Mining, Metallurgy & Exploration (2021) 38:567–574
https://doi.org/10.1007/s42461-020-00325-3

Assessing the Feasibility of a Commercially Available Wireless Internet of Things System to Improve Conveyor Safety

R. Jacksha[1] · K. V. Raj[1]

Received: 8 May 2020 / Accepted: 28 September 2020 / Published online: 6 October 2020
© This is a U.S. government work and its text is not subject to copyright protection in the United States; however, its text may be subject to foreign copyright protection 2020

Abstract
Conveyor systems persist in being a source of injuries and fatalities in the mining industry. To reduce these incidents, better methods are needed to enhance the monitoring of probable hazards and improve situational awareness during the normal operation and maintenance of conveyor systems. To address these issues, researchers from the National Institute for Occupational Safety and Health (NIOSH) continue to investigate emerging technologies that show the potential to improve miner safety around conveyors. This paper presents a feasibility assessment by NIOSH researchers of a fully integrated, commercially available wireless Internet of Things (IoT) system to improve situational awareness around conveyor systems. Included are discussions of a full-scale laboratory test bed that was designed to simulate a working conveyor system as well as the challenges and successes of integrating the IoT system with the test bed.

Keywords Internet of Things · Conveyor safety · Data acquisition · Wireless communication

1 Introduction

Injuries and fatalities associated with conveyor systems at sand and gravel mining operations continue to be a problem in the mining industry. Research performed by the National Institute for Occupational Safety and Health (NIOSH) showed that from 2000 to 2007, 14% of all mining-related accidents involved conveyors, with most accidents occurring at surface operations [1]. The Mine Safety and Health Administration (MSHA) has also recognized this problem, stating in a recent request for information (RFI): "Since 2007, there have been 17 fatalities related to working near or around belt conveyors, of which 76 percent were related to miners becoming entangled in belt drives, belt rollers, and discharge points. Factors that contribute to entanglement hazards include inadequate or missing guards, inadequate or an insufficient number of crossovers in strategic locations, and/or inappropriate lock out/tag out procedures. Systems that can sense a miner's presence in hazardous locations; ensure that machine guards are properly secured in place; and/or ensure machines are properly locked out and tagged out during maintenance would reduce fatalities" [2].

To address the problem of entanglement-related accidents, NIOSH researchers continue to investigate emerging technologies that may be beneficial in improving conveyor safety, specifically through enhanced situational awareness. In 2013, NIOSH researchers reported on a wireless miner tracking system, which was repurposed to provide intelligent machine guard monitoring to improve miner safety [3]. More recently, NIOSH researchers developed and installed a proof-of-concept wireless Internet of Things (IoT)–based system to provide real-time monitoring of machinery and conveyors during operation and maintenance [4, 5].

While the above-mentioned systems showed great potential for improving conveyor safety, they required an immense amount of technical expertise to set up and deploy. However, small mines with 10 or fewer employees had the highest incident rate for machine-related severe accidents, and these operations may not have the technical resources or finances to deploy such systems [1]. For these reasons, NIOSH researchers believed a more cost-effective solution requiring less technical expertise to deploy was needed. With IoT making inroads into the mining sector and continually evolving to meet industry needs, low-cost commercially available IoT systems that are fully integrated (turnkey) solutions were explored [6, 7]. This paper describes one example of a commercial off-the-shelf (COTS) wireless IoT system and how it was

✉ R. Jacksha
rjacksha@cdc.gov

[1] CDC/NIOSH/Spokane Mining Research Division, 315 E Montgomery Ave., Spokane, WA 99207, USA

implemented on a purpose-built conveyor test bed to assess its feasibility to improve conveyor safety. Included are discussions of the successes and challenges of the implementation.

