Autonomous haulage systems in the mining industry: cybersecurity, communication and safety issues and challenges

Gaber, T, El Jazouli, Y, Eldesouky, E and Ali, A

http://dx.doi.org/10.3390/electronics10111357

electronics

MDPI

Review

Autonomous Haulage Systems in the Mining Industry: Cybersecurity, Communication and Safety Issues and Challenges

Tarek Gaber [1,2], Yassine El Jazouli [3], Esraa Eldesouky [1,4] and Ahmed Ali [4,5,*]

1 Faculty of Computers and Informatics, Suez Canal University, Ismailia 41522, Egypt; t.m.a.gaber@salford.ac.uk (T.G.); em.eldesouky@psau.edu.sa (E.E.)
2 School of Science, Engineering, and Environment, University of Salford, Manchester M5 4WT, UK
3 Suncor Energy, 111 5th Ave. SW, Calgary, AB T2P3Y6, Canada; Yassine.el@networksharks.ca
4 Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al-kharj 11942, Saudi Arabia
5 Higher Future Institute for Specialized Technological Studies, Cairo 3044, Egypt
* Correspondence: a.abdalrahman@psau.edu.sa

Abstract: The current advancement of robotics, especially in Cyber-Physical Systems (CPS), leads to a prominent combination between the mining industry and connected-embedded technologies. This progress has arisen in the form of state-of-the-art automated giant vehicles with Autonomous Haulage Systems (AHS) that can transport ore without human intervention. Like CPS, AHS enable autonomous and/or remote control of physical systems (e.g., mining trucks). Thus, similar to CPS, AHS are also susceptible to cyber attacks such as Wi-Fi De-Auth and GPS attacks. With the use of the AHS, several mining activities have been strengthened due to increasing the efficiency of operations. Such activities require ensuring accurate data collection from which precise information about the state of the mine should be generated in a timely and consistent manner. Consequently, the presence of secure and reliable communications is crucial in making AHS mines safer, productive, and sustainable. This paper aims to identify and discuss the relation between safety of AHS in the mining environment and both cybersecurity and communication as well as highlighting their challenges and open issues. We survey the literature that addressed this aim and discuss its pros and cons and then highlight some open issues. We conclude that addressing cybersecurity issues of AHS can ensure the safety of operations in the mining environment as well as providing reliable communication, which will lead to better safety. Additionally, it was found that new communication technologies, such 5G and LTE, could be adopted in AHS-based systems for mining, but further research is needed to considered related cybersecurity issues and attacks.

Keywords: cybersecurity; autonomous haulage systems; operating technology; mining industry; cyber-physical systems; communication; safety

Citation: Gaber, T.; El Jazouli, Y.; Eldesouky, E.; Ali, A. Autonomous Haulage Systems in the Mining Industry: Cybersecurity, Communication and Safety Issues and Challenges. *Electronics* **2021**, *10*, 1357. https://doi.org/10.3390/electronics10111357

Academic Editor: Victor A. Villagrá

Received: 1 May 2021
Accepted: 2 June 2021
Published: 7 June 2021

1. Introduction

Since the launch of Industry 4.0, smart machinery and intelligent services have been unveiled, including quality-controlled systems [1]. Industry 4.0 redirected organizations' perspective on technology along with its role in developing a viable business model that increases their profits. Industry 4.0 aims to integrate Operating Technology (OT) and Information Technology (IT) ecosystems to cope with current business requirements, such as information sharing and controlling. In the heart of Industry 4.0, Cyber-Physical Systems (CPS) were shown to be a revolutionary development. CPS are "engineered systems that integrate information technologies, real-time control subsystems, physical components and human operators to influence physical processes by means of cooperative and (semi)automated control functions" [2]. CPS combine real-time communications and

computer processes with physical world applications to enable autonomous and/or remote control of physical systems [3].

Mining is an industry that inherits the full advantage of Industry 4.0 by using cutting-edge driverless vehicles called Autonomous Haulage Systems (AHS) or Autonomous Haulage Trucks (AHT). These trucks can carry up to four hundred tons of ore and accurately transport it without human interaction. AHS is the state-of-the-art in the mining industry for autonomous vehicles. Since their first system development endeavor in Chile in 2005, AHS have attracted attention in the last decade from haulage truck manufacturers such as Caterpillar and Komatsu. The successful reputations of existing autonomous mines around the world notably increased the demand for AHS in surface mining during the last few years. Komatsu America has reported that its FrontRunner system has achieved a new milestone record of more than two billion tons of material that was transported autonomously at CODELCO's Gabriela Mistral in Chile since the opening of its first autonomous copper mine in 2008 [4]. Generally, Autonomous Trucks (ATs) have been designed to reduce the vulnerability to the risk of equipment contact with auxiliary equipment or Equipped Manual Vehicles (EMVs).

According to the definition of CPS above, the AHS could be seen as a kind of CPS. The AHS equipment exceedingly relies on wireless communications, including object avoidance/detection systems, Global Positioning Systems (GPS), e.g., GNSS, and artificial intelligence. Inside the AHS intelligence system (i.e., FrontRunner for Komatsu and Command for Caterpillar), all data obtained are compiled so that the software can make a suitable decision. Calculating the maximum speed allowed to a nearby equipment or the estimated time for an AT to break are possible decisions. Thus, determining the exact location of every AT and EMV is mandatory for the trucks to prevent accidents, which increases safety and decreases the maintenance or replacement cost [5]. ATs have demonstrated notable fuel consumption performance as a result of their driving consistency. They can operate on a 24/7 schedule with no idling time as there is no shift change and no breaks required. Manual truck operators can affect 35% of fuel economy whereas ATs can improve fuel usage by 4% with 25–50% reduced idle time [5].

