VTT TECHNOLOGY 412 Autonomous mobile machines in mines...

VTT

Autonomous mobile machines in mines using 5G enabled operational safety principles

Timo Malm | Daniel Pakkala | Eetu Heikkilä

VTT TECHNOLOGY 412

VTT TECHNOLOGY 412

Autonomous mobile machines in mines using 5G enabled operational safety principles

Timo Malm, Daniel Pakkala & Eetu Heikkilä

VTT

ISBN 978-951-38-8774-2

VTT Technology 412

ISSN-L 2242-1211
ISSN 2242-122X (Online)
DOI: 10.32040/2242-122X.2023.T412

JULKAISIJA – PUBLISHER

VTT
PL 1000
02044 VTT
Puh. 020 722 111
https://www.vtt.fi

VTT
P.O. Box 1000
FI-02044 VTT, Finland
Tel. +358 20 722 111
https://www.vttresearch.com

Cover image: Sandvik

Preface

This research has been conducted as a part of the Next Generation Mining (NGMining) project, which is mainly funded by Business Finland. The companies and research institutes at the project are: Nokia, Sandvik, Etteplan, Iiwari, Terrasolid, Outsight, Wizense, Unikie, Indagon, Millisecond, Noptel, Satel, Huld, Epec, Oulu University and VTT. The working group writing this report is Timo Malm, Daniel Pakkala, Eetu Heikkilä, Jere Backman and Pekka Pääkkönen. Information and ideas to the report are collected also from discussions with Sandvik: Jussi Puura, Jussi Ahola, Ari Konttinen and Pasi Julkunen; Satel: Petri Hyvärinen; Epec: Jyrki Sauramäki; Nokia: Seppo Hämäläinen, Eero Paukkonen and Oscar Lindfors.

Contents

Executive Summary

Industrial 5G technology is expected to increase the efficiency and safety of mining operations by improving situational awareness and increasing the level of autonomy of mining machinery. The main contributions of 5G in mining are related to the reliable, fast, and low-latency communications. This deliverable provides functional safety aspects within the NGMining project.

Functional safety is here part of the overall safety relating to the machine and its control system that depends on the correct functioning of the safety-related systems. Safety-related systems have safety functions, which guarantee the safe operation and, by definition, whose failure can result in an immediate increase of the risk(s).

List of Figures

List of Tables

Acronyms and abbreviations

Asset (cybersecurity)	Physical or logical object owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization [IEC 62443-1-1].
Authenticity	Property that an entity is what it claims to be. [IEC 27000:2017]
Black channel	Defined communication system containing one or more elements without evidence of design or validation according to IEC 61508. Note 1 to entry: This definition expands the usual meaning of channel to include the system that contains the channel. [IEC 61784-3]
Category	Classification of the safety-related parts of a control system in respect of their resistance to faults and their subsequent behaviour in the fault condition, and which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability [ISO 13849-1]
Common cause failure, CCF	Failures of different items, resulting from a single event, where these failures are not consequences of each other [ISO 13849-1]
Conduit (cybersecurity)	Logical grouping of communication assets that protects the security of the channels it contains [IEC 62443-1-1]
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [IEC 27000:2017]
CRC	Cyclic Redundancy Check [IEC 61784-3]. Source of the message creates checksum (CRC), which is calculated from the message (based on the remainder of a polynomial division of their contents). The receiver recalculates the CRC and checks that the result is the same as received CRC. There are a lot of standardized CRCs having different lengths.
Cybersecurity	Actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets [IEC 62443-1-1]
Dangerous failure	Failure which has the potential to put the safety-related part of control system in a hazardous or fail-to-function state [ISO 13849-1]

DC	Diagnostic Coverage is measure of the effectiveness of diagnostics, which may be determined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures. Note 1 to entry: Diagnostic coverage can exist for the whole or parts of a safety-related system. For example, diagnostic coverage could exist for sensors and/or logic system and/or final elements. [ISO 13849-1]
Digital model	Digital model is pure virtual object used in simulations and planning, but it does not have physical connection to physical world
Digital shadow	Entity, where virtual entity reflects physical entity status
Digital twin	Virtual entity with 2-way connection to the corresponding physical entity
Diversity	Different means of performing a required function Note 1 to entry: Diversity may be achieved by different physical methods or different design approaches. [IEC 61784-3]
DT	Data and Telecommunication
Error	Discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition. Note 1 to entry: Errors may be due to design mistakes within hardware/software and/or corrupted information due to electromagnetic interference and/or other effects. Note 2 to entry: Errors do not necessarily result in a failure or a fault. [IEC 61784-3]
Failure	Termination of the ability of an item to perform a required function. Note 1 to entry: After a failure, the item has a fault. Note 2 to entry: “Failure” is an event, as distinguished from “fault”, which is a state. Note 3 to entry: The concept as defined does not apply to items consisting of software only. Note 4 to entry: Failures which only affect the availability of the process under control are outside of the scope of this part of ISO 13849. [ISO 13849-1]
Fault	Abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function. Note 1 to entry: IEC 60050-191:1990, 191-05-01 defines "fault" as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources. [IEC 61784-3]

Fieldbus	Communication system based on serial data transfer and used in industrial automation or process control applications. [IEC 61784-3]
Functional safety	Part of the overall safety relating to the EUC (Equipment under control) and the EUC control system that depends on the correct functioning of the E/E/PE (Electrical/Electronic/Programmable Electronic System) safety-related systems and other risk reduction measures. [IEC 61508-4]
Harm	Physical injury or damage to health [ISO 12100].
Hazard	Potential source of harm. Note 1 to entry: A hazard can be qualified in order to define its origin (e.g. mechanical hazard, electrical hazard) or the nature of the potential harm (e.g. electric shock hazard, cutting hazard, toxic hazard, fire hazard). [ISO 13849-1]
Integrity cybersecurity)	Condition of guarding against improper modification or destruction of information [CEN ISO/TR 22100-4:2020]
Message	(Information theory and communication theory) Ordered sequence of characters (usually octets) intended to convey information. [IEC 61784-3]
Mission	Hierarchical set of work tasks
MTTF_D	Mean Time To Dangerous Failure [ISO 13849-1]
PFH, (PFH_D)	Average frequency of dangerous failure (1/h) per hour. [IEC 61784-3]
Performance level (PL)	Discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions. PL a is the lowest level and PL e is the highest level. [ISO 13849-1]
Redundancy	Existence of more than one means for performing a required function or for representing information. [IEC 61784-3]
Risk	Combination of the probability of occurrence of harm and the severity of that harm. [ISO 13849-1]
Risk (cybersecurity)	Expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence [IEC 62443-1-1].
Risk assessment	Overall process comprising a risk analysis and a risk evaluation. [ISO 12100] Risk analysis: combination of the specification of the limits of the machine, hazard identification and risk estimation. [ISO 12100]

Risk assessment (cybersecurity)	Process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources, quantifies loss exposures and consequences based on probability of occurrence, and (optionally) recommends how to allocate resources to countermeasures to minimize total exposure. Types of resources include physical, logical and human. [IEC 62443-1-1]
Safety function	Function of the machine whose failure can result in an immediate increase of the risk(s) [ISO 13849-1]
Safety integrity	Probability of an SCS or its subsystem satisfactorily performing the required safety function under all stated conditions within a stated period of time. [IEC 62061]
Safety integrity level (SIL):	Discrete level (one out of a possible four) corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest. [IEC 61508-4]
Safety measure (communication)	Measure to control possible communication errors that is designed and implemented in compliance with the requirements of IEC 61508. Note 1 to entry: In practice, several safety measures are combined to achieve the required safety integrity level. [IEC 61784-3]
Security zone	Grouping of logical or physical assets that share common security requirements [IEC 62443-3-1].
Systematic failure	Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors [ISO 13849-1]
Threat (cybersecurity)	Any IT-security (cybersecurity) incident with the potential to adversely impact machinery operations [ISO/TR 22100-4: 2020] Potentially damaging action (intended or unintended) or capability (internal or external) to adversely impact through a vulnerability [IEC 62443-3-1]
Timeliness	The generic safety property timeliness requires the detection of the following communication errors according to: unacceptable delay, unintended repetition, incorrect sequence, loss. [IEC 61784-3]
Validation	Confirmation by examination (e.g. tests, analysis) that the safety-related control system (SCS) meets the functional safety requirements of the specific application [IEC 62061].

Verification	Confirmation by examination (e.g. tests, analysis) that the SCS, its subsystems or subsystem elements meet the requirements set by the relevant specification EXAMPLE: Verification activities include • reviews on outputs (documents from all phases) to ensure compliance with the objectives and requirements of the phase, taking into account the specific inputs to that phase; • design reviews; • tests performed on the designed products to ensure that they perform according to their specification; • integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together in the specified manner. [IEC 62061].
White channel	Defined communication system in which all relevant hardware and software elements are designed, implemented and validated according to IEC 61508. Note 1 to entry: This definition expands the usual meaning of channel to include the system that contains the channel. [IEC 61784-3]
Vulnerability (cybersecurity	Weakness in the security of an IT-system that can be exploited or triggered by a threat [CEN ISO/TR 22100-4:2020]. Weakness of an asset or control that can be exploited by one or more threats [SFS-EN ISO/IEC 27000:2020].

1 Introduction

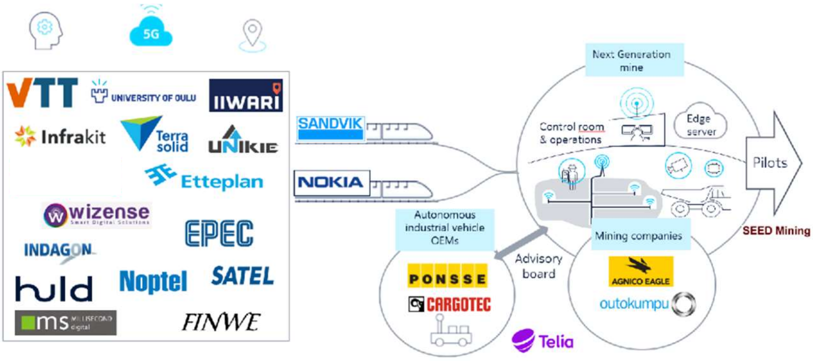


Figure 1. Next Generation mining project ecosystem.

Specification of new 5G-enabled operational principles and definition of the main Use Cases:
The reliable high-speed connectivity provided by 5G networks brings many opportunities for the mining industry. It provides new possibilities for operational principles and approaches for organizing the mining operations, for example by enabling new data-driven tools for managing the utilization and maintenance of machinery and other assets. In order to maximise the benefits that 5G can provide to underground operations, use cases should be planned, designed and deployed considering a long-term view and a holistic approach encompassing not only operational but also safety, environmental and commercial aspect of the business.

The main objective of this deliverable is to lay the foundations for the safety principles in the NGMining project by pointing out risks, mitigation strategies, functional safety principles and communication safety principles. This document is structured as follows: first, a brief overview of state-of-the-art of mining industry, related risks and risk mitigation strategies. Effects of 5G on safety concepts. Functional safety principles are introduced and then communication risks and risk mitigation examples. Cybersecurity issues from functional safety perspective have been considered in one section. Some examples of safety functions and their properties are presented.

1.1 Main risks and mitigation strategies of autonomous mobile machines

Autonomous mobile machines are typically large and all collisions cause considerable damages. If a person is involved with the collision the severity is considered fatal in the risk assessment. The collision can also cause a fire, which can be dangerous even if there are no persons nearby. A hazardous situation may arise also after the collision during rescue operation. These examples of risks show that risk is high when a person is near, but risk is possible even if persons are far from the immediate collision location. Especially, in mines a fire and its smoke can suffocate persons far away from the accident place. Fire hazard is not considered here specifically, since it is related also to manual machines and similar precautions are required with autonomous systems too. The mentioned risks are general, but in this report the focus is on mine operations and collision risks.

To avoid collisions between autonomous machines and persons or vehicles the separation distance between the autonomous vehicle and other objects need to be adequate. There are several ways to keep objects far enough from each other and typically more than one way is needed in each application. Four strategies are presented here.

a) A safe way to get good separation distance is to use fences, gates or virtual gates (e.g. light curtains) and arrange area access control, which prevents moving objects from moving to the same area. The devices at gates or virtual gates can have high PL (Performance Level), which means that the safety functions and control systems can be safe. If for example a light curtain detects a person (or another object) it triggers stop, which requires manual reset and checking that nobody is at hazardous zone. However, overall safety requires more comprehensive risk assessment to evaluate safety. One disadvantage of this kind of strategy is that it is rather solid and all changes to the system can be laborious. An example of the concept is shown at Figure 2, case a). Human occupies the area, where he is and also one area beside it. Furthermore, all autonomous mobile machines at the occupied area are stopped.

b) A more sophisticated, but more challenging way to keep separation distance is to track all moving objects. This can be done by using terrain sensors, onboard tags or active transmitters to calculate or inform the location of the moving object to the traffic/fleet control. The traffic control tracks all objects and gives access rights to vehicles and persons. The idea is that, for example, in an intersection there is only one object at a time. The terrain sensors may be needed to inform the machine that another machine is approaching from behind a corner. An example of the concept is shown at Figure 2, case b). All persons and mobile machines are tracked, and traffic control keeps the separation distance between objects adequate by reducing speed. If the separation distance is too short a stop command is initiated. The recovery of the situation can be automated, if it is safe according to risk assessment.

c) Third way to control separation distance to the autonomous mobile machine is to have onboard sensors, which detect objects towards the moving direction and slow the motion to avoid collision (see Figure 2, case c)). One concept related to this strategy is to have separate short-distance and long-distance sensors. The long-distance sensors have low PL, detect objects far away (e.g. 10 m) and slow motion is initiated. Short distance sensors have high PL (e.g. PL d) and stopping is initiated. Separate sensors for long distances are a practical solution, since currently it is difficult to find long-distance, PL d sensors for outdoors use. One possibility related to this strategy is to apply lidars and form a model from point cloud, and furthermore detect objects. There are several different sensors, like, laser- scanners, lidars, radars and cameras, which can be applied to form a safeguarding field around the autonomous mobile machine.

d) Forth way to improve traffic safety are traffic rules. Traffic rules are necessary for autonomous mobile machines and traffic, but usually they are not considered to be adequate enough, but also other mentioned means are necessary. It is also possible to give situational awareness information for persons with lights (operational state and direction of movement) or voice signals. It is common that industrial trucks show blue spot in front of them to show their direction of movement and it can be seen also behind a corner. Figure 2, case d) shows some devices, which can be applied in traffic control, like, traffic signs, traffic lights, booms and walkways.

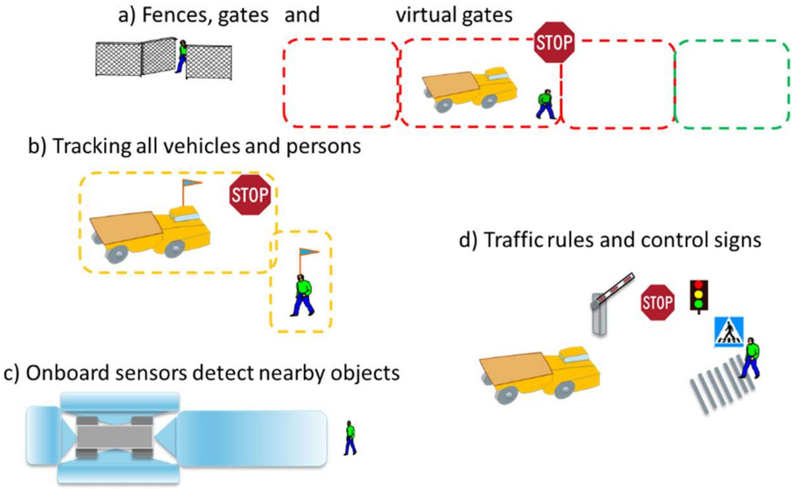

a) Fences, gates and virtual gates
STOP
b) Tracking all vehicles and persons
STOP
d) Traffic rules and control signs
STOP
c) Onboard sensors detect nearby objects

Figure 2. Examples of collision risk mitigation strategies.