2 IoT System Description

The wireless IoT system selected for assessment has many features and options which lends itself to a straightforward deployment. The option of a non-cloud-based server with a fully developed Windows-based Human-Machine Interface (HMI) pre-installed, coupled with the availability of a wide variety of sensor nodes and a control node, allows the solution to be easily optimized to enhance conveyor safety for mining operations. The server with HMI software pre-installed is priced at $2500 and sensors, control nodes, and gateways range from $150 to $350, making the solution cost effective for even the smallest deployment.

The system was configured as a non-cloud-based solution utilizing a local server. This addressed two possible concerns. Foremost, some mining operations are located in remote geographical areas that may not have reliable, or any, access to cloud storage service providers. Second, a local off-network server could ease any security concerns operators may have regarding cloud-based storage of proprietary data [8, 9].

A closed platform Windows-based HMI is used to configure sensors, display sensor data, and provides an interface to historical sensor data. If connected to a network, the HMI is capable of being set up to send email and text alert notifications based on sensor threshold data. Figure 1 shows the HMI's sensor status screen.

The system's wireless components operate in the 915 MHz Industrial, Scientific, and Medical (ISM) frequency band using the frequency-hopping spread spectrum (FHSS) non-time synchronized protocol method (non-TSPM) for data transmission [10]. This combination is especially well suited for low-data rate, large-scale IoT applications [11, 12]. The system employs a star network topology where all sensors communicate directly through a dedicated gateway to the system server [13].

The system sensors were fully programmable and powered by 3.6-V 2400-mA/h batteries. The level of programmability varied by sensor, but all had basic settable parameters such as data acquisition rate, minimum and maximum data thresholds, data transmission rate during the period while thresholds were exceeded, and network connection status check-in interval. The sensors, described in detail later, transmitted data immediately when thresholds were exceeded but otherwise only transmitted on the set interval for system check-in. The control nodes were powered from 110-V mains and had the ability to open or close a pair of 30-Amp relays based on predefined sensor data. A sensor, control node, and gateway (left to right) are shown in Fig. 2.

The combination of the star network topology and non-TSMP method for data transmission allowed for a lower sensor transmit duty cycle and enhanced battery life over mesh-based networks using traditional TSMP methods [14].

Independent of the IoT system, six other components were selected to enhance the functionality of the solution. A pair of point-to-multipoint wireless Ethernet bridges operating in the 2.4 GHz ISM band were selected to extend the range between the sensor gateway and the system server. To allow handheld wireless devices, such as tablets and smart phones, to access the system server's HMI remotely, 2 Gb wireless access points (WAPs), a network router, and network switch were also selected.

3 Conveyor Test Bed

A purpose-built conveyor test bed was developed to assess the selected IoT system's potential to improve conveyor safety. The core of the test bed was a pair of small "troughing" conveyors, one 12 ft. in length and the other 16 ft. (Fig. 3.)

Since the conveyors came standard with 110-V motors controlled using simple toggle switches, motor controllers were designed and fabricated in-house to simulate those typically used in the sand and gravel mining sector. Separate motor controllers for each conveyor included a mains voltage disconnect, a three-pole motor contactor, momentary switches for start and stop, an emergency stop (E-Stop), and front panel lamps to indicate the presence of mains voltage, the status of the motor contactor, and the existence of a hazardous situation.

The conveyors were also modified to allow for monitoring of the motor guard placement, motor mains voltage, and bearing temperature of the idler and return rollers. The feed-discharge L-shape layout of the two conveyors is allowed for proximity detection at the transfer point.

