacture or design of the devices in 2009. In U.S. the public

Manufacturer and User Facility Device Experience Database MAUDE database comprises medical device reports of device-associated deaths, injuries and malfunctions (FDA 2020). A search on MAUDE can be done e.g. by criteria about errors or failures of warning related to alarms as a product problem and a malfunction as an event type, this producing currently seven reports from the last decade (FDA 2020).

According to the US ECRI Institute (2013) a study in a hospital environment tells that to 70% of alarms (n = 400 alarms) were not responded to by medical staff. Of the 34 significant and potentially life-threatening alarms 41% were not answered immediately (ECRI 2013).

In the 2019 list of Top 10 Health Technology Hazards published by the ECRI Institute, the risk of brain injury and death due to incorrect alarm settings on the respiratory system (ventilator) was ranked fourth. Ranked in the top seven are improper modifications to the alarm settings of physiological monitoring devices, which may cause the absence of alarms. (ECRI 2018.)

The monitoring, control and situation awareness systems must be designed and configured so that the operating environment achieves a balance between too many activated alarms and too few activated alarms to prevent alarm fatigue and ADT for users. Modifying alarms and their settings can help to achieve this balance. Modification refers to the selection of alarm thresholds and settings suitable for operational needs, so that an inactive state or condition is not activated and unnecessary alarms, i.e., missed alarms, are not generated. In the target mode, an activated alarm should always trigger the correct functional response. The system should support alarm management by enabling the editing of alarms. According to ECRI research, in 2018, two fatal cases were caused by incorrect breath minute volume and low-pressure alarm settings. (ECRI 2018.)

The AAMI (Association for the Advancement of Medical Instrumentation), at its meeting on 4-5 November 2011, identified research needs on:

- risk analysis of what is being monitored and what is not being monitored
- an analysis of which software, hardware and tools are causing (can cause) system alarms

- consolidate research into alert management
- alert user response
- the impact and effect of alarms
- prioritization and source-specific typing of auditory alarm signal
- to adjust the volume of the alarms according to background noise and time of day.

There have also been some proposals as sensor alarm architectures or frameworks in healthcare applications of cyber-physical systems, in order to detect false alarms, based on various classifications of vital signs. However, they must be further studied and treated with caution, as sometimes their developers do not have the medical expertise, but the knowledge comes only from the point of view of data analytics. For example, due to the vast amount of versatile patient conditions, forms of treatment, therapeutic environments and care situations a simple and straightforward reasoning for algorithms of false or nuisance alarms might result to a safety risk.

Kane-Gill et al. (2017) conducted a systematic literature review on alert fatigue, expecting to find studies evaluating systems in terms of alert fatigue. Although they found no such studies, they proposed a quality improvement program focused on appropriate alert implementation and management in order to reduce alert fatigue. Components of a quality improvement actions involve (1) design of alerts for prevention and detection of events with clear delineation of the alert purposes, (2) determination of the priority and clinical significance of alerts before implementation with organization support and alignment, (3) determination of the responsible responding to the alert, the mode of delivery, and a reasonable response time, (4) evaluation of the performance characteristics of the alerts after implementation, (5) revision of the alerts based on the performance characteristics, (6) alteration of alerts based on changes in practice, and finally (7) education and implementation planning to support alert introduction and expectations. Interventions for reducing alert fatigue in a clinical environment include prioritizing alerts based on severity and clinical relevance, learning from previously overridden alerts to avoid future alerting, focusing on atypical or rare prescribing events, taking

note of end user opinion in use of alerts, and customizing systems. (Kane-Gill et al. 2017.)

According to Schulz et al. (2016), the majority of situation awareness errors in anaesthesia and critical care were the first level errors, i.e. errors in perception. They conducted a study on reports in the Critical Incident Reporting Systems (CIRS), which is an anonymous platform for voluntary reporting of errors and near misses in Europe, similar to the Aviation Safety Reporting System. Of two hundred cases, situation awareness errors were identified in 163 (82%; in accordance with findings from aviation where the frequency of situation awareness problems in operational errors ranged between 59 % and 88 %). Besides the majority (38% in level 1), almost as much was identified in level 2, i.e. in comprehension. Only 12% were attributed to level 3 errors, i.e. in projection. Less errors on the level of perception and more errors on the levels of comprehension and projection were found, as a comparison to aviation. The errors can be associated with wrong clinical decisions, resulting in patient harm, such as a case of an anaesthesiologist incorrectly assuming that a drug syringe was ready to use, but in reality, drugs were not prepared (error in level 2, comprehension). Surprisingly, the frequency of situation awareness errors and their level of were independent from the location (e.g. Intensive Care Unit) and from other categorical data (e.g. professional status, work experience, routine vs. emergency case). (Schulz et al. 2016.)

There is no publicly open database to search for hazardous incidents, but health care providers store notifications of incidents and near misses in their own systems. The most commonly used system in Finland is HaiPro, but neither it does record events from the perspective of loss of situational awareness. Mainly corresponding to situation awareness errors are the event types of communication and information flow (gaps in the use of available information), of operating methods (poor availability and comprehensibility of task-related and decision-making information), and of work environment, tools and resources (workload, information system problems, deficiencies in the physical environment) (HaiPro 2015).

In 2014, approximately 14000 HaiPro notifications were made at Helsinki University Hospital, of which 44% were near misses and 22% were incidents related to the flow of information. The Patient Safety Report (Helsinki University Hospital 2015) mentions that the inconsistent IT programs in use affected data processing and management. 5% of cases related to the equipment and its use (e.g. equipment malfunction) were recorded, which is estimated to be underreported. As for comparison, number of incident reports were 6341 pcs in 2018 at Northern Ostrobothnia Hospital district, of which 41% being near misses (Oulu University Hospital 2018).

The Finnish Institute for Health and Welfare collects indicators on the digitalisation of healthcare and the results of the 2017 information system survey for healthcare professionals were i.a. the following: 5% thought that system malfunction has caused harm (handicap), 31% thought that system malfunction has caused a risk, 46% thought that the functions are arranged logically in the screen views, 30% thought that the information systems behave in an unexpected way, from 21% to 33% thought that the information systems cause workload, 68% thought that the information systems displace the attention from the patient, and 69% thought that the terminology is clear (Finnish Institute for Health and Welfare 2019). Unfortunately, some of these figures are not very flattering.

5.5 Results of the database search of investigation reports

As for this study aimed to determine about the errors related to situation awareness, the situation awareness levels of Endsley's model and the SHELL model was used. The results are illustrated in the tables below.

Reports	
Finland	
Aviation	14
Norway	
Aviation	3
Railways	1
Marine	3
U.S.	
Aviation	4
Total	25
Aviation	21
Railways	1
Marine	3

Erros in SHELL interfaces	
Environment-Environment	0
Environment-Hardware	2
Environment-Software	1
Environment-Liveware	2
Hardware-Hardware	1
Hardware-Software	10
Hardware-Liveware	1
Software-Software	0
Software-Liveware	11
Liveware-Liveware	10

Errors at SA level	
1	18
2	10
3	15

Databases
Safety Investigation Authority Finland
Accident Investigation Board Norway
National Transportation Safety Board U.S.

Table 3. Result tables

Due to the small amount of research reports and the disproportionate distribution of the sample, only the sum result is shown in the Table 3 above. Thus, errors of situation awareness levels and interfaces are not divided into different domains.

The results show that in a single accident, errors at different levels and at different interfaces can occur simultaneously. Situational awareness was most weakened by problems in perception (level 1), but in these reports, problems were fairly evenly distributed between perception, understanding and comprehension (level 2), and projection and decision-making (level 3). Most errors were found in human-software interactions, but almost as many in hardware-software interactions and in human-to-human interactions. The errors found included factors such as:

- design errors, e.g. alarm functionality was completely missing so it could not be communicated at all, meaning that the initial information was already incomplete
- design errors, e.g. unclear or inadequate visualization of alarms

- system operating limitations, e.g. configuration errors of alarm parameters or lack of system interoperability
- system failures, e.g. a device (sensor) had stopped working, or an alarm message was not visualized, or different systems gave conflicting alarms or warnings
- misinterpretation or ignorance of the situation
- performance deficits or errors due to situational pressures, cognitive workload or inadequate instructions and operating procedures
- deliberate operative errors, e.g. disregard for warnings (resetting, suppressing or shelving) and lack of cooperation between the central control and the local operator
- unintentional operative errors due to the problem of perception and detecting alarms, unresponsiveness to warnings, or missing cross-checks as verification mechanism
- general negligence or lack of competence caused by an inadequate safety culture.

