Wireless Coexistence in Mining: A Case Study

Carl B. Sunderman†, Jason B. Coder‡, Susanna Mosleh‡, Nadia P. Yoza-Mitsuishi‡, and Dan P. Terzi†

†Spokane Mining Research Division, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, Spokane, WA, USA
‡Spectrum Technology and Research Division, Communications Technology Lab, National Institute of Standards and Technology, Boulder, CO, USA

***Abstract*— Mining is increasingly relying on wireless communication for a diverse set of functions in the mine. As additional wireless devices and systems are added to the mining cycle, they must continue to function acceptably in the presence of the other wireless devices and systems currently in use. This paper presents a case study to illustrate the importance of testing for wireless coexistence in the mining sector. A commercial wireless Emergency Stop (E-Stop) system is evaluated for wireless coexistence with another technology commonly found in mines: IEEE 802.11 WLAN. Two hypothetical E-Stop application use cases are presented. Functional wireless performance and key performance indicators are defined, and testing is performed. Analyses of the results are shown as they pertain to each application use case. The results indicate that unintended signals can impact the wireless performance of the E-Stop system devices in certain circumstances. The conclusion is that evaluating and understanding wireless coexistence performance can lead to safer and more reliable wireless system deployments on or around safety-critical mining equipment.**

***Index Terms*—Frequency Hopping Spread-Spectrum, Internet of Things, Mining, WLAN, Wireless Coexistence**

I. Introduction

The demand for and use of wireless systems in mining is growing significantly. Automation, real-time monitoring and control, Internet of Things, asset and personnel tracking, emergency communication, and other implementations guarantee that several wireless systems will eventually need to function simultaneously in the same physical area and maintain their stated performance when surrounded by other systems. To help validate the wireless performance of a system, ANSI/USEMCSC C63.27 [1] provides methods to assess wireless coexistence. This standard arose from a need for tests that accurately evaluate the ability of wireless devices to operate in their intended environments, particularly in the vicinity of nearby in-band and adjacent-band transmitters. The medical device sector is a primary user of this standard. However, ANSI/USEMCSC C63.27 is generic and can be used in any sector, frequency band, or with any set of wireless technologies. This paper suggests that evaluating wireless coexistence under ANSI/USEMCSC C63.27 is useful in ensuring the stated performance of safety-critical mining wireless systems.

Coexistence testing typically follows a formal or informal application risk assessment. In the medical device sector, the link between risk assessment and coexistence testing is outlined in AAMI TIR69 [2]. This guideline follows the international organization for standardization (ISO) 14971 [3] - "Medical Devices — Application of risk management to medical devices." and defines four risk categories: Major, Moderate, Minor, and Negligible. ANSI/USEMCSC C63.27 defines three testing tiers: Tier 1, Tier 2, and Tier 3. Tier 1 is the most rigorous and includes thorough testing for both in-band and out-of-band signals, Tier 2 is more rigorous than Tier 3 and may include testing out-of-band signals, while Tier 3 includes a subset of test cases attempting to achieve the greatest confidence with the minimum amount of testing. Under AAMI TIR69, the assignment of risk category maps directly to one of the C63.27 testing tiers. Major to Tier 1, Moderate to Tier 2, Minor to Tier 3, and Negligible to not requiring testing. However, for machine safety applications, other definitions of risk like ISO 12100-"Safety of Machinery" [4] may have different interpretations related to the assignment of testing tier. Thus, in the absence of specific guidance for machine safety coexistence testing, this paper does not address risk assessment, however, [5] provides an example of applying risk assessment for conveyor applications. Instead, this paper provides hypothetical conveyor use cases presenting different levels of risk that, in the absence of specific guidance, arguably could lead to a different assignment of testing tier for each case.

The coexistence of wireless networks operating in the Industrial Scientific and Medical (ISM) bands have been studied, with [6] and [7] being two popular examples. However, these analyses focus on medical devices. The use cases and operating environments in the mining sector have significant differences from their medical counterparts and have not yet been the subject of a published coexistence case study. This paper presents a coexistence case study between two sets of technologies commonly found in surface and underground mines. We walk through the entire process of evaluating wireless coexistence, including identifying the subset of device functionality related to its wireless function, defining "functional wireless performance" (FWP) based on a use case, performing testing, and interpreting the results. We examine two different use cases for the same system to demonstrate the importance of defining FWP and show how the results may be interpreted differently for each use case.

The system under evaluation is a commercial-off-the-shelf (COTS) Emergency Stop (E-Stop) system that operates in the 2.4 GHz ISM band and utilizes a frequency hopping spread-spectrum (FHSS) protocol. It is evaluated against IEEE 802.11n wireless local area network (WLAN).