4 IoT System and Test Bed Integration

The purpose of integrating the IoT system with the test bed was to assess its potential to enhance situational awareness associated with conveyor system operation and maintenance. As implemented, should sensor data (status) indicate an abnormal (fault) condition that results in a hazardous situation, such as a guard not in place, personnel would be notified, but the conveyor(s) would not be automatically shut down. However, personnel would have the option of shutting down the conveyors using E-Stops on the motor controller enclosures. Conversely, should a fault condition exist before starting a conveyor, the system would automatically prevent the conveyors from being started. Further, handheld devices, such as smart phones or tablets, could be used to access the

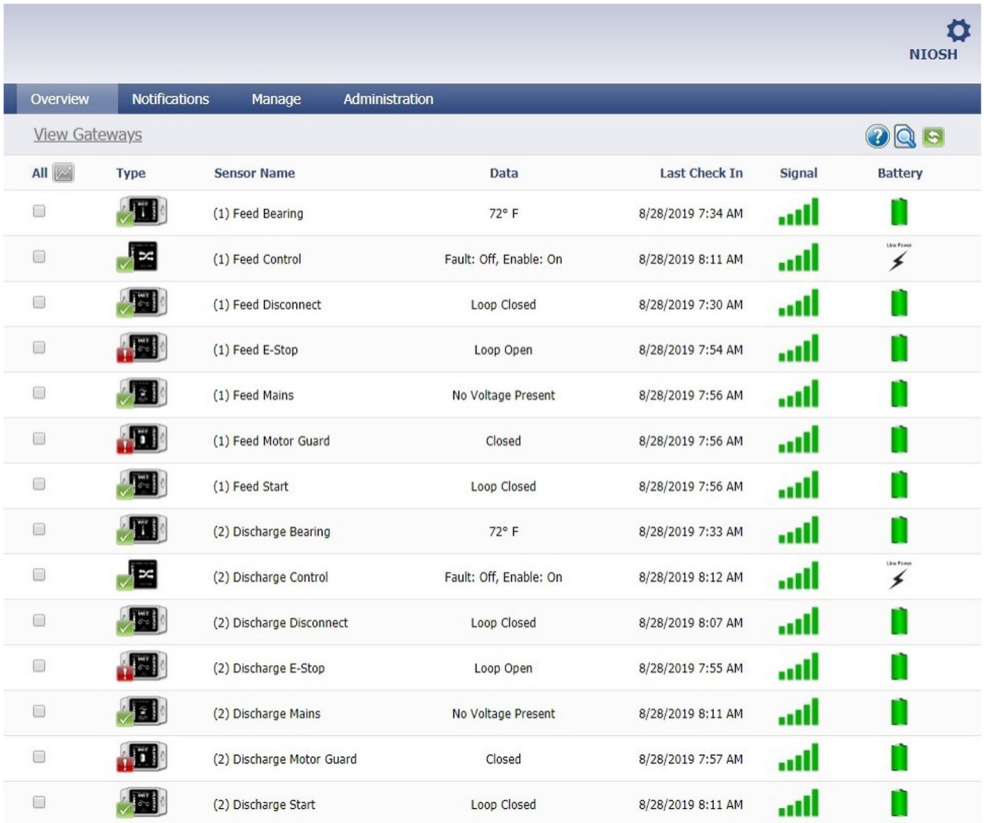

Fig. 1 IoT system Human-Machine Interface (HMI)

server's HMI via the WAPs. This would allow for remote verification of guard, mains voltage, bearing temperature, and E-Stop status, or for checking conveyor startup attempts or worker proximity to hazards. Remote access to the HMI would be especially useful as part of a lockout/tagout (LOTO) procedure before beginning conveyor maintenance or restarting when maintenance is complete.

A block diagram of the system as implemented is shown in Fig. 4. One controller and conveyor sensor set is omitted for clarity.