The results support the conception of the literature review of this study brought out about the Human Factor and the importance of user interfaces to security. These results providing only a rough picture, it is justified to propose a more detailed analysis of the research material in order to increase the reliability of the study.

6 CONCLUSIONS

The aim of this study was to investigate how situational awareness systems can implement situational awareness through visual usability in user information, and to consider the risks associated with the reliability, integrity and availability of situation information through user interface, and impact of this information on user decision making. The focus of situation information was on alarms using a derived theoretical research assumption of a malicious attacker causing alert fatigue and loss of situational awareness by triggering unnecessary or false alarms, or by influencing to alarm data otherwise. The study succeeded in achieving the learning objective.

The answers to the first research question (1a and 1b) were presented in Chapters 2 and 3. This study demonstrated that understanding of human cognitive functions is essential in situation awareness. These functions are represented in theoretical models of situation awareness, for example, in Endsley's model, as well as in SHELL-model. Interactions between people, programs, systems and devices must work flawlessly to meet the requirements of cybersecurity within the field of information exchange in every level of situation awareness. Nowadays, information systems are wide-ranging compositions and configurations providing several functionalities and utilizing multiple information sources. Human expertise and knowledge is integrated as properties in order to maintain goal-orientation, control and supervision for continuous developing. Robustness and resilience are obtained through parallel data collection and analysation methods. The design of user interaction in situation awareness systems is supported with multiple instruments, such as design guides and standards. These instruments promote the situation awareness of a user in the context of alarm functionalities by offering both general as well as domain-specific guidelines for appropriate and safe design and implementation. Guides and standards are widely applied in safety critical industries, for example, in nuclear industry and aviation domain, serving as bywords for other domains.

The answers to the second (2a and 2b) research questions were presented in Chapter 5. To conclude these findings, a short synthesis is introduced herein. As

stated in the very beginning of this study, the loss of situational awareness might lead to severe and fatal accidents. The factors of these accidents are manifold and thus, situation awareness has also been lost for a number of reasons, instead of only one particular reason. Accident and investigation reports show that the causes have mostly been a sum of many factors, such as a human error combined with a hardware or software failure and a communication defect. In practice, misconfiguration causes misinformation and leads to misunderstanding and misinterpretation. Several reports indicated that the lack of alarm functionality in the systems causes misperception leading to misinterpretation of the situation, which in turn contributes to a human malfunction at the situational awareness level 2 (understanding) and 3 (anticipation, projection), resulting finally in incorrect decisions in mental pressure situations. These public reports are widely available and accessible, and especially in the field of aviation numerous reports in various databases of the situation awareness loss can be found. On the contrary, alarm-related events were estimated to be underreported especially in healthcare domain. Besides this, the loss of situation awareness is not usually classified as a category of its own in taxonomies of databases or accident criteria, but the reports related to it can be searched by using it or its compound for a key word. False alarms or cyber-attacks related to them are not classified at all in these databases. Indeed, the need to develop a classification has been identified herein. For the time being, the interpretation of the reports requires careful reading in order for the conclusions to be correct.

As for an example of incident reporting, The Federal Aviation Administration has developed the Aviation Safety Information Analysis and Sharing ASIAS system, which enables users to perform integrated queries across multiple databases. However, conducting a search in World Aircraft Accident Summary WAAS, FAA strongly instructs (2020), that considerable care and caution when interpreting the meaning of the data should be exercised, due to a number of definitional and statistical problems. Signifying, that interpretation of the data can result in misleading and erroneous conclusions, when the data is used as a measure of safety performance, especially in evaluating individual airline safety performance. This also indicates the existence of reporting problems.

The answers to the third research questions (3a and 3b) were presented in Chapter 4. As indicated previously, failures in attention are a frequently cited reason for accidents. A misplaced, or a dominant or latent source of information, such as a flashing warning message wrongly configured and prioritised, can be a distraction from the formation of situational awareness. Information overload due to alarms produced by a large number of technological devices and systems predisposes humans to excessive workload leading to alert fatigue and Attention Deficit Trait disorders. This is especially relevant in the healthcare domain, where the major contributing factors to losing situation awareness were stated to be inadequacy of an alarm system or its settings or integrations, or quality of alarms, all these contributing to alarm fatigue. On the other hand, high levels of automation combined with perceived excessive comfort in the work environment and a low level of human activation and participation can also weaken situation awareness. Finally, malicious and criminal activity in the form of attacks against critical systems can take place resulting to a loss of correct and actual situation picture. These attacks are performed by using various techniques, such as data manipulation or signal spoofing, in order to generate false alarms. Although the alarm functions must be designed to minimize the effects of false and nuisance alerts by preventing the presentation of an inappropriate or unnecessary alert, it has been proved that by hacking an alarm system, creation of a wrong situational picture is possible. As an example of that was the turning on of 156 emergency sirens for about two hours in Dallas 2017 (Khandelwal 2018), and similar events have even occurred after that. Another alarm-related incident was the Hawaii false missile alert in 2018 (Cohen 2018), which occurred by reason of insufficient management controls, poor computer software design, and human factors. This false alert had many undesirable consequences, such as people rushing overspeed to seek shelter, authority offices inundated with phone calls, jammed data services, and even a death of a person caused by a heart-attack due to fear. These events have also had positive effects in the form of policy and procedure reviews and updates, aiming to avoid false and nuisance alarms. The effects include corrections and patching of system weaknesses and vulnerabilities as well, so that exploitation of those would no longer be possible.

Furthermore, the research material showed that there are shortcomings in various situation awareness systems, especially in traffic management. For example, in an air traffic control system, an air traffic controller could not properly separate snow machines from aircraft, or runways due to deficiencies in vehicle detectors. The system was subsequently developed so that airplanes and land vehicles were clearly distinguishable on the screen. Development work had been done for a long time, but the system implementation had to be postponed, i.e. because of the biases and conflicts in object identification. (Safety Investigation Authority 2018b.)

With respect to described above, it should not be overlooked the fact of situation awareness loss often resulting from inappropriate design of information systems. There is a lack of utilizing Design Science and Human Factors, as the focus being on sheer Information Engineering and solely on technical elements (except on aviation domain, being a forerunner on many things). As Naderpour et al. (2015) stated, well understood hardware reliability techniques contributes to that, whereas the handling of human factors is experienced as difficult and costly to be taken into attention in system and software development. This as in respect to previously indicated growing need of cognitive decision support systems. Continuing on the issues that Naderpour et al. (2015) indicated, there is also room for improvement on to what extent humans are able to generate descriptions of system purpose and form, or explanations of system functioning, or observations of system states, and predictions of future states. This is a question of a mental model, being treated as default or base information before forming a higher level of situation awareness. (Naderpour et al. 2015.)

Related to the demands of an end user and the experience of how the system supports the work, the Quality of Service concept could be used as a tool in system development. This supports the idea of Endsley & Robertson (Endsley 2000), according to which, in order to discover possible methods for improving situation awareness is to observe in what conditions and how situation awareness errors occur, or to identify situations when individuals are able to develop and maintain situation awareness. Effective monitoring and cross-checking can be the last line of defence that prevents an accident, because detecting an error or unsafe

situation may break the chain of events leading to an accident (National Transportation Safety Board 2014).

Maintaining situation awareness and avoiding false alarms requires systems thinking, familiar with safety sciences. Cognitive work and task analysis methods, such as Critical Decision Method (CDM) for analysis of special and unusual events, developed in the field of cognitive ergonomics can be utilized to analyse work and work processes. The operational safety of systems is promoted by applying and simulating human cognition and the functioning of natural ecosystems. As stated previously, a human error should be considered as a symptom of the system and its design. This is true in the Systems Theoretic Accident Model and Process STAMP and its predictive risk assessment method, System-Theoretic Process Analysis STPA, which can be used for hazard and accident analysis in complex systems (Leveson and Thomas 2018). Another useful framework is the Emergency Response Protocol developed by EU to improve cyber preparedness. This framework introduces the phases of early detection and identification, threat classification, emergency response coordination, early warning notification, operational action plan, investigation and analysis, and emergency response protocol closure for a major cyber-attack in the cybersecurity ecosystem (IOCTA 2019).

For the improvement of situation awareness, there are multiple methods for conducting situational assessments analysis, including measurements based on observation of on-going activities i.e. process indices and performance measures (e.g., WOMBAT and SABARS), or direct measurements i.e. think aloud technique and real-time probes and freezing techniques (e.g., SAGAT), or retrospective measurement techniques (e.g., SARS), or team situation awareness measurements (e.g., CARS) (Human Factors Methods 2020).

