Timo Malm*, Daniel Pakkala and Eetu Heikkilä

Autonomous mobile machines in mines and 5G enabled safety principles

Abstract: There is a strong need to have autonomous or semi-autonomous mobile machines in mines. They enable increased productivity and improved safety, as workers do not need to be continuously present in the most dangerous areas of the mine. Several strategies are needed to minimize risks related to collisions. Fences or virtual fences can provide a good safety level, but they are laborious to configure in a continuously changing environment. Tracking of all persons and vehicles, combined with on-board sensors for object detection, could be able to provide dynamic safety without compromising productivity. However, capability in all environmental conditions is not yet adequate. Traffic rules are good additional means to improve safety, but not sufficient for autonomous systems. Almost always, good communication is required between machines, operators and infrastructure. Lost integrity or availability of communication can have impacts on safety and production. 5G introduces new possibilities to build reliable and quick networks.

Keywords: Functional safety, mining operations, autonomous mobile machines

***Corresponding Author: Timo Malm** VTT Technical Research Centre of Finland Ltd., E-mail: timo.malm@vtt.fi

Daniel Pakkala, VTT Technical Research Centre of Finland Ltd., E-mail: Daniel.pakkala@vtt.fi

Eetu Heikkilä: VTT Technical Research Centre of Finland Ltd., E-mail: eetu.heikkila@vtt.fi

1 Introduction

This paper focuses on new safety principles enabled by 5G, pointing out risks, mitigation strategies, functional safety principles and communication safety principles. A comprehensive study will be available in VTT Technology publication "Autonomous mobile machines in mines using 5G enabled operational safety principles" [1]. This paper introduces selected ideas of safety functions, which can be applied with autonomous mobile machines in mines. The focus is on cases where 5G communication is applied.

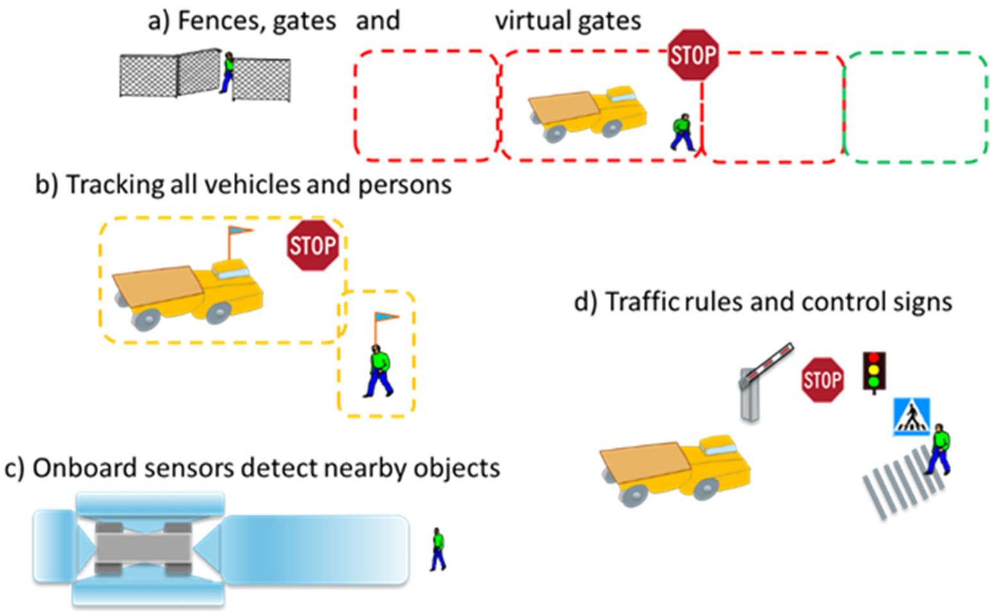

Figure 1 Strategies to mitigate autonomous mobile machines collisions.

The focus of this article is on collision avoidance and related communication. 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. Also, a collision of two driverless vehicles can have hazardous consequences in mines.

The strategies to mitigate risks are here divided into 4 groups presented in Figure 1: a) fences, gates and virtual gates/fences, b) tracking of persons and vehicles, c) on-board sensors to get an overview of objects in the vicinity, d) traffic rules. To make a safe mobile machinery system in mines often several mitigating strategies are needed. Communication between machines, operators, fleet control and infrastructure, is necessary in all of the strategies. Sensors onboard the mobile machine (case c) at the figure) could operate for a while without communication, but there must be means to stop all machines and for emergency stop, communication is required. [1]

One aspect related to communication is that safety means are concentrated on safety layer, which is above actual communication protocols [2]. In many cases, messages need to be sent via several stations using wireless or wired communication. The logical communication between safety layers of two nodes is considered black channel, which may have different safety capabilities, which can be difficult to evaluate in a dynamic environment.