2024 IEEE Industry Applications Society Annual Meeting (IAS) | 979-8-3503-7271-7/24/$31.00 USG | DOI: 10.1109/IAS55788.2024.11023777

II. Use Cases

One of the key aspects of evaluating a system for wireless coexistence is the definition of the use case and, thus, the FWP of the device. FWP is defined in [1] as: "The subset of the total functionality that both uses the wireless capabilities of the equipment under test (EUT) and would result in unacceptable consequences if degraded or disrupted." In some cases, the E-Stop (our EUT) is used in a safety-critical application where the loss of wireless functionality could result in serious injury. In other cases, the EUT is used as a secondary, backup, or non-critical application where the loss of wireless functionality results in a nuisance to the user.

For the first use case, we consider an application where the E-Stop device is used as a backup to lockout/tag-out during maintenance of a conveyor belt system. In this use case, the wireless E-Stop would be used as an additional safety measure to traditional lockout/tag-out procedures commonly used while performing maintenance on a conveyor belt system. Workers performing the maintenance would all carry wireless E-Stops. In the event the primary lockout is inadvertently removed and the conveyor started, workers could immediately shut down the conveyor. This is a fairly low-risk case for the wireless E-Stop because of the primary administrative and engineering controls already in place around normally de-energized equipment, so we will assign this use case to Tier 3 of ANSI/USEMCSC C63.27.

The second use case we consider presents a higher level of risk. In this use case, personnel working near a conveyor could shut it down immediately should a hazardous situation or accident occur. While a conveyor would have a traditional wired E-Stop, it may be placed away from where the hazardous situation or accident is occurring. It could take time for an individual to travel to the wired E-Stop under these circumstances, and the individual may have been hurt during the accident and unable to reach the wired E-Stop, or would enable shutdown of the equipment from a safe distance without the need to enter a potentially hazardous location post-incident. In either case, the severity of injuries may be reduced by decreasing the time to activate the wired E-Stop. This is a medium risk case because, although there are other engineering controls in place, the equipment is in operation during use of the wireless E-Stop system, so we will assign this use case to Tier 2 of ANSI/USEMCSC C63.27.

The primary failure of this EUT is the inability to successfully transmit an E-Stop signal; however, a secondary failure can occur when the wireless link is lost. If the link is lost, it automatically signals an emergency stop command to the conveyor control system. This is known as a "false-trip". Depending on the control system intervention, a false-trip could have an economic or safety impact due to conveyor damage from a sudden stop. Additionally, false-trips, if occurring regularly, could have an impact on productivity and increase the risk of someone bypassing the safety system.

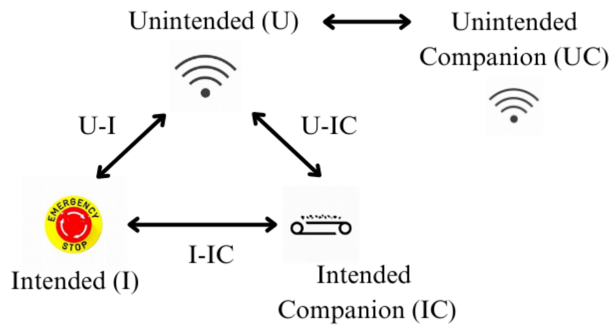

Fig. 1: System Configuration

Figure 1 shows a diagram of the devices used in this study[2]. The EUT ("I" for intended) is a roving E-Stop pushbutton unit that a worker wears. Its primary function is to signal an E-Stop condition to the controller which we will refer to as the EUT companion ("IC" for intended companion) device. The controller unit is located in a fixed location and forms a wireless link with the roving E-Stop pushbutton unit. When an E-Stop event is triggered by the pushbutton unit, the controller unit passes it on to the main control system of the conveyor. There, the control system will execute a procedure to bring the equipment to a safe state. This system is evaluated against an unintended signal from another wireless device ("U" for unintended) present in the environment that could potentially affect the wireless performance of the pushbutton to the controller link. Note also that the unintended device may also form a link to its companion ("UC" for unintended companion) device but, for our purposes in this paper, the UC will be configured to have an insignificant effect on the pushbutton or controller unit.

In the following section, we outline the process of evaluating wireless coexistence as specified in ANSI/USEMCSC C63.27. For reference, Figure 2 [1] presents the flowchart from C63.27 we will use in development of coexistence tests.

III. Test Plan Development

A. Functional Wireless Performance

Before embarking on any coexistence evaluation, it is crucial to consider what aspects of the EUT we need to evaluate. Coexistence testing does not evaluate the entire device; rather, only the subset of functions that use the wireless capability *and* would result in unacceptable consequences if degraded are evaluated. As described in Section II, when the E-Stop button on I is depressed, the I transmits that state to the IC. The IC in turn de-energizes a safety relay which signals the conveyor to enter the E-Stop state. When the E-Stop button is reset on I, the relay will then again energize, allowing the machinery to be restarted. Thus, the FWP for the I-IC system can be defined as both the ability to successfully transmit an

[2]Ordinarily, a photograph of the EUT and a citation to its datasheet would be included. This has been omitted because the authors are prohibited from endorsing a commercial product or its suitability for use.