Regarding the development of technology, although it was previously stated that researchers are currently developing more pleasant, quieter, and more informative alert methods to prevent i.a. alert fatigue, will this not be sufficient to inhibit all alert-related hazards. There is going to be a hurry, if the estimation of quantum computing ending the effectiveness of currently used encryption methods within

the next five years proves to be true, especially if the criminal use of artificial intelligence increases at the same time (IOCTA 2019). It also remains to be seen, how e.g. 9D technologies or virtual, mixed and augmented reality offers possibilities by changing perception based on our five senses. Capturing user's focus can be done through sense of sight, hearing, touch, or even taste or smell, all in a whole new kind of cyber environment.

Artificial intelligence solutions are constantly evolving. Utilization of artificial intelligence for situational awareness requires the definition of perception and the solution of related means in order to automate situational imaging systems. Situational awareness artificial intelligence research focuses on i.a. research into human-machine interaction, the areas of which include e.g. ergonomics, data and information visualization, and perceptual psychology. The most significant in the development of technologies related to perception are i.a. machine vision and image analysis, radars (radio-frequency, Lidar), ultrasound (radars), natural language analysis, voice and speech, positioning and tactile. When developing artificial intelligence technologies, the utilization of other disciplines and methods and the combination of data-based and symbolic artificial intelligence methods are central from the perspective of the system level and system effects. Perhaps most important, however, is the emphasis on a better understanding of biological systems and natural intelligence. (Ailisto et al. 2018.)

This study sought to indicate situational awareness risks in the context of alarm systems entity in order to prevent adverse effects such as accidents. Reading the narrative investigation reports is subject to interpretation, as it is according to hermeneutical research method. Therefore, the same research material can provide other points of view as well. This affects to the reliability of the study, but on the other hand opens up opportunities for new syntheses. The author expected to see evidence of false alarms (i.a. as a malicious activity) causing hazardous events in report databases, but had to settle for few news and theoretical research articles.

Topics for further research were identified in this study, the most significant of them being a development of taxonomy for situation awareness systems security

incidents as the factor of accidents and hazardous events. Security incidents are recorded by several different security authorities, but the incident information is not recorded from an information system perspective, i.e. incidents related to the information system entity are not recorded, and no public classification has been created for them, at least in Finland. Exceptions related to information systems are equally possible and significant in relation to other classified anomalies, and therefore knowledge of them is needed to provide the most complete security picture possible. Here it would be possible to utilize exception handling and event management concepts. The second most significant topic is proposed to be an execution of a detailed analysis of the causes of false alarms and development of preventive measures and alarm management as a case study. The third most significant topic would be an empirical research on the application of different theoretical models and frameworks to improve situational awareness and develop a safety culture in the organization.

Situation awareness as a topic is always current providing many possibilities for study. This is also reflected in the fact that on November 18 2019, Yle (Nyyssönen 2019) reported on testing new technologies developed for government use in the Toxi Triage project, which develops CBRN (Chemical, Biological, Radiation and Nuclear) rescue, treatment and incident management. The objective is to speed up the identification and response of the nature and extent of the hazard and the achievement of situational awareness by reducing the assessment time to less than five minutes in order to improve protection and survival (Toxi Triage 18.11.2019).

In the same interview by Yle, Project Manager Jaana Kuula from the Faculty of Information Technology at the University of Jyväskylä states that new technologies bring extensions to the human senses and physical abilities. He goes on to say that technology has great potential for improving people's safety. Technology plays an important role in intelligence, situational awareness and sharing, and new types of security technologies are being developed at universities and companies. Jaana Kuula explains that the starting point is to better protect the society from various threats in the future, and here understanding the situation facilitates decision-

making and gives people security, completes Jyri Silmäri, the rescue manager of the South Savo Rescue Department. (Nyyssönen 2019.)

The loss of situation awareness has significance in each level, from individual human level, organization level, system level, up to society level. It is justified to state that situation awareness cannot afford being lost. If the amount of accidents and incidents keep on increasing, the trust in situation awareness systems tend to weaken and the security, usability and effectiveness will no longer be at required level. Also, a user should be able to trust to an alert generated by the system, as in the same way the public needs to be able to trust that when a government issues an alert it is indeed a credible alert.

Regarding global situation awareness, Multinational Experiment 7 (MNE7) was an international co-operation pilot project conducted in the early 2010s that focused on the use of global operating environments - seas, airspace, space and global information networks - and defined situational awareness according to Endsley (Kuusisto 2014). In this project structures, roles, processes and tool requirements for gaining and maintaining effective situation awareness in cyberspace were defined. The Cyber Situational Awareness was defined as the perception of environmental elements with respect to time and/or space, the comprehension of their meaning, and the projection of their status after some variable has changed, such as time. Definition continues, that situational awareness involves being aware of what is happening in the vicinity to understand how data and information, network events, and SOCs' own actions will affect goals and objectives, both immediately and in the near future. (MNE7 2013.)

Finally, a good start point is definition of an alarm philosophy, as described in ANSI/ISA-18.2-2009, that serves as the framework to establish the criteria, definitions and principles for the alarm lifecycle stages by specifying items including the methods for alarm identification, rationalization, classification, prioritization, monitoring, management of change, and audit to be followed. Recent technological instruments, such as machine learning algorithms that are nowadays commercialized as services, can be utilized. Most of all, users' workflows and information needs should be considered, suppliers ought to be educated and the

user-centric design required. Like Lehto stated 2019, when building a solution, a balance must be found between cybersecurity, system functionality, and user experience. Inappropriate solutions in functionality and convenience create a very high degree of vulnerability within the organization. This is the groundwork for the protection of the critical infrastructure.

REFERENCES

AAMI. 2011. Alarm research gaps identified at the summit. Clinical Alarms Summit 4.-5 November 2011. WWW document. Available at: https://www.aami.org/events/eventdetail.aspx?ItemNumber=1153&navItemNumber=1114 [Accessed 22 November 2019].

Accident Investigation Board Norway AIBN. 2012. Report on investigation into marine accident M/V Godafoss V2pm7 grounding in Løperen, Hvaler on 17 february 2011. Investigation report Sjø 2012/09. PDF document. Available at: https://www.aibn.no/Marine/Published-reports/2012-09-eng [Accessed 27 April 2020].

Accident Investigation Board Norway AIBN. 2013. Report on derailment near Nykirke station, the Vestfold line, on 15 February 2012, train 12926. Investigation report JB 2013/02. PDF document. Available at: https://www.aibn.no/Railway/Reports/2013-02-eng [Accessed 27 April 2020].

Ailisto, H., Heikkilä, E., Helaakoski, H., Neuvonen, A., & Seppälä, T. 2018. Tekoälyn kokonaiskuva ja osaamiskartoitus. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 46/2018. Valtioneuvoston kanslia. PDF document. Available at: http://urn.fi/URN:ISBN:978-952-287-549-5 [Accessed 22 May 2020].

Aviation Accidents. No date. Accident reports. WWW document. Available at: http://www.aviation-accidents.net/?s=situation+awareness [Accessed 22 November 2019].

Baylon, C., Brunt, R. & Livingstone, D. 2015. Cyber Security at Civil Nuclear Facilities - Understanding the Risks. Chatham House Report September 2015. Chatham House, the Royal Institute of International Affairs. PDF document. Available at: https://www.chathamhouse.org/sites/default/files/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstoneUpdate.pdf [Accessed 11 May 2020].

Benyon, D. 2011. Designing Interactive Systems: A comprehensive guide to HCI and interaction design. Pearson Education Limited 2nd edition 2011. Book.

Biesecker, C. 2017. Boeing 757 Testing Shows Airplanes Vulnerable to Hacking, DHS Says. Avionics International. Aviation Today. Article 8 November 2017. Available at : https://www.aviationtoday.com/2017/11/08/boeing-757-testing-shows-airplanes-vulnerable-hacking-dhs-says/ [Accessed 5 May 2020].

Blasch, E. 2012. High-Level Information Fusion Management and Systems Design PDF document. Available at: https://www.cs.utah.edu/~tch/notes/BRECCIA/refs/Fusion15-HLIF_Tutorial_Lesson01_Intro_HLIF_CD.pdf [Accessed 19 March 2020].