As mentioned all of the four strategies, described at Figure 2 may be needed in future sophisticated dynamic safety system. The vision can be that the separation distance between moving machine is all the time adequate by controlling the speed of the machine. The machine can also reroute itself to get a free route to the goal or, in some cases, also the goal can be changed. When the machine is stopped, the recovery can be automated. To achieve good routes to the goal, continuous communication with the traffic control is needed and the routes need to be optimized from the complete system viewpoint.

Communication between autonomous mobile machines and traffic control is essential in all of the strategies shown at Figure 2. There can be communication also between machines, area access control, local infra. In most of the cases the communication is not straight between sender and receiver, but several repeaters are needed. In case a) communication is needed to open doors and occupy virtual gates. In case b) there is continuous wireless communication between traffic control and moving objects. In case c) the autonomous machines may be able to drive small parts of the travel without traffic control, but wireless communication is needed to receive new tasks, emergency commands and to travel safely in critical places, like, in intersections. In case d) communication is needed for traffic lights and boom controls.

1.2 State-of-the-art mining operations and communication

There are many kinds of hard rock underground mines, and the structure can be changing rapidly. Each mining tunnel (process: drill/blast/haul/dump) can advance roughly about 18 m/day [1]. Mines can have new mining tunnels 10 km/year or even more. This means that also the communication network needs to change often. One aspect is that some tunnels are made for traveling and there can be rather stable communication network. Typically, the tunnel ends, which are under construction, are changing rapidly. There are areas, where humans may not go, since they are not sufficiently supported. Figure 3 and Figure 4 show two examples of mining structures.

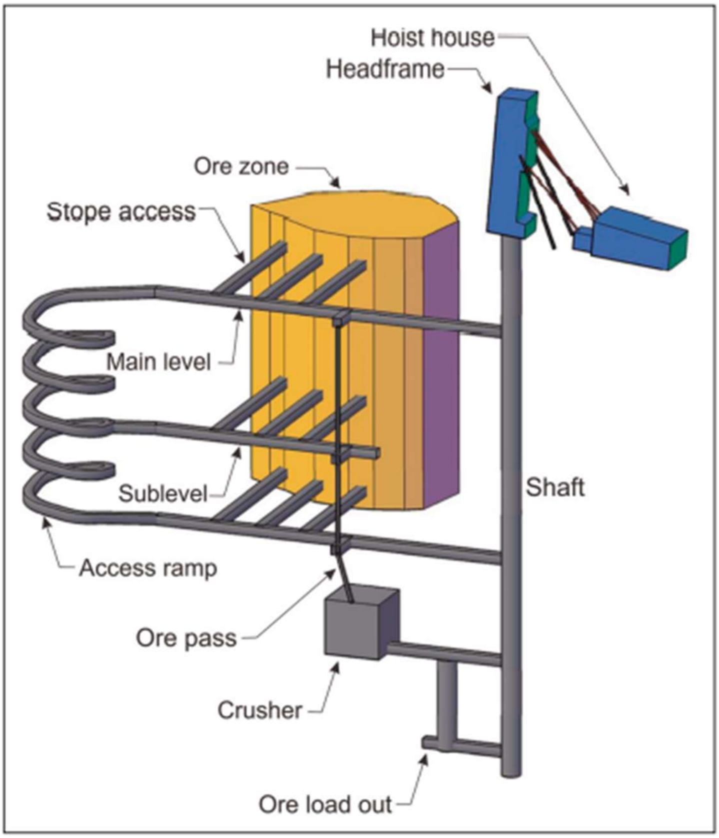


Figure 3. Example one mining structures. [1]

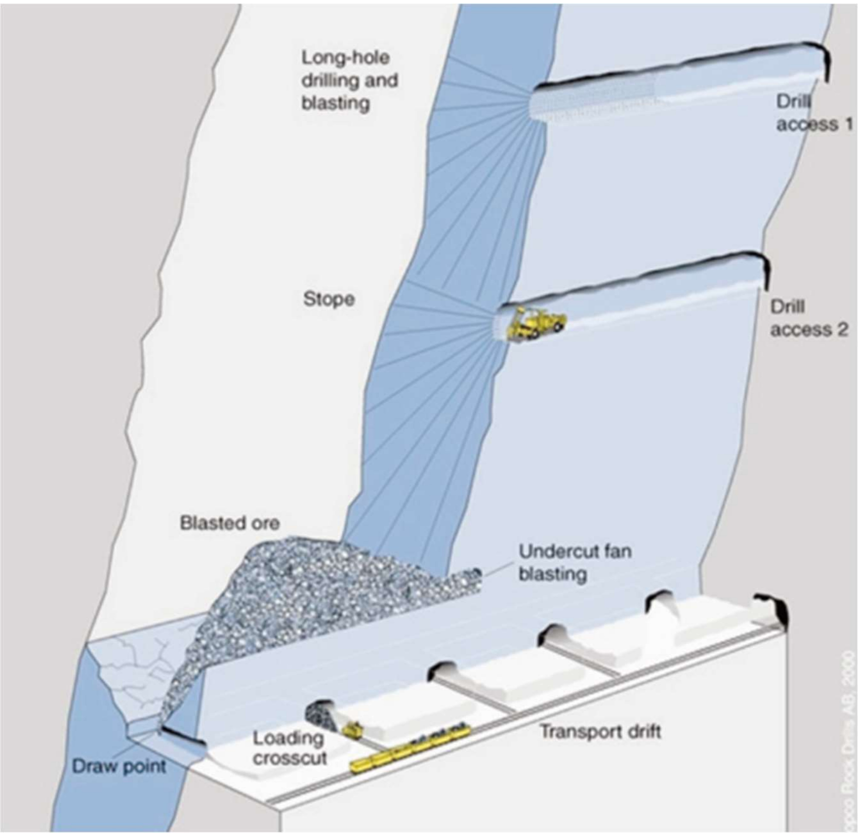


Figure 4. Example two of mining structures. [1]

1.3 Effects of 5G on mining operations

5G enables new approaches on how the mining operations are developed, organized and how machinery and other assets are utilized and maintained. These aspects have been studied in the project preparation phase to outline the project with the specification of the Next Generation Mining Technology Vision.

One aspect related to good communication is that it enables digital twins and digital shadows to be applied in systems. In digital twins there is 2-way digital connection between system/fleet control and machine and this enables both commands and information transfer, whereas digital shadow is applied only to feed information to system control. Both of them can be related to digital model, which is applied in designing operations.

The main contributions of 5G in mining are related to the reliable, fast, and low-latency communications that can be applied for safer and more efficient operation. 5G is expected to be a key enabler in many aspects of mining operations – especially in increasing the level of autonomy of mining machines.

5G applies regulated frequencies and the network is established and maintained by accepted operator. The Wi-Fi network may be established by anybody, it applies only specific frequencies (2,4 GHz and 5 GHz), there are power limitations and many other devices can apply the same frequencies causing disturbances. Advantages of 5G compared to Wi-Fi are typically:

- In 5G the handover between stations is made by comparing stations and choosing station according to signal strength, signal/noise ratio, and by avoiding swapping of station too often (hysteresis). In Wi-Fi, there is no comparison of signals and the communication needs to end before establishing communication via new station/repeater. There can be also a short period of weak signal, before communication ends, which may cause delays.
- The applied frequency of 5G can be chosen so, that no other devices apply the frequency and the disturbances are so minimized. Usually lower frequency travels longer distance, but it does not carry so much information.
- When the 5G network can be established by avoiding disturbances, it may be possible to lower the number of stations, but there is balance between reliable communication and number of stations. Usually, the stations neep to be placed at places, where is long line-of-sight and therefore possibility to lower the number of stations can be small.

The mentioned factors mean that there are possibilities for 5G to provide more reliable network than Wi-Fi can. One aspect is that the network standards are developed continuously and new features can be applied in the future, such as, more precise timing, location (triangulation) and variant communication routes. 3GPP (Third Generation Partnership Project) provides new versions of 5G standard almost annually. Release 15 was published 2018 and release 16 at 2020 [EDN: 3GPP Release 16: What are the key enhancements and new features?].

Autonomy of the machines is characterized by perception, situational awareness, and decision-making capabilities of the machine. Autonomy is a key player in improving the safety of mining operations: fewer people are needed in underground areas as the work is transferred to remote monitoring types of positions. 5G will be a key enabler for the increase of autonomy of the mining machinery as it offers fast and reliable communication of the locations and statuses of the machines. In addition to connectivity, robust sensor technologies and analytics methods are needed to perceive the environment and to build comprehensive situational awareness.

Even at high levels of autonomy, situations requiring intervention from human operators may emerge. Many of such situations can be handled by remote operation. To do this, large amounts of data need to be reliably transferred for real-time operations. For example, high-resolution video feed and other information are needed for control room functions and remote operation tasks. Additionally, to improve flexibility of operations, various ways of human-machine interactions are expected to be needed in the mine as well. Safety principles need to be studied to ensure the safe coexistence of humans and autonomous machines within the mine.

Technology development is needed to enable the functions related to autonomy. In NGMining project, the research and development activities are related to the key technologies structured so that the research activities pursue the increased productivity and safety.

Cybersecurity issues can be handled in Wi-Fi and 5G by using cryptography and specific frequencies. WI-Fi can be more vulnerable, since anybody can establish new stations and the applied frequency is common, however, protective measures can be applied. In addition to lower layer protective measures, there can be an additional virtual private network (VPN) for safety-related communication at safety layer 8 (or application layer) and the 5G or Wi-Fi network is considered to be black channel.

2 Functional safety

2.1 Functional safety principles

General safety aspects of mines are changing as automation increases. The responsibility of safety is turning from individual persons in manual systems to technology in automated systems. Actually, technical safety systems are vital part of autonomous systems. One essential safety aspect is increased communication and 5G is an important possibility. Safety related communication deep inside mines can be related, for example, to area access control, position of machines and persons, mine area map changes, warnings, emergency stops, emergency instructions, accident information, etc. These factors are related to functional safety, which means correct and safe functioning of the control system (includes input devices, logic and controls of actuators).

One general aspect related to safety requirements is that there are already many requirements and history shows that the number of requirements is increasing, and the requirements show how required safety level is continuously getting higher and more details are defined. It is not feasible to introduce commercial systems, which would be less safe than previous systems. Research project is introducing ideas and it can be presented what kind of measures are needed in the case study to fulfill functional safety requirements.

One should note that all safety issues are usually not related to functional safety, such as fire safety, electrical safety and dust exposures. In some cases, these risks can be mitigated using functional safety principles. Functional safety can also be associated to "three step method" according to ISO 12100 [13]. The method describes three steps, which should be used in design, in the defined order. Each step must be applied in sufficient measure and for example information for use may not substitute previous steps.

- First step: inherently safe design measures should be used. The risk is designed out, for example, a finger may be crushed into a squeezing clamp, but if the finger does not fit to the clamp (gap < 5 mm), the risk is designed out. This first step is not related to functional safety.
- Second step: safeguarding and/or complementary protective measures. Related to the second step many safety sensors and

functions are related to functional safety, but for example fences and other mechanical guards are not.

- Third step: information for use. Where risks remain despite inherently safe design measures, safeguarding and the adoption of complementary protective measures, the residual risks must be informed to the user. This third step is not related to functional safety.

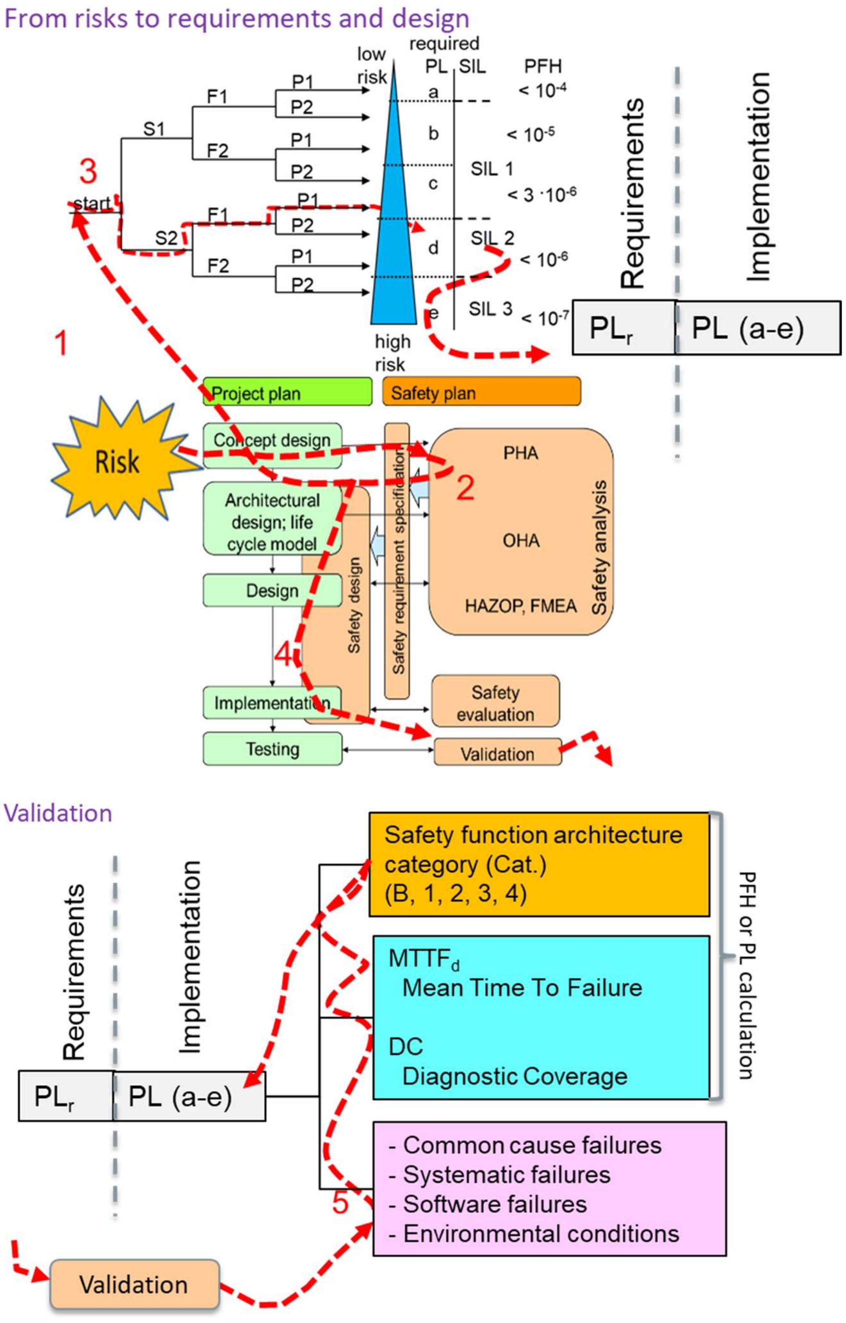
Functional safety is related to safety functions of control systems, which are made to prevent accidents. Usually, safety function consists of input devices (e.g. sensors, pushbuttons), logic and actuators (e.g. brake controls, speed control, power cut off circuits). The need for safety functions can be found in risk assessment, which show the risk level and the need for a safety function and control system. The requirements and safety functions are categorized to PLs (Performance Levels according to ISO 13849-1), which are from lowest to highest level PL a, PL b, PL c, PL d and PL e [18]. The idea is to categorize the risk, set the requirement accordingly (PL_r) and then design matching safety function (similar PL), which lower the probability of the accident to the specified level. The IEC 61508 standard family present Safety Integrity Levels (SIL), which are in machinery sector SIL 1, SIL 2 and SIL 3. SIL 4 is related to catastrophes, and SIL 4 is not relevant in machinery sector. There are also other standards, which categorize risks and requirements with other acronyms (e.g. ASIL, MPL and AgPL). Standards ISO 13849-1:2015 and IEC 62061:2021 are harmonized, which means that by applying them the designer can make a presumption that relevant Machinery Directive Annex I requirements are fulfilled. Most of the machinery standards refer to PLs, since they all are ISO standards. One aspect is that ISO 13849-1:2015 standard also considers hydraulics and pneumatics. The new IEC 62061:2021 standard also considers hydraulics and pneumatics, although it is based on electrical systems.