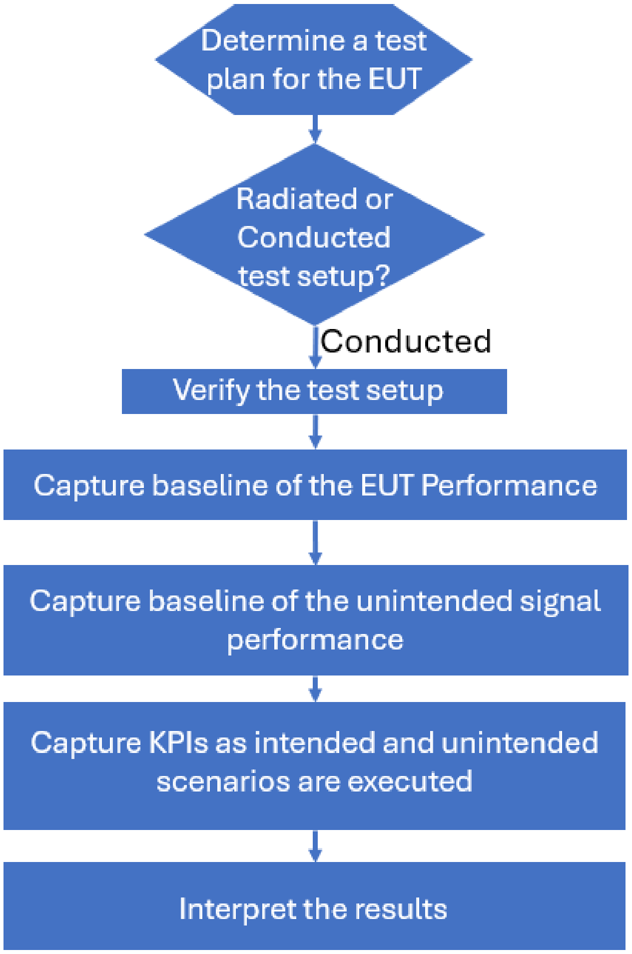

Fig. 2: Test flowchart for coexistence testing [1]

emergency stop signal if (and only if) the button on I has been pressed and to send a reset signal once the switch on I has been reset.

B. Unintended Signal

Selecting the unintended signal(s) requires careful consideration of what other wireless systems and signals are present in the deployment environment. Ideally, this would be informed by a spectrum survey [2], but those can be costly and difficult to perform. More often, the selection is based on the specifications of other systems known to be deployed in the operating environment.

In mining applications, the presence of WLAN signals is becoming increasingly common. An E-Stop system operating in the 2.4 GHz ISM band will likely encounter WLAN signals in its deployment environment. The E-Stop system may also encounter additional wireless signals, but for illustrative purposes, we evaluate a single unintended signal type. Additional unintended signal types could be added to coexistence evaluations by simply repeating the measurement and interpretation process.

WLAN, as the unintended signal, is informative in that it presents a challenge for the FHSS protocol used by the E-Stop EUT. FHSS, like other forms of frequency spreading signals, is generally insensitive to other narrow-band interference, but it is affected by wide-band interference such as from WLAN [8].

C. Key Performance Indicators

With the defined FWP and unintended signal, we can examine what quantities or Key Performance Indicators (KPIs) should be monitored during the coexistence test. Monitoring KPIs serves two purposes in a coexistence test. First, it provides a way to quantify the EUT's coexistence performance. Second, it provides insight into ensuring the test is being run as expected.

In this example, our EUT is a relatively simple device. The signal is either communicated or not, and the link between the I and IC is either functioning or not. To identify if the link between the I and IC is functioning, the relay output on the IC was wired to an LED indicator. This indicator served as the KPI for the I to IC link. As the coexistence test was performed, this indicator would be observed for changes of state. The states observed were normal operation, where the indicator would be lit, intermittent operation, where the indicator would periodically blink over a period of 30 seconds, and failure, where the indicator would be not lit. It should be kept in mind that "Black box" devices, such as this E-Stop system, may not expose interfaces to measure typical KPI's such as throughput, latency, and packet error rate, so simpler KPI's, such as the relay state, must be used instead.

To ensure the test was running as expected, the WLAN link's throughput was used as the unintended signal's KPI and monitored during all phases of the coexistence test. If the throughput dropped or the link became unstable, testing was paused, and the WLAN link reset.