Blasch, E., Kadar, I., Salerno, J., Kokar, M. M., Das, S., Powell, G. M., Corkill, D. D. & Ruspini, E. H. 2006. Issues and Challenges in Situation Assessment (Level 2 Fusion). PDF document. *Journal of Advances in Information Fusion*, Vol 1, 2 December 2006. Available at: https://www.academia.edu/8939577/Issues_and_Challenges_in_Situation_Assessment_Level_2_Fusion_ [Accessed 19 March 2020].

Blyth, A. 2018. SCADA and Other Dangerous Things. Open Web Application Security Project OWASP. Presentation 26 April 2018. PDF document. Available at: https://owasp.org/www-chapter-london/assets/slides/OWASPLondon-SCADA-Forensics-Prof-Andrew-Blyth-20180426-PDF.pdf [Accessed 8 May 2020].

Charitoudi, K. & Blyth, A. 2012. A Socio-Technical Approach to Cyber Risk Management and Impact Assessment. *Journal of Information Security*, 2013, 4, 33-41, published Online January 2013 in http://www.scirp.org/journal/jis. PDF document. Available at: http://dx.doi.org/10.4236/jis.2013.41005 [Accessed 8 13 March 2020].

Cohen, Z. 2018. Missile threat alert for Hawaii a false alarm; officials blame employee who pushed 'wrong button'. CNN Article 14 January 2018. WWW document. Available at: https://edition.cnn.com/2018/01/13/politics/hawaii-missile-threat-false-alarm/index.html [Accessed 22 March 2020].

Cooper, P. 2017. Aviation Cybersecurity - Finding Lift, Minimizing Drag. Atlantic Council. Brent Scowcroft Center on International Security November 2017. PDF document. Available at : https://www.atlanticcouncil.org/wp-content/uploads/2017/11/Aviation_Cybersecurity_web_1107.pdf [Accessed 4 May 2020].

Crane, T. & French, C. 2017. The Problem of Perception. The Stanford Encyclopedia of Philosophy. WWW document. Available at: https://plato.stanford.edu/archives/spr2017/entries/perception-problem [Accessed 4 March 2020].

Dainton, B. 2017. Temporal Consciousness. The Stanford Encyclopedia of Philosophy. Edition by Zalta, E. N. Winter 2018. WWW document. Available at: https://plato.stanford.edu/entries/consciousness-temporal/#BerHusRusBro [Accessed 14 April 2020].

Digirail. 2020. Article 2.4.2020. WWW document. Available at: https://digirata.fi/kohti-digitaalista-ja-alykasta-rautatieliikennetta/ [Accessed 19 May 2020].

Disso, J. P. 2016. Building a resilient ICS. Open Web Application Security Project OWASP. Presentation 12 May 2016. PDF document. Available at: https://owasp.org/www-chapter-cambridge/presentations/prev/Building_a_resilient_ICS.pdf [Accessed 8 May 2020].

ECRI Institute. 2013. Clinical Alarms. Healthcare Risk, Quality, & Safety Guidance – Guidance, 23 December 2013. WWW document. Available at:

https://www.ecri.org/components/HRC/Pages/CritCare5.aspx?tab=2 [Accessed 22 November 2019].

ECRI Institute. 2018. 2019 Top 10 Health Technology Hazards. Executive Brief, A Report from Health Devices. PDF document. Available at: https://www.ecri.org/Resources/Whitepapers_and_reports/Haz_19.pdf [Accessed 22 November 2019].

Emerson 2019. Advanced Alarming Techniques. White Paper October 2019. PDF document. Available at: https://www.emerson.com/documents/automation/white-paper-advanced-alarming-techniques-deltav-en-6116368.pdf [Accessed 18 May 2020].

Endsley, M. R. 1996. Automation and Situation Awareness. PDF document. Available at: http://www.aerohabitat.eu/uploads/media/Automation_and_Situation_Awareness_-_Endsley.pdf [Accessed 9 February 2020].

Endsley, M. R. 1999. Situation Awareness and Human Error: Designing to Support Human Performance. PDF document. Available at: https://www.researchgate.net/publication/252848339_Situation_Awareness_and_Human_Error_Designing_to_Support_Human_Performance [Accessed 2 February 2020].

Endsley, M. R., 2000. Theoretical underpinnings of Situation Awareness: A critical review. In Endsley, M. R. & Garland D., J. (Eds.): Situation Awareness Analysis and Measurement. PDF document. Available at: https://www.researchgate.net/publication/230745477_Theoretical_underpinnings_of_situation_awareness_A_critical_review [Accessed 15 February 2020].

Estonian Safety Investigation Bureau ESIB. 2019. Accident, loss of control with Airbus A320-214 near Tallinn Airport on 28.02.2018. Safety Investigations. Investigation report ESIB: A2802118 EECAIRS: EE0180. PDF document. Available at: https://turvallisuustutkinta.fi/material/attachments/otkes/tutkintaselostukset/rHuiLIZhp/ee0180_es_san_investigation_report_0.pdf [Accessed 8 May 2020].

European Centre for Cybersecurity in Aviation ECCSA. 2020. WWW document. Available at: https://www.easa.europa.eu/eccsa [Accessed 11 May 2020].

Europol. 2019. Internet Organized Crime Threat Assessment 2019. IOCTA Report 2019 published by European Union Agency for Law Enforcement Cooperation and European Cybercrime Centre. PDF document. Available at: https://www.europol.europa.eu/iocta-report [Accessed 2 May 2020].

Europol. 2020. Cybercrime. WWW document. Available at: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime [Accessed 2 May 2020].

Everaert-Desmedt, N. 2013. Peirce's Semiotics. WWW document. Available at: http://www.signosemio.com/peirce/semiotics.asp [Accessed 11 January 2020].

Fachot, M. 2018. Protecting railway networks from cyber threats. IEC e-tech news. Article February 2018. WWW document. Available at: https://iecetech.org/index.php/Technology-Focus/2018-02/Protecting-railway-networks-from-cyber-threats [Accessed: 19 May 2020].

Federal Aviation Administration. 2010. Advisory Circular AC No: 25.1322-1 13 December 2010. PDF document. Available at: https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_25.1322-1.pdf [Accessed 22 May 2020].

Federal Aviation Administration. 2020. Aviation Safety Information Analysis and Sharing (ASIAS). World Aircraft Accident Summary (WAAS) Subset Business Rules. WAAS Subset System Information Business Rules. WWW document. Available at: https://www.asias.faa.gov/apex/f?p=100:45:::NO::P45_REGION_VAR:2 [Accessed 13 February 2020].

Fernandez, F., Sanchez, A., Velez, J. F. & Moreno, B. 2017. A Cognitive Architecture Framework for Critical Situation Awareness Systems. IWINAC 2017, Part I, LNCS 10337, pp. 53–62, 2017. DOI: 10.1007/978-3-319-59740-9 6. PDF document. Available at: https://publik.tuwien.ac.at/files/publik_266621.pdf [Accessed 10 November 2019].

Fialkowki, C. 2012. Using alarm suppression. Effective alarm systems improve operations. Automation IT publication March/April 2012. WWW document. Available at: https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/2012/april/automation-it-using-alarm-suppression1/ [Accessed 18 May 2020].

Finnish Institute for Health and Welfare. 2019. Sote-digitalisaatiota kuvaavat indikaattorit tietokantaraportteina. Database reports. WWW document. Available at: https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/mita-tiedonhallinta-on-/sote-digitalisaation-seuranta/sote-digitalisaatiota-kuvaavat-indikaattorit-tietokantaraportteina [Accessed 3 May 2020].

Finnish Maritime Administration. 2007. Alusonnettomuusanalyysi 2001–2005. Merenkulkulaitoksen julkaisuja 5/2007. PDF document. Available at: https://julkaisut.vayla.fi/pdf5/mkl_2007-5_alusonnettomuusanalyysi.pdf [Accessed 12 May 2020].

Finnish Transport Agency. 2014. Turvallisuuspoikkeamatiedon keruu vuonna 2013. PDF document. Available at: https://julkaisut.vayla.fi/pdf8/lr_2014_turvallisuuspoikkeamatiedon_keruu_2013_web.pdf [Accessed 8 April 2020].

Finnish Transport Infrastructure Agency. 2014. Turvallisuuspoikkeamatiedon keruu, Liikenneviraston rautatietoimintojen turvallisuuspoikkeamat. Vuosikatsaus 2013 5.5.2014. Liikennevirasto. PDF document. Available at:

https://julkaisut.vayla.fi/pdf8/turvallisuuspoikkeamat_rata_2013.pdf [Accessed 11 May 2020].