With the use of the AHS, several mining activities have been strengthened due to increasing the efficiency of operations. Such activities require ensuring accurate data collection from which precise information about the state of the mine should be generated in a timely and consistent manner. Consequently, the presence of secure and reliable communications is crucial in making AHS mines safer, productive, and sustainable. The availability and security issues of communication of AHS the mine environment will be discussed below.

The availability of communication is an essential service in AHS systems. To the best of our knowledge, the current AHS mines rely entirely on wireless communication [6], which employs standard 802.11 Wi-Fi technology operating in the unlicensed spectrum. In the meantime, technologies (e.g., Wi-Fi) were deemed unfit for industrial communications due to the lure of Industry 4.0, and the flexibility offered by these technologies made Wi-Fi attractive for AHS solutions. Specifically, ATs require seamless connectivity to the network at all times [7]. The geographical challenges and the nature of CPS (AHS) running in the mine make wireless communications the only possible way to keep track and ATs connected. Yet, these wireless technologies lead to a set of challenges—for example, frequency interference, channel utilization, and signal jamming. Furthermore, some special design concerns should be considered, such as signal propagation and dynamic topology as the mine keeps growing, so as to obtain efficient and stable contact.

With the integration of OT and IT as in the case of AHS, information sharing becomes more susceptible to disclosure, intrusion, and other cybersecurity issues and attacks. As shown above, AHS can be considered as a CPS system, and thus the former can be integrated with OT using mechanisms that are vulnerable to malicious attacks such as Wi-Fi De-Auth attacks [8], GPS attacks [9], and camera attacks [9,10]. Thus, safety remains an area of concern as being targeted by traditional cyber-attacks due to the similarities in

infrastructure with the conventional IT environment. The authors of [11] emphasize that a lack of security can lead to equipment damage, loss of production, severe injuries, and fatalities, thus greatly endangering safety.

In this paper, within the mining environment, we aim to identify and discuss the relation between safety of AHS in the mining environment and both cybersecurity and communication. We argue that addressing cybersecurity issues of AHS can ensure the safety of operations in the mining environment, and that providing reliable communication leads to a better safety. Specifically, we surveyed the literature aiming to study the relation between (1) cybersecurity and safety and (2) communication and safety of AHS in the mining environment. In this paper, the term *safety* refers to the control of any hazards in order to avoid human injury and mechanical risk. The survey's main objective is to identify the pros and cons of the published work at this point as well as to highlight some open issues for further investigation regarding this field of study.

This paper is organized as follows. Section 2 summarizes the literature review related to safety accompanied by cybersecurity and communication. In Section 3, future directions and open issues related to cybersecurity, communication, and safety in AHS are discussed. Finally, the paper is concluded in Section 4.

2. Literature Review

In the literature review, we investigate AHS mines from three different angles, which are communication challenges, cybersecurity, and safety. We argue that the AHS environment is a subset of the industrial environment that faces similar challenges to other OT systems with some particularities to the mining environment (e.g., the terrain) and the associated elements with specific challenges that we try to resolve in this study. We also contend that business decision making is significantly affected by information shared between the industrial and IT environments, which invokes the problem of information accessing or sharing with untrusted networks, e.g., the Internet. We study the standard communication technologies that arise in the industrial environment and their drawbacks as well as the possibility to re-enforce them in order to make them more secure. Furthermore, we argue that if communication in the AHS environment is not secure and reliable, the safety of equipment can be impacted since safety is dependent on the availability of communication. Finally, we conclude that safety by association is a security service in the industrial environment, whereas a cyberattack can lead to disastrous consequences.

2.1. Relation between Cybersecurity and Safety in AHS

Security problems have increased and mutated with Industry 4.0; the security issues in the age of Industry 4.0 are discussed in [12]. In addition, the authors clarify how evolving innovations have brought new security risks to the industrial climate. In addition, the convergence of these technologies has provided a gap for new attack surfaces, such that applying unlicensed wireless communication to mining activities moved current hazards and challenges of the underlying technology to the OT ecosystem and introduced a potential for new attacks on the field equipment (AHS trucks).

CPS are dense heterogeneous systems that encompass various sensors and actuators connected to a pool of computing nodes [13]. Hence, a CPS machine works on perceiving and analyzing the surrounding physical environment. Accordingly, it acts appropriately based on the sensed data using intelligence decisions in an autonomous manner. As a result, ATs are classified as CPS networks, making them susceptible to the same type of OT attacks. These attacks might threaten communications, storage, actuators, computing nodes and perceiving sensors [14].

ATs are endpoints (e.g., sensors, actuators) connected to networks and communicating through a command center with different tiers of security. The authors of [15] address how the unawareness manipulation of logical and physical controls of devices is the most devastating effect of taking control of the endpoints, such as field equipment. A successful

attack on a CPS (e.g., MITM) could be catastrophic [14]. As a result, such attacks may lead to a loss of quality of services, data integrity/quality, as well as human life.