D. Test Matrix

The system under test communicates with a proprietary, non-adaptive, FHSS modulation. For the purposes of this study we did not specifically use Annex A of C63.27 because proprietary FHSS devices are not covered. The test plan we developed considered the testing in Annex A but was modified to be more appropriate for our FHSS EUT. We operate the unintended signal at its maximum duty cycle corresponding to the maximum WLAN link throughput as in Annex A, but adjust bandwidth, transmit power, and center frequency. Our unintended signal, IEEE 802.11n, can operate with a 20 or 40 MHz bandwidth and up to 30 dBm transmit power. We test at 30, 20, and 10 dBm to observe the effect on the FWP due to transmit power. Bandwidth is tested at 20 and 40 MHz. The center frequency of the WLAN signal is tested in the low (2.422 GHz), medium (2.447 GHz), and high (2.452 GHz) end of the FHSS spectrum, which occupies the entire 2.4 GHz ISM band, from 2.4 to 2.483 GHz. Table I shows the possible set of these parameters.

In Table I, the test cases are divided between testing tiers (either Tier 2 or 3) based on the use case they represent. For the use cases in this study the testing and analysis will be similar, the difference being that one will encompass a subset of the other. The lower-risk use case corresponds with Tier 3 and is the least strenuous of the coexistence testing tiers. In this case, Tier 3 includes testing based on placing the WLAN link at different frequencies and at different bandwidths.

By design, Tier 2 testing is meant to be a more strenuous test necessitating more test cases due to higher risk. Our Tier 2 testing includes the Tier 3 set of measurements but adds measurements to assess the EUT's response to the power of the WLAN link.

IV. Method

Testing was performed with the conducted test method described in Annex B of C63.27 and is shown in Figure 3. A diagram of the conducted measurement setup is also shown in Figure 4. In Figure 3, A_x are considered ideal step attenuators, and L_x are cable, insertion, and other losses. The C63.27 conducted test apparatus' s-parameter losses are S_x. Before attaching the devices under test, the programmable attenuators were adjusted so that losses on all ports connected to the devices under test were equal and balanced. Those values were stored, and any additional attenuation was recorded as the L_x attenuations. For device isolation, each of the I, IC, U, and UC devices were placed in their own small, shielded enclosure as demonstrated in Figure 4. All four devices had easily accessible conducted ports. Cables were run from the devices, through a bulkhead connector, then into the test apparatus. The WLAN unintended (U) signal is produced with a COTS development board used as an access point (AP) and a COTS WLAN client device (UC) connected to a computer through USB. The WLAN development board is equipped with open-source software that enables control of the transmit power, frequency channel, and channel bandwidth. It can be programmed to output power up to 30 dBm and produce IEEE 802.11n signaling for both 20 MHz and 40 MHz channel bandwidths in the 2.4 GHz ISM band. WLAN traffic was generated using Transmission Control Protocol (TCP), and the maximum achieved data throughput was 65 Mbps and 130 Mbps for channel bandwidths of 20 MHz and 40 MHz, respectively, simulating full channel utilization. Throughput was sent from the access point to the client. Though there was minimal traffic in the opposite direction, to ensure it did not influence the outcome of the test, a 30 dB attenuator was attached to the client. This meant that any uplink traffic was of significantly lower amplitude compared to the signal from the AP.

For each set of wireless parameters listed as Tier 2 in Table I, the attenuators connected to I and IC were adjusted systematically to simulate an actual radio link loss between them and the U signal. In actual use, this radio link loss would consist of antenna and cable losses in addition to the path loss of propagation. As the attenuators were adjusted, the state of the safety relay was monitored for when the E-Stop system entered and exited the false-trip state. The procedure was as follows. First, the attenuation on the IC (i.e., A_{IC}) was fixed at 0 dB. Next, the attenuation on the I (i.e., A_I) was incrementally increased from 0 dB to 90 dB in 1 dB steps, observing and recording the state of the relay over a period of 30 seconds. Then, the process of adjusting the I attenuation was repeated as the IC unit attenuation was gradually increased to 90 dB in fixed increments of 1 dB. Finally, the entire process was repeated, but this time the fixed attenuations on the I (IC) units were adjusted in steps of 5 dB, from 0 dB to 35 dB.

TABLE I: Testing Tier Matrix

Power (dBm)	Bandwidth (MHz)	Center Frequency		
		High	Medium	Low
30	40	Tier 2, 3	Tier 2, 3	Tier 2, 3
	20	Tier 2, 3	Tier 2, 3	Tier 2, 3
20	40		Tier 2	
	20		Tier 2	
10	40		Tier 2	
	20		Tier 2	