Finnish Transport Infrastructure Agency. 2019a. Rautatietoimintojen turvallisuuspoikkeamat 2017. Väyläviraston julkaisuja 4/2019. PDF document. Available at: https://julkaisut.vayla.fi/pdf12/vj_2019-04_rautatietoimintojen_2017_web.pdf [Accessed 11 May 2020].

Finnish Transport Infrastructure Agency. 2019b. Rautatietoimintojen turvallisuuspoikkeamat 2018. Väyläviraston julkaisuja 24/2019. PDF document. Available at: https://julkaisut.vayla.fi/pdf12/vj_2019-24_rautatietoimintojen_2018_web.pdf [Accessed 19 May 2020].

Flynn, L. 2018. Rapid Construction of Accurate Automatic Alert Handling. Poster October 2018. Carnegie Mellon University. PDF document. Available at: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=528985 [Accessed 8 May 2020].

Francis, R. 2017. False positives still cause threat alert fatigue. CSO. Article 3 May 2017. WWW document. Available at: https://www.csoonline.com/article/3191379/false-positives-still-cause-alert-fatigue.html [Accessed 13 February 2020].

Franssila, H., Okkonen, J. & Savolainen, R. 2014. Tietotyön informaatioergonomian arviointi- ja kehittämismenetelmä. Tampereen yliopisto, Informaatiotieteiden yksikkö. TRIM. WWW document. Available at: https://trepo.tuni.fi/bitstream/handle/10024/96397/tietotyon_informaatioergonomian_2014.pdf?sequence=1 [Accessed 2 December 2019]

Gaba, D. M., Lau, N. & Desaulniers, D. 2013. Human Factors and Human Reliability in Healthcare and Nuclear Power. Risk and Reliability in Healthcare and Nuclear Power, AAMI. PDF document. Available at: https://www.nrc.gov/docs/ML1301/ML13017A267.pdf [Accessed 24 November 2019].

General Finnish Ontology (Yleinen suomalainen ontologia) YSO. 2020. Situation picture (tilannekuva). WWW document. Available at: https://finto.fi/yso/fi/page/p25187 [Accessed 4 March 2020].

Giraldo, J., Urbina, D., Cardenas, A., Valente, J., Faisal, M., Ruths, J., Tippenhauer, N. O., Sandberg, H. & Candell, R. 2018. A Survey of Physics-Based Attack Detection in Cyber-Physical Systems. ACM Computing Surveys, Vol. 51, No. 4, Article 76. Publication date July 2018. Available at: https://doi.org/10.1145/3203245 [Accessed 3 February 2020].

Gorkowienko, A. 2018. Securing oil and gas production systems from cyber-attack. Open Web Application Security Project OWASP. Presentation. PDF document. Available at: https://owasp.org/www-chapter-cambridge/presentations/prev/A.Gorkowienko-

Securing_Oil_and_Gas_Systems_From_Cyber-attack_v1.1.pdf [Accessed 8 May 2020].

Goward, D. 2017. Mass GPS Spoofing Attack in Black Sea. The Maritime Executive. Article 7 November 2017. WWW document. Available at: https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea [Accessed 3 May 2020].

Haavisto, M-L. 2006. Kognitiivinen ergonomia lisää työn sujuvuutta ja turvallisuutta. Terveysportti. Article ttl00351 (000.351). Suomen Työterveyslääkäriyhdistys r.y. 2020. WWW document. Available at: https://www.terveysportti.fi/dtk/shk/avaa?p_artikkeli=ttl00351 [Accessed 15 February 2020].

HaiPro. 2015. Potilasturvallisuusilmoituksen käsittely. Ohje potilasturvallisuusilmoituksen käsittelijälle 30 September 2015. PDF document. Available at: http://www.haipro.fi/ohjeet/haipro_kasittelijan_ohje.pdf [Accessed 10 May 2020].

Hallowell, E. 2004. Overloaded Circuits. Why Smart People Underperform. Harvard Business Review Article. PDF document. Available at: https://portal.addca.com/files/library/Hallowell_ADT_HBR_article_01.05.pdf [Accessed 3 December 2019].

Helsinki University Hospital HUS. 2015. Helsingin ja Uudenmaan sairaanhoitopiirin potilasturvallisuusraportti 2014. Helsingin ja Uudenmaan sairaanhoitopiiri. PDF document. Available at: https://www.hus.fi/potilaalle/Documents/HUS_potilasturvallisuusraportti_2014_18%205%202015_hallitukseen.pdf [Accessed 3 May 2020].

HFACS Inc. 2014. The HFACS Framework. WWW document. Available at: https://hfacs.com/hfacs-framework.html [Accessed 22 April 2020].

Homeland Security News Wire. 2015. Strengthening U.S. cybersecurity capabilities by bolstering cyber defense, deterrence. Article published 2 October 2015. WWW document. Available at: http://www.homelandsecuritynewswire.com/dr20151002-strengthening-u-s-cybersecurity-capabilities-by-bolstering-cyber-defense-deterrence [Accessed 21 March 2020].

Human Factors Methods. No date. Situational Awareness Analysis. WWW document. Available at: http://hfmethods.weebly.com/situational-awareness-analysis.html [Accessed 3 May 2020].

Huovila, H., Korpi, J., Kortström, J., Kotovirta, V., Molarius, R., Nissilä, M., Mikkonen, P., Mäntyniemi, P., Rauhala, J., Tourula, T., Wessberg, N. & Yliaho, J. 2010. Uhkatilanteiden hallinta. Hälytys-, tilannekuva- ja varoitusjärjestelmän kehittäminen. VTT tiedotteita 2543. PDF document. Available at: https://cris.vtt.fi/en/publications/managing-the-emergencies-developing-an-alarm-common-operational-p [Accessed 12 December 2019].

InfoSec Institute. 2014. Cyber Threats against the Aviation Industry. Article 8.4.2014. WWW document. Available at : https://resources.infosecinstitute.com/cyber-threats-aviation-industry/ [Accessed 18 May 2020].

International Maritime Organization IMO. 2020. Maritime cyber risk. WWW document. Available at: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx [Accessed 12 May 2020].

Iowa State University of Science and Technology, Center for Excellence in Learning and Teaching. No date. Revised Bloom's Taxonomy. WWW document. Available at: https://www.celt.iastate.edu/teaching/effective-teaching-practices/revised-blooms-taxonomy/ [Accessed 29 January 2020].

Joint Commission. 2013. Medical device alarm safety in hospitals. Sentinel Event Alert, Issue 50, 8 April 2013. WWW document. Available at: https://www.jointcommission.org/resources/patient-safety-topics/sentinel-event/sentinel-event-alert-newsletters/sentinel-event-alert-issue-50-medical-device-alarm-safety-in-hospitals/ [Accessed 8 January 2020].

Kalakoski, V. 2016. Cognitive ergonomics. Finnish Institute of Occupational Health. WWW document. Available at: https://oshwiki.eu/wiki/Cognitive_ergonomics [Accessed 10 November 2019].

Kane-Gill, S. L., O'Connor, M. F., Rothschild, J. M., Selby, N. M., McLean, B., Bonafide, C. P., Cvach, M. M., Hu, X., Konkani, A., Pelter, M. M., & Winters, B. D. 2017. Technologic Distractions (Part 1): Summary of Approaches to Manage Alert Quantity With Intent to Reduce Alert Fatigue and Suggestions for Alert Fatigue Metrics. The Society of Critical Care Medicine and Wolters Kluwer Health, Inc. *Critical Care Medicine*. DOI: 10.1097/CCM.0000000000002580. WWW document. Available at: https://www.scopus.com/record/display.uri?eid=2-s2.0-85021972547&origin=inward&txGid=88c8cc4feffea84996d65992eee40227 [Accessed 14 April 2020].

Kari, M. 2018. Tiedustelun epäonnistuminen. Lecture at Jyväskylä University 30 October 2018.

Khandelwal, S. 2015. Hackers Could Crash Trains by Hacking Rail Traffic System. *The Hacker News* 24 April 2015. WWW document. Available at: https://thehackernews.com/2015/04/hacking-train-crash.html [Accessed 19 May 2020].

Khandelwal, S. 2018. Flaw in Emergency Alert Systems Could Allow Hackers to Trigger False Alarms. The Hacker News 10 April 2018. WWW document. Available at: https://thehackernews.com/2018/04/hacking-emergency-alert-sirens.html [Accessed 27 April 2020].

