EM Risk Management for Wireless Communications: First Look and Case Study

Brian Leeman[1], Laura De Baets[1], Sofie Pollin[2], Hans Hallez[3], Davy Pissoort[1], Tim Claeys[1]
[1]ESAT-WaveCore, Bruges, KU Leuven, 8200 Bruges, Belgium
[2]ESAT-WaveCore, Leuven, KU Leuven, 3001 Leuven, Belgium
[3]CS-DistriNet, Bruges, KU Leuven, 8200 Bruges, Belgium
{brian.leeman, laura.debaets, sofie.pollin, hans.hallez, davy.pissoort, tim.claeys}@kuleuven.be

***Abstract* — With the increased application of wireless communication in mission and safety-critical applications, such as autonomous vehicles, concerns have been raised regarding the reliability and safety of these technologies. Especially of interest is the dependability of these technologies under Electromagnetic Interference (EMI). In the field of Electromagnetic Compatibility (EMC), the idea of Electromagnetic Risk Management (EMRM) forms a promising way of tackling dependability related issues stemming from EMI. In the field of wireless communications, research for mission and safety-critical applications have resulted in Ultra-Reliable Low-Latency Communication (URLLC) technologies. This paper draws parallels between EMRM and URLLC and provides a view on EMRM for wireless communications, which aims to make URLLC systems dependable under EMI. To support the idea of EMRM for wireless communications, a small case study is provided which shows the vulnerability of Orthogonal Frequency Division Multiplexing (OFDM) frame synchronization to Narrowband Interference (NBI) and indicates a necessity for research into EMRM for wireless communications.**

***Keywords* — Mission and Safety-Critical Applications, EM Risk Management, URLLC, OFDM, Narrowband Interference**

I. Introduction

In recent years, the idea of using wireless communications for mission and safety-critical applications has seen a tremendous surge. This includes wireless communication for autonomous vehicles and drones, medical surgical robots, wireless industrial control in an Industry 4.0 setting, etc. [1]. However, there is a major difference between the "classical" applications and these mission and safety-critical applications: losing connectivity, even very briefly, can no longer be viewed as just a nuisance, since a loss of connectivity can be a cause for major safety concerns.

In this context, researchers in the field of wireless communications are trying to solve the problem of how wireless communication for mission and safety-critical applications can be ultra-reliable while having an extremely low latency. To this end, they have started researching so called Ultra-Reliable Low-Latency Communication (URLLC) technologies from a communication theoretic perspective [2] [3] [4].

In the field of Electromagnetic Compatibility (EMC), there has been an increased interest in recent years to look at mission and safety-critical applications and how dependable they are when experiencing Electromagnetic Interference (EMI). This idea has grown into the field of research called Electromagnetic Risk Management (EMRM), where the goal is to try and manage dependability risks when technology is under the influence of EMI [5] [6].

Since wireless communications is particularly vulnerable to EMI, the idea of applying EMRM principles to wireless communication technologies for mission and safety-critical applications is a logical next step. The IEC defines EMI as "degradation in the performance of equipment or a transmission channel or a system caused by an Electromagnetic Disturbance (EMD)" [7]. Common sources of EMDs include power electronics, such as power inverters used in electrical cars, but also wireless power transfer technologies and general electronics with EMC problems.

The goal of this paper is to draw parallels between the EMRM and URLLC research fields as they are presented in literature, because as it turns out, very similar ideas are being developed in both fields of research. With these parallels, a combined vision of EMRM and URLLC can be developed, which we call EMRM for wireless communications. Additionally, a small case study is provided to illustrate this idea of EMRM for wireless communications. In this small case study, light will be shed on a particularly interesting problem, namely that of Orthogonal Frequency Division Multiplexing (OFDM) based frame synchronization under the influence of Narrowband Interference (NBI).

The remainder of the paper is structured as follows. In Section II an overview of the current state of the art with regards to EMRM and URLLC is given and parallels between both fields are drawn. In Section III, the case study on OFDM frame synchronization under the influence of NBI is presented. This section explains the importance of OFDM as a wireless technology, briefly explains its known vulnerability to NBI and continues with illustrating an as of yet unknown/un-researched problem in the state of the art. Lastly the main conclusions of this paper are drawn in Section IV.