4.1 IoT System Installation

The conveyor motor controllers were designed with the installation of sensors and a control node in mind. The mains disconnect, start switch, and E-Stop were each monitored by a separate sensor. A control node was used to prevent conveyor startup in the event of a fault condition as well as illuminate the lamp on the motor controller enclosure's front cover, indicating a fault condition exists. It must be noted that the E-Stop was hardwired in the motor controller to shut down the conveyor as well as prevent it from being started. Since disconnecting the mains voltage to the motor controller assembly would disable the control node itself and it would have taken some finite amount of time to re-establish a connection to the gateway when powered back up, a battery and associated charger were included to keep the control node powered for up to 30 days in the event of a mains disconnect. The three sensors and control node shared a common antenna via a radio frequency (RF) combiner. An instrumented motor controller

Fig. 2 IoT system sensor, control node, and gateway (left to right)

Fig. 3 Test bed conveyors

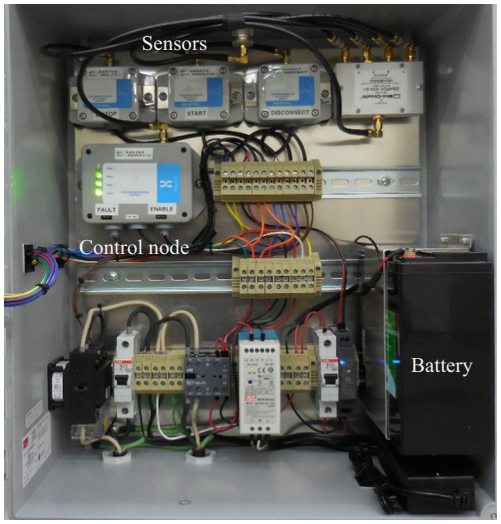

Fig. 5 Conveyor motor controller

is shown in Fig. 5. Three sensors monitoring the disconnect switch, start switch, and E-Stop are shown in the upper left. The control node is just below the sensors with the battery backup in the lower right.

On each conveyor, guard status, bearing temperature, and motor voltage were each monitored by a separate sensor. The transfer point was monitored by a single proximity sensor installed on one conveyor. Figure 6 shows three sensor nodes mounted on a conveyor.

Table 1 summarizes the installed sensors and node names, functions, and locations.

The system server and sensor gateway were intentionally located in different rooms of the laboratory to simulate a surface mine setting where an office could be located some distance from a conveyor. A pair of wireless Ethernet bridges were used to connect the server and gateway. On the server end, the bridge was connected to the server on the firewall side of a network router. The purpose of the router was twofold. First, it functioned as a Dynamic Host Control Protocol (DHCP) server, which assigned an Internet Protocol (IP) address to handheld devices accessing the HMI. Second, it provided a network port for a WAP located in the system server area. On the gateway end, the bridge was connected to the gateway through a network switch. This provided a network port for a WAP located near the test bed. The enclosure housing the gateway is shown in Fig. 7. The Ethernet bridge is shown at the top center, the sensor gateway in the upper right, and the network switch to the lower right. The WAP is out of frame mounted to the wall well above the enclosure.

4.2 IoT System Configuration

Sensors were configured to optimize battery life while not sacrificing situational awareness performance. Other than