2 Methods

The research was done in NGMining project, and the ideas of safety strategies have emerged in literature, discussions, presentations and workshops in the project. There have been several case studies in the project related to communication (mainly 5G). The results are gathered more detailed to VTT Technology publication 412: Autonomous mobile machines in mines using 5G enabled operational safety principles [1].

3 Communication and safety in mines

Communication in mines

Wired high-speed communication is usually arranged from surface to specific control rooms, which can provide wired or wireless communication to other parts of the mines. Radio waves cannot go through rock and therefore line-of-sight contact between radio stations is needed or so-called leaky feeders (cable radiates/communicates to its vicinity) are applied.

It is important to choose communication topology according to mine structure and environment, in order to minimize consequences of failures. Common communication ideal topology models in mines are :

- bus topology, which has all nodes connected to a single linear connection,
- ring topology, which has all nodes connected to a ring,
- mesh topology, which has nodes, which are connected to all the other nodes (in the vicinity),
- star topology, which has central hub, where other nodes are connected via dedicated path.

Real topologies are combinations of ideal topology models.

Currently Wi-Fi is very common technology for wireless communication in mines, due to low purchase price and general knowledge. However, in mines reliability and, especially, availability is important property due to very expensive unavailability costs. 5G has some advantages related to reliability. Here are some reliability-related properties of 5G compared to Wi-Fi [1]:

- 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 need to be placed at locations, where is long line-of-sight and therefore possibility to lower the number of stations can be small.

Safety of communication

Currently, it is very difficult to make safe mine automation by applying only on-board systems (sensors, warning devices). Of course, there are also other than safety needs for communication. Safety-related needs for communication are for example:

- safety messages, like emergency stop, fire alarm, acknowledgements, failure/malfunction information,
- area access control requests, permissions and commands,
- tunnel blocked/reserved or digital terrain map,
- situational awareness is needed for workers to know, where machines are
- situational awareness for fleet control to know status and where (position, speed and direction) autonomous and manual mobile machines and persons are,
- traffic lights, open/close gate.

According to Machinery Directive: “For cableless control, an automatic stop must be activated when correct control signals are not received, including loss of communication” [4]. Autonomous mobile machines were not yet defined when Machinery Directive was published (2006) and there was no need to mention exceptions. According to new proposal of Machinery regulation: “For wireless control, a failure of the communication or connection or a faulty connection shall not lead to a hazardous situation” [5]. Similarly, standard ISO 17757 Autonomous and semiautonomous machine system safety requires risk assessment and safe state, which may mean also other functions than stopping of the machine [6]. There can be places in mines, where wireless communication is not available. If there is no communication, then for example emergency stop command cannot be delivered and risk assessment is needed to assess has the mobile machine adequate situational awareness to continue the operation and on which conditions. The detection capability of the machine sensors needs to be adequate without blind spots and safety performance of the stopping function (including sensors, logic and actuators) needs to be typically PL d (Performance Level) according to ISO 13849-1. The safe performance of the autonomous mobile machine is difficult to prove if the communication has failed and therefore operation can continue only for a short time (defined by risk assessment). Actually, it can be a matter principle, may the autonomous mobile machine continue operation, if there is no possibility to stop it remotely.

Safe communication structure

Figure 2 shows how communication between two safety layers can be divided into logical connection and black channel. The failures of the black channel are not defined and there can be failures, or the failures can be detected, but the safety layer does not trust the possible protective means. Safety layer builds up its own protective shield, which covers timeliness, authenticity, data integrity and if needed, also security. According to OSI model (Open Systems Interconnection model) communication is operated through standardized layers: physical layer, data link layer, network layer, transport layer, session layer, presentation layer, application layer and above them is safety layer [1].

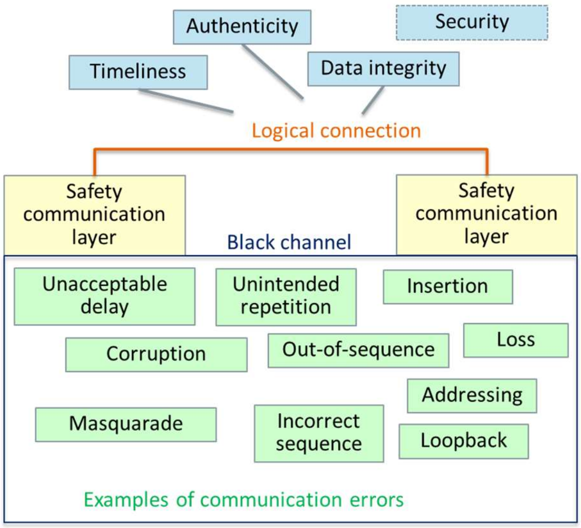

Figure 2. Black channel from a functional safety communication profile perspective [1], [2].