Figure 5 shows process how requirements are defined using a risk graph (PL assignment) and then input devices, logic and actuators of the safety function are validated against the assigned PL. The figure shows also risk graph to assign PL and equivalent SIL and PFH_D. Each PL and SIL equals to probability of dangerous failure per hour (PFH_D). The right side of the figure shows, which factors need to be analysed quantitatively or qualitatively. PFH_D refers to quantitative approach and the parameters needed in calculation are architecture, $MTTF_D$ (Mean Time To Dangerous Failure) values of components and diagnostic coverage of system/subsystem. Common cause failure factor (CCF, β) is semi-quantitative factor, which is related to the standard test, which needs to be passed or in IEC 61508 standard family it may have a figure, like, 10% which represents estimated share of common cause failures. The basis for the common cause failure assessment is that duplicated system is not perfect and there are single failures, which can impair the safety function. The probability of common cause failures needs to be low enough according to the applied assessment method. Systematic failures and software are verified using qualitative means. Environmental aspects are tested according to defined (by manufacturer) environmental requirements.

The user chooses devices, which are suitable for the environmental conditions. The bottom left corner of the Figure 5 shows how the functional safety design can be connected to overall design. The phases described in Figure 5 are:

1. The Hazard or risk is found in the risk assessment.
2. Each risk is considered and if it is related to control system, functional safety requirements are specified. Risk graph can be used to if standards do not give suggestions to PL requirements.
3. The required PL (PLr) specified for each safety function.
4. Protective measures match the safety requirements (PLr).
5. Each safety function validated according to the safety requirements.

Software requirements for each PL/SIL can be found in functional safety standards. The software requirements are equivalent to corresponding PFH_D, but the software probabilities are not calculated, but estimated according to the relevant requirements. There are many qualitative requirements, and, in addition, there are highly recommended methods, recommended methods and not recommended methods to be applied in software design. There is also rigor factor or thoroughness of applying the method in different SILs.


From risks to requirements and design

Validation

Figure 5. Model that shows the connection between risk, PL/SIL assignment, design, and validation.

2.2 Assigning PL or SIL

The required PL or SIL for each safety function can be achieved in some cases from standards, but in many cases the PL or SIL needs to be defined according to risk assessment. The risk assessment is made to the plain system, which do not have safety devices related to safety functions. This is because safety devices may not diminish their own requirements. For example, high speed limiting requirements may not be diminished because machine is driving at slow speed due to speed control (perimeter conclusion). Gates, fences and mechanical shields can be considered to be there before the analysis.

First the severity of the risk need to be defined. Serious consequences, like death or irreversible injury lead to S2. Secondly frequency of the accident is considered so that if the risk is present more often than once per 15 min or the accumulated exposure time exceeds 1/20 of the overall operating time, then F2 is chosen. Thirdly the possibility to avoid risk is considered. Factors, which affect this parameter (P) are for example: how suddenly the hazard arises (e.g. quickly or slowly), possibilities for hazard avoidance (e.g. by escaping), practical safety experiences relating to the process, whether operated by trained and suitable operators and operated with or without supervision. P1 should only be selected if there is a realistic chance of avoiding a hazard or of significantly reducing its effect. If the probability of occurrence of a hazardous event can be proven low according to reliability data and history of accidents then PL requirement level can be reduced one level. The avoidance parameter may be defined more precisely in the future ISO 13849-1 standard, but this may affect the generic nature of the PL assignment.

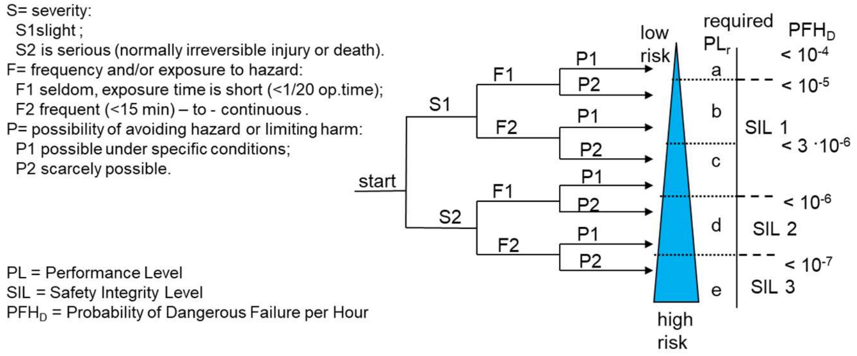
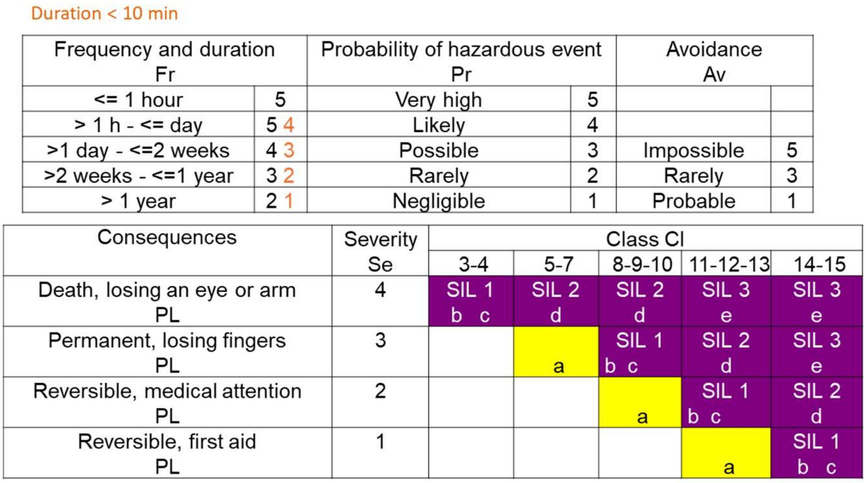

S= severity:
S1slight ;
S2 is serious (normally irreversible injury or death).
F= frequency and/or exposure to hazard:
F1 seldom, exposure time is short (<1/20 op.time);
F2 frequent (<15 min) – to - continuous .
P= possibility of avoiding hazard or limiting harm:
P1 possible under specific conditions;
P2 scarcely possible.
PL = Performance Level
SIL = Safety Integrity Level
PFH$_D$ = Probability of Dangerous Failure per Hour
start
S1
S2
F1
F2
F1
F2
P1
P2
P1
P2
P1
P2
P1
P2
low risk
high risk
required PL$_r$
a
b
c
d
e
SIL 1
SIL 2
SIL 3
PFH$_D$
< 10^{-4}
< 10^{-5}
< $3 \cdot 10^{-6}$
< 10^{-6}
< 10^{-7}

Figure 6. Assigning PL according to ISO 13849-1 [18].

Figure 7 shows SIL assignment method according to IEC 62061. In this method, first frequency and duration, probability of hazardous event, and avoidance are considered and classified according to numbers shown at Figure 7. For frequency parameter, the lower value at the column can be applied if the duration is less than 10 min. The numbers are added together and result is read at the lower table at the relevant severity row.



Duration < 10 min

Frequency and duration Fr		Probability of hazardous event Pr		Avoidance Av	
<= 1 hour	5	Very high	5		
> 1 h - <= day	5 4	Likely	4		
>1 day - <=2 weeks	4 3	Possible	3	Impossible	5
>2 weeks - <=1 year	3 2	Rarely	2	Rarely	3
> 1 year	2 1	Negligible	1	Probable	1

Consequences	Severity Se	Class Cl				
		3-4	5-7	8-9-10	11-12-13	14-15
Death, losing an eye or arm PL	4	SIL 1 b c	SIL 2 d	SIL 2 d	SIL 3 e	SIL 3 e
Permanent, losing fingers PL	3		a	SIL 1 b c	SIL 2 d	SIL 3 e
Reversible, medical attention PL	2			a	SIL 1 b c	SIL 2 d
Reversible, first aid PL	1				a	SIL 1 b c

Figure 7. SIL assignment according to IEC 62061. [7]

The risk graph method is not mandatory and it is possible to apply other methods, like the matrix method described at Figure 7. The SIL and PL can be exchanged according to Figure 6. The SIL assignment can be made also according to IEC 61508-5.

Standard “Earth-moving machinery. Functional safety. Part 1: Methodology to determine safety-related parts of the control system and performance requirements (ISO 19014-1:2018)” defines required machinery performance level (MPL), which are MPL a, b, c, d and e. These resemble the PLs of ISO 13849-1. However the assignment of MPL is made by applying parameters severity, exposure, controllability, alternative controls, awareness of hazard and ability to react. These parameters differ considerably from ISO 13849-1 and IEC 62061, but the standard could be applied for earth-moving and mining machinery. The controllability is in the standard an important factor, although it is not considered in the harmonized standards ([18], [7]). The parameters do not clearly consider the risks of autonomous vehicles, but they resemble more a manual vehicle functionality. Therefore it may be difficult to apply the standard to autonomous mobile machines.

2.3 Safety performance according to performance levels (PL)

ISO 13849-1 standard presents designated architectures (see Figure 8) for control systems, which can be applied to calculate PFH$_D$ values. The standard provides tables with PFH$_D$ values, which are precalculated with Markov models for designated architectures. The designated architectures are one and two channel architectures with different diagnostic properties. The final system architecture can be built up using the provided designated architecture blocks. Three channel architecture is not provided in the set of designated architectures and therefore three channel calculations need to be made by using pessimistic assumptions, which may give adequate results if the values are clearly above the target threshold. The assumptions need to be chosen carefully. IEC 61508 family provides analytical equations for calculating also some three channel architectures. The analytical equations (IEC 61508) give a little bit different results than Markov models (ISO 13849-1), but both methods can be applied. There are also some differences in parameters of the calculation methods.

Figure 8 show designated architectures, related categories, PLs and maximum PFH$_D$s. Categories B and 1 have only one channel, categories 3 and 4 have two channels and category 2 has one primary channel and a diagnostic channel.

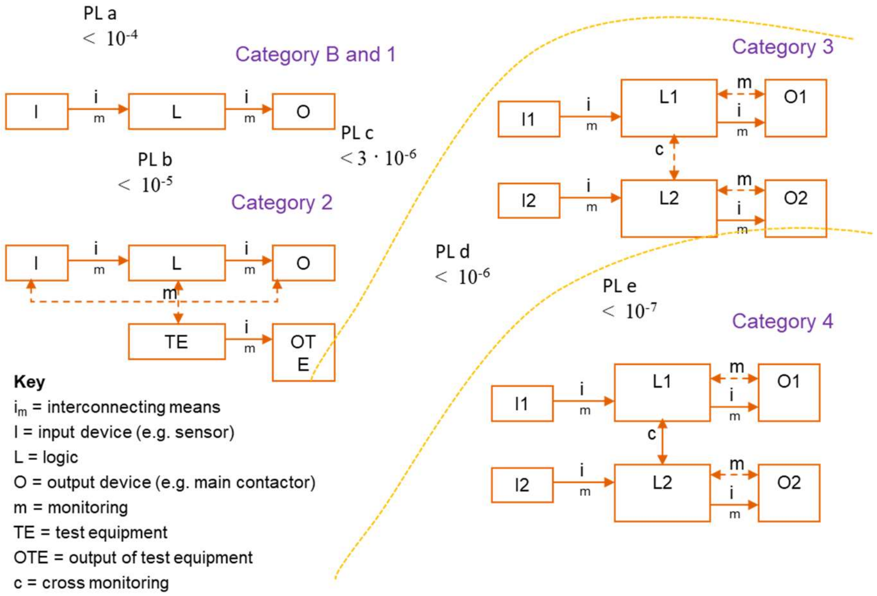


Figure 8. Designated architectures, their block diagrams, categories, PLs and maximum PFH$_D$. [18]

Figure 9 presents how ISO 13849-1 shows graphically relation between category (resistance to faults and their subsequent behaviour in the fault condition which has corresponding designated architecture), $\mathrm{MTTF_D}$ and diagnostic coverage (DC). In the figure each column is divided to three or less parts according to $\mathrm{MTTF_D}$ value (low, medium and high). The dotted area in the middle of the column represents medium $\mathrm{MTTF_D}$ (10 – 30 years). In the figure the selected PL d area (diagonal stripes) represents two channel architecture (category 3), DC between 60 % to 90 % (low), and $\mathrm{MTTF_D}$ between 10 to 30 years (medium). Figure 10 show the same case as in Figure 9, but it is illustrated as a (logarithmic) diagram.
Diagnostic coverage (DC) is measure of the effectiveness of diagnostics, which may be determined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures. Diagnostic coverage can be estimated for the complete function or for parts of the safety-related system. For example, diagnostic coverage could exist for sensors and/or logic system and/or final elements. [18]
$\mathrm{MTTF_D}$ is expectation of the mean time to dangerous failure. [18]
Category is classification of the safety-related parts of a control system in respect of their resistance to faults and their subsequent behaviour in the fault condition, and which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability. Each category can be associated to specific designated architecture. [18]

Category is related to the channels (one or two channels and a diagnostic channel) of the system, but it resembles also fault tolerance, which is described in IEC 61508-2. Fault tolerance is associated to minimum number of failures, which the system can withstand without a hazard. For example, fault tolerance 1 is typically associated to a duplicated system or category 3. Fault tolerance is applied in estimation of architectural constraints.