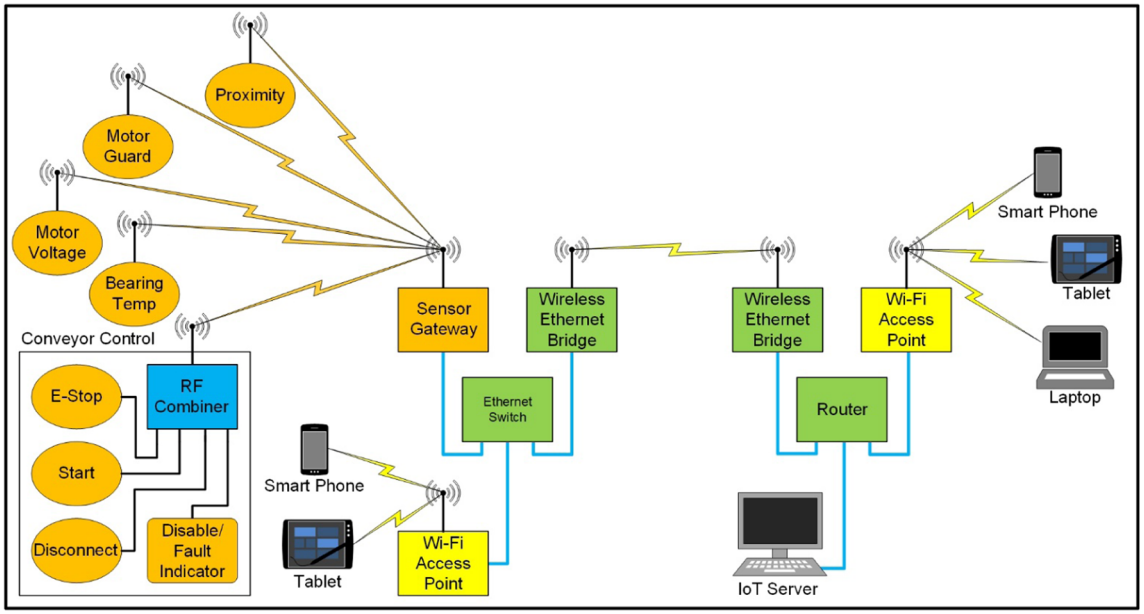

Fig. 4 IoT system implementation block diagram

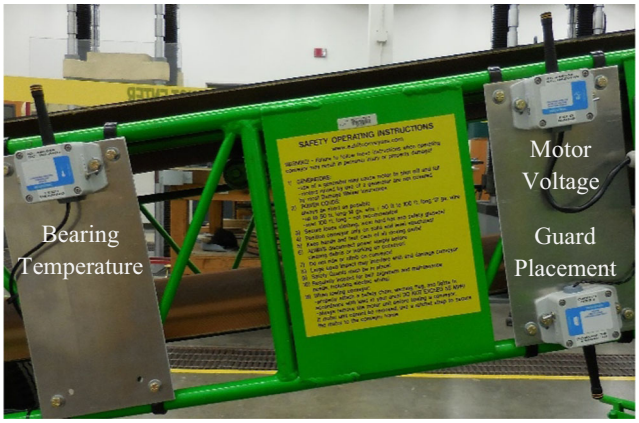

Fig. 6 Sensor nodes installed on a conveyor

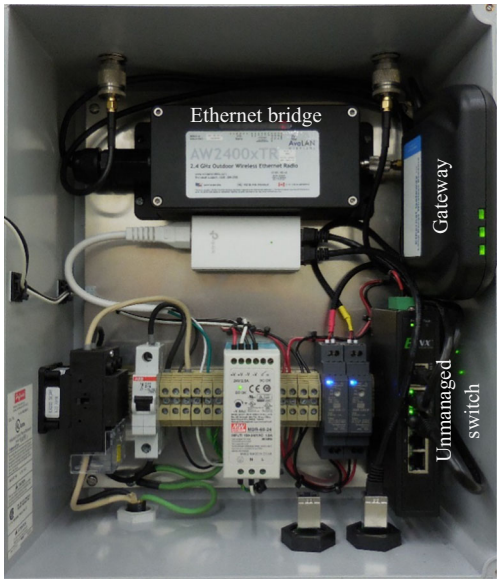

Fig. 7 Sensor gateway enclosure

system check-ins hourly, sensors were set up to only communicate with the gateway in the event of a state change or in the case of bearing temperature, if temperature thresholds were exceeded or returned to normal.

Motor guard, proximity, and bearing temperature sensor state change indicating a fault condition resulted in a control node illuminating a fault indicator and disabling the ability to start a conveyor. Since an E-Stop electrically stopped a conveyor as well as prevented it from being started, a sensor state indicating that an E-Stop had been activated resulted only in illumination of a fault indicator. Figure 8 shows a motor controller enclosure with the fault indicator illuminated.