Koho, S. 2018. Hypitkö tehtävästä toiseen ilman taukoja? Aivotutkijat: Jatkuva kiire voi aiheuttaa ADT:n. *Uusi Suomi* 15 August 2018. WWW document. Available at: https://www.uusisuomi.fi/uutiset/hypitko-tehtavasta-toiseen-ilman-

taukoja-aivotutkijat-jatkuva-kiire-voi-aiheuttaa-adtn/d8eb8d19-d51a-3993-95f2-2629212ce0ef [Accessed 3 December 2019].

Koistinen, M. 2011. Tilannetietoisuus ja tilannekuva operatiivisessa liikenteenhallinnassa. Liikenneviraston tutkimuksia ja selvityksiä 54/2011. Liikennevirasto. PDF document. Available at: https://julkaisut.vayla.fi/pdf3/lts_2011-54_tilannetietoisuus_ja_tilannekuva_web.pdf [Accessed 13 May 2020].

Koponen, J., Hildén, J. & Vapaasalo, T. 2016. Tieto näkyväksi Informaatiomuotoilun perusteet. Aalto-yliopisto, Taiteiden ja suunnittelun korkeakoulu. Aalto-yliopiston julkaisusarja 1/2016. Book.

Koppa. 2009; 2010; 2015; 2018. Menetelmäpolku. Jyväskylän yliopisto, Digipalvelut, Korppi, Avoimen yliopiston Koppa. 28 April 2009, 25 February 2010 10 April 2015, 23 April 2015 and 29 January 2018. WWW document. Available at: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku [Accessed 3 December 2019].

Koskinen-Kannisto, A. 2013. Situational awareness concept in a multinational collaboration environment - Challenges in the information sharing framework. Department of Military Technology, National Defense University. Doctoral dissertation 20 April 2014. PDF document. Available at: http://urn.fi/URN:ISBN:978-951-25-2452-5 [Accessed 3 April 2020].

Kotkansalo, A., Parkkila, L. & Tarvainen, J. 2017. Riskianalyysimenetelmien tarkastelu. Lapin AMK:n julkaisuja. Sarja B. Tutkimusraportit ja kokoomateokset 23/2017. Kirjallisuusselvitys. WWW document. Available at: https://www.lapinamk.fi/loader.aspx?id=14f882d8-7843-42f6-bff1-48b9507169c6 [Accessed 14 March 2020].

Kumar, M. 2019. Hackers Target Indian Nuclear Power Plant – Everything We Know So Far. The Hacker News. Article 30 October 2019. WWW document. Available at: https://thehackernews.com/2019/10/nuclear-power-plant-cyberattack.html [Accessed 11 May 2020].

Kuusisto, T. 2014. Kybertaistelu 2020. Maanpuolustuskorkeakoulu, Taktiikan laitos, Operaatiotaito ja taktiikka. PDF document. Available at: http://urn.fi/URN:ISBN:978-951-25-2618-5 [Accessed 3 May 2020].

Lal, R. 2013. Evolution of User Interface. Digital Web & Design Innovation Summit SFO 20 September 2013. WWW document. Available at: https://www.slideshare.net/rajeshlal/evolution-of-user-interface-26414802 [Accessed 20 November 2019].

Lehto, M. 2019. Kybermaailman ilmiöitä ja määrittelyjä. Jyväskylän yliopisto, Informaatioteknologian tiedekunnan julkaisu 26 April 2019, v10.0, 13. PDF document. Available at: https://www.jyu.fi/it/fi/hae-opiskelemaan/hakukohteet/kyberturvallisuuden-seka-turvallisuus-ja-strateginen-

analyysi-maisteriohjelmien-yhteisvalinta/kybermaailma_v10-0.pdf [Accessed 12 September 2019].

Leisti, T. 2019. GPS-häirintä ulottui Lappiin Naton sotaharjoituksen aikana – häirinnästä on epäilty Venäjää. Yle News 9 and 13 November 2019. Available at: https://yle.fi/uutiset/3-10498891 [Accessed 3 December 2019].

Leveson, N. G. & Thomas, J. P. 2018. STPA handbook March 2018. PDF document. Available at: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf [Accessed 22 April 2020].

Library of Congress. 2020. Situational awareness. WWW document. Available at: http://id.loc.gov/authorities/subjects/sh2007007736.html [Accessed 4 March 2020].

Liu, Y., Ning, P. & Reiter, M. K. 2011. False Data Injection Attacks against State Estimation in Electric Power Grids. ACM Transactions on Information and System Security, Vol. 14, No. 1, Article 13, Publication date: May 2011. PDF document. Available at: DOI = 10.1145/1952982.1952995 http://doi.acm.org/10.1145/1952982.1952995 [Accessed 13 February 2020].

Llinas, J., Bowman, C., Rogova, G., Steinberg, A., Waltz, E. & White, F. 2004. Revisiting the JDL Data Fusion Model II. US Navy SPAWAR Systems Center, Program Development. July 2004. PDF document. Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a525721.pdf [Accessed 20 March 2020].

Lähdeniemi, N. 2013. Cognitive ergonomics of knowledge work and the methods of ‘new ways of working’. Tampere University of Technology, Master’s Degree Programme in Information and Knowledge Management, Master of Science Thesis. PDF document. Available at: https://core.ac.uk/display/196554724?recSetID= [Accessed 9 January 2020].

Magee, T. 2018. Can you hack a ship? Global maritime industry ripe for hacking. Techworld. Article 3 April 2018. WWW document. Available at: https://www.techworld.com/security/can-you-hack-ship-global-maritime-industry-ripe-for-hacking-3674517/ [Accessed 5 May 2020].

MITRE. 2020. CWE Common Weakness Enumeration. A Community-Developed List of Software & Hardware Weakness Types. CWE List Version 4.0 20 February 2020. WWW document. Available at: https://cwe.mitre.org/data/index.html [Accessed 14 May 2020].

MNE7. 2013. Access to the Global Commons, Outcome 3 Cyber Domain Objective 3.5, Cyber Situational Awareness Concept of Employment for Cyber Situational Awareness, Within the Global Commons, Version 1.0 Dated 25 Feb 2013. PDF document. Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a587471.pdf [Accessed 20 May 2020].

Mo, Y. & Sinopoli, B. 2010. False Data Injection Attacks in Control Systems. PDF document. Available at: https://ptolemy.berkeley.edu/projects/truststc/conferences/10/CPSWeek/papers/scs1_paper_7.pdf [Accessed 11 February 2020].

Mujinga, M., Kroeze, J. H. & Eloff, M. 2017. A socio-technical approach to information security. Conference paper August 2017. PDF document. Available at: https://www.researchgate.net/publication/320288245 [Accessed 14 April 2020].

Munro, K. 2018. Hacking, tracking, stealing and sinking ships. Blog. WWW document. Available at: https://www.pentestpartners.com/security-blog/hacking-tracking-stealing-and-sinking-ships/ [Accessed 16 May 2020].

Murdock, J. 2018. In-flight airplanes can now be hackes from the ground, cyber expert warns. *Newsweek*. Article 6 June 2018. WWW document. Available at: https://www.newsweek.com/flight-airplanes-can-now-be-hacked-ground-cyber-expert-warns-962420 [Accessed 5 May 2020].

Naderpour, M., Nazir S. & Lu, J. 2015. The role of situation awareness in accidents of large-scale technological systems. *Process Safety and Environmental Protection*, Volume 97, September 2015, Pages 13-24. PDF document. Available at: https://doi.org/10.1016/j.psep.2015.06.002 [Accessed 12 February 2020].

National Institute of Standards and Technology NIST. No date. Wireless Infusion Pump Security. WWW document. Available at: https://www.nist.gov/industry-impacts/wireless-infusion-pump-security [Accessed 11 January 2020]

National Institute of Standards and Technology NIST. 2018. Securing Wireless Infusion Pumps in Healthcare Delivery Organizations. WWW document. Available at: https://csrc.nist.gov/publications/detail/sp/1800-8/final [Accessed 11 January 2020].

National Institute of Standards and Technology NIST. 2020a. National Vulnerability Database. Search results. WWW document. Available at: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=false+alarm&search_type=all [Accessed 14 May 2020].

National Institute of Standards and Technology NIST. 2020b. National Vulnerability Database. Search results. WWW document. Available at: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=false+alert&search_type=all [Accessed 14 May 2020].

National Institute of Standards and Technology NIST. 2020c. Vulnerabilities. WWW document. Available at: https://nvd.nist.gov/vuln [Accessed 14 May 2020].