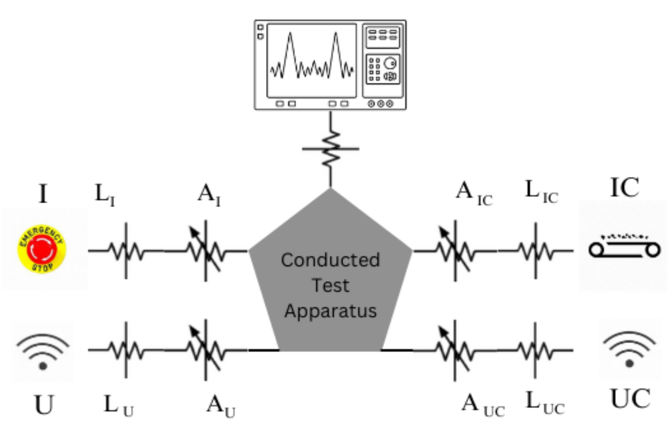

Fig. 3: Test Setup Schematic

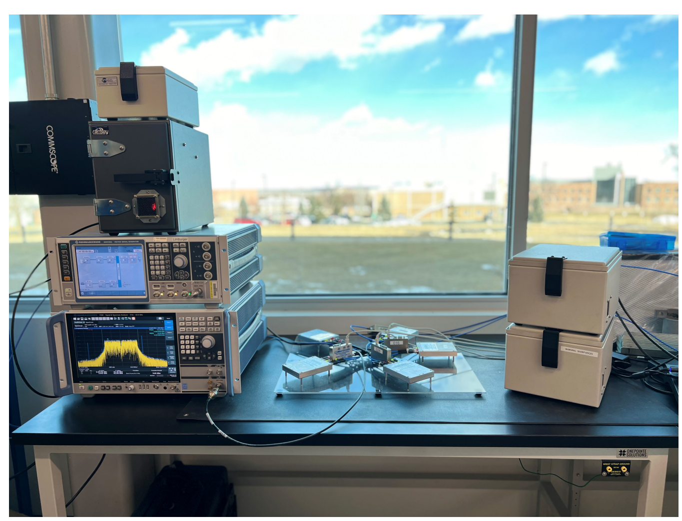

Fig. 4: Photograph of the conducted measurement setup.