Since there are no predefined standards that constitute the precise handling of complex industrial environments, it is feasible to use the existing variety of standards and re-direct them for a specific purpose [12]. Yet, the integration of cybersecurity issues in an industry based on ad hoc structures is a naïve approach that can lead to misleading results. This is because a generic attack study may ignore the main security clues of the CPS, which aim to achieve a balance among usability, risk, cost, and convenience [13]. CPS could also be operating in a safe and controlled environment that is secured by other means. Furthermore, as attacks are generalized, defense perimeter modeling and Root of Trust (RoT) mechanisms are often overlooked [13].

Cybersecurity issues have posed a serious problem and complex threats to organizations looking to make the transition to engage in the Industry 4.0 model, according to [16]. The authors established three vulnerability factors in a cyber-physical infrastructure that may be exploited by cyber-attacks: physical, network, and computation. The potential of interfering with wireless network communication in the mining community through a subsequent survey is addressed in [12]. A successful wining attack can have a significant negative impact on service protection and availability (for example, one of the security CIA services). A solution called "security by design" is proposed by the authors of [14,15], which take into consideration several criteria of cybersecurity architecture. Feasibility, robustness, extensibility, as well as authentication, authorization, network enforced policy, and secure analytics are counted as security measures [15].

Another area of contention is the exchange of knowledge over dynamic networks in both industrial and non-industrial atmospheres (i.e., IT) given that the two atmospheres are geographically or logically isolated. In the age of Industry 4.0, data sharing between the OT and IT environments is essential for making the optimal business decisions (i.e., usually higher management is located in a different facility than current operations) [17]. However, this raises the vulnerability of such sensitive infrastructure, which can be exposed to untrustworthy networks and attacks. The dynamic nature of the CPS portion, such as a complex environment, necessitates a unique approach (i.e., considering cybersecurity and safety). Most data exchange methods, according to [17], are incapable of grasping high-dynamic scenarios in which several parties (i.e., vendors) cooperate to achieve a shared purpose, particularly where privacy is factored in. The same authors suggested a solution based on establishing a dynamic trust zone in which decisions are automatically made through identifying flows, evaluating them, and deciding whether to allow the flow or not [17]. Yet, this strategy increases concern about data protection and confidentiality in a multivendor setting. An additional RoT model is introduced in [13], where a heterogeneous and static environment is built to manage confidentiality problems such as key delivery instead of handling each individual variable. This is considered the most effective way to avoid confidentiality issues.

The protection of GPS positions against malicious attacks is one of the main concerns in AHS. Haulage trucks depend on GPS-derived positional coordinates, which are supplemented by a detailed map. In an essential feature in automated AVs, these driverless devices select the shortest routes to reach new locations even without prior knowledge, which gives rise to vulnerability from malware attacks. Ren et al. [9] demonstrated a number of realistic GPS attacks that were presented under two categories: spoofing and jamming. One of the most frequent GPS attacks is to deviate the correct location of the victims to an incorrect position (i.e., spoofing) by fabricating a spurious signal. Nulling, another advanced attacking mechanism, aims to cancel GPS signals by encrypting negative signals that could be used to launch stealthy attacks. Authors in [18] suggested a recent attack strategy that utilizes selected fake locations to direct the AHT into a predefined area, using Google Maps, for example. Unfortunately, the inefficient protection of GPS data can lead to catastrophic truck collisions, which is another safety concern in the AHS.

Furthermore, since the distinction between industrial and IT networks is becoming blurred, a need for a coordinated approach becomes evident. As shown in [19], applying a defense-in-depth strategy to the industrial fields is emphasized since we now have the capability of mounting new threats that were not inherent in OT. These tactics aim to improve the overall system's CIA security triad (i.e., confidentiality, integrity, and availability). This can be accomplished by enabling the implementation of solutions such as RoT introduced in [13], which was previously addressed. Meanwhile, when applying security strategies, antiviruses, patch management technology support, and security compliance, these strategies should take into consideration the distinctions between IT and OT environments. Such strategies are deemed to be effective when we put the environment we are working under into perspective. In our situation, for example, we physically secure the autonomous truck in the beginning, and then the wireless communications on the truck. Afterwards, we ensure secure tower communications and finally the network backbone.

Autopilots rely extensively on computer vision and Artificial Intelligence (AI) techniques since a vehicle perceives visual data very differently than a person does. Cameras are critical in autonomous trucks for a variety of tasks, including lane detection, obstacle detection, parking, and sign recognition [9,10], which raises another security risk. A blurred camera's performance breaks a safety standard, increasing the likelihood of fatal accidents triggered by camera attacks. A typical attack involves the use of a laser matrix to blind cameras at a close range of less than half a meter, for a few seconds, inflicting irreversible damage and thereby ruining the autonomous procedures. Optical features are the camera's weak point, as physical attacks can hinder the existence of a completely secure camera system. Nonetheless, Petit et al. [20] suggest that removable near-infrared cut filters and photochromic lenses provide adequate protection from various angles. A recent study addresses the use of machine learning to detect and mitigate remote attacks via a dedicated anti-hacking device [21]. Notably, these attacks sometimes may not require any physical access to the truck, such as attacks with lasers, and their consequences can be critical. Yet, some of these assaults do not require physical access to the truck and their effects may be serious.

Concerning autonomous mining, Labbe [6] notes that existing AHS standards and literature have always placed a premium on the system's protection aspect, but never on its cybersecurity components. In addition, the proposed study [6] claims that developing a generic threat model for AHS systems is important, which would be applicable to any OEM and mining facility. In that, Labbe [6] introduces an under development solution called MM-ISAC, that would align with safety requirements such as ISO17757:2017 and security standards such as ISO/IEC 27000:2016, ISA99. Although this initiative is still in its early stages, we anticipate that the MM-ISAC will collaborate closely with vendors to refine the system specification across all affected areas, including infrastructure, communications, and cybersecurity, in order to come up with a sound threats model.

