Autonomous Haulage Systems

Subjects: Engineering, Industrial
Contributor: Tarek Gaber

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.

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

1. Introduction

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). 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. 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).

The AHS equipment exceedingly relies on wireless communications, including object avoidance/detection systems, Global Positioning Systems (GPS), e.g., GNSS, and artificial intelligence. 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 [1].

2. 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 [2]. 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 [3]. 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 [4].

ATs are endpoints (e.g., sensors, actuators) connected to networks and communicating through a command center with different tiers of security. The authors of [5] 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 [4]. 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 [2]. 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 [3]. 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 [3].

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 [6]. 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 [2]. 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 [4][5], 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 [5].

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) [7]. 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 [7], 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 [7]. Yet, this strategy increases concern about data protection and confidentiality in a multivendor setting. An additional RoT model is introduced in [3], 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. [8] 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 [9] 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 [10], 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 [3], 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 [8][11], 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. [12] 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 [13]. 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 [14] 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 [14] 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 [14] 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. [15] 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 [15], 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. [7] 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.

3. 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. [16] 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 [17], 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 [14], 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 [17]. 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 [14] 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 [18] show how existing wireless standards are insufficient to meet the demands of Industry 4.0. Sisinni et al. [19] 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 [17].

In addition, Kiziroglou et al. [20] 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 conditions 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 [21]. 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 [22]. In [22], 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 [23]) 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 [24]. Regarding mining truck autonomy, Abdellah and Paul [25] 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.

References

1. Parreira, J. An Interactive Simulation Model to Compare an Autonomous Haulage Truck System with a Manually-Opera ted System, Autonomous Haulage Truck, Simulation Model. 2013. Available online: (accessed on 30 April 2021).
2. Alani, M.M.; Alloghani, M. Industry 4.0 and Engineering for a Sustainable Future; Springer: Berlin/Heidelberg, Germany, 2019.
3. Chattopadhyay, A.; Lam, K.Y. Security of autonomous vehicle as a cyber-physical system. In Proceedings of the 2017 7 th International Symposium on Embedded Computing and System Design (ISED), Durgapur, India, 18–20 December 2 017; pp. 1–6.
4. Kim, S.; Won, Y.; Park, I.H.; Eun, Y.; Park, K.J. Cyber-physical vulnerability analysis of communication-based train contr ol. IEEE Internet Things J. 2019, 6, 6353–6362.
5. He, H.; Maple, C.; Watson, T.; Tiwari, A.; Mehnen, J.; Jin, Y.; Gabrys, B. The security challenges in the IoT enabled cyb er-physical systems and opportunities for evolutionary computing & other computational intelligen. In Proceedings of th e 2016 IEEE Congress on Evolutionary Computation (IEEE CEC), Vancouver, BC, Canada, 24–29 July 2016; pp. 1015 –1021.
6. Lezzi, M.; Lazoi, M.; Corallo, A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. Comput. Ind. 2018, 103, 97–110.
7. Al-Ali, R.; Heinrich, R.; Hnetynka, P.; Juan-Verdejo, A.; Seifermann, S.; Walter, M. Modeling of dynamic trust contracts f or industry 4.0 systems. In Proceedings of the 12th European Conference on Software Architecture: Companion Proce edings, Madrid, Spain, 24–28 September 2018; pp. 1–4.
8. Ren, K.; Wang, Q.; Wang, C.; Qin, Z.; Lin, X. The security of autonomous driving: Threats, defenses, and future directio ns. Proc. IEEE 2019, 108, 357–372.
9. 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 stealt hy manipulation of road navigation systems. In Proceedings of the 27th USENIX Security Symposium (USENIX Securit y 18), Baltimore, MD, USA, 15–17 August 2018; pp. 1527–1544.
10. Nccic, I.C. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategie s Industrial Control Systems Cyber Emergency Response Team. 2016. Available online: (accessed on 30 April 2021).
11. Cheng, H.Y.; Jeng, B.S.; Tseng, P.T.; Fan, K.C. Lane detection with moving vehicles in the traffic scenes. IEEE Trans. I ntell. Transp. Syst. 2006, 7, 571–582.
12. 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.
13. 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 20 20; pp. 476–481.
14. Labbe, R. Securing Autonomous Systems, Mining and Metals Information Sharing and Analysis Centre, Canadaian Inst itute of Mining, AHS, Cybersecurity. 2019. Available online: (accessed on 30 April 2021).
15. Abdo, H.; Kaouk, M.; Flaus, J.M.; Masse, F. A safety/security risk analysis approach of Industrial Control Systems: A cy ber bowtie–combining new version of attack tree with bowtie analysis. Comput. Secur. 2018, 72, 175–195.
16. Joshua, A.M.; Adrian, B.; Eduardo, N.; Steven, S. Robotics and the Handbook. In Springer Handbook of Robotics; Spri nger: Berlin/Heidelberg, Germany, 2016; pp. 1–6.
17. Li, X.; Li, D.; Wan, J.; Vasilakos, A.V.; Lai, C.F.; Wang, S. A review of industrial wireless networks in the context of indus try 4.0. Wirel. Netw. 2017, 23, 23–41.
18. Varghese, A.; Tandur, D. Wireless requirements and challenges in Industry 4.0. In Proceedings of the 2014 internationa l conference on contemporary computing and informatics (IC3I), Mysore, India, 27–29 November 2014; pp. 634–638.
19. 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.
20. 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.
21. Raza, S.; Faheem, M.; Guenes, M. Industrial wireless sensor and actuator networks in industry 4.0: Exploring requirem ents, protocols, and challenges—A MAC survey. Int. J. Commun. Syst. 2019, 32, e4074.

22. Brown, G. Private LTE Networks-Qualcomm. Qualcomm 2017, 1–11. Available online: (accessed on 3 June 2021).
23. 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.
24. 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.
25. Chehri, A.; Fortier, P. Autonomous Vehicles in Underground Mines, Where We Are, Where We Are Going? In Proceedin gs of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 25–28 May 2020; p p. 1–5.