II. EMI Resilient URLLC through EM Risk Management

A. Ultra-Reliable Low-Latency Communication (URLLC)

Ultra-Reliable Low-Latency Communication (URLLC) aims to provide wireless connectivity to applications where

this would previously not have been possible because of latency and reliability concerns. The goal is to make wireless technologies as dependable as wired ones while meeting specific application requirements such as data rate and latency.Notably, 5G includes a service category for URLLC, but the term itself applies more broadly. Different applications have varying reliability and latency needs. Examples include V2X communication with a reliability, expressed in the percentage of successfully transmitted packets, of 99.999% or $1 - 10^{-5}$ and a user-plane radio latency of 1ms. Secondly, Industrial wireless control with a reliability of $1 - 10^{-5}$ and a user-plane radio latency of 1 ms. And lastly, the tactile internet (e.g. remote surgical robot control) reliability of $1 - 10^{-9}$ and a round-trip latency as low as 1 ms [2].

To achieve wireless URLLC, important work has been conducted by Popovski et al. [2] [3] and by Bennis et al. [4]. On the one hand, these papers provide a communication-theoretic framework to model and analyse URLLC-based communication systems. One important topic is the inherent trade-off between reliability, latency, data-rate, bandwidth and energy usage. The trade-off between latency and reliability is shown in Fig. 1. Here, the blue curve shows the probability that a packet was delivered within a certain latency, x. If the delivery time misses a deadline, the packet is deemed lost. It is clear that the higher the allowed latency is (higher x), the higher the reliability of the system. On another note, if the latency can be arbitrarily large, then the reliability is equal to $1-P_e$ with P_e the residual packet error probability, but is never one, since certain packets never arrive. One important goal of URLLC is, therefore, to design wireless systems where this blue curve is as steep as possible [2]. To do this, trade-offs with the other system parameters, e.g. data-rate, bandwidth and energy usage need to be made.

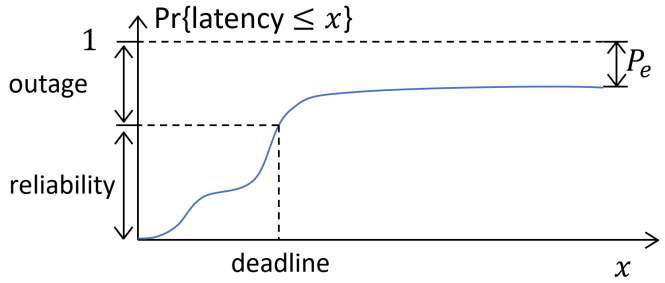

Figure 1. Reliability vs Latency. (based on [2] and [3])

On the other hand, the papers by Popovski and Bennis also describe another need for URLLC, namely the need for managing risks with unexpected/rare events. Rare events is a broad category which generally means conditions which have not been modeled in the communication system or "tail" behaviour of the statistical nature of the system model [4]. This is an interesting evolution since, traditionally, communication system design relies on a communication theoretic approach, seeking optimal solutions for problems. These solutions typically assume a noisy frequency-selective fading channel, and attempt to ensure good average system performance. However, when rare events (such as EMI) occur, these solutions are no longer "optimal," leading to system performance degradation. This is even directly stated in the context of interference (general interference), in [2]: "*The interference in unlicensed, but also sometimes in licensed bands, can be regarded as the most significant 'unknown unknown' in the system model and one should use risk-based methods to assess its impact for URLLC communication*".

Lastly, the reliability/performance of auxiliary processes is very important for URLLC. These auxiliary processes handle tasks such as synchronization between the transmitter and receiver, channel state estimation, and additional protocol exchanges. It is stated that the reliability of these processes can no longer be assumed to be perfect, since their performance affects the overall system reliability, necessitating extra attention [3].

B. Electromagnetic Risk Management

The idea of Electromagnetic Risk Management (EMRM) started from several observations. First, the amount of electronic devices being used for mission and safety-critical applications is exploding. Think about autonomous vehicles, Industry 4.0 and personal medical devices. Secondly, electronic devices are increasingly vulnerable to EMI due to a lower intrinsic immunity because of a continuous demand for smaller and less power hungry devices and an increasing complexity of EM environments because of new technological trends [5]. And lastly, immunity testing can not guarantee the functional safety of a device to a degree that is satisfactory for mission and safety-critical applications. This is in large because of the immense amount of different test combinations that would need to be performed to cover all (or even "enough") bases and because immunity testing standards don't replicate real-life environments to a satisfactory degree [6].

There is data backing up these observations. This data comes from the Manufacturer and user Facility Device Experience (MAUDE) database, which contains reports of adverse events related to medical devices, called medical device reports (MDRs). Analyzing this database for events related to EMC, EMI/RFI, ESD and Wireless Communications problems results in the graph shown in Fig. 2 [8]. It is clear from this graph that there is a rising trend in the reported number of malfunctions and injuries and even a slight increasing trend in the reported number of deaths.