Finally, Abdo et al. [22] argue that safety and cybersecurity should be seen in tandem. Currently used risk assessment approaches treat safety and cyber threats as two distinct entities, while in the Industry 4.0 era, a safety risk is also a cybersecurity risk. Consider an AHT and a manual haulage truck; both provide certain safety measures to safeguard and protect the equipment and operators. However, the only safety concern regarding a manual truck is if the operator tampers physically with the truck. On the contrary, an AHT poses the same safety concerns plus a residual risk of it being a CPS connected to an open network (i.e., Wifi). Hence, the cybersecurity risks is a critical factor that might affect the safety of the mine. The bowtie and attack tree analysis are utilized by [22], combining safety and security in risk analysis to generate an exhaustive representation of risk scenarios. Unfortunately, this method would necessitate the collection of qualitative and quantitative data to calculate the probability of safety risks. These data are private and often proprietary to manufacturers as well as not always accessible for analysis, making this study difficult to conduct further studies to confirm or improve the results. Al-Ali et al. [17] propose

creating a trust zone to handle sharing such information, but this entails the acceptance of all parties. Table 1 summarizes some proposed solutions and their challenges.

Table 1. Summary of literature on cybersecurity and safety.

Papers	Used Techniques/Technologies	Security and Safety Challenges Addressed	Advantages	Disadvantages
[6]	Combination of existing standards, e.g., ISO 27000, ISA99	Existing solutions are focused on safety aspects of AHS applications only	Utilizing well-established standards in different environments	Proposed solution is still immature and has yet to be evaluated in AHS environment
[12]	Combine pre-existing standards to address the complexity of OT environment	Same forms of attacks that occur in the IT world can be observed in the industrial arena. Lack of standardized approach	Some standards are mature and proven to be effective	Standards do not take into consideration the wireless environment within AHS setups. Adopting some practices could be risky as they are not environment specific
[13,14]	AHTs is a CPS	textbfFocus on specific application rather than standardized specifications that were designed to support general purposed devices	CPS can benefit from a wide range of existing applications in other areas	Manipulating the CPS without systems' owner knowledge, e.g., MITM attack. Loss of integrity that could result in loss of lives
[15]	Security by design	Physical, network, and computation are three fields that may be exploited	Enforce, Authentication, Authorization, Network Enforced Policy, and Secure Analytics as measures to reinforce security	Approaching cybersecurity problems in an industrial ad hoc manner can lead to misleading findings because generalized attack studies lack the specifics of security objectives
[17]	OT–IT data sharing	Address how to access/share data between different environments	Dynamic trust zone where decisions are dynamically made by defining and analyzing flows, then intelligently determine whether the flow is permitted	Raises concerns about data privacy and confidentiality, especially in a multivendor environment
[9]	Superior signals extraction to identify targeted GPS attacks	The GPS data must be protected to avoid GPS-based collisions and ATs deviation from the target positions	Practical techniques can figure out vital characteristics of the network such as signal strength	Secure GPS strategies are not considered in intended AHS and need to be investigated further, especially in terms of spoofing and jamming
[21]	Defense Strategies (removable near-infrared-cut filters, and photochromic lenses)	Camera attacks (a blurred camera's outputs break a safety standard and increase fatal accidents as well)	Photochromic lenses and removable near-infrared cut filters offer sufficient protection from a variety of angles	There are no concrete solutions for camera protection in ATs. Camera attacks can cause inaccurate detections of obstacles, lanes, or traffic signs
[22]	Bowtie analysis and attack tree analysis	Cybersecurity impacts safety of mining equipment	Produce an exhaustive representation of risk scenarios. To measure the risk of safety threats, quantitative and qualitative data are required	Data are usually privately owned by manufacturers and are not always available for analysis, which would pose a challenge to conduct such a study

2.2. Relation between Communications and Safety in AHS

AHS systems have prospered in surface mining with outstanding results, which increased the demand to adopt autonomous mining. Manufacturers have placed the greatest emphasis on safety, which is seen as the essence of mining operations. From collisions to high weather temperatures to difficult ground conditions, robotic autonomy has aided in operating in such harsh environments. This can be done either by improving

the efficiency or by allowing robots to operate in areas that humans find inoperable. Marshall et al. [11] discuss how robotics have contributed to mining and other domains regarding the following areas:

- Assist workers in hazardous environments that pose health risks, such as excessive heat, dust, poisonous smoke, or hydrogen sulfide (H2S).
- Fulfill labor shortages.
- Provide an opportunity to increase health and safety.
- Outperform humans in terms of performance.

Reliable communication has a significant role in the prosperity of AHS systems. ATs can communicate via various communications with the command center to collect data from neighbors, control telemetry, and monitor the health and safety of components. Using a secure communication system, the command center can guide trucks as well as manage them to enable tracking the mining operations. It is important to note that the mining environment is the same as any other industrial environment. That is, mining operations would effectively benefit from technological advancement in communications, but they also suffer from the same vulnerabilities with some particularities pertaining to the mining environment. In particular, AHS in mining relies heavily on wireless communications that were considered unfit for industrial operation at some point. However, as stated in [8], with the industrial revolution 4.0 and the integration of CPS and IoT systems in mining (i.e., in the industry in general), communication technologies have become essential for daily operation. Indeed, an autonomous truck must maintain continuous communication with central control. Otherwise, communication failure, even for a single piece of equipment, means the whole fleet will stop running. Technically, this is called "mine shutdown" due to communication loss. According to [6], AHS relies entirely on wireless technology for secure production and supervisory control. As a result, a stable network infrastructure (wired and wireless) is critical to AHS operations.