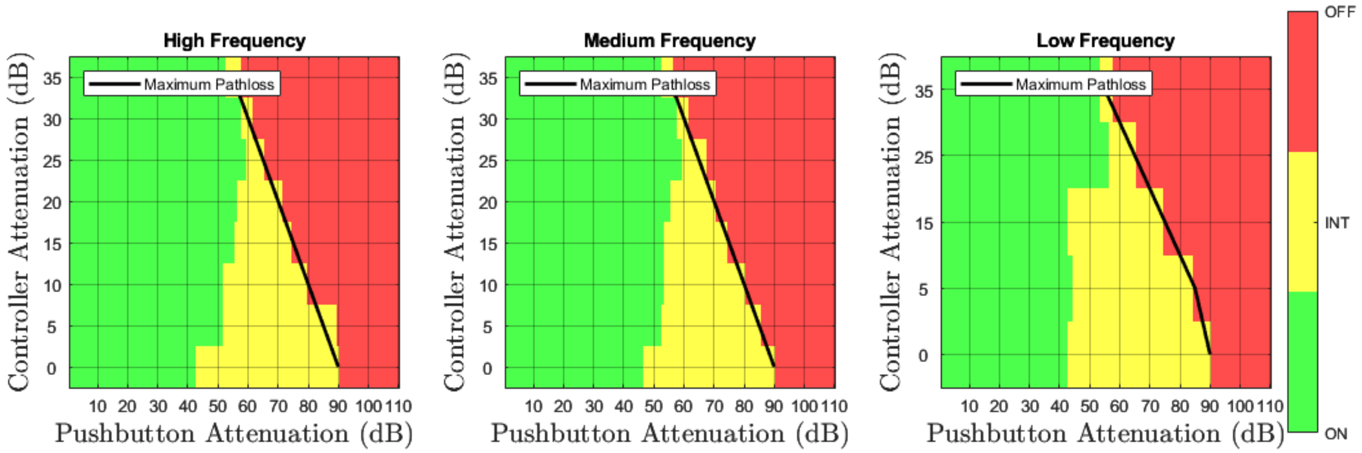

Fig. 5: E-Stop Link Quality for Different WLAN Center Frequencies

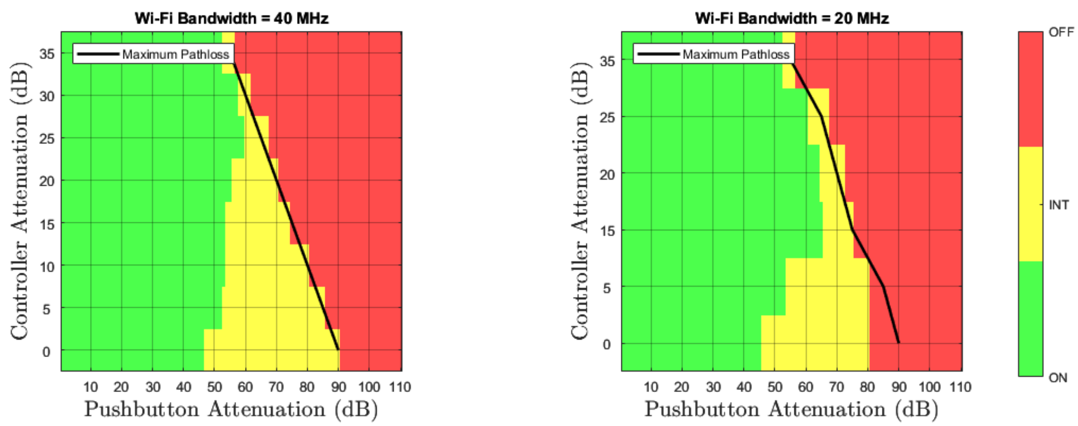

Fig. 6: E-Stop Link Quality for Different WLAN Bandwidths

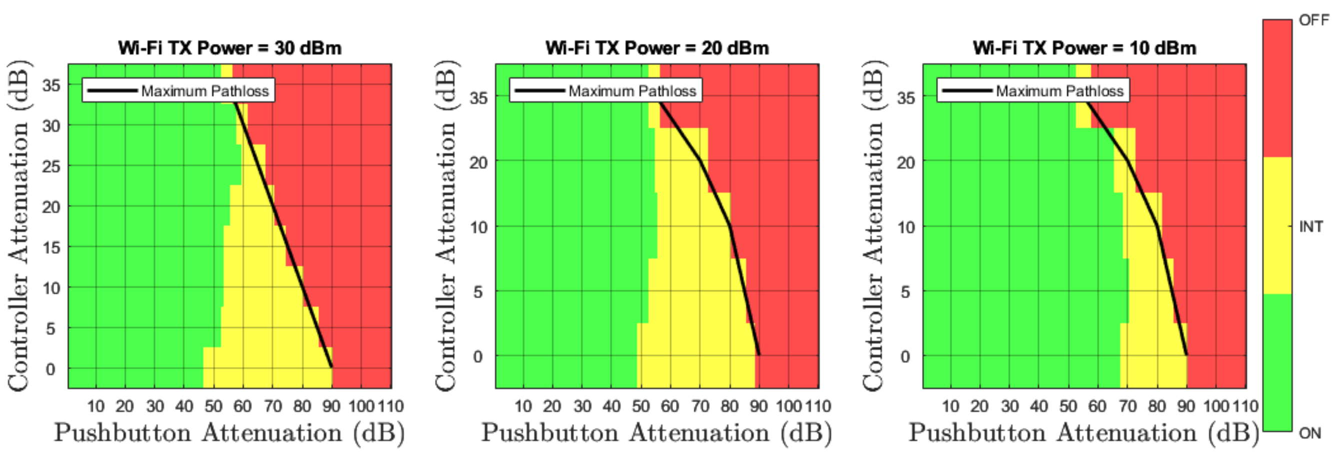

Fig. 7: E-Stop Link Quality for Different WLAN TX Powers

V. Results

Figures 5 through 7 illustrate the impact of WLAN interference on the E-Stop link quality. These plots are shaded to illustrate the link quality variations in response to changes in attenuation at both the I (pushbutton) and IC (controller), as explained in Section IV. The x-axis represents the attenuation adjustments at the I, while the y-axis corresponds to those at the IC. The color gradient demonstrates three distinct states of link quality: "ON," "INT" (intermittent), and "OFF." The system exhibits consistent performance in areas where the link is "ON," indicated by the green color, suggesting optimal conditions for stable communication. The "INT" regions, marked by yellow, highlight the false-trip state scenario with variability in link quality, where the indicator would periodically blink over a period of 30 seconds. Lastly, the “OFF” state, shown in red, represents conditions under which the link is completely lost. These plots provide a comprehensive overview of how varying attenuation levels impact the overall link quality. The solid black line on each plot represents the point at which the I-IC link fails due to path loss, regardless of whether or not there is an unintended signal present.

Figure 5 demonstrates how varying WLAN center frequency affects link quality, while Figure 6 showcases the effect of WLAN bandwidth on the link quality. Both of these figures are part of the Tier 3 testing. Figure 7 focuses on the influence of different WLAN power levels and corresponds with Tier 2 testing.

In interpreting each of these figures, the impact of the WLAN on the I-IC link can be seen as the yellow intermittent region. Comparing the size and shape of these regions across plots can provide insight into understanding which WLAN parameters impact the I-IC link. For example, the impact of different WLAN powers shown in Figure 8 can be seen in the decreasing yellow shaded area as the WLAN power is decreased from 30 to 20, and finally to 10 dBm.

During testing, only False-trip behavior in the EUT was observed. In no instance did we observe a situation where the E-Stop pushbutton failed to send an actual E-Stop signal. Thus, the remainder of our discussion will focus on the false-trip response. This fact is important when evaluating the test results of the two use cases.