These observations gave rise to the idea of managing risks associated with EMI. The goal of EMRM can be stated as managing the risks associated with EMI of a system to the extent that the system can be deemed dependable under any EMI during its lifespan [5]. There are three big components to EMRM:

1) EM Risk Analysis: As the name suggest, this analysis is responsible for identifying possible risks and estimating their severity. This can happen on a system level, e.g. the risks of EMI on an autonomous vehicle. Alternatively, this analysis can be on a more technical

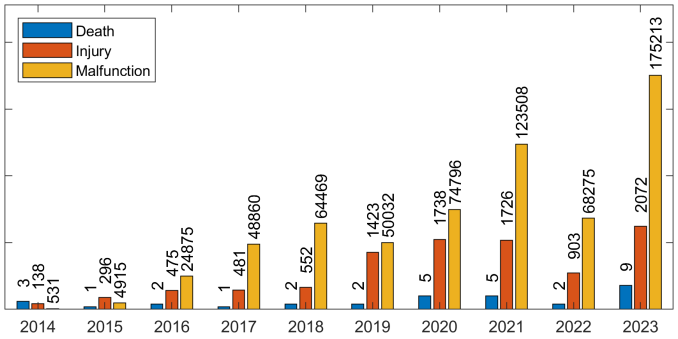

Figure 2. Adverse events with medical devices reported in Maude database related to problems with wireless communications, EMC, EMI/RFI and ESD [8].

level, i.e., how can EMI affect specific technologies, e.g. a wireless communication protocol/system, and how severe is this behaviour.

2) EM Risk Mitigation Techniques: Based on the risk analysis, techniques are developed/used which attempt to make the system more dependable in the face of EMI to an degree that is satisfactory based on system requirements. These kinds of techniques are already readily being applied in existing technology, e.g. error correction codes, differential signaling and filtering to name a few. However, the vision of EMRM is to expand and optimize these types of techniques to ensure maximal risk mitigation in sometimes very specific scenarios. For example, In 2020 the IEEE 1848 standard was released detailing techniques and measures for dealing with functional safety and other risk associated with electromagnetic disturbances. These techniques are meant to give a system inherent resilience towards any EMI, to reduce functional safety and other risks with the system.
3) Validation and Verification: Lastly, before applying EM risk mitigation techniques, they need to be validated and verified for their suitability and performance compared to other methods and system requirements.

C. Electromagnetic Risk Management for Wireless communications

The idea of applying the EMRM principles to wireless communications, is a logical consequence of the issues that EMRM tries to address. After all, wireless communications are particularly vulnerable to EMI. Note the slight difference between interference that is commonly studied in wireless systems, i.e. InterSymbol Interference (ISI), InterCarrier Interference (ICI), co-channel and adjacent-channel interference, and the types of EMI we are interested for EMRM. The commonly studied interferences in wireless communication are usually a result of system design or radio resource management issues. Thus, they can usually be solved using proper and well-known radio resource management techniques. For EMRM we are primarily interested in EMI that we have no control over, e.g. interference from wireless technologies in unlicensed bands or EMI caused by EMDs generated faulty electronics such as power converters. It is this type of EMI where risk based methods become valuable.

This leads to the main point of comparison. URLLC literature calls for a risk based approach for rare events, of which EMI is an example. Since EMRM provides a risk-based methodology for dealing with EMI, let us apply this methodology to the problem of EMI in wireless communications. This is the primary idea of EMRM for wireless communications.

Let us look at a concrete example: the reliability of auxiliary processes, e.g. frame synchronization, in wireless communications under EMI. The importance of these processes for URLLC was stated in Section II-A. The first step is an EM Risk Analysis of these frame synchronization techniques under a specific type of EMD. Such an analysis would likely happen in simulation, where an EMD would be added to the frame synchronization signal and the synchronization performance would be compared to the same signal without the EMD. This comparison then shows the severity of the potential EMI caused by the EMD and should identify the failure mechanisms. The second step is the exploration EM Risk Mitigation Techniques for frame synchronization under the specific EMI. Based on the identified failure mechanisms, highly specialized methods are designed which allow frame synchronization to operate more effectively under EMI. These methods could be adapted techniques which complement existing synchronization techniques, or they could be completely novel. In the latter case, however, performance without the presence of an EMD should be ensured to be on par with existing synchronization techniques. These techniques will likely require a trade-off such as increased receiver complexity, or higher energy usage. Lastly, the EM Risk Mitigation technique performance needs to be validated and verified for the specific targeted application, e.g. is the resulting reliability adequate for V2X communications.

Finally we arrive at a combined vision of EMRM for wireless communications which has three goals. Firstly performing EM Risk Analyses where the effects of a specific EMI on a specific wireless communication systems and their causes are analyzed. Secondly, the exploration/development of EM risk management techniques where targeted counter measures for specific wireless communications against a specific EMI are designed. And lastly, the validation and verification of the developed EM risk management techniques.