Since the advent of Industry 4.0, Wi-Fi technology has been an integral part of industrial operation [8]. Wireless Networks (WNs) have also opened new opportunities for business, such as easy deployment with lower cost. Despite the essential role of WNs in linking field devices and mobile assets, they face some difficulties that could affect both credibility and availability of operations. Labbe [6] demonstrates that AHS communications are susceptible to known attacks such as Wi-Fi De-Auth, which is a DoS assault on key operations. The authors in [7] show how existing wireless standards are insufficient to meet the demands of Industry 4.0. Sisinni et al. [23] argue that the advent of IoT and CPS in the industrial environment have caused existing Wi-Fi standards to lose traction as they are not capable of handling dense and large-scale deployments. Signal interference, topology control in the mining environment, and signal jamming are some of the issues inherited from 802.11 standards [8].

In addition, Kiziroglou et al. [24] address the relevance of wireless sensor networks (WSNs) and their capacity to improve safety as well as availability in a mining environment. The authors also highlight current challenges and how the mining industry should take advantage of WSNs. For that reason, WSNs could assist in the following areas of mining operations:

- Localization services, especially for AHS vehicles that require high precision and low latency.
- Data collection and analysis to minimize downtime that is a critical factor in extending the lifetime of an operation along with aiding in optimizing operations and achieving proactive maintenance.
- Health and safety are paramount in mining industry; sensing technology may assist in gathering data from the field to monitor both employee and equipment health, especially in areas where toxic gases are present (e.g., H2S). Furthermore, proximity sensors are designed to prevent and detect obstacles along with dangerous condi-

tions while trucks are driving in an autonomous mode, which is essential in mining operations.

Despite the advantages of WSNs implementation (e.g., low cost, flexible design, and real-time monitoring), they still suffer from some significant drawbacks that restrict their application to specific areas [25]. For instance, WSNs protocols rely on the 802.15.4 standards with lower energy consumption as a primary aim. Thus, the majority of these protocols are designed for low-data-rate proximity applications, which makes them ideal in smaller environments (i.e., mining environments would require a high data rate and significant proximity). Although some 802.14.5 protocols, such as WilressHART, are built to support security in the industrial environment, ensuring confidentiality might be challenging. That is, WSNs sensors consume lower energy that limits their ability to encrypt with more secure algorithms.

Private LTE (pLTE) is a viable alternative solution to traditional 802.11 technology (Wi-Fi) that could provide robust communication and evade WSNs limitations [26]. In [26], the authors demonstrate how pLTE addresses performance attributes. Additionally, they highlight how the global LTE ecosystem enables private enterprises to deploy and operate LTE networks independently of licensed service providers. Furthermore, the provision of an open-access spectrum (e.g., 3.5 GHz in the United States and 5 GHz worldwide [27]) enables organizations to deploy pLTE networks. In addition, pLTE networks guarantee adequate coverage, particularly in remote areas such as mines. It also has the potential to uplink/downlink traffic capacity, especially where video streaming is used. Subsequently, organizations with private LTE have increased control over network traffic, Quality of Service (QoS), and security, and the network can be customized to optimize reliability and latency in challenging environments, such as mining.

Additionally, pLTE would reduce maintenance costs since Long-Term Evolution (LTE) infrastructure does not need as many towers as traditional Wi-Fi due to its higher spectral efficiency. It also could alleviate contention issues associated with other existing networks. In terms of security, pLTE leverages well-established cellular network security infrastructure, e.g., Classic SIM-based and non-SIM options security. Due to the above, pLTE seems to be the savior solution, although it comes with a high price tag and the assumption that there is already an infrastructure ready to be deployed. Furthermore, pLTE solutions might be subject to approval and discretion by local governments, especially when it comes to the licensed spectrum.

Nowadays, several ongoing advancements proceed in the field of autonomous vehicle technologies. Specified standards developed by the IEEE team (i.e., IEEE 802.11p) for vehicular networks are known as Wireless Access for Vehicular Environment (WAVE). Furthermore, Dedicated Short Range Communications (DSRC) is one among these technologies that is deployed for short- to medium-range communications, especially for vehicular networks. The DSRC/WAVE technology has been utilized for distinct vehicular applications including infotainment, resource efficiency, and safety applications [28]. Regarding mining truck autonomy, Abdellah and Paul [29] survey the performance of different routing protocols when used for cooperative collision warning in mines. This study could serve as guidance for the design of new traffic control systems that prioritize safety applications. In addition, faster data packet dissemination is emphasized for cooperative collision notification in underground mining such as deploying 5G technology. In addition, the authors in [29] address the compatibility of vehicular networks (i.e., AHS in our case) with communication standards such as IEEE 802.11x, WiMax, and DSRC/WAVE standards. Table 2 summarizes the most recent technologies, their characteristics and limitations in AHS environments.

Table 2. Summary of literature on cybersecurity and safety.