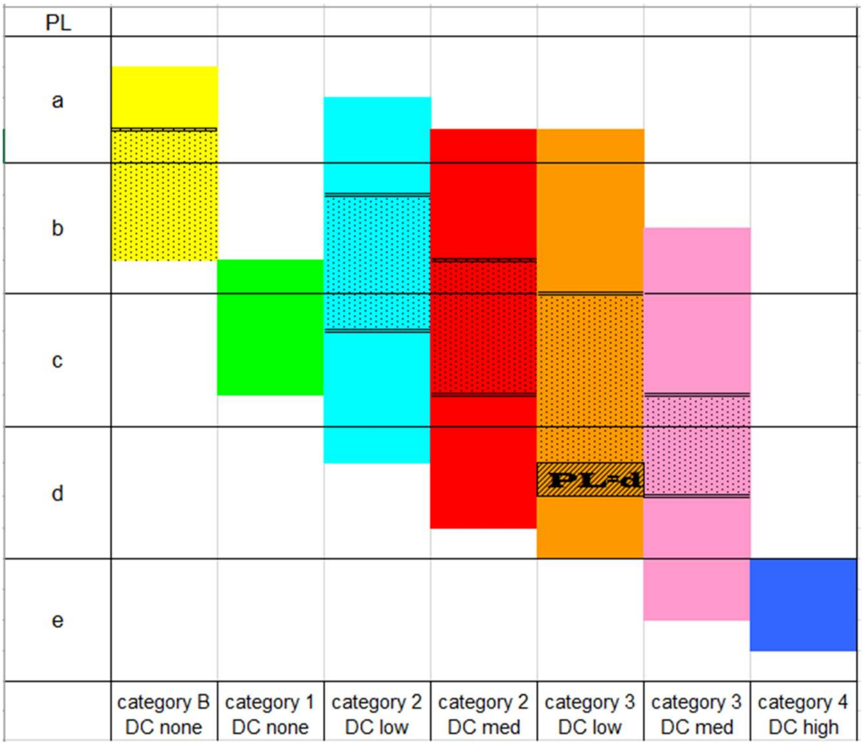


Figure 9. Graphical presentation of relations between PL, category, MTTF$_D$ and diagnostic coverage.

In Figure 10 each coloured line represents designated architecture. The logarithmic scale of PFH shows the real distances between different solutions and it shows how far the PFH target. Cat B and Cat 1 are actually at the same line, but Cat 1 represents system with more well-tried components and safety principles. In practice e.g. complex integrated circuits, like microprocessors are not considered well-tried, and therefore complex electronic circuits cannot fulfil category 1 requirements. Some lines are associated to same Category, but different DC (Diagnostic Coverage). The figure shows that better DC improves PFH value. Cat 4 resembles Cat 3, but it has better DC and it also fulfils Cat 4 specific requirements. Cat 4 safety function typically endures one or more failures without jeopardizing safety.

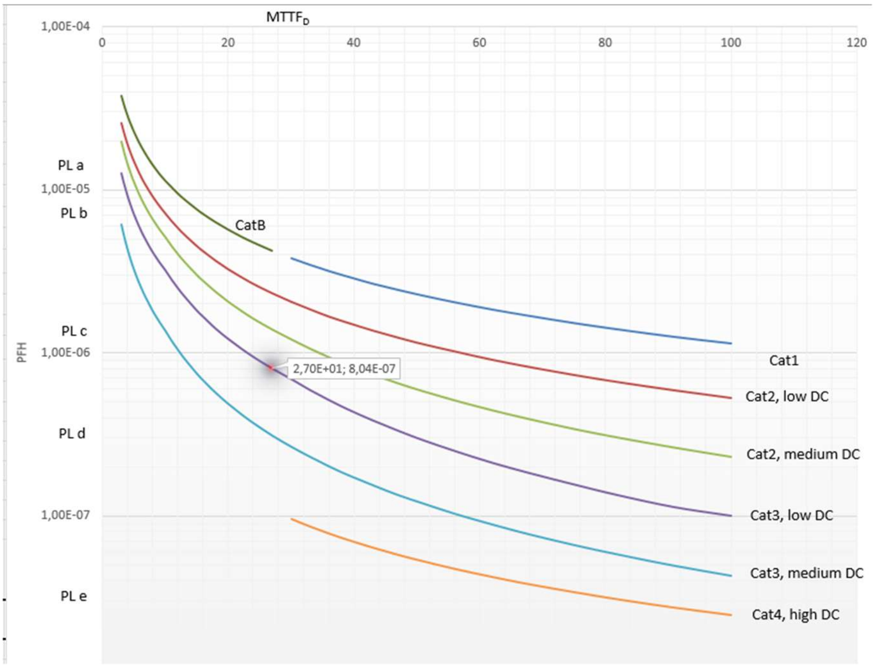


Figure 10. Diagram presentation of the relation between PL, DC, category and MTTF$_D$.

3 Communication and functional safety

One should note that machinery system builder usually buys a complete communication system(s), which includes defined safety features. The acquired communication system needs to fulfil relevant safety, cybersecurity, environmental and performance requirements. The idea is that the user buys commercial communication network with adequate properties, defines communication operator, which maintains the features and in addition the user applies the network as required and adds possibly some application dependant features. Only in some cases, where adequate components are not available (e.g. too exotic environment or conditions for commercial components) the machine builder need to have tailored systems, which can fulfil all the requirements.

3.1 Communication concepts

For communication in mines currently widely applied technologies have been: analogue telephones, voice over internet protocol (VOIP), digital radio system, wireless network (Wi-Fi), cellular network (LTE), WAN and LAN [1]. LTE is an IP-based wireless communications technology that constitutes an OSI model Layer 4 (transport; see Figure 12). In this project the focus is on LTE and 5G.

In the mines, communication is operated using cables or line-of-sight wireless communication. Cables are applied usually in areas, which are not changing and wireless connections in areas, which are changing, like tunnel ends. Figure 11 shows an example of current Wi-fi communication in the end of a tunnel. [1]

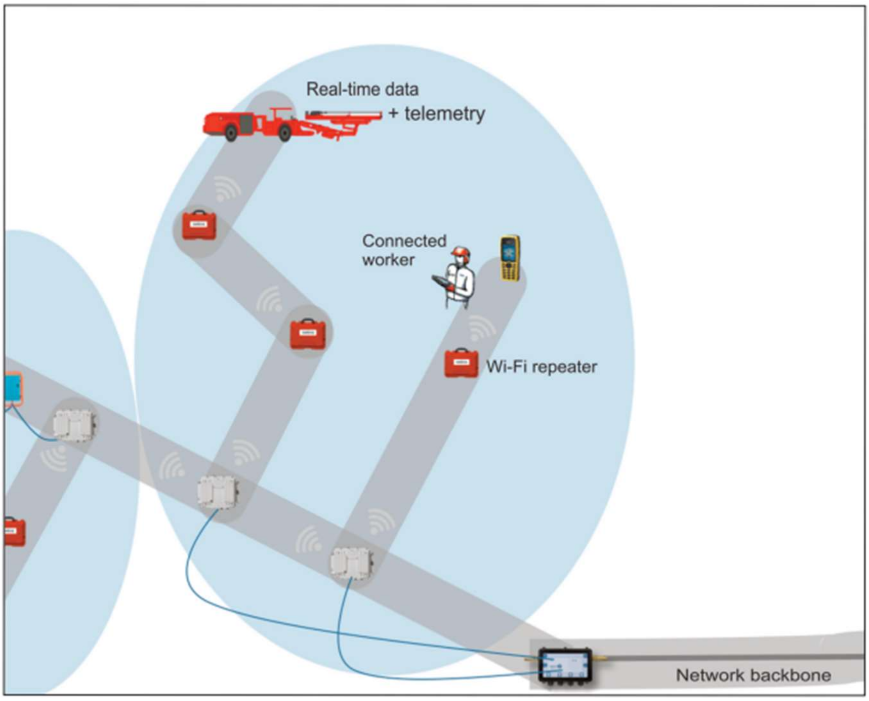


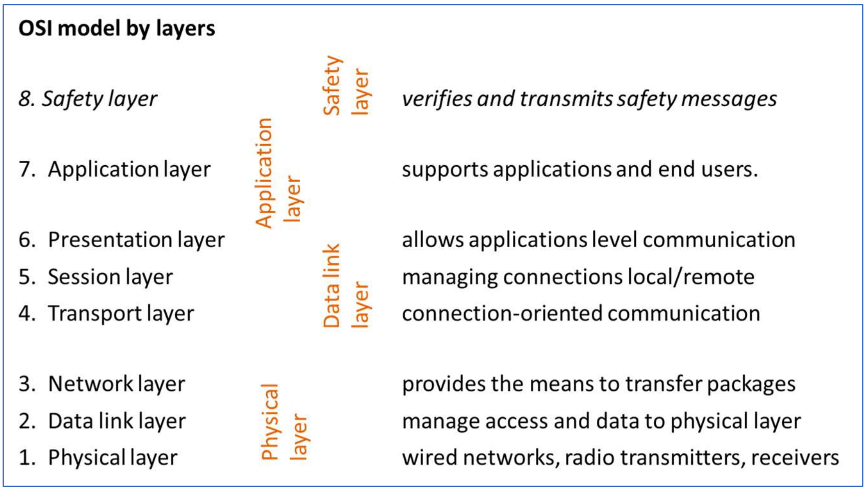
Figure 11. An example of Wi-Fi communication in the end of mining tunnels.[1]

There are many ways to structure underground communication. It is typical that wireless communication requires line-of-sight connection between communication nodes, which means that it is difficult to construct communication network. It is often a best practice to be flexible and leverage more than one topology within a mine to overcome constraints. The main network topologies that are commonly used in underground mines [1]:

- Bus topology: All nodes are directly connected to a single linear cable. Example: Leaky feeder (radiating cable).
- Ring topology: All nodes are connected via a ring of cable. Example: resilient Ethernet
- Mesh topology: Network in which each node has a direct connection to all others; in a partial mesh topology, some nodes are connected to all others, while others are only connected to those nodes with which they exchange data; may be wired or wireless. Example: the Internet
- Star topology: All nodes are connected to a central hub via a dedicated path. Example: traditional Ethernet.

OSI model

OSI model (Open Systems Interconnection model) is a conceptual model that describes communication functions. The actual safety layer is above the original model layers and the first seven layers are similar to non-safe communication [1], [Wikipedia]. One may also consider that the first 7 layers form a black channel and all the safety features are provided by the safety layer. It is also possible to apply so called white channel, in which all layers comply with safety requirements of IEC 61508-2 [7], [9]. The first three layers (physical, data link and network) are related to hardware devices, like, wires, connectors, transmitters and receivers. These are all components that cause typically signal attenuation if they fail completely (e.g. open wire). The network system needs to be designed so, that these failures are detected and a proper safety function is initiated. Transient bit errors, due to e.g. electromagnetic interference or weak signal, are considered as message corruption and error-handling procedures take care of them. All the other layers are related more to software.



OSI model by layers

8. Safety layer	*verifies and transmits safety messages*
7. Application layer	supports applications and end users.
6. Presentation layer	allows applications level communication
5. Session layer	managing connections local/remote
4. Transport layer	connection-oriented communication
3. Network layer	provides the means to transfer packages
2. Data link layer	manage access and data to physical layer
1. Physical layer	wired networks, radio transmitters, receivers

Figure 12. OSI model by layers. [1], [9]

Black and White channel communication

When parts of the communication channel are not designed or validated according to the IEC 61508 series the channel is called “black channel”. It is assumed that the black channel itself does not detect all errors. Therefore, the errors, and possibly a combination of errors are detected by the check within the safety layer of the receiver [7]. All the measures necessary to implement transmission of safety data in accordance with the requirements of IEC 61508 are performed by an additional "safety communication layer". Figure 13 show an example of black channel communication. Figure 14 shows black channel from a functional safety communication protocol (FSCP) perspective. This includes logical connection and black channel for real communication. Logical connection can be associated to timeliness, authenticity and data integrity and furthermore it can be affected by security problems. The actual black channel can be affected by many kinds of communication errors and although there can be error detection and other measures to better communication, only the safety layer of the FSCPs is considered for safety purposes. The safety layer has the needed safety features (see Figure 17 in the middle), like, it can detect all errors as specified and it can request repetition. It is not dependent on safety measures inside the black channel, since they are assumed to be unknown. All FSCPs assume that safety communication take place through black channel [9]. Black channel can be assumed to be more practical to use, when the fieldbus contains both safety and non-safety messages. More FSCPs are described in IEC 61784-3-X standards.

When the entire communication channel is be designed, implemented and validated according to the IEC 61508 series and IEC 61784-3 or IEC 62280 series, then the channel is called "white channel".

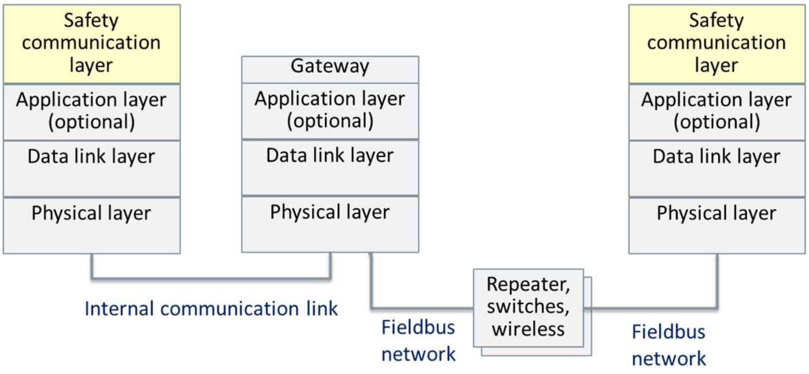

Safety communication layer
Application layer (optional)
Data link layer
Physical layer
Gateway
Application layer (optional)
Data link layer
Physical layer
Safety communication layer
Application layer (optional)
Data link layer
Physical layer
Internal communication link
Fieldbus network
Repeater, switches, wireless
Fieldbus network

Figure 13. An example of black channel communication [9].

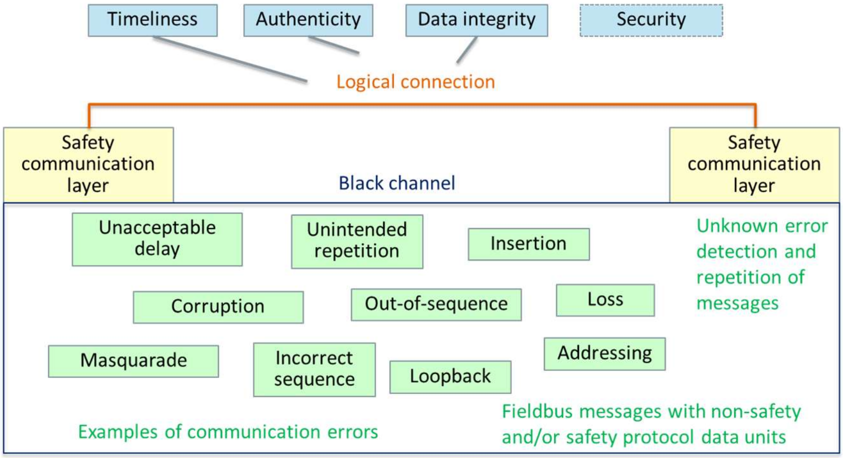

Timeliness
Authenticity
Data integrity
Security
Logical connection
Safety communication layer
Black channel
Safety communication layer
Unacceptable delay
Unintended repetition
Insertion
Unknown error detection and repetition of messages
Corruption
Out-of-sequence
Loss
Masquarade
Incorrect sequence
Loopback
Addressing
Fieldbus messages with non-safety and/or safety protocol data units
Examples of communication errors

Figure 14. Black channel from a functional safety communication profile (FSCP) perspective [9].

Example of safety-related communication

Figure 15 shows an example of safety-related messaging between a machine and area access control. Inside the automated area there is supervised area, which can be entered only if there is permission. When the automated machine enters the area, other machines or persons may not enter the area in automated mode. The area is released when the automated machine exits the area. The critical messages need to be acknowledged by the other party. If the message is not acknowledged, the message is resent. The next operation phase can begin after receiving acknowledge message and fulfilling other possible start conditions. The messages are generated by safety logic (safety communication layer) and the message can be transmitted via several nodes (e.g. 5G) between the sender and receiver. The error detection and message repetition procedures are not considered to be part of the safety system and therefore the communication system is considered to be black channel.