National Supervisory Authority for Welfare and Health (Valvira). No date. Vaaratilanneilmoitus. PDF document. Available at:

https://www.valvira.fi/documents/14444/42787/Vaaratilanneilmoitus.pdf [Accessed 9 January 2020].

National Transportation Safety Board NTSB. 2014. Aviation Accident Final Report published 19 February 2014. WWW document. Available at: https://app.ntsb.gov/pdfgenerator/ReportGeneratorFile.ashx?EventID=20120618X00755&AKey=1&RType=HTML&IType=LA [Accessed 29 March 2020].

National Transportation Safety Board NTSB. 2015. Controlled Flight Into Terrain in Visual Conditions. Safety Alert SA-013 January 2008, revised December 2015. PDF document. Available at: http://www.ntsb.gov/safety/safety-alerts/documents/SA_013.pdf [Accessed 29 March 2020].

Nielsen, J. 2001. Error message guidelines. 23 June 2001. WWW document. Available at: http://www.nngroup.com/articles/error-message-guidelines/ [Accessed 4 April 2020].

Nikkinen, T. 2018. Tilannetietoisuuden muodostaminen Helsinki-Vantaan lentoaseman poikkeustilanteissa. Laurea ammattikorkeakoulu, Turvallisuusalan koulutusohjelma. Opinnäytetyö. PDF document. Available at: https://www.theseus.fi/bitstream/handle/10024/156730/Nikkinen.Teemu.ONT.pdf?sequence=4&isAllowed=y [Accessed 23 16 April 2020].

Nyyssönen, T. 2019. Uudella teknologialla voidaan säästää ihmishenkiä suuronnettomuuksissa – Suomessa tekniikan käyttöönottoa jarruttaa byrokratia. Yle Uutiset 18 November 2019. WWW document. Available at: https://yle.fi/uutiset/3-11055008 [Accessed 20 November 2019].

OASIS. 2010. Common Alerting Protocol Version 1.2. OASIS Standard 1 July 2010. WWW document. Available at: http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.html [Accessed: 9 May 2020].

Onnettomuustutkintakeskus. 1997. Lentoturvallisuutta vaarantanut tapaus Kuopion lentoaseman lähestymisalueella 4.4.1997. Investigation report C8a/1997L. PDF document. Available at: https://turvallisuustutkinta.fi/material/attachments/otkes/tutkintaselostukset/fi/ilmailuonnettomuuksientutkinta/1997/c8a1997l_tutkintaselostus/c8a1997l_tutkintaselostus.pdf [Accessed 19 November 2019].

Onnettomuustutkintakeskus. 2000. Porrastuksen alitus Espoon yläpuolella 15.12.2000 Lentokoneiden häviäminen lennonjohdon tutkanäytöltä. Investigation report C 19/2000L. WWW document. Available at: https://turvallisuustutkinta.fi/material/attachments/otkes/tutkintaselostukset/fi/ilmailuonnettomuuksientutkinta/2000/c192000l_tutkintaselostus/c192000l_tutkintaselostus.pdf [Accessed 19 November 2019].

OPC Foundation. 2017. The Industrial Interoperability Standard. Unified Architecture. WWW document. Available at: https://opcfoundation.org/developer-tools/specifications-unified-architecture/part-9-alarms-and-conditions/ [Accessed 17 April 2020].

Open Web Application Security Project OWASP. 2015. Category: Principle. Modified 29 July 2015. WWW document. Available at: https://wiki.owasp.org/index.php/Category:Principle [Accessed 14 April 2020].

Open Web Application Security Project. 2017. OWASP Top Ten. WWW document. Available at: https://owasp.org/www-project-top-ten/ [Accessed 14 April 2020].

Oulu University Hospital. 2018. Laadunhallinta ja potilasturvallisuus. Pohjois-Pohjanmaan sairaanhoitopiiri. WWW document. Available at: https://www.ppshp.fi/Sairaanhoitopiiri/Toiminta-ja-talous/Tilastot/Pages/Laadunhallinta-ja-potilasturvallisuus.aspx [Accessed 10 May 2020].

Paganini, P. 2016. Modern railroad systems vulnerable to cyber attacks. Blog 2 January 2016. WWW document. Available at: https://securityaffairs.co/wordpress/43196/hacking/railroad-systems-vulnerabilities.html [Accessed 19 May 2020].

Perezgonzales, J. D. 2009. ICAO: fundamental human factors concepts. *Aeroscience*. ISSN 2324-4399, 2012, pages 4-7. AviationKnowledge edited 10 May 2013. WWW document. Available at: http://aviationknowledge.wikidot.com/aviation3:icao-hf1 [Accessed 14 April 2020].

Perry, M. J. 2010. SHELL Model Interface Errors. AviationKnowledge edited 22 August 2010. WWW document. Available at: http://aviationknowledge.wikidot.com/aviation:shell-model-interface-errors (2010) [Accessed 14 April 2020].

Perry, M. J. & Perezgonzales, J. D. 2010. SHELL model. AviationKnowledge edited 22 August 2010. WWW document. Available at: http://aviationknowledge.wikidot.com/aviation:shell-model [Accessed 14 April 2020].

Porup, J. M. 2019. Boeing's poor information security posture threatens passenger safety, national security, researcher says. CSO. Article 5 November 2019. WWW document. Available at: https://www.csoonline.com/article/3451585/boeings-poor-information-security-posture-threatens-passenger-safety-national-security-researcher-s.html [Accessed 15 May 2020].

Railway Technology. 2017. Digital railway: is it cyber secure? Analysis 23 March 2017. WWW document. Available at: https://www.railway-technology.com/features/featurea-digital-railway-is-it-cyber-secure-5770312/ [Accessed 19 May 2020].

Rider, D. 2018. Cyber Security at Sea: The Real Threats. The Maritime Executive 3 October 2018. WWW document. Available at: https://www.maritime-executive.com/blog/cyber-security-at-sea-the-real-threats [Accessed 8 May 2020].

Rügamer, A. & Kowalewski, D. 2015. Jamming and Spoofing of GNSS Signals – An Underestimated Risk?! *FIG Working Week* 2015 17-21 May 2015. PDF document. Available at: https://www.fig.net/resources/proceedings/fig_proceedings/fig2015/papers/ts05g/TS05G_ruegamer_kowalewski_7486.pdf [Accessed 3 December 2019].

Saaranen-Kauppinen, A. Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto. Yhteiskuntatieteellinen tietoarkisto. Tampere. WWW document. Available at: https://www.fsd.uta.fi/menetelmaopetus/ [Accessed 3 December 2019]

Safety Investigation Authority. 2004. Väsymyksen syyt ja yleisyys komentosiltatyöskentelyssä. Investigation report S3/2004M. PDF document. Available at: https://turvallisuustutkinta.fi/material/attachments/otkes/tutkintaselostukset/fi/vesilikenneonnettomuuksientutkinta/2004/s32004m_tutkintaselostus/s32004m_tutkintaselostus.pdf [Accessed 9 April 2020].

Safety Investigation Authority. 2013a. Vesilentokoneen onnettomuus Kuopion Vehmersalmella 29.6.2013. Investigation report L2013-04 published 14 February 2014. WWW document. Available at: https://turvallisuustutkinta.fi/fi/index/tutkintaselostukset/ilmailuonnettomuuksientutkinta/tutkintaselostuksetvuosittain/ilmailu2013/l2013-04lento-onnettomuusvehmersalmella29.6.2013.html [Accessed 15 March 2020].

Safety Investigation Authority. 2013b. Liikennelentokoneen ajautuminen ulos kiitotieltä laskukiidossa Helsinki-Vantaan lentoasemalla 19.8.2012. Investigation report L2012-08 15/2013. PDF document. Available at: https://turvallisuustutkinta.fi/material/attachments/otkes/tutkintaselostukset/fi/ilmailuonnettomuuksientutkinta/2012/5k7GtSaRD/Tutkintaselostus.pdf [Accessed 13 March 2020].

Safety Investigation Authority. 2016. Theme Investigation on wrong routings in train traffic in 2015. Investigation report R2015-S1 published 8 July 2016. WWW document. Available at : https://turvallisuustutkinta.fi/fi/index/tutkintaselostukset/raideliikenneonnettomuuksientutkinta/tutkintaselostuksetvuosittain/2015/r2015-s1teematutkintavuoden2015junaliikenteenvirheellisistakulkuteista.html [Accessed 4 May 2020].