Papers	Used Techniques/Technologies	Security and Safety Challenges Addressed	Advantages	Disadvantages
[8]	Wi-Fi technology is essential in AHS mining and Industry 4.0	AHS trucks require constant communication with central command and with each other	Presented new advantages for the business, such as low cost and easy deployment	Vulnerabilities such as Wi-Fi De-Auth, which is DoS attacks on critical operations. The authors of [7] explain how the current wireless standards alone are not adequate to address Industry 4.0 requirements
[24]	WSNs to increase safety	Monitor safety of equipment and operators when applicable in mining environment	Collect real-time data in the field and send the data to command centers to monitor persons and equipment in high-risk areas. A proximity sensor is designed to identify and avoid hazards while trucks are in autonomous mode, particularly in mining operations	WSN protocols are based on the 802.15.4 standard with a low energy usage objective. 802.14.5 protocols support security in the industrial environment, e.g., WilressHART, while ensuring confidentiality might be a challenge due to the limited battery life of sensor nodes that affects their ability to encrypt with more secure algorithms
[26]	Use of pLTE as medium of communication in the mine	Lack of topology and coverage issues	Private organizations can (in some countries) deploy and operate LTE networks without relying on licensed service providers. Additionally, pLTE networks allow organizations to guarantee coverage, especially in mines, and the potential to increase the capacity of uplink/downlink traffic for better video streaming	The lack of ASH-based research addressing potential new threats/attacks and their impact on the safety of mines
[29]	DSRC for autonomous mining vehicles	Applying several routing protocols under DSRC/WAVE standards for autonomous vehicles in underground mines	The first to address the usage of DSRC/Wave in the underground mine topology with the Rayleigh fading channel for emergency message dissemination protocols. It also provides a cooperative collision warning in underground mining environment	The lack of research into potential attacks and communication protection in underground mining using DSRC technology

3. Open Issues

Since our primary design goal is functionality, it is not unexpected nor rare to discover security flaws in applications that were designed to perform a particular task. However, lack of security can be detected once these applications are placed in open networks. Hence, we quickly realize the significant degradation effect in functionality because security was not a part of the initial design as mentioned earlier by Kim et al. [14]. Autonomous mines (i.e., mines in general) are not an exception to this phenomenon in which manufacturers strived to develop smart machinery that can be remotely operated and controlled as well as autonomously perform the work. Nevertheless, the cybersecurity aspect of this equipment is being implemented as an afterthought. In such a context, the aim of the cyberattacks may be to sabotage or slow down the ATs due to a competitive company in the market. Through this survey, we lightened how securing communication in an industrial environment is highly dependent on general practices and guidelines, as stated in [6].

According to the literature and discussion above, more real cases should be considered for study to understand the impact of the GPS attacks on AHS in the mining industry. Aspects including the signal strength, direction of arrival, and signal clock can be considered so as to identify fake signals as well prevent GPS attacks. A successful GPS attack can deviate the ATs from the target's true positions. A catastrophic collision of two or more trucks can also occur, resulting in the loss of people and resources. On the other hand, camera attacks are discussed in several studies, such as [9,21,30,31]. These papers have highlighted ideas about protection from camera attacks, without presenting practical solutions or countermeasures to camera attacks. Camera attacks are extremely dangerous since ATs may be unable to detect obstacles or recognize traffic signs in the mine resulting in ATs collisions. Thus, more investigations and solutions are still needed to observe the effect of camera attacks on the safe operations of the AHS environments.

The discussion in Section 2.1 revealed that most of the cybersecurity challenges that exist recently in mining are due to the absence of standardization and oriented solutions. The availability, productivity, and safety of operations are subjected to the security of communications when we project these challenges onto real-world applications, e.g., AHS. Wireless communication technologies such as LTE and 5G would achieve a rapid transformation of the AHS in the mining environment [32]. Thus, incorporating these technologies into the mining operations will give rise to opportunities for new attack vectors in the industrial environment. This leads us to the earlier claim that there is a current necessity for a well-studied procedure or guideline to tackle specific issues in the mine. As an example, what is the ultimate channel utilization and power transmit (Tx) within the mine? How can rouge access points be prohibited from injecting traffic into the mining network in the presence of mine challenges with signal processing? Is the IEEE802.11 wireless protocol a viable mining solution (i.e., especially for AHS) or should different solutions be suggested, e.g., pLTE, 4G, and 5G systems?

Furthermore, there is a strong relationship between cybersecurity and communication technologies in the mining industry. DSRC-WAVE technology is also considered a suitable vehicular communication technology (i.e., vehicle to everything (V2X)) for autonomous vehicles in the mining industry, according to Abdullah et al. [29]. This technology enables a variety of applications for autonomous vehicles, including safety and resource efficiency applications [28]. As a result, the investigation of DSRC communication technology in the mining industry, especially the AHS, is still an open issue. For example, an unauthorized emergency message disseminated among the autonomous trucks can cause disruption in the mining operation. The integrity of the propagated message is not maintained, which could lead to wrong decisions related to the mining operations. Although these communication technologies will outperform current technologies in terms of bandwidth and latency, they would be exposed to different variant of cybersecurity attacks, such the case of jamming attacks [33].

5G, pLTE, and DSRC-WAVE, as any previous wireless communication technologies, are vulnerable to common attacks such as jamming attacks, which produce deliberate interference in order to obstruct genuine users' communication. Such types of attacks (i.e., jamming attacks) pose a serious risk to public safety, and hence mining safety too. Therefore, the mining industry, when developing AHS systems adopting any of these technologies, should develop a comprehensive security strategy for enabling these technologies in automated mines using AHS-based systems.