VI. Interpretation and Discussion

While the plots of data in Figures 5-7 are useful for examining and comparing the results of coexistence measurements in a graphical way, additional work may be necessary to give the results practical meaning. There are many possible ways of interpreting the test results. Here we will show two: intended-to-unintended (I:U) ratio and a distance approximation [6].

The I:U ratio is the ratio of the peak received intended signal power to the peak received interference (unintended signal) power. This measurement is taken at the spectrum analyzer and adjusted for system losses calculated at the EUT. The I:U ratio can be helpful because it establishes the threshold where the unintended signal can significantly degrade the performance or reliability of the intended link. In practice, this can be used as a guideline for establishing distances between systems to ensure reliable wireless performance.

From Figure 3, the path loss between I and IC is the sum of the attenuations and losses between them. The path loss between the WLAN link and I, and similarly, the WLAN link and IC, is also the attenuations and losses between them. The I:U ratio, in this case, is the difference between these path losses:

$$\frac{I}{U} = [(A_I + A_{IC}) + (L_I + L_{IC}) + S_{I,IC}] - [(A_I + A_U) + (L_I + L_U) + S_{I,U}] \quad (1)$$

TABLE II: I:U and IC:U Ratio for Wi-Fi Middle Frequency Center

Wi-Fi Bandwidth	I:U Ratio (dB)		IC:U Ratio (dB)	
	Wi-Fi Power	Value	Wi-Fi Power	Value
40 MHz	30dBm	40	30dBm	49
	20dBm	49	20dBm	58
	10dBm	68	10dBm	86
20 MHz	30dBm	46	30dBm	64
	20dBm	60	20dBm	79
	10dBm	79	10dBm	86

$$\frac{IC}{U} = [(A_I + A_{IC}) + (L_I + L_{IC}) + S_{I,IC}] - [(A_{IC} + A_U) + (L_{IC} + L_U) + S_{IC,U}] \quad (2)$$

Since the losses in the system are balanced and equal, the I:U and IC:U ratios are:

$$\frac{I}{U} = A_{IC} - A_U \quad (3)$$

$$\frac{IC}{U} = A_I - A_U \quad (4)$$

As the I:U ratio decreases, the effect of the unintended signal on the intended signal increases. The I:U ratio was extracted from some of the test data discussed in Section IV and shown in Table II. Two observations can be made. First, decreasing the WLAN bandwidth from 40 to 20 MHz significantly improves the I:U ratio. Second, linearly reducing the transmit power level of the WLAN signal has a non-linear effect on the I:U and IC:U ratios. These results highlight the variability that each device under test might exhibit during testing and show where modeling as in [6] might differ from measured data.

Figure 8 presents the effect of WLAN (U) transmit power on the transition from the operational (ON) to intermittent (INT), or false-tripped state. In this figure WLAN bandwidth is held constant (40 MHz) at the middle center frequency. It displays the transition in terms of free-space separation distance between the U:I (y-axis) and I:IC (x-axis) signal paths. Free-space separation distance was calculated from the experimental path loss data by applying the Friis transmission equation using 2.15 dBi for all antennas (ideal dipoles).

The solid lines represent the measured test data, while the dashed lines are extrapolations of the I:U ratios to the origin. These extrapolations show the general trend expected in the data rather than its exact shape. To the right in this figure, the test data approaches a vertical asymptote, indicating maximum path loss, at around 126 dB (or around 30 km). To the left, the extrapolated region covers a path loss area not attainable with the conducted test apparatus due to its amount of fixed losses. The x-axis is scaled logarithmically, and although it visually appears to extrapolate down to 1 cm, this is primarily for illustrative purposes. In real-world scenarios, distances below 1 meter are typically not relevant. Therefore, the extrapolated region should be considered in this context, highlighting trends