Safety Investigation Authority. 2018a. Vakavat vaaratilanteet Helsinki-Vantaan lentoasemalla 23.1.2018 ja 24.1.2018. Investigation report L2018-02 04/2018. PDF document. Available at: https://turvallisuustutkinta.fi/material/attachments/otkes/tutkintaselostukset/fi/ilmailuonnettomuuksientutkinta/2018/4p8d1hKAb/L2018-02_Helsinki-Vantaa_TUTKINTASELOSTUS.pdf [Accessed 15 March 2020].

Safety Investigation Authority. 2018b. Uniform reporting and classification of deviations Recommendation 2016-S12 published 1 February 2018, updated 30 August 2019. WWW document. Available at:

https://turvallisuustutkinta.fi/fi/index/turvallisuussuositukset/suositukset/1517505611634.html [Accessed 20 April 2020].

Santos, J. C. S., Tarrit, K. & Mirakhorli, M. 2017. Common Architectural Weakness Enumeration (CAWE). A Catalog of Security Architecture Weaknesses. In 2017 IEEE International Conference on Software Architecture (ICSA). IEEE. PDF document. Available at: http://design.se.rit.edu/catalog/ [Accessed 14 April 2020].

Schulz, C. M., Krautheim, V., Hackemann, A., Kreuzer, M., Kochs, E. F. & Wagner, K. J. 2016. Situation awareness errors in anesthesia and critical care in 200 cases of a critical incident reporting system. *BMC Anesthesiology.* Article published 17 January 2016. WWW document. Availabe at: https://dx.doi.org/10.1186%2Fs12871-016-0172-7 [Accessed 17 May 2020].

Siwicki, B. (2018). Cybercriminals turning to smaller providers and health IoT in 2018. Healthcare IT News 5 January 2018. WWW document. Available at: https://www.healthcareitnews.com/news/cybercriminals-turning-smaller-providers-and-health-iot-2018 [Accessed 7 April 2020].

SKYbrary. 2018. Controller Position Design. Edited on 9 February 2018. WWW document. Available at: https://www.skybrary.aero/index.php/Controller_Position_Design [Accessed 12 January 2020].

SKYbrary. 2017. Electronic Centralized Aircraft Monitor (ECAM). WWW document. Available at: https://www.skybrary.aero/index.php/Electronic_Centralized_Aircraft_Monitor_(ECAM) [Accessed 7 May 2020].

SKYbrary. 2019. Human Factors Analysis and Classification System HFACS. Edited 31 July 2019. WWW document. Available at: https://www.skybrary.aero/index.php/Human_Factors_Analysis_and_Classification_System_(HFACS) [Accessed 2 May 2020].

SKYbrary. 2020. Situational awareness. WWW document. Available at: https://www.skybrary.aero/index.php/Situational_Awareness [Accessed 4 March 2020].

Sobczak, B. & Behr, P. 2017. Nuclear breach opens new chapter in cyber struggle. E&E News, Energywire. Article 27 June 2017. WWW document. Available at: https://www.eenews.net/stories/1060056628 [Accessed 11 May 2020].

Software Engineering Institute SEI. 2020. The CERT Division. WWW document. Available at: https://www.sei.cmu.edu/about/divisions/cert/index.cfm#cert-division-what-we-do [Accessed 13 May 2020].

Steinberg, A. N., Bowman, C. L. & White, F. E. 1999. Revisions to the JDL Data Fusion Model. *Sensor Fusion*, Architectures, Algorithms, and Applications,

Proceedings of the SPIE, Vol. 3719 1999. PDF document. Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a391479.pdf [Accessed 20 March 2020].

STT. 2019. ADT on nykymaailman ongelma – tekee ihmisistä ylikuormittuneita ja levottomia. *ESS News* article 26 October 2019. WWW document. Available at: https://www.ess.fi/uutiset/kotimaa/art2577394 [Accessed 3 December 2019].

The Helsinki Term Bank for the Arts and Sciences. 2016. Hermeneutiikka. WWW document. Available at: https://tieteentermipankki.fi/wiki/Filosofia:hermeneutiikka [Accessed 12 January 2020].

The International Air Transport Association IATA. 2015. Introduction to Cyber Security Threats. Aviation Cyber Security Toolkit. 2nd edition July 2015. PDF document. Available at: https://www.iata.org/contentassets/2b86abad14734d1f8ae6433a4ba68162/toc-acst-02-ed-intro-threats-20150709.pdf [Accessed 18 May 2020].

The International Civil Aviation Organization ICAO. 2019. Aviation Cybersecurity Strategy. Security and Facilitation Strategic Objective October 2019. PDF document. Available at: https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf [Accessed 18 May 2020].

The Ministry of Transport and Communications. 2020. Towards digital and intelligent rail transport - Final report of the Digi Rail study. Liikenne- ja viestintäministeriön julkaisuja 2020:6. PDF document. Available at: http://urn.fi/URN:ISBN:978-952-243-589-7 [Accessed 19 May 2020].

Timonen, T. 2013. Funktionaalinen analyysi - Lähtökohdat ja perusteet kliinisessä psykologiassa ja kognitiivisessa käyttäytymisterapiassa. PDF document. Available at: http://users.jyu.fi/~teentimo/eteva/analyysiIV.pdf [Accessed 29 January 2020].

Tscholl, D. W., Rössler J., Said, S., Kaserer, A., Spahn, D. R. & Nöthiger, C. B. 2020. Situation Awareness-Oriented Patient Monitoring with Visual Patient Technology: A Qualitative Review of the Primary Research. Institute of Anesthesiology, University and University Hospital Zurich. *Sensors 2020*, 20(7) 2112 published 9 April 2020. WWW document. Available at: https://dx.doi.org/10.3390%2Fs20072112 [Accessed 17 May 2020].

Toxi Triage. 2019. Project. WWW document. Available at: http://www.toxi-triage.eu/ [Accessed 19 November 2019].

U.S. Food and Drug Administration FDA. 2020. MAUDE database. WWW document. Available at: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/search.cfm [Accessed 11 January 2020].

U.S. Nuclear Regulatory Commission. 2012. Human-System Interface Design Review Guidelines. NUREG-0700, Revision 3. PDF document. Available at:

https://www.nrc.gov/docs/ML1815/ML18158A333.pdf [Accessed 21 February 2020].

Vocabulary Center TSK ry. 2018. Kyberturvallisuuden sanasto. Sanastokeskus TSK ry. Security Committee (Turvallisuuskomitea). PDF document. Available at: https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/ [Accessed 19 November 2019].

West P., Abbott, P. & Probst, P. 2014. Alarm Fatigue: A Concept Analysis. *OJNI* Volume 18, Number 2 1 June 2014. WWW document. Available at: https://www.himss.org/alarm-fatigue-concept-analysis [Accessed 19 November 2019].

Wikipedia. 2020a. False positives and false negatives. WWW document. Available at: https://en.wikipedia.org/wiki/False_positives_and_false_negatives [Accessed 11.4.2020].

Wikipedia. 2020b. False alarm. WWW document. Available at: https://en.wikipedia.org/wiki/False_alarm#Signal_detection_theory [Accessed 11.5.2020].

Zetter, K. 2012. Hackers Breached Railway Network, Disrupted Service. Wired. Article 24 January 2012. WWW document. Available at: https://www.wired.com/2012/01/railyway-hack/ [Accessed 19 May 2020].

Zhao, J., Mili, L. & Wang, M. 2018. A Generalized False Data Injection Attacks Against Power System Nonlinear State Estimator and Countermeasures. IEEE Transactions on Power Systems, Vol. 33, no 5, September 2018. DOI 10.1109/TPWRS.2018.2794468. PDF document. Available at: https://ieeexplore.ieee.org/document/8260948 [Accessed 18 March 2020].

Zlatkus. A. 2019.Design Guide: Alerts. 3 June 2019. WWW document. Available at: https://medium.com/swlh/design-guide-alerts-f563fa139853 [Accessed 4 April 2020].

Yeh, M., Swider, C. Jin Jo, Y. & Donovan, C. 2016. Human Factors Considerations in the Design and Evaluation of Flight Deck Displays and Controls. Federal Aviation Administration, Final Report December 2016, Version 2.0. PDF document. Available at: https://www.volpe.dot.gov/sites/volpe.dot.gov/files/docs/Human_Factors_Considerations_in_the_Design_and_Evaluation_of_Flight_Deck_Displays_and_Controls_V2.pdf [Accessed 19 November 2019].

LIST OF FIGURES AND TABLES

APPENDICES

Appendix 1 Chain of events