All of these issues inspired us to pose even more in-depth questions and investigate different directions. For instance, in areas where both AHS and manual mining might be simultaneously used, what are the cybersecurity ramifications of having them both on the same network? Up until the writing of this paper, there were no industry standards or regulations that impose any specifications. Instead, organizations are repurposing other industry standards to fit within the mining environment, as previously mentioned. Overall, this study seeks to bridge the gap between existing standards and mining applications in cybersecurity, specifically network infrastructure. Yet, we believe a comprehensive solution

would take into consideration security during the design phase as well as build solutions purposely to accommodate the mining environment and its applications, such as the AHS system.

4. Conclusions

In this paper, a type of Cyber-physical Systems (CPS), i.e., an AHS in the mining environment, was discussed in terms of cybersecurity, reliable communication, and safety. AHS-based trucks have been shown to be very useful in the mining industry. However, the safety of using such trucks has not been thoroughly investigated. The literature was then surveyed to identify and discuss the relation between safety of AHS in the mining environment and both cybersecurity and communication. The relation between cybersecurity and safety in AHS systems was discussed and it was found that compromising cybersecurity would threaten the safety of mining operations leading to loses in people and equipment. In addition, we have shown that the reliability of wireless communication is mandatory for the safety of AHS operations. Through this survey, there are several open issues and challenges that may entail further studies and investigations. It was discussed that new technologies such 5G, pLTE and DSRC-WAVE could be good alternatives for the currently used IEEE 802.11. Although these communication technologies would outperform current technologies in terms of bandwidth and latency, they would be exposed to traditional or new cybersecurity threats or attacks, which still need to be considered while designing AHS systems and studied in the mining environment.

Author Contributions: Conceptualization, T.G. and Y.E.J.; methodology, T.G.; E.E.; and A.A.; validation T.G.; analysis, T.G.; E.E.; and A.A.; investigation, T.G. and Y.E.J.; E.E.; and A.A.; resources, T.G. and Y.E.J.; writing—original draft preparation, T.G. and Y.E.J.; writing—review and editing, T.G.; E.E.; and A.A.; supervision, T.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: We would like to acknowledge with much appreciation Prince Sattam Bin Abdulaziz University for its ongoing support to our research.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CPS	Cyber-physical Systems
AHS	Autonomous Haulage System
OT	Operating Technology
ATs	Autonomous Trucks
EMV	Equipped Manual Vehicle
ICS	Industrial Control Systems
AHT	Autonomous Haulage Trucks
RoT	Root of Trust
IT	Information Technology
AI	Artificial Intelligence
H2S	Hydrogen Sulfide
GPS	Global Positioning System
WNs	Wireless Networks
WSNs	Wireless Sensor Networks
LTE	Long-Term Evolution
DSRC	Dedicated Short Range Communications
WAVE	Wireless Access for the Vehicular Environment
pLTE	private LTE
QoS	Quality of Service