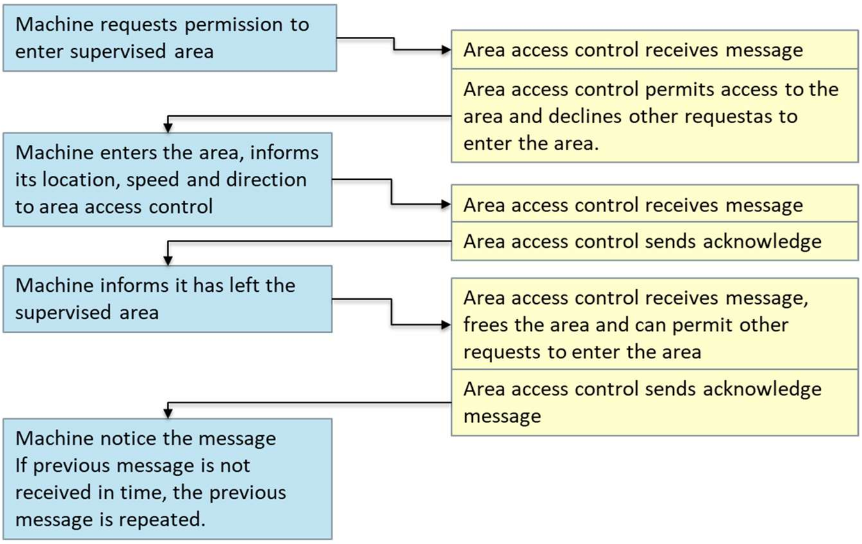

Machine requests permission to enter supervised area
Area access control receives message
Area access control permits access to the area and declines other requestas to enter the area.
Machine enters the area, informs its location, speed and direction to area access control
Area access control receives message
Area access control sends acknowledge
Machine informs it has left the supervised area
Area access control receives message, frees the area and can permit other requests to enter the area
Area access control sends acknowledge message
Machine notice the message If previous message is not received in time, the previous message is repeated.

Figure 15. An example of messaging between machine and area access control.

3.2 Safe communication

3.2.1 Communication safety requirements

Machinery Directive (2006/42/EC) gives simple requirement for cableless systems: For cableless control, an automatic stop must be activated when correct control signals are not received, including loss of communication [12]. More detailed requirements can be found from standards. Regarding to the automatic stop, the time to stop is defined using risk assessment. However, standard “EN 13557 + A2:

2008 Cranes – Controls and control stations" gives limit 500 ms to initiate stop after loss of communication. This can be a good estimation to initiate stop also for autonomous mobile machines if there is no better knowledge. For more information see also section 4.1.7 Response time.

Functional safety basics of communication is defined in IEC 61784-3. The functional safety of control systems is defined generally in IEC 61508 standards and more specifically for machinery in IEC 62061 and ISO 13849-1. There are also other aspects related to communication, such as, communication networks, fieldbuses, EMC and electrical safety. Figure 16 (from IEC 61784-3 modified) shows relations between functional safety communication and some other standards. In the figure, standards inside yellow blocks are safety related standards and standards inside blue blocks are related to fieldbuses or other related topics.

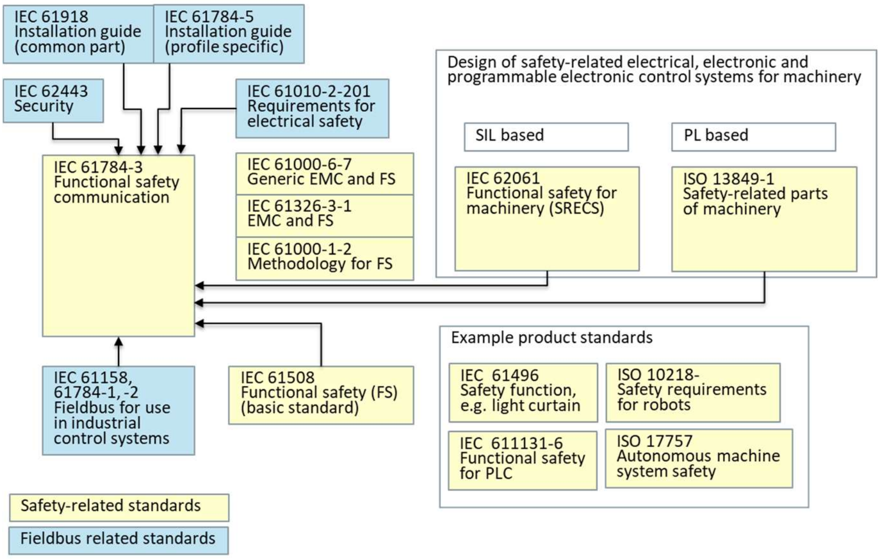


Figure 16. Relations between functional safety communication and other standards.

3.2.2 Communication threats and message errors

Communication system threats can also be related to devices, systems or software, which control the messages or communication system (see Figure 17 right side). These threats are often considered in the control system functional safety analysis and not in communication safety analysis. There are communication related threats related to communication design and environment (see Figure 17, left side). These factors affect bit-error rate and reliability, but they have an indirect effect on safety.

The safety standards, like IEC 61508-2 [7] and IEC 61784-3 [9], focus on safety threats related to messages (see Figure 17 in the middle). If the messages are correct, then safety is under control. If bit-error rate is too high, it affects messages and furthermore acceptable messages cannot be received and a specific safety function is initiated to maintain safety. Bit-error rate can be associated to corruption and corruption is typically the threat that requires quantitative approach to be verified. There is also a limit to acceptable bit-error rate, in order to minimize the probability of random acceptable message.

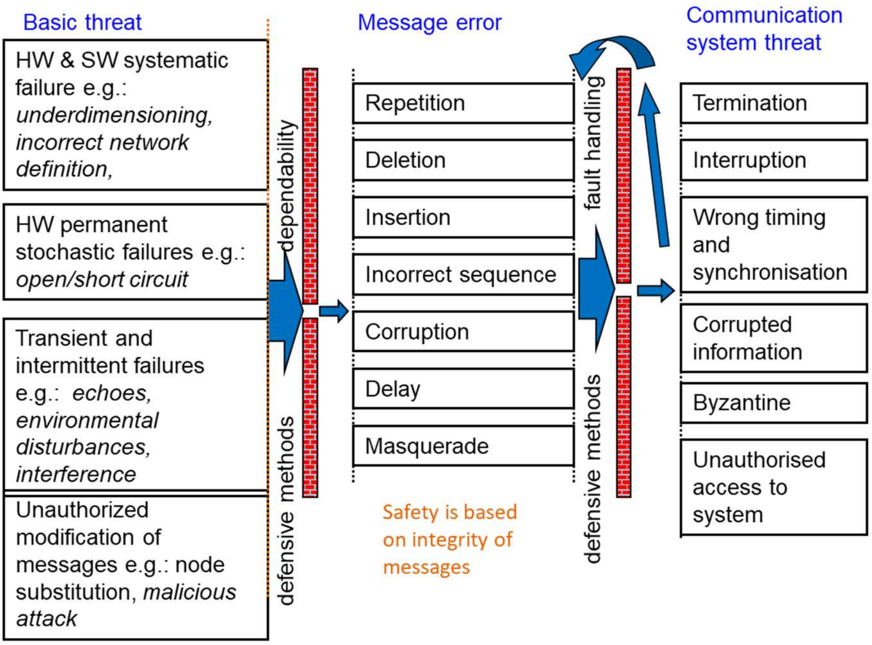

Basic threat
HW & SW systematic failure e.g.: *underdimensioning, incorrect network definition,*
HW permanent stochastic failures e.g.: *open/short circuit*
Transient and intermittent failures e.g.: *echoes, environmental disturbances, interference*
Unauthorized modification of messages e.g.: node substitution, *malicious attack*
dependability
defensive methods
Message error
Repetition
Deletion
Insertion
Incorrect sequence
Corruption
Delay
Masquerade
Safety is based on integrity of messages
fault handling
defensive methods
Communication system threat
Termination
Interruption
Wrong timing and synchronisation
Corrupted information
Byzantine
Unauthorised access to system

Figure 17. Concept of communication errors.

There must be safety measures to all of the seven threats related to messages (see Figure 17 in the middle) [7]:

- repetition; same message is sent continuously (no new information) or it may disturb other messages; repetition by sender is normal when receiver detects a missing message and asks for recent,
- deletion; message is not received correctly,
- insertion; additional unexpected message is received from other network or node,
- incorrect sequence; sequence is wrong due to two paths through several nodes,
- corruption; bits of the message are changed due to e.g. disturbances or weak signalling; message errors are normal in communication and receivers detect them with high probability

and erroneous messages are recent or in some cases recovered (recovery may lead to an additional risk), here a corrupted message is erroneously accepted; if an acceptable message is not received within acceptable timeframe, a message is classed as unacceptable delay,

- delay; a message is received too late,
- masquerade; message outfit mimics wrong message type or address.

“Addressing” error is mentioned by IEC 61784-3 as an additional threat, but IEC 61508-2 includes it to other threats.

The mentioned threats are related to single channel communication. If there are also safety-related high availability requirements, then a single channel is probably not enough, but second or third channel is required. High availability means here that it is not possible to stop the machine, but continuous control is required. This can be related for example to continuous control of stability, cooling or ventilation.

According to IEC 61508, a risk analysis will define safety functions. These safety functions can be decomposed to parts that contribute to the overall safety function (for example, Sensor(s) – Safety communication channel – Programmable Electronic System(s) – Safety communication channel – Actuator(s)).

It is recommended that any logical connection of the safety communication channels of a safety function does not consume more than 1 % of the maximum PFH of the target SIL for which the functional safety communication profile is designed [9]. This means that the target PFH for SIL 2 communication is 10^{-8} and for the complete safety function maximum PFH is 10^{-6}.

Table 1 describes examples of safety measures, which can be applied against message errors/threats. In safety-related communication, at least one measure against each threat should be applied. Each method can be applied in different intensity according to the threat probability and required SIL. For example when the requirements are higher a longer identifier or CRC polynomial can be applied. Redundancy of communication like two or more connections or repeated messages can be needed to reach higher SIL or to increase availability. In commercial fieldbuses the safety measures are already integrated into the system. The measures are similar in wireless communication, but the bit-error rate is higher in wireless communication and therefore some additional measures may be needed, especially, against corruption.

Table 1. Examples of safety measures against communication message errors.[9]

Communication errors	Safety measures							
	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message (also e.g. orig. CRC)	Data integrity assurance (e.g. CRC)	Redundancy with cross checking	Different data integrity assurance systems
Corruption					X	X	X	
Unexpected repetition	X	X					X	
Incorrect sequence	X	X					X	
Loss	X				X		X	
Unacceptable delay		X	X					
Insertion	X	X		X	X		X	
Masquerade				X	X			X
Addressing				X				
- Time expectations define specific time window for messages and it is needed in all safety communication. - Connection authentication refers to source and destination identifiers. - CRC (Cyclic Redundancy Check) detects well bit errors, but there are also other efficient Hash functions. Hash function is (mathematical) function that maps values from a large set of values into a smaller range of values to detect data corruption. Common hash functions include parity, checksum and CRC. - Feedback message can include e.g. CRC of the received message, echo the complete message or the identifier of the message. - Redundancy with cross checking can be applied when two messages are sent through independent transceivers. There can be one or two DLL/FAL/PhL (Data Link Layer / Fieldbus Application Layer / Physical Layer) and one or two transmission medias. - Different data integrity systems include different encoding principles (e.g. different CRC polynomials) for safety data and non-safety data.								

CRC is common measure to ensure integrity of data. Note that there are plenty of standardised good CRC polynomials, which are good for specific message lengths. One CRC can be excellent in average, but it may have poor Hamming distance related to specific error number. This means that in specific case an error of only some bits (Hamming Distance is difference between two messages in bits) can cause hazardous function. This means that CRC polynomial needs to be chosen carefully. Note that due to long messages residual error probability (RP) is difficult/laborious to calculate exactly, but there are simplified equations e.g. for calculating estimation for RP_x = P("error case x takes place") × P("error case x is not detectable") [9].

3.2.3 Cybersecurity

The significance of cybersecurity is increasing and in EU new Cyber Resilience Act will be published in few years. A draft is already available (EU 2019/1020. 15.9.2022). Some targets of the act are products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risk. There should be no known exploitable vulnerabilities. The product with digital elements shall be accompanied among others with the point of contact where information about cybersecurity vulnerabilities of the product can be reported and received [3]. Currently cybersecurity vulnerabilities are often secrets, but the draft implies more openness.

Cybersecurity standards can be divided into two groups: IT security (Information Technology) and OT security (Operational Technology). One can compare the objectives of the systems. In IT security priority order (beginning the highest priority) is confidentiality, integrity and availability. In OT security the priority order is availability, integrity and confidentiality [2]. One can compare this to functional safety, where only integrity and availability are important. This could be interpreted so that OT security has more common with functional safety.

IT security is more related to office technology and important standards are IEC 27000 [20] and its daughter standards, like, IEC 27005 (Information security risk management). The standard presents vast checklists related to threat and vulnerability [21]. There are also several cybersecurity standards for specific domains (e.g. nuclear security), which are related more to OT security.

Cybersecurity in automation and industry

An important OT security standard family is “IEC 62443 Industrial communication networks. Network and system security”. The standard family can be divided into four groups of standards, which are dedicated to specific stakeholders: general, asset owner, system integrator and component provider. The machine user is close to asset owner, but machine builder needs to provide and probably buy services and therefore know something about all parts of the standard family. The standard family covers, among others, security lifecycle, policies, objectives, procedures, stakeholder roles, technologies, systems and components. Security levels (SL) are presented and they represent the confidence that a system, zone, and/or its components can provide the desired level of security and they are free from vulnerabilities and they function in the intended manner. Here are shortly the introduced security levels characterized by the level of protection that is provided against attacks [5].

- SL 0: No special requirement or protection provided.
- SL 1: Protection against unintentional or accidental misuse.

- SL 2: Protection against intentional misuse by simple means with few resources, general skills and low motivation.
- SL 3: Protection against intentional misuse by sophisticated means with moderate resources, specific knowledge about industrial automation and control systems and moderate motivation.
- SL 4: Protection against intentional misuse using sophisticated means with extensive resources, specific knowledge about industrial automation and control systems and high motivation.

The main steps of IEC 62443 can be presented as shown in Figure 18. The procedure resembles functional safety process and some equivalences can be found. Risk assessment is needed to the system under consideration, requirements are defined according to risks and the system is designed to fulfil the cybersecurity requirements. Figure 18 points out that security assessment is made first in high level and then in detailed level and it can be an iterative process.

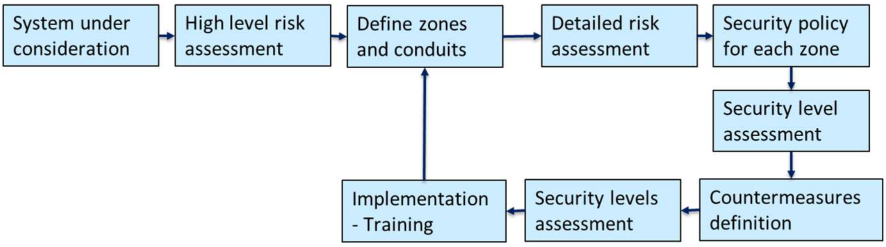

System under consideration
High level risk assessment
Define zones and conduits
Detailed risk assessment
Security policy for each zone
Security level assessment
Countermeasures definition
Security levels assessment
Implementation - Training

Figure 18. The main steps of IEC 62443 standard family. [7]

Cybersecurity in machinery sector

There is also ISO technical report CEN ISO/TR 22100-4:2020, which gives guidance for machine manufacturers to cybersecurity aspects [2]. Since it is report, there are no requirements, but it compares well the machine safety and cybersecurity aspects. It presents five steps, which are good to follow in cybersecurity design:

- Identify; the cybersecurity threats and vulnerabilities.
- Protect; the appropriate counter measures to protect the machine.
- Detect; identify the occurrence of a cybersecurity attack.
- Respond; take action regarding a detected cybersecurity attack.
- Recover. maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity attack.