State changes of the mains disconnect, start switch, and motor voltage sensors were considered normal during conveyor operation and maintenance. Therefore, these sensor state changes did not result in control node actions. However, under a LOTO scenario, sensor states could be reviewed through the server's HMI to ensure that mains voltage had been disconnected from the motor controllers, the start switch had been pressed to guarantee the conveyor would not start, and no voltage had been delivered to the motor.

5 IoT System Assessment

The research goal of the project was to assess the feasibility of a fully integrated (turnkey), cost-effective, COTS IoT system to improve conveyor safety. With this in mind, the assessment focused on three areas—technical expertise required for system deployment, system reliability, and mostly importantly, the ability of the system to provide timely notifications of potential safety hazards.

While technical expertise was not essential to deploy or maintain the system, there were challenges and setbacks that required perseverance as well as basic troubleshooting skills to resolve. Documentation for the HMI and system components was primarily available online and was often not up-to-date with current product versions. And, while specifically described as an off-network solution, the HMI and server were optimized to have internet connectivity. These two factors resulted in system settings and sensors being misconfigured on numerous occasions. Subsequently, an excessive amount

Table 1 Sensor or node name, function, and location summary

Sensor or node name	Function	Location
E-Stop	Monitor E-Stop status	Conveyor controllers
Disconnect	Monitor conveyor controller mains voltage input disconnect switch	Conveyor controllers
Start	Monitor attempt to start conveyor	Conveyor controllers
Disable/fault indicator	Prevent conveyor startup and illuminate fault indictor	Conveyor controllers
Motor guard	Monitor status of motor guard placement	Conveyors
Motor voltage	Monitor for presence of conveyor motor mains voltage	Conveyors
Bearing temp	Monitor for excessive conveyor roller bearing temperature	Conveyors
Proximity	Monitor for worker presence near transfer point	Conveyor transfer point

Fig. 8 Motor controller with Power and Fault indicators illuminated

of time was spent troubleshooting issues and determining the correct settings and configurations.

Initial component reliability was also of concern. Out of 25 sensors and control nodes deployed, one would not power up on arrival, two failed within a week, and a fourth became intermittent within a month. The failed sensors and node were returned under warranty along with a request for failure analysis reports. As of this writing, these reports were not yet available.

Once fully deployed, the system predominantly functioned as designed. Under fault conditions, the ability to start conveyors was disabled, and fault indicators on the motor controllers were illuminated. Sensor and gateway data were logged to the system server, and historical trends were easily viewed using the HMI. The HMI could also be successfully accessed using wireless devices via a WAP. While the system server did have the ability to send email and text notifications—an excellent feature to improve situational awareness—this functionality was not assessed due to the off-network nature of the system.

Sensor network reliability was, for the most part, reasonable with sensors and control nodes checking in at their predefined intervals as well as reporting and taking action on fault conditions promptly. In most circumstances, latency between the occurrence of a fault condition and a resultant system notification and action was typically less than 5 s. However, at one point during the assessment, latencies degraded from seconds to minutes. After extensive troubleshooting, it was discovered that a transceiver (radio) operating on a channel in the center of the 915 MHz ISM band had been placed in close proximity to the IoT system's gateway. This resulted in wireless channel congestion [15, 16]. Reconfiguring the radio to a channel on the lower end of the ISM band resolved the issue. This behavior did, however, validate a concern over data transmission latency for wireless systems operating in ISM bands [17]. It also highlighted the fact that considerable technical expertise in troubleshooting radio frequency (RF) issues could be required to deploy and maintain a wireless IoT system [18].

Another area of concern was race conditions between sensors. It was observed that occasionally a motor controller's fault indicator would not be illuminated when a fault condition existed. Working closely with the system's manufacturer, it was determined that if two sensors indicated fault conditions simultaneously and one sensor then returned to a nonfault condition, the system would re-enable the conveyor's ability to start and turn off the motor controller's fault indicator. This would occur even though the other sensor remained in a fault condition. While the system's manufacturer stated the race conditions could be resolved by reconfiguring monitoring and control algorithms in the HMI, as of this writing the correct algorithm configurations had not yet been identified.