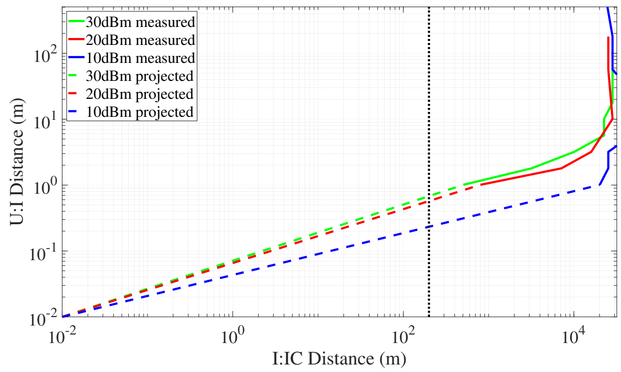

Fig. 8: Path Loss/Distance Relationship at 40MHz BW, Middle Frequency

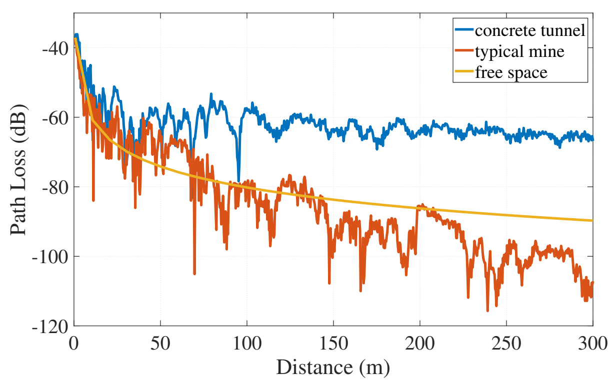

Fig. 9: Path Loss vs. Separation Distance Comparison

rather than suggesting practical measurement ranges below 1 meter.

The manufacturer's datasheet for the E-Stop system specifies an operational range of 200 m. This 200-m point is marked with a vertical dotted line in Figure 8. The point on the y-axis where this line intersects the data effectively represents the separation distance allowed between I and U before the link begins to fail at any point in the operational range. For shorter I to IC ranges, the U to I range is similarly predicted by finding the intercepts to the traces.

The analysis using the Friis transmission equation should be used only for illustrative purposes. Propagation mechanisms in surface locations, and especially so in underground locations, can be different. Cross-sectional tunnel dimensions, other tunnel variations, and antenna polarization effects will cause the path loss to be significantly different [9]. As an example, Figure 9, derived from the propagation model described in [9], plots path loss versus separation distance for free space, smooth concrete tunnel, and a typical eastern coal mine [9]. Note that some underground locations produce an enhancement to propagation over free space path loss while others cause a reduction.

VII. Conclusion

A case study of a wireless coexistence evaluation in the mining sector is presented. The entire process, from use-case formulation, testing tier assignment, device testing, and analysis is discussed. Test plan development and the resulting analysis resulted in one use case being a subset of the other. Data is interpreted in two different ways to demonstrate how laboratory measurements can lead to practical conclusions. For this EUT, we have presented useful colored charts easily showing the effect of changes on the EUT by changes in the wireless parameters of the unintended signal. Also, we have shown approximate separation distance estimates for a selected parameter by extrapolation of the data. It is hoped that this work will increase awareness in not only the mining sector, but also in other industrial sectors, to the significance of coexistence testing in safety-critical industrial applications.

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), or National Institute of Standards and Technology (NIST). Certain equipment, instruments, software, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement of any product or service by NIST or NIOSH, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

References

[1] "American National Standard for Evaluation of Wireless Coexistence," in ANSI/USEMCSC C63.27-2021 (Revision of ANSI C63.27-2017), pp.1-77, 21 Nov. 2021.

[2] AAMI TIR69:2017 "Risk Assessment of Radio-Frequency Wireless Coexistence for Medical Devices and Systems," pp. 1-61, 2017.

[3] "Medical devices — Application of risk management to medical devices," ISO 14971:2019, Edition 3, 2019.

[4] "Safety of Machinery- General Principles for Design- Risk Assessment and Risk Reduction," ISO 12100:2010, 2010.

[5] V. Kecojevic, Z.A. Md-Nor, D. Komljenovic, and W. A. Groves "Risk Assessment for Belt Conveyor-Related Fatal Incidents in the US Mining Industry." Bulk Solids Powder-Sci. Technol., c. 3, sy. 2, pp. 63-73. 2008.

[6] M. O. Al Kalaa, J. Guag, S. J. Seidman, Y. Ma, and J. Coder, "A Case Study of Medical Device Wireless Coexistence Evaluation," in *IEEE Electromagnetic Compatibility Magazine*, vol. 9, no. 4, pp. 47-53, 4th Quarter 2020.

[7] M. O. Al Kalaa, S. J. Seidman, and H. H. Refai, "Estimating the Likelihood of Wireless Coexistence Using Logistic Regression: Emphasis on Medical Devices," in *IEEE Transactions on Electromagnetic Compatibility*, vol. 60, no. 5, pp. 1546–1554, Oct. 2018.

[8] F. Bawahab, E.di Kurniawan, E. Yuniarti, B. Widiyatmoko, and D. Bayuwati, "Performance Evaluation and Mathematical Analysis of Direct Sequence and Frequency Hopping Spread Spectrum Systems under Wideband Interference," in *International Journal of Advances in Intelligent Informatics*, vol. 4, no. 3, Nov. 2018.

[9] C. Zhou, T. Plass, R. Jacksha and J. A. Waynert, "RF Propagation in Mines and Tunnels: Extensive measurements for vertically, horizontally, and cross-polarized signals in mines and tunnels," in *IEEE Antennas and Propagation Magazine*, vol. 57, no. 4, pp. 88-102, Aug. 2015.