The report points out some aspects related to risk in machinery sector and in cybersecurity. Figure 19 shows that severity (machinery) and negative impact (cybersecurity) both express how bad the consequences can be and probability and likelihood express expectation of the occurrence. In cybersecurity risk is often expressed as probability that a particular threat will exploit a particular vulnerability with a particular consequence [11].

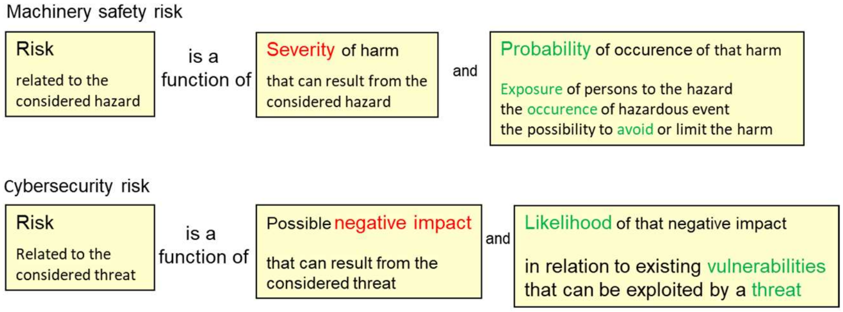

Machinery safety risk
Risk
related to the considered hazard
is a function of
Severity of harm
that can result from the considered hazard
and
Probability of occurence of that harm
Exposure of persons to the hazard
the occurence of hazardous event
the possibility to avoid or limit the harm
Cybersecurity risk
Risk
Related to the considered threat
is a function of
Possible negative impact
that can result from the considered threat
and
Likelihood of that negative impact
in relation to existing vulnerabilities that can be exploited by a threat

Figure 19. Comparison of machinery safety risk and cybersecurity risk [2].

In the machinery sector risk definition is related to harm against a person. In cybersecurity sector the risk is related to negative impact against physical assets, logical assets and/or human assets. Asset is here something that has value to the organization. In cybersecurity sector the risk definition is much wider. This means that in cybersecurity risk assessment one needs to consider many aspects that are negligible in machinery sector (e.g. confidentiality).

One risk property/parameter is probability/likelihood. In machinery sector (functional safety) risk is often related to probability of random events, software properties or systematic failures. Cybersecurity risk is often related to malicious deliberate act. This is related more to attacker resources and knowledge about vulnerabilities and not so much to probability. Therefore in cybersecurity the risk considered to be qualitative, whereas in machinery sector (functional safety) it is often quantitative. [17], [11]

When looking at the machinery safety process diagram (in ISO/TR 22100-4), it can be seen that security threats can have an effect on safeguarding and complementary risk reduction methods and perhaps in some cases inherently safe design measures. The effect means that cybersecurity threat can cause a harm by exploiting vulnerabilities of the safeguarding or complementary risk reduction measures. [2] This looks only a small part of the process, which includes risk assessment, requirement specification, design and validation, but it includes the design of safety-related control functions. This could be interpreted so that cybersecurity and functional safety assessments have different paths, but same assets are under consideration in the design of safety-related control functions.

Common consequences related to functional safety and OT security are integrity and availability. In functional safety sector safety integrity levels are calculated and it reflects the importance of the safety integrity. Availability can be important functional safety factor in some communication cases, but in large majority of cases low availability cause machine to stop and it turns to a safe state. In these cases availability is not a safety issue. Poor availability is typically a productivity issue. Availability can be a safety issue when stopping can be hazardous and continuous control is required. This can be the case for example when controlling stability, ventilation, cooling, fire emergency devices and other emergency devices, like, emergency stop devices.

Cybersecurity issues need to be considered especially in wireless communication. Typical measures against cybersecurity threats are related to isolation (e.g. fire walls), authentication (e.g. passwords) and cryptography. Cryptographical methods can be chosen so that in addition to providing confidentiality and prevention of service blocking the method also detects corruption errors (see e.g. IEC 9797-1, Message Authentication Codes). In some cases the advantage is that it can be difficult for an attacker to crack both authentication and corruption prevention code at the same time, since incorrect messages are deleted. Cryptographical coding and encoding is done in application layer of OSI model (see Figure 12). Cryptographical methods are needed before any functions related to the received message are realised and on the other hand, at lower layers the connection between transmitter and receiver is not yet completely established. Cryptography is possible also in lower layers, but then it is not necessarily specific for the application, but it provides confidentiality in general.

Vulnerability can be considered as a weakness of the system and the designer can affect more to vulnerability than threat. The vulnerabilities can be treated by

- designing security risk out by avoid vulnerabilities),
- reducing or limiting security risk by mitigating risks (e.g. more powerful passwords) or limiting consequences (e.g. firewalls, security zones),
- providing information about the residual security risk and the measures to be adapted by the user,
- transferring or sharing the security risk to a third entity (e.g. insurance, security provider) or
- accepting the security risk (risk is estimated to be small) [2], [17].

When a good countermeasure is needed in cybersecurity, typically, the concept defence in depth is applied. This involves applying multiple countermeasures in a layered or stepwise manner [11]. In practice, it means that large share of interfaces, conduits and security zones have separate counter measures to improve security. This means e.g. different passwords and cryptographical methods for each conduit or security zone. A malicious attacker may find the weakest asset (e.g. persons, communication systems) of the system and mobilize the attack through it. In functional safety, redundancy is applied to improve safety. In practice, it means that special efforts (e.g. duplication and diagnostics) are applied only to the critical parts of the system. Machinery systems have plenty of non-critical parts, which cannot cause immediate harm and their weakness is not a safety issue.

4 Examples of safety functions

4.1 Considering some prominent safety functions

4.1.1 Stopping

Stopping is very common safety function and it is applied if something critical fails or a hazardous situation is about to happen (e.g. collision). Stopping function stops typically all movements. Emergency stopping is applied if the situation is critical, but usually a softer stopping is applied to avoid damaging equipment and the load.

Stopping function is realised by applying brakes and adjusting speed setpoint to zero. Brakes are necessary, since for example the mobile machine may roll downwards without brakes. To reach good performance also the motor needs to stop and in some cases engine or power source is cut off to ensure stopping. When estimating worst case stopping distance for safety dimensioning all the equipment needed for stopping need to have good performance.

PL of the stopping function depends on the situation and it is not always the same. If, for example, a person is detected in front of the mobile machine and the machine must stop to avoid collision, the requirement for detecting the person is typically PL d and the same requirement applies for stopping. In this case, detecting a person, logic for generating stop command and the stopping actuators are related to the same safety function and the same PL requirements applies to all of these devices. The exception are the brake actuators, which have their own requirements (ISO 3450:2011) and typically functional safety calculations for the mechanical parts are not made.

There are also stop categories (not related to functional safety), which define how effectively electrical power is cut off [1]. Each stop category may have any PL depending on the system requirements.

- Stop category 0. Stopping by immediate removal of power to the machine actuators [1]. In some cases it is not safe to cut power quickly, but the speed need to be slowed down. Stop category 0 can be realised with simple circuits and a high PL can be achieved easily. Safe torque off (STO) function of a power drive system in accordance with IEC 61800-5-2 is an example of stop category 0 function. Stop category 0 stopping requires manual restart.

- Stop category 1. A controlled stop with power available to the machine actuators to achieve the stop and then removal of power when the stop is achieved [1].
- Stop category 2. A controlled stop with power remaining available to the machine actuators [1]. Stop category 2 is not safe without additional measures. Safety-rated monitored stop (described in robot standard ISO 10218-1) is stopping function with additional sensors to detect movements. If the machine is still moving after safety-rated monitored stop, a stop category 0 stop is initiated. Safety-rated monitored stop can have high PL and the system is quick to restart after it.

4.1.2 Emergency stop

According to ISO 12100 emergency stop function is intended to avert arising or reduce existing hazards to persons, damage to machinery or to work in progress, and be initiated by a single human action [13]. The colour and shape are defined in standards (see ISO 13850), it overrides all other functions, there are limitations to restarting and there are requirements also for the control path. Emergency stop can be applied for cableless control stations, but it may not be the sole means of initiating the emergency stop function of a machine and confusion between active and inactive devices must be prevented. The PL is typically PL d (see e.g. ISO 3691-4:2020), but if the risks are minor also PL c is possible. Emergency stop is obligatory for machines, but it is called complementary protective measure and it may not substitute other safeguarding. Emergency stop must be realised using either stop category 0 or 1 [15]. Restart after emergency stop requires first manual acknowledgement and then manual start-up.

4.1.3 Propulsion

Throttle control, transmission, gear selection and engine shut down are all functions, which affect propulsion of the machine. For driverless trucks [14] requirement for speed control is PL d, if speed control is related to personnel detection. The requirement is PL c, if it is related to over speed detection (speed> truck rated speed).

One aspect related to propulsion or actually the speed of the machine is relation to other safety functions. High speed means long stopping distance. If stopping function has high PL, and there is a relation between propulsion and stopping, i.e.

applied stopping distance requires slower speed than maximum speed, then also propulsion should have similar PL requirements as stopping. Otherwise, the maximum speed need to be applied instead of real speed, when calculating stopping performance. The relation between safety functions may require more complex reasoning.

4.1.4 Safety-rated reduced speed

Safety-rated reduced speed refers here to speed, which is below normal speed, it is monitored and exceeding the speed cause protective stop. The reduced speed needs to be defined in risk assessment and the selected speed should give persons possibility to avoid collision. For robots, the safety-rated reduced speed limit is 250 mm/s (ISO 10218-1:2011) and according to draft ISO/DIS 13849-1.2:2021 there are possibilities to avoid collision if the speed is below 1 m/s. It is difficult to say which speed could always give possibilities to avoid collision, but a large mobile machine is easier to detect than a robot arm and persons keep naturally longer distance to a mobile work machine.

The safety function “Safety-rated reduced speed” can be realised with speed sensors, the control logic and actuators integrated into the machine (large part of the control system becomes safety-rated) or it can be a separate measuring function, which reacts only, if the speed is exceeded. In both cases the speed control safety function relies on speed measuring sensors. When the machine is already in use, the separate measuring system is easier to add, but it may lack some functionality (precise speed control) compared to the integrated system.

The performance level of the “Safety-rated reduced speed” safety function needs to be defined according to PL assignment process (see Figure 6). Another possibility is to check from standards, which PL they recommend. For example, ISO 3691-4 “Driverless Industrial Trucks and their systems” standard recommends PL d for practical speeds (>0,3 m/s) [14].

4.1.5 Steering

Steering is controlling the direction, where the mobile machine is going according to automated or manual commands. The steering function of large mobile machines is realised with hydraulic cylinders, since the required forces are high. The hydraulics receives commands, typically, from a safety PLC, which communicates with other control systems. The steering system (e.g. the safety PLC) receives commands from e.g. navigation system and it realises the adjusted steering direction. If the steering function fails, the machine may go to the right although the command is to the left. The steering control system can be duplicated, but then during a failure if the first control channel commands to the left and the second to the right, then it is difficult to conclude which is correct. Apparently one of the steering controls is correct, since discrepancy has happened most probably due to a steering channel failure. Average steering direction would be wrong, since then the failure affects steering definitely. When the speed is slow, continuation of the old direction can minimize hazards until the speed is zero. The safe steering direction can be achieved by voting between different control commands. This means at least duplicated architecture with an additional safety feature or a 2oo3 architecture (two-out-of-three architecture).

Duplicated architecture can be built up using primary and separate secondary steering system. The secondary steering system is applied in emergency cases and it has priority over the primary steering system. If the primary steering system fails, control is switched to the secondary channel and the speed is slowed down using propulsion and brakes controls. Figure 20 shows an example of the system with primary and secondary channel. It is assumed that since primary channel is doing most of the work, it also has more failures. If primary and secondary channels have different outputs, then it is assumed that the secondary channel has most probably correct output mainly, because there is safety logic to give commands.

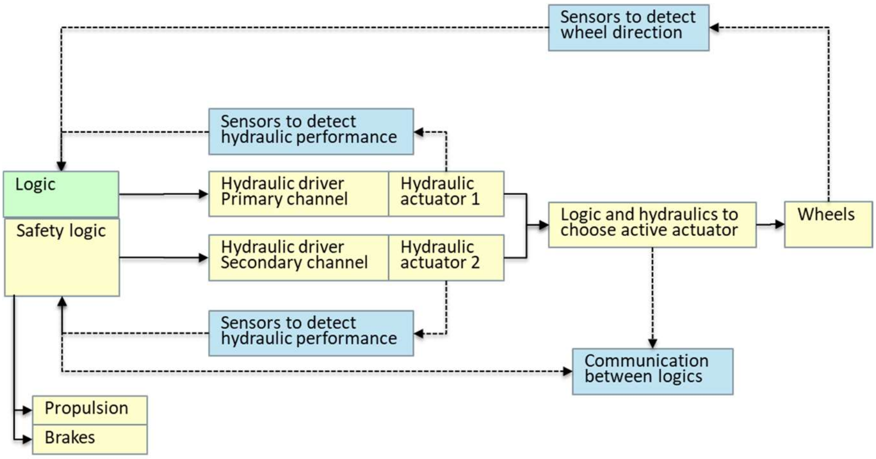

Sensors to detect wheel direction
Sensors to detect hydraulic performance
Logic
Safety logic
Hydraulic driver Primary channel
Hydraulic actuator 1
Hydraulic driver Secondary channel
Hydraulic actuator 2
Logic and hydraulics to choose active actuator
Wheels
Sensors to detect hydraulic performance
Communication between logics
Propulsion
Brakes

Figure 20. An example of duplicated steering control and connections to brakes and propulsion control.

If the steering function fails then typically speed setpoint value becomes zero and braking begins. Also Machinery Directive [16] has requirements related to power-assisted steering and new Machinery Regulation draft also to autonomous mobile machinery steering function. The requirements are related to controllability and maintaining safety before it can be stopped. If the steering direction is uncertain, then the mobile machine needs to stop or a secondary steering system needs to be applied. According to “ISO 5010:2019 Earth-moving machinery — Wheeled machines — Steering requirements” no uncontrolled steering movement shall occur [12]. If the maximum speed is over 20 km/h then there must be a secondary steering system, which turns on automatically if primary steering system loses power. According to the old ISO 5010:2007 standard, if the steering function fails and maximum speed is over 20 km/h the steering performance must be maintained. If the steering direction fails, braking with high speed is not quick enough to avoid collision, but the steering performance needs to be maintained. When the speed is slow then after steering failure, it can be safe enough to stop the machine without steering manoeuvres.

If steering has failed and machine has stopped, it may be possible to continue travel using manual or remote driving at a very slow speed (limping mode). In some cases, there can be also a specific interface for emergency driving.