Sensor battery life exceeded expectations. Over the 6-month period of system fabrication, configuration, and assessment, no sensor battery needed replacing, and the HMI status screen showed that all sensors still had healthy battery statuses at the end of the system assessment (Fig. 1.) It must be taken into consideration that this assessment was with sensors configured for hourly check-ins. Should the sensors have been configured to check in more frequently for increased confidence in system reliability, it would have had a direct impact on battery life.

6 Discussion

The evaluation of this particular IoT system revealed several challenges in implementing this technology for safety-critical applications, i.e., applications where failure could result in loss of life [19, 20]. While the system has potential uses for increasing situational awareness during operation and maintenance, improvements must be made to increase reliability.

As hoped, an in-depth level of technical expertise was not required to deploy the system. However, the addition of the WAPs and a network router required a basic knowledge of how to assign IP addresses. The increased latency due to channel congestion was not totally unexpected and is a potential issue with any wireless IoT system operating in an ISM band. The two limiting factors of the system were the poor initial reliability of system components and the sensor race conditions. These factors, along with potential latency issues associated with operating in an ISM band, indicate that the particular system evaluated should probably not be considered for safety-critical applications. However, should component reliability improve and the sensor race conditions be resolved, the system may be acceptable as a means to enhance existing safety policies, procedures, and safety controls through

improved situational awareness. But even if used for situational awareness, a system must reliably indicate the status of critical sensors, or it will not be trusted.

Through the deployment and assessment, it was found that many factors must be considered when selecting wireless IoT systems for safety applications:

1) A fully integrated (turnkey) IoT system, while perhaps requiring less technical knowledge to deploy, may not be easily configured to meet critical functionality, as was discovered in the case of the sensor race condition. Also, a fully integrated solution may not have sensors available to meet specific needs. While less cost-effective and necessitating greater technical expertise and effort to deploy, open platform sensors used in conjunction with a commercial HMI software application could provide more flexibility in monitoring needs.
2) The reliability of components, systems, and networks must be of principal concern. An understanding of any system's long-term component fail rate is essential. Even though 100% reliability is not practically achievable, five-nines reliability should be considered a minimum for safety-critical applications [21].
3) The RF environment in which a system will be operated must be fully understood. This includes not only the potential for wireless channel congestion but also any possible sources of RF interference that may impact wireless network reliability [15, 16].
4) From a practical standpoint, sensor battery life must be considered. A large-scale implementation could employ hundreds of sensors, and battery replacement could become an overwhelming, but network critical task.

7 Conclusion

This study suggests that low-cost wireless IoT technologies may not always be suitable for safety critical applications. However, with some improvements and if used in conjunction with existing policies, procedures, and safety controls, a wireless IoT system shows potential to improve mine worker safety around conveyors through enhanced situational awareness [4, 5]. An IoT system can be configured to generate visual warnings—and potentially text and email notifications—to indicate guard removal, status of mains voltage disconnects, worker proximity to hazardous locations, and other unsafe conditions. A system can also be used to implement engineering controls such as preventing conveyor startup until an unsafe condition has been resolved.

This study also suggests the current state of IoT technologies is not "plug and play." Some technical knowledge of computer networking and RF environments is needed to deploy and maintain even the simplest "turnkey" wireless IoT systems.

Compliance with Ethical Standards

Conflict of Interest The authors declare that they have no conflict of interest.

Disclaimer The findings and conclusions in this paper are those of the authors and do not necessarily represent the official position of the National Institute for Occupational Safety and Health (NIOSH), Centers for Disease Control and Prevention (CDC). Mention of any company name or product does not constitute endorsement by NIOSH.