Figure 3 shows an example how message is first built up at the safety communication layer, it is delivered through lower layers and internal communication link to the gateway. Next the message goes through fieldbus and possible other communication media to the target node and its layers finally to the safety layer. Safety layer checks authenticity, integrity and timeliness. Failed messages are discarded. Failed message is often detected before safety layer and the message is asked to be repeated.

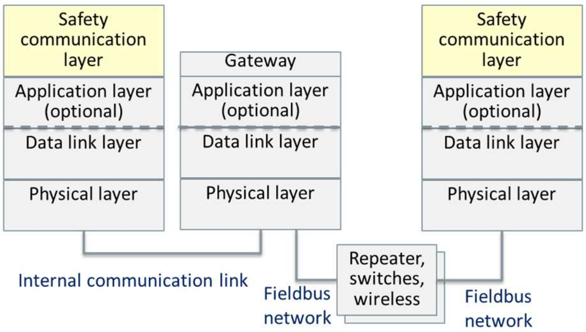

Figure 3. An example of black channel communication [1], [2].

The safety of communication and safety layer relies very much on timeliness, authenticity and data integrity of messages. Actually, the system needs to have adequate means to control defined errors/threats: repetition, deletion, insertion, incorrect sequence, corruption, delay and masquerade (and sometimes addressing, depending on error definitions). [1], [2]

Cybersecurity or security are described in different standards than functional safety issues. Cybersecurity issues can be controlled in several layers and therefore it does not have to be on safety layer. However, properties like integrity and in some cases, availability are common for both cybersecurity and functional safety. In some cases, there can be contradictory objectives for functional safety and cybersecurity. Uncertain communication leads often to stopping of the machine due to safety reasons, but from cybersecurity objective point of view stopping means unavailability, which should be avoided. On the other hand, cyber-attack may lead to countermeasures, which limit access to communication media. However, from functional safety viewpoint, the safety messages may not be limited or otherwise the complete system needs to be stopped.

The machine automation designers select the communication system according to requirements. This means that system needs to fit to the environment, performance is adequate for the application and safety performance level (PL) is according to made PL assignment for each safety function.

4 Results and conclusions

The safety and availability of communication are important factors in mines, especially in future digitalized mining, where physical mining process are increasingly automated and executed by teleoperated or fully autonomous mining machines. In highly digitalized and automated mining operations the availability of communication had key role in ensuring continuity of production at the mining site. Safety issues are often related to integrity of messages and there are requirements for integrity, for example, safety integrity level 2 (SIL) (=PL d). Availability requirements can be related to safety, but typically loss of communication leads to a safe state i.e., stopping. The time to endure communication delays needs to be defined in risk assessment. For example, in bridge cranes the acceptable time delay is typically 500 ms and similar value can be applied in mobile machines too. Although availability issues do not usually cause safety issues, a long-lasting communication loss can cause huge financial losses due to lost production.

The communication systems in mines are changing continuously as new tunnels are built. Therefore, some parts of the communication can be difficult to be defined as white channel according to IEC 61508-2 [7]. Safety measures can be done also in sender and receiver in their safety layer. This means that the communication is made in black channel, which includes 5G. Since 5G is inside the black channel, its properties are not considered in safety assessment of the communication channel. However, reliable communication affects the share of messages that the safety layer accepts and furthermore it has an effect on dependability in general.

A relatively new category of risks in mine communication are related to cybersecurity. The mines are usually deep underground and therefore general cybersecurity threats/attacks are rare. However, it is wise to consider vulnerabilities of communication and control systems to avoid cybersecurity issues.

Strategies and principles to mitigate collision risks need to be chosen. Most of the strategies require safety functions, which are related to control systems and communication. Safety functions are related to functional safety, including safety integrity levels (SIL) and performance levels (PL). Furthermore, control systems are related also to cybersecurity and dependability in general.

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.

5 Bibliography

[1] Malm T., Pakkala D., Heikkilä E. 2023 . W Autonomous mobile machines in mines using 5G enabled operational safety principles. VTT Technology 412. 65 p. https://cris.vtt.fi/en/publications/autonomous-mobile-machines-in-mines-using-5g-enabled-operational-

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

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

[4] 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.

[5] Proposal for a Regulation of the European Parliament and of the Council on machinery products. 25.1.2023. https://data.consilium.europa.eu/doc/document/ST-5617-2023-INIT/EN/pdf

[6] ISO 17757 2019 2019. Earth-moving machinery and mining — Autonomous and semiautonomous machine system safety. 36.

[7] 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.