4.1.6 Required minimum distance for stopping to avoid collision

Minimum distance for stopping (separation distance) is related to the capability of the machine to stop before any collision can happen. Figure 21 shows the factors to be consider, when estimating needed minimum distance for stopping. Related to the machine one needs to consider also: machine real speed versus max. speed, load, posture during braking, outreach of the axis and load. Max. stopping distance related to max. speed, machine outreach and load can be used, instead of the actual parameters, if the stopping parameters are not known. Constant deceleration is often applied if there is no other information. Outreach of a person is arm length (e.g. 850 mm) can be applied if necessary. More information about minimum/safe distances can be found from EN 13855 [16].

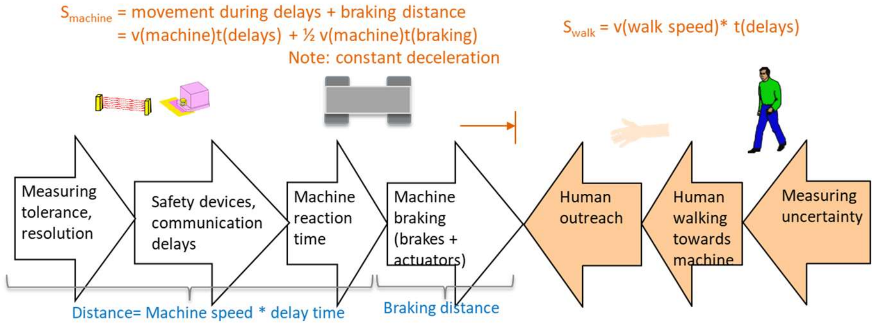

$S_{machine}$ = movement during delays + braking distance
= v(machine)t(delays) + ½ v(machine)t(braking)
Note: constant deceleration
S_{walk} = v(walk speed)* t(delays)
Measuring tolerance, resolution
Safety devices, communication delays
Machine reaction time
Machine braking (brakes + actuators)
Human outreach
Human walking towards machine
Measuring uncertainty
Distance= Machine speed * delay time
Braking distance

Figure 21. Minimum distance for stopping

4.1.7 Response time

Response time is related to safety functions and it is not alone a safety function, but a property of a safety function. The maximum accepted response time is determined according to risks that may be realised if there is delay in response time. On the other hand, in many cases slow response time can be compensated by increasing safety margin, i.e. safety function begins earlier.

- For example, if the speed of a mobile machine is 10 m/s and quick stopping (no brakes, sensors, communication delays) takes 1 s, and an object is detected in front of the mobile machine. The stopping command needs to be given at least 5 m before the object. Assuming constant deceleration without delays (stopping distance = s=vt/2). This simple reasoning does not yet consider any delays, safety margin or safety performance.
- If in another case it takes 2 s to stop, at speed 10 m/s then the object is detected and stopping command given at least 10 m before the object.
- If in another case, the system is not capable to detect the object at 10 m range, then the speed needs to be reduced. When the speed is 5 m/s, object is detected at 5 m distance and stopping time is 2 s, then the performance is adequate.

The calculations above are made without delays. If the delay is for example 1 s, it means 10 m additional distance, when the speed is 10 m/s.

Typically, if the sensors are on-board the mobile machine, then maximum speed needs to be adjusted to match stopping/response time. If the sensors are at the infra/terrain or the fleet management concludes separation distance according to object positions, then the required separation distance is adjusted to match the stopping/response time. If the distance detect an object is too short, then the speed of the machine needs to be reduced to match the stopping distance.

As described, there is some flexibility in determining the response time, but when the maximum response time is defined, it may not be exceeded. The reason is that many safety functions (e.g. separation distance) are determined according to the maximum response time. If the determined response time is exceeded, then a predefined harder safety function (typically protective stopping) is initiated. If the determined response time is too optimistic, then the hard safety function (protective stopping) is initiated often, which may be wearing for the machine. The hard safety function is determined so that the response time failure does not cause hazard, i.e. stopping is quicker than normally. However, usually there is only one stop function, which needs to match the response time.

The response time is sum of several delays, which are related to machine, devices, uncertainty and human. Here is list of factors, which affect response time:

- Measuring tolerance, uncertainty, resolution of sensors (on-board). Tolerance is turned to delay according to machine speed.

- Machine reaction time, delay in making decisions and delays in internal communication.
- Machine actuator delays (brakes, speed control).
- Consider: machine speed, real speed (PL and reliability) or maximum speed, load, posture, terrain.
- Communication delays on-board the machine (sensors).
- Communication delays to fleet management, other mobile machines, area access control etc.
- Delays related to sensors (at the infra), measuring uncertainty (turned to separation distance or time).
- Human walking (1,6 m/s) towards the machine during delays. Distance can be added to separation distance.
- If a manual machine is moving towards the detection system, then the speed (estimated, real or maximum) of the manual machine need to be changed to distance travelled during delays and added to the separation distance. One aspect is that we need to assume that the manual machine is braking, since otherwise collision is inevitable.
- Human reach may be added to separation distance, if it is relevant. Human hand can reach 850 mm toward the machine, but quite often the risk is considered small.

There are also safety messages, like fire alarm or brake failure, which need to be considered according to the specific risk and the required response time can be much longer.

The response time is related also to communication breaks. If communication breaks for a predetermined time, safety cannot be guaranteed. Usually, there must be a way to stop the system and Machinery Directive [16] and many standards mention that if communication is interrupted the machine must stop. For example, crane standard (Controls and control stations EN 13557) gives limit 500 ms for the communication interruption. The idea is that no hazards may happen during communication interruption and risk assessment is needed to verify it. Autonomous mobile machines may be able to drive safely without communication in specific conditions for a while, but even if navigation, object sensing and area access control would fulfil high safety requirements, the machine must be stopped if the time limit, defined by risk assessment, for communication loss is exceeded. Some factors, which have an effect on the maximum accepted communication loss are for example: navigation capability, object detection capability, capability to detect forbidden zones and area type (empty, traffic, persons).

4.1.8 Braking and reducing speed

Braking is related many safety functions, which intend to reduce speed. During braking there should not be power, which tries to increase the speed (propulsion). Gravity effects are though compensated. Usually each wheel has its own brake and there can be also other brakes at the wheels. Usually the brakes are not studied according to functional safety calculations or estimations, but according to relevant brake requirements (e.g. ISO 3450:2011. Earth-moving machinery — Wheeled or high-speed rubber-tracked machines — Performance requirements and test procedures for brake systems). The mechanical parts of the brakes consists of multitude of duplicated parts and we can assume that the procedure (maintenance, testing, diagnostics, several units) for brakes is sufficient from functional safety viewpoint.

There are electrical and hydraulic systems, which control the brake actuators. The controls are considered according to functional safety measures. The functional safety requirements for brakes follow typically the requirements of stopping or emergency stopping. The PL requirement for braking function cannot be lower than PL of stopping, since otherwise the stopping requirement cannot be fulfilled (assuming brakes perform stopping). The lowest PL of the subsystems in series in the safety function shows the maximum PL that the overall safety function can have. This means that PL requirement for autonomous mobile machine braking control function is usually PL d.

The requirements for braking depends also on the maximum speed of the mobile machine. If the maximum speed is slow, there are not so many requirements and failure of a single brake cause only minor increase to the stopping time and distance. If the speed is mediocre (< 20 km/h), then the machine can be stopped without considering much steering, but stopping performance must be good. If the speed is high, then the control of the machine must be good and this includes braking and steering.

Stopping of the mobile machine starts by stopping the propulsion and perhaps also brake with the motors. Brakes are needed to support the speed reduction. Usually stopping performance is determined by applying both motor and brakes. All the parts that are needed in controlling the brakes and speed reduction are considered.

As mentioned, a mobile machine has a multitude of braking devices, which all have their own control systems. One may consider, what happens if one brake fails (e.g. 1oo4 architecture system) – usually the mobile machine stops a little bit slower. One question is that: is the stopping time longer than the claimed stopping time? If the mobile machine is not able reach the claimed stopping performance, then a specific safety function is needed. This can be e.g. limping mode, which provide slower speed and perhaps reduced functionality or stopping the machine.

4.1.9 Implements (raise, lower, left, right of all linkage movements, powered quick coupler)

The boom movements and other additional movements need to be made using PL assignment of ISO 13849-1 (IEC 62061 or maybe ISO 19014-1:2018). Standard "EN 16228-1:2014. Drilling and foundation equipment - Safety - Part 1: Common requirements." shows some minimum PL requirements for Drilling rigs operations.

Typically, the minimum requirement for movements is PL c. This can be a good estimation for safety functions related to boom movements.

4.1.10 Others

There are also other kind of safety functions, which can be related to operator presence, door interlocks, area access control, lock out systems for maintenance, remote control systems and collision avoidance systems. The PL for these safety functions need to be assigned e.g. according to ISO 13849-1 risk graph.

Collision avoidance and person detection can have different requirements. Person detection is presented at 4.2, Person detection. Person detection and manual vehicle detection resemble each other, since in both cases there is a person involved. If we are sure that there are no persons in the operation zone, then if two autonomous machines collide, it is only an indirect safety issue, since no persons are immediately hurt and PL or SIL cannot be defined, since severity is negligible. However, as a consequence a collision may lead to fire, which can be hazardous and therefore safety requirements need to be stated.

4.2 Examples of assigning PL for safety functions

The examples of safety functions are picked up here from NGMining demonstration. The safety functions represent safety functions that are needed in autonomous mobile machines. However, this is only small portion of the overall amount of safety functions in an autonomous mobile machine system. Furthermore these cases are represented only in general level with reasoning of the selected PL. Other cases may have different results if there are different assumptions. The selected safety functions are described at Table 2.

Table 2. Examples of safety functions associated to NGMining demonstration.

Storyline	Safety function
2. The loader comes online -> registers into the DT system (Data and Telecommunication system) as an actor (actorID) with a mission.	**Communication related to safety functions**. The loader is connected to the network and the communication of safety functions is established. The loader is starting on the fleet and it can move autonomously according to mission, navigation and safety commands.

5. An employee is entering the automated operation zone to do a maintenance task, and is detected real-time by an operations safety monitoring algorithm.	**Person detection**. On-board sensors, sensors in infrastructure, safe fleet and object supervising system track persons and initiate stop function, if separation distance between the person and autonomous machine is too short.
6. The operations safety monitoring algorithm send the ’people on route’ event information to machine/fleet control system.	**Safe route reservation.** Navigation keeps the loader at the reserved route and other autonomous vehicles out of the route.
7. Machine lowers the speed and prepares to encounter people on the route, employee is alerted about approaching machine with information about the route conflict/safe place to go.	**Reduced speed.** The speed of the autonomous machine is reduced to give persons more time to avoid collision and more time to the mobile machine to stop before collision.
8. The employee goes to a safe place and clears the alert towards the operations safety monitoring system.	**Person position monitoring.** Acknowledgement command and person tracking to verify that there are no persons at the hazardous zone.

4.2.1 Communication related to safety functions

Each machine must have emergency stop (some exceptions) (ISO 13850, [15]) and therefore wireless connection for the emergency stop must be established. There are also messages, which can be hazardous, if they fail. Here is list of critical messages mainly from fleet management to machine from standard ISO 17757:2019:

- a) safety critical signal not delivered, inability to stop the machine remotely or in an emergency,
- b) a lack of access to situational awareness information,
- c) inaccurate terrain data,
- d) lost or delayed command input,
- e) insufficient intersection control,
- f) loss of machine coordination,
- g) loss of derate information (e.g. delay of log information),
- h) lost or delayed hazard information,
- i) inaccurate position (due to lacking communication),

- j) inaccurate planning information,
- k) inaccurate personnel tracking,
- l) loss of remote ability to activate the fire protection system and
- m) erroneous control message.

The minimum requirement for emergency stop is PL c according to Emergency stop function standard ISO 13850 [15]. According to ISO 3691-4 “Driverless Industrial Trucks and their systems” emergency stop performance level requirement is PL d, which is applied here [14]. Messages mentioned at the list of critical messages (see above) can have requirement PL d, but the standard ISO 17757 does not give PL estimations. The decision about PL requirement needs to be done according to Figure 6 risk graph for each safety function separately. The communication related to emergency stop is assigned to PL d and other safety functions may have lower PL, but the system may be less complicated if all safety functions are applying the same wireless communication have similar requirements. On aspect is maximum response time for the safety functions. If the maximum response time is exceeded, then a predefined safety function is executed, i.e. usually stopping the mobile machine. Figure 22 shows an example of messages, which can be safety-critical. There is an estimated PL for each safety function. The PL is picked up from standard ISO 3691-4:2020 [14], if there has been a similar case and otherwise the PL is an educated estimation. The example shows that different safety functions can have different PLs. The PL values are just an example and they should not be considered as a requirement in another case.

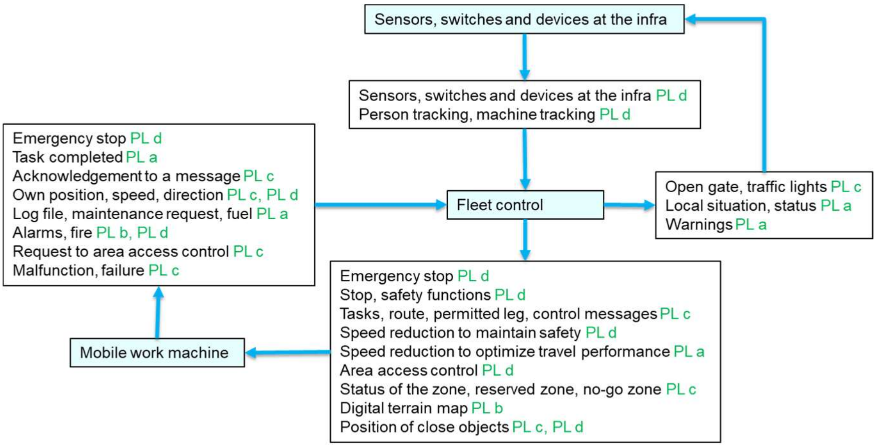

Sensors, switches and devices at the infra
Sensors, switches and devices at the infra PL d
Person tracking, machine tracking PL d
Emergency stop PL d
Task completed PL a
Acknowledgement to a message PL c
Own position, speed, direction PL c, PL d
Log file, maintenance request, fuel PL a
Alarms, fire PL b, PL d
Request to area access control PL c
Malfunction, failure PL c
Fleet control
Open gate, traffic lights PL c
Local situation, status PL a
Warnings PL a
Mobile work machine
Emergency stop PL d
Stop, safety functions PL d
Tasks, route, permitted leg, control messages PL c
Speed reduction to maintain safety PL d
Speed reduction to optimize travel performance PL a
Area access control PL d
Status of the zone, reserved zone, no-go zone PL c
Digital terrain map PL b
Position of close objects PL c, PL d

Figure 22. An example of messages, which can be more or less safety-critical.

4.2.2 Person detection

Here the sensors for person detection are mainly on board the machine, but some sensors can be also stationary in the infrastructure. The person/object detection sensors aim to stop the mobile machine (or reduce the speed) if proceeding the speed and direction would cause a collision. In some cases the detection sensors increase situational awareness and they are then not part of safety stop function and the PL requirement can be different. The PL requirements apply for each complete safety function and not only for separate sensors. The required PL can be achieved also by using sensor fusion (see IEC TS 62998-1:2019). There are several aspects to consider with respect to the sensor and complete system capability (see IEC TS 62998-1:2019 and ISO 17757:2019):

- sensor capability to cover specific zone, detection range,
- sensor fusion, system capability to cover the safeguarded zone without blind spots,
- detection dependability, reliability, accuracy, standard deviation of measurements, uncertainty of measurements,
- dependability under environmental conditions (water, dust, etc.), lighting, detection of poor environmental conditions and possibility to deny autonomous use in poor conditions,
- vibration and swaying of the detection fields (due to machine movements and terrain shapes).