References

1. Ruff T, Coleman P, Martini L (2011) Machine-related injuries in the US mining industry and priorities for safety research. Int J Inj Control Saf Promot 18(1):11–20
2. MSHA. Safety improvement technologies for mobile equipment at surface mines, and for belt conveyors at surface and underground mines. Proposed rule. Fed Register 83 FR 29716 (to be codified at 30 CFR 56 and 75). 2018 [cited 2019 August 7]; Available from: https://www.federalregister.gov/documents/2018/06/26/2018-13603/safety-improvement-technologies-for-mobile-equipment-at-surface-mines-and-for-belt-conveyors-at. Accessed 7 Aug 2019
3. Reyes MA, King GW, Miller GG (2013) Intelligent machine guard monitoring: a wireless system to improve miner safety. IEEE Ind Appl Mag 20(2):69–75
4. Parks D et al (2019) Intelligent monitoring system for improved worker safety during plant operation and maintenance. Min Eng 71(3):34–38
5. McNinch M, Parks D, Jacksha R, Miller A (2019) Leveraging IIoT to improve machine safety in the mining industry. Mining, Metallurgy, & Exploration 36(4):675–681
6. Zhou C, Damiano N, Whisner B, Reyes M (2017) Industrial Internet of Things (IIoT) applications in underground coal mines. Min Eng 69:50–56
7. inmarsat (2020) The Rise of IoT in Mining. [cited 2020 August 4]; Available from: https://research.inmarsat.com/2020/. Accessed 4 Aug 2020
8. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. Journal of network computer applications 34(1):1–11
9. Ren K, Wang C, Wang Q (2012) Security challenges for the public cloud. IEEE Internet Comput 16(1):69–73
10. Pister K, Doherty L (2008) TSMP: time synchronized mesh protocol. IASTED Distributed Sensor Networks 391:398
11. Sandoval R et al (2017) Evaluating the more suitable ISM frequency band for IoT-based smart grids: a quantitative study of 915 MHz vs. 2400 MHz. Sensors 17(1):76
12. Rao S (2005) Make the most of the unlicensed ISM Band. [cited 2019 August 7]; Available from: https://www.eetimes.com/document.asp?doc_id=1273378. Accessed 7 Aug 2019
13. McGrath MJ, Scanaill CN (2013) Sensor network topologies and design considerations, in sensor technologies: healthcare, wellness, and environmental applications. Apress: Berkeley, CA p 79-95
14. Lu G, Krishnamachari B, Raghavendra CS (2004) Performance evaluation of the IEEE 802.15. 4 MAC for low-rate low-power wireless networks. In IEEE International Conference on Performance, Computing, and Communications. IEEE

15. Salameh HB, et al (2017) Security-aware channel assignment in IoT-based cognitive radio networks for time-critical applications. In 2017 Fourth International Conference on Software Defined Systems (SDS). IEEE
16. Al-Fuqaha A et al (2015) Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Communications Surveys Tutorials 17(4):2347–2376
17. Kloc M, et al (2016) Low latency evaluation of an adaptive industrial wireless communications system for ISM bands. In 2016 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet). IEEE
18. Wetzker U, et al (2016) Troubleshooting wireless coexistence problems in the industrial internet of things. In 2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC) and 15th International Symposium on Distributed Computing and Applications for Business Engineering (DCABES). IEEE
19. Knight JC (2002) Safety critical systems: challenges and directions. In Proceedings of the 24th International Conference on Software Engineering. ACM
20. Encyclopedia.com. Safety-critical system. 2019 [cited 2019 September 27]; Available from: https://www.encyclopedia.com/computing/dictionaries-thesauruses-pictures-and-press-releases/safety-critical-system. Accessed 27 Sept 2019
21. Yu R (2016) Verifying SmartMesh IP >99.999% Data Reliability for Industrial Internet of Things Applications. [cited 2019 August 26]; Available from: https://www.analog.com/media/en/technical-documentation/white-papers/wp008fa.pdf. Accessed 26 Aug 2019

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.