References

1. de Vass, T.; Shee, H.; Miah, S. IoT in Supply Chain Management: Opportunities and Challenges for Businesses in Early Industry 4.0 Context. *Oper. Supply Chain Manag. Int. J.* **2021**, *14*, 148–161. [CrossRef]
2. Carreras Guzman, N.H.; Wied, M.; Kozine, I.; Lundteigen, M.A. Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. *Syst. Eng.* **2020**, *23*, 189–210. [CrossRef]
3. Lee, E.A.; Seshia, S.A. *Introduction to Embedded Systems: A Cyber-Physical Systems Approach*; Mit Press: Cambridge, MA, USA, 2017.
4. Roth, M. Komatsu's Autonomous Haulage System Sests Record for Surface Material Moved. 2018. Available online: https://www.mining.com/web/frontrunner-autonomous-haulage-system-sets-new-record-latest-industry-milestone/ (accessed on 30 April 2021).
5. Parreira, J. An Interactive Simulation Model to Compare an Autonomous Haulage Truck System with a Manually-Operated System, Autonomous Haulage Truck, Simulation Model. 2013. Available online: https://open.library.ubc.ca/collections/24/items/1.0074111 (accessed on 30 April 2021).
6. Labbe, R. Securing Autonomous Systems, Mining and Metals Information Sharing and Analysis Centre, Canadaian Institute of Mining, AHS, Cybersecurity. 2019. Available online: https://store.cim.org/en/securing-autonomous-systems (accessed on 30 April 2021).
7. Varghese, A.; Tandur, D. Wireless requirements and challenges in Industry 4.0. In Proceedings of the 2014 international conference on contemporary computing and informatics (IC3I), Mysore, India, 27–29 November 2014; pp. 634–638.
8. Li, X.; Li, D.; Wan, J.; Vasilakos, A.V.; Lai, C.F.; Wang, S. A review of industrial wireless networks in the context of industry 4.0. *Wirel. Netw.* **2017**, *23*, 23–41. [CrossRef]
9. Ren, K.; Wang, Q.; Wang, C.; Qin, Z.; Lin, X. The security of autonomous driving: Threats, defenses, and future directions. *Proc. IEEE* **2019**, *108*, 357–372. [CrossRef]
10. Cheng, H.Y.; Jeng, B.S.; Tseng, P.T.; Fan, K.C. Lane detection with moving vehicles in the traffic scenes. *IEEE Trans. Intell. Transp. Syst.* **2006**, *7*, 571–582. [CrossRef]
11. Joshua, A.M.; Adrian, B.; Eduardo, N.; Steven, S. Robotics and the Handbook. In *Springer Handbook of Robotics*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 1–6.
12. Alani, M.M.; Alloghani, M. *Industry 4.0 and Engineering for a Sustainable Future*; Springer: Berlin/Heidelberg, Germany, 2019.
13. Chattopadhyay, A.; Lam, K.Y. Security of autonomous vehicle as a cyber-physical system. In Proceedings of the 2017 7th International Symposium on Embedded Computing and System Design (ISED), Durgapur, India, 18–20 December 2017; pp. 1–6.
14. Kim, S.; Won, Y.; Park, I.H.; Eun, Y.; Park, K.J. Cyber-physical vulnerability analysis of communication-based train control. *IEEE Internet Things J.* **2019**, *6*, 6353–6362. [CrossRef]
15. He, H.; Maple, C.; Watson, T.; Tiwari, A.; Mehnen, J.; Jin, Y.; Gabrys, B. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligen. In Proceedings of the 2016 IEEE Congress on Evolutionary Computation (IEEE CEC), Vancouver, BC, Canada, 24–29 July 2016; pp. 1015–1021.
16. Lezzi, M.; Lazoi, M.; Corallo, A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Comput. Ind.* **2018**, *103*, 97–110. [CrossRef]
17. Al-Ali, R.; Heinrich, R.; Hnetynka, P.; Juan-Verdejo, A.; Seifermann, S.; Walter, M. Modeling of dynamic trust contracts for industry 4.0 systems. In Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings, Madrid, Spain, 24–28 September 2018; pp. 1–4.
18. Zeng, K.C.; Liu, S.; Shu, Y.; Wang, D.; Li, H.; Dou, Y.; Wang, G.; Yang, Y. All your GPS are belong to us: Towards stealthy manipulation of road navigation systems. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, USA, 15–17 August 2018; pp. 1527–1544.
19. Nccic, I.C. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies Industrial Control Systems Cyber Emergency Response Team. 2016. Available online: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf (accessed on 30 April 2021).
20. Petit, J.; Stottelaar, B.; Feiri, M.; Kargl, F. Remote attacks on automated vehicles sensors: Experiments on camera and lidar. *Black Hat Eur.* **2015**, *11*, 995.
21. Kyrkou, C.; Papachristodoulou, A.; Kloukiniotis, A.; Papandreou, A.; Lalos, A.; Moustakas, K.; Theocharides, T. Towards artificial-intelligence-based cybersecurity for robustifying automated driving systems against camera sensor attacks. In Proceedings of the 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Limassol, Cyprus, 6–8 July 2020; pp. 476–481.
22. Abdo, H.; Kaouk, M.; Flaus, J.M.; Masse, F. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie–combining new version of attack tree with bowtie analysis. *Comput. Secur.* **2018**, *72*, 175–195. [CrossRef]
23. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial internet of things: Challenges, opportunities, and directions. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4724–4734. [CrossRef]
24. Kiziroglou, M.E.; Boyle, D.E.; Yeatman, E.M.; Cilliers, J.J. Opportunities for sensing systems in mining. *IEEE Trans. Ind. Inform.* **2016**, *13*, 278–286. [CrossRef]
25. Raza, S.; Faheem, M.; Guenes, M. Industrial wireless sensor and actuator networks in industry 4.0: Exploring requirements, protocols, and challenges—A MAC survey. *Int. J. Commun. Syst.* **2019**, *32*, e4074. [CrossRef]
26. Brown, G. Private LTE Networks-Qualcomm. *Qualcomm* **2017**, 1–11. Available online: https://www.qualcomm.com/media/documents/files/private-lte-networks.pdf (accessed on 3 June 2021).

27. Ratasuk, R.; Mangalvedhe, N.; Ghosh, A. LTE in unlicensed spectrum using licensed-assisted access. In Proceedings of the 2014 IEEE Globecom Workshops (GC Wkshps), Austin, TX, USA, 8–12 December 2014; pp. 746–751.
28. Ng, H.H.; Vasudha, R.; Hoang, A.T.; Kwan, C.; Zhou, B.; Cheong, J.; Quek, A. BESAFE: Design and implementation of a DSRC-based test-bed for connected autonomous vehicles. In Proceedings of the 2018 21st International Conference on Intelligent Transportation Systems (ITSC), Maui, HI, USA, 4–7 November 2018; pp. 3742–3748.
29. Chehri, A.; Fortier, P. Autonomous Vehicles in Underground Mines, Where We Are, Where We Are Going? In Proceedings of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 25–28 May 2020; pp. 1–5.
30. Khadka, A.; Karypidis, P.; Lytos, A.; Efstathopoulos, G. A benchmarking framework for cyber-attacks on autonomous vehicles. *Transp. Res. Procedia* **2021**, *52*, 323–330. [CrossRef]
31. Stottelaar, B.G. Practical Cyber-Attacks on Autonomous Vehicles. Master's Thesis, University of Twente, Enschede, The Netherlands, 2015.
32. Conway, G. The Evolving Role of Communications for the Digital Mine. *Eng. Min. J.* **2020**, *221*, 54–55.
33. Arjoune, Y.; Faruque, S. Smart jamming attacks in 5G new radio: A review. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; pp. 1010–1015.