Also objects and terrain affect the uncertainty of detection:

- object properties, like surface, colour, size, dimensions compared to detection zone (e.g. object dimensions above or below the detection zone), speed and relative speed of objects,
- other obstacles behind, beside or in front of the object,
- background, terrain shapes, blind spots due to inclined terrain.

The PL requirements for the safety functions:

- PL of each safety function is assigned,
- PL can be assigned according to functional safety standards: risk graph (ISO 13849-1:2015), matrix (IEC 62061:2021) or table (ISO 19014-1:2018) or
- PL can be achieved by comparing the case (safety function) to examples of type C standards.

Risk graph according to ISO 13849-1 is presented at Figure 6. According to the risk graph severity is 2 (high), frequency and exposure 1 (low), when the frequency worker presence at the hazardous zone is less than once per 15 min, and possibility of avoiding hazard is scarcely possibly (2). The result of this quick estimation is typically PL d. Similar result (PL d = SIL 2) is got also using the IEC 62061 method (see Figure 7).

Standard ISO 3691-4:2020 [14] presents PL requirements for driverless industrial truck safety functions and the requirement for person detection is PL d. Driverless industrial trucks are used in quite stable indoor applications, where the sensors are more reliable than in outdoor applications. However, the outdoor/indoor dilemma should not affect PL assignment, but it affects the selection of sensors, where specific sensors can be used.

4.2.3 Safe route reservation

Navigation keeps the loader at the reserved route. The fleet management keeps other moving autonomous vehicles out of the route. If the navigation fails or other vehicles access the route then collision is possible unless other safety functions can prevent the collision. “Safe route” safety function can be an additional safety function, which can lower the risk of collision especially with other autonomous vehicles. Also traffic lights, walkways and virtual area access control can be economical ways to control safe routes, if everybody would know and obey the rules. The autonomous vehicles are supposed to keep their permitted routes according to the reliability requirements (see PFH_D at section 2.1) related to the PL. One question is: can we trust on manual vehicles and pedestrians or should we limit their access to the autonomous zone during autonomous drive. The limitations are usually needed.

The required PL depends on the role of the safety function and on complete system. The required PL is then typically something between PL b to PL d.

4.2.4 Reduced speed

Reduced speed is applied from safety viewpoint to $^{a)}$ give humans more time to avoid collision or $^{b)}$ give the mobile machine more time to stop quickly enough to avoid collision.

- a) If the aim is to give humans more time to avoid collision, the idea is to the change the parameters of Figure 6. The only parameter that the reduced speed affects is “possibility to avoiding hazard” (from 2 to 1). However, it may be difficult to justify it and if it can be justified, the result would be only change (e.g.) from PL d to PL c. Standard draft ISO/DIS 13849-1.2:2021 presents that one aspect (among others) to lower the parameter, i.e. human has possibility to avoid collision, is that the machine speed should be below 1 m/s.
- b) Reduced speed can enable reduced stopping distance (and time) of the mobile machine. When reduced speed and stopping distance are linked with each other, it can be justified to have similar safety requirements for the reduced speed function and the stopping function, since then the actual safety function is adequate separation distance, which includes both stopping and reduced speed. This kind of reasoning may depend on the case.

The PL requirement can be achieved from Figure 6 as follows:

- Severity is serious (S2), since worst case severity is death (collision to a pedestrian) or at least bone fraction,
- frequency is seldom (F1), since the frequency of human presence is, typically, less than 1/15 min,
- possibility to avoiding hazard is scarcely possible (P2), since speed > 1 m/s, and the movements are not always predictable,
- the result is PL d according to the Figure 6 graph.

Also ISO 3691-4 “Driverless Industrial Trucks and their systems” standard recommends PL d for speeds above 0,3 m/s.

4.2.5 Person position monitoring and acknowledgement

The person position monitoring and acknowledgement safety function is based on two systems: acknowledgement and person tracking. The acknowledgement safety function is applied to verify that a specific person is not at hazardous zone or he is at reserved safe zone. The person, who is acknowledging (e.g. pressing pushbutton) is at safe position. Depending on the system it may be necessary also to identify the person, in order to verify uncertain tracking information. In this case all persons and manual vehicles at the hazardous zone need to be tracked, in order to keep separation distance to autonomous mobile machines adequate.

The monitoring technology can be on-board the mobile machines and persons or stationery at the infra of the mine. The monitoring may also include reasoning to location information, which is related to feasibility, reliability and accuracy. For example, missing location information leads to increasing size of an uncertain zone, where a person can be undetected. Also a rapid location information change or an impossible location information may indicate a sensor failure or disturbance. The idea is that all moving autonomous mobile machines have adequate separation distance to persons and critical objects. The autonomous mobile machine must be able stop within the separation distance before any collision.

Manual or automated acknowledgement can be arranged safely (PL d) for example with manual switches or light curtains. It is more difficult to realise safe (PL d) location information especially with on-board sensors. The PL requirement for person position monitoring and acknowledgement safety function needs to be assigned using Figure 6. The result is PL d and the reasoning resembles the “reduced speed” safety function case.

It is also possible to apply safeguarding supportive system, according to standard ISO/TR 22053:2021. The device is mobile (like mobile phone app) and it can be applied, for example, to person identification, localization, information deliverer (display or voice; task list, situational reporting), permission asking (access a zone or perform a task) and acknowledgment. The safeguarding supportive system is newly defined device, and applications may be still rare. It may be difficult to realise e.g. PL d safety functions with the safeguarding supportive system, but for identification and situational awareness functions it can be applicable.

5 Conclusions

As defined in IEC 62061:2021, functional safety means part of the overall safety of the machine and the machine control system that depends on the correct functioning of the safety-related control system and other risk reduction measures[10]. The machinery system has many other safety aspects as functional safety, but this document is focusing on functional safety and communication in mining environment. Functional safety aspects become essential, as the system has plenty of safety functions. Functional safety of communication is essential, when safety functions are sent via communication systems. Since there are mobile machines, the communication needs to be partly wireless and 5G is suggested here. Mining environment means that in some cases the distance between communication repeaters is short (e.g. 20 m), because radio waves stop effectively in the rock and line-of-sight between repeaters is often required. The autonomy of machines means that large share of the safety functions are initiated automatically.

Functional safety is related to safe successful communication. However, stopping a machine can be a safety function and it is initiated if no acceptable messages are received and then the machine turns to safe state. This can happen for example if the autonomous machine is too far from repeaters. Dangerous communication failures are related to situations, where message is corrupted and its meaning has changed or correct messages are received in wrong order (like start and stop). There are protective measures against message errors and the probability of an error can be low, such as, the share of communication system dangerous failures per hour is less than 10^{-8} related to SIL 2 / PL d functions and the probability of the dangerous failures per hour for complete safety function is less than 10^{-6}.

Safe communication is achieved when timeliness, authenticity, integrity and to some extent also cybersecurity aspects are considered adequately. Values for safe integrity (no changes compared to the original message) can be calculated as shown in previous paragraph, timeliness is related to accepting only messages received in correct time window and authenticity (addressing and inserting errors related to wrong sender, receiver or operation mode). Cybersecurity issues can be related to functional safety, if a malicious attack can threat operation of safety functions. Such aspects can be related to integrity, availability or authenticity.

Quite often cybersecurity issues are related to confidentiality, which is usually not a safety issue.

Safety functions of autonomous mobile machines can be similar to manual machines, but there are many safety functions, which are applied to safeguard autonomous operations. Stopping is applied as a safety function, when there is a hazard and stopping can eliminate it or uncertain situation. There can be several functions, which are related to stopping like, emergency stop, braking and speed control setpoint to zero. Reduced speed is applied to reduce the risk of a collision by giving others time to move away, shorten stopping time and distance to match capabilities to detect objects and brake before collision. Also steering is an important safety function, since if the machine loses the correct direction it should be going a collision is possible. Steering is more important function, when the machine speed is high. There are also safety functions, which are related to control of implements, like boom or communication with other systems, like area access control. A group of safety functions are related to situational awareness of the machine and other machines or persons. These can be sensors, which can for example detect or track persons, or systems, which can inform the location of the machine.

In the future, especially situational awareness of the autonomous mobile machines is supposed to advance clearly, as better safety sensors for object detection and communication systems for informing others about machine intentions are developed.

Acknowledgements

This research has been conducted as a part of the Next Generation Mining (NGMining) project. We gratefully acknowledge the funding of Business Finland and the contributions of participating companies.

References

[1] Britannica. tunnels and underground excavations. Retrieved 8.11.2021. https://www.britannica.com/technology/tunnel

[2] CEN ISO/TR 22100-4:2020. Safety of machinery. Relationship with ISO 12100. Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects. 23 p.

[3] Cyber Resilience Act. Brussels, 15.9.2022. Proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. 103 p. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

[4] EN 60204-1. 2018. Safety of machinery - Electrical equipment of machines - Part 1: General requirements. 150 p.

[5] Matteo Giaconia, Xavier Bignalet. 2021. Demystifying ISA/IEC 62443 and Secure Elements. AN3983. Microchip. 17 p. Retrieved 13.7.2021. http://ww1.microchip.com/downloads/en/Appnotes/Demystifying-ISA-IEC-62443-and-Secure-Elements-DS00003983.pdf

[6] GMG. 2019. Underground mine communications infrastructure guidelines Part III: General guidelines. Global Mining Guidelines Group. 54 p. Underground Mine Communications Infrastructure (gmggroup.org)

[7] Jean-Pierre Hauet. 2012. ISA99/IEC 62443: a solution to cyber-security issues? ISA Automation Conference – Doha (Qatar) - 9 & 10 December 2012. 52 p. Retrieved 13.7.2021. http://www.kbintelligence.com/Medias/PDF/ISA_Doha_hauet.pdf

[8] IEC 61508-2:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems. 167 p.

[9] IEC 61784-3:2010 Digital data communication for measurement and control – Part 3: Profiles for functional safe communication in industrial networks. (obsolete) 59 p.

[10] IEC 62061. 2021. Safety of machinery – Functional safety of safety-related control systems. 143 p.

[11] IEC/TS 62443-1-1:fi:2009. Industrial communication networks. Network and system security. Part 1-1: Terminology, concepts and models. 153 p.

[12] ISO 5010. 2019. Earth-moving machinery — Wheeled machines — Steering requirements. 18 p.

[13] ISO 12100. 2010. Safety of machinery. General principles for design. Risk assessment and risk reduction. 77 p.

[14] ISO 3691-4:2020. Industrial trucks — Safety requirements and verification — Part 4: Driverless industrial trucks and their systems. 84 p.

[15] ISO 13850:2015. Safety of machinery — Emergency stop function — Principles for design. 11 p.

[16] Machinery Directive 2006/42/EC. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast). 63 p.

[17] Timo Malm, Toni Ahonen & Tero Välisalo. 2018. Risk assessment of machinery system with respect to safety and cyber-security. VTT Research Report VTT-R-01428-18. 26 p.

[18] SFS-EN ISO 13849-1. 2015. Safety of machinery Safety-related parts of control systems Part 1: General principles for design. Finnish Standards Association SFS. 193 p.

[19] SFS-EN ISO 13855:2010. Safety of machinery. Positioning of safeguards with respect to the approach speeds of parts of the human body. 82 p.

[20] SFS-EN ISO/IEC 27000:2020. Information technology. Security techniques. Information security management systems. Overview and vocabulary

[21] SFS-ISO/IEC 27005:2018. Information technology. Security techniques. Information security risk management. 55 p.

Series title and number

VTT Technology 412

Title	**Autonomous mobile machines in mines using 5G enabled operational safety principles**
Author(s)	Timo Malm, Daniel Pakkala & Eetu Heikkilä
Abstract	This report presents general functional safety principles and how they can be implemented to mining environment. Functional safety is related to safety functions and operations applying sensors, control systems and actuators. Safe operation in mines requires good situational awareness, navigation capabilities and communication between units. Examples of common safety functions of autonomous mobile machines in mines are described. In practice, many functional safety features are needed to ensure overall functional safety requirements. One new option for communication is 5G technology. Safety and cybersecurity risks of communication are presented in general level.
ISBN, ISSN, URN	ISBN 978-951-38-8774-2 ISSN-L 2242-1211 ISSN 2242-122X (Online) DOI: 10.32040/2242-122X.2023.T412
Date	March 2023
Language	English, Finnish abstract
Pages	65 p.
Name of the project	Next Generation Mining (NGMining)
Commissioned by	
Keywords	Functional safety, mining operations, autonomous mobile machines
Publisher	VTT Technical Research Centre of Finland Ltd P.O. Box 1000, FI-02044 VTT, Finland, Tel. 020 722 111, https://www.vttresearch.com

Julkaisun sarja ja numero

VTT Technology 412

Nimeke	**Autonomiset liikkuvat työkoneet kaivoksissa hyödyntämässä toiminnallisen turvallisuuden ja 5G teknologian tuomia mahdollisuuksia**
Tekijä(t)	Timo Malm, Daniel Pakkala & Eetu Heikkilä
Tiivistelmä	Tämä raportti esittää toiminnallisen turvallisuuden periaatteita ja kuinka niitä voidaan soveltaa kaivosympäristössä. Toiminnallinen turvallisuus liittyy turvafunktioihin ja operaatioihin liittyen antureihin, ohjausjärjestelmään ja toimilaitteisiin. Turvallinen toiminta kaivoksissa edellyttää hyvää tilannetietoisuutta, navigointikyvykkyyttä ja kommunikointia järjestelmän osien välillä. Käytännössä monia toiminnalliseen turvallisuuteen liittyviä ominaisuuksia ja laitteita tarvitaan toteuttamaan toiminnallisen turvallisuuden vaatimukset. Raportissa kuvataan esimerkkejä autonomisten liikkuvien työkoneiden turvatoiminnoista. Myös kommunikoinnin turvallisuus- ja kyberturvallisuusriskejä kuvataan yleisellä tasolla. Yksi uusi mahdollisuus turvallisuuteen liittyvässä kommunikoinnissa on 5G.
ISBN, ISSN, URN	ISBN 978-951-38-8774-2 ISSN-L 2242-1211 ISSN 2242-122X (Verkkojulkaisu) DOI: 10.32040/2242-122X.2023.T412
Julkaisuaika	Maaliskuu 2023
Kieli	Englanti, suomenkielinen tiivistelmä
Sivumäärä	65 s.
Projektin nimi	Next Generation Mining (NGMining)
Rahoittajat	
Avainsanat	Toiminnallinen turvallisuus, liikkuvat työkoneet, kaivoskoneet
Julkaisija	Teknologian tutkimuskeskus VTT Oy PL 1000, 02044 VTT, puh. 020 722 111, https://www.vtt.fi/

Autonomous mobile machines in mines using 5G enabled operational safety principles

This report presents general functional safety principles and how they can be implemented to mining environment. Functional safety is related to safety functions and operations applying sensors, control systems and actuators. Safe operation in mines requires good situational awareness, navigation capabilities and communication between units. In practice, many functional safety features are needed to ensure overall functional safety requirements. Examples of common safety functions of autonomous mobile machines in mines are described. Also safety and cybersecurity risks of communication are presented in general level. One new option for communication is 5G technology.

ISBN 978-951-38-8774-2
ISSN-L 2242-1211
ISSN 2242-122X (Online)
DOI: 10.32040/2242-122X.2023.T412