III. Case study: OFDM Frame Synchronization under NBI

To illustrate EMRM for wireless communications, this section shows the basic EM risk analysis of a particularly interesting problem, namely that of OFDM frame synchronization under NBI. This problem shows a potential dependability concern for wireless systems which could further be addressed using risk mitigation techniques.

A. *Overview of OFDM Frame Synchronization*

OFDM technology has been the foundation for popular protocols like Wi-Fi, 5G and DAB. These protocols are now being considered as the basis for URLLC systems. For example, Wi-Fi has dedicated version for V2X communication, IEEE 802.11db, often referred to as Dedicated Short-Range Communication (DSRC) [9] and 5G has a URLLC service category.

However, OFDM systems are vulnerable to NBI [10], i.e. an EMI with a relatively small bandwidth compared to the wireless system bandwidth. This vulnerability manifests itself in multiple ways. Firstly, NBI experiences spectral leakage due to the DFT operator used during OFDM demodulation, smearing the NBI across multiple subcarriers [11]. A second, lesser-known, issue is NBI's impact on OFDM frame synchronization. These synchronization processes estimate and correct carrier frequency, carrier phase, sampling frequency, and timing offset. This is necessary because the Local Oscillator (LO) at the transmitter and receiver cannot be phase synchronized and have small frequency errors. In [12] this vulnerability was shown with respect to timing synchronization. The correlation-based nature of synchronization processes, while optimal for Additive White Gaussian Noise (AWGN) channels, makes them susceptible to NBI, which has an inherently high auto-correlation.

The disruption of OFDM frame synchronization procedures because of NBI is a worrying phenomenon for mission and safety-critical applications. If the synchronization procedure fails at the wrong moment and safety-critical communication is disrupted, them the system as whole, e.g. an Autonomous Vehicle, might end up in an unsafe condition. A first step to preventing this is a EM risk analysis like the one presented in this case study.

Before discussing this vulnerability further, let us look at some of these OFDM frame synchronization procedures in more detail when there is only AWGN present. As stated before, OFDM synchronization algorithms are almost exclusively correlation based, such as one of the most widely used synchronization algorithms, the Schmidl & Cox algorithm [13]. The working principle of these algorithms is as follows. Somewhere during data transmission a known sequence/signal is embedded into the frame. This sequence is usually added to the beginning of the frame and is often referred to as the preamble. This is the case for Wi-Fi. However, the sequence can also be added somewhere else in the frame, such as in LTE and 5G. This known sequence is then searched for using correlation operations, resulting in timing synchronization, i.e. knowledge in the exact timing boundaries of the OFDM symbols in the frame. For example, doing a cross-correlation search on the signal received by the RF front-end, i.e. the received baseband signal, and the known preamble in baseband (or a part thereof) will result in a high correlation when two signals are almost identical. Carrier frequency errors are also estimated using correlation operations. Interestingly, this is possible because the phase output of a correlation is equivalent to the average phase difference between corresponding samples in the correlation, which is related to the frequency offset of the signal.

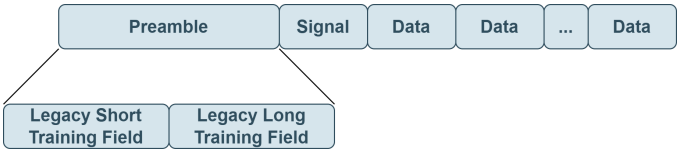

Figure 3. Wi-Fi (IEEE802.11a) physical layer frame.

Let us take a quick look at the physical layer Wi-Fi frame and preamble structure as an example. The simplest Wi-Fi frame, commonly referred to as the Physical layer Protocol Data Unit (PPDU), is constructed as shown in Fig. 3. This was the first frame structure used in the Wi-Fi protocol which was designed for OFDM systems, i.e. in IEEE802.11a. The frame design for newer versions is largely similar, the parts of interest for this discussion remain identical, only with slightly expanded preamble and signal designs to accommodate features such as MIMO. The IEEE802.11a PPDU consists of three main sections: a preamble, a signal, and data symbols. The signal field contains information for physical layer demodulation: the length of the data field and the coding rate. The data field consists of multiple OFDM symbols which contains the frame data and padding. Lastly, there is the preamble which is divided in two separate parts: the Legacy Short Training Field (LSTF) and Legacy Long Training Field (LLTF), each of which serve different purposes for frame synchronization. For example, the LSTF is used for packet detection and initial carrier frequency synchronization, while the LLTF is used for precise timing and precise carrier frequency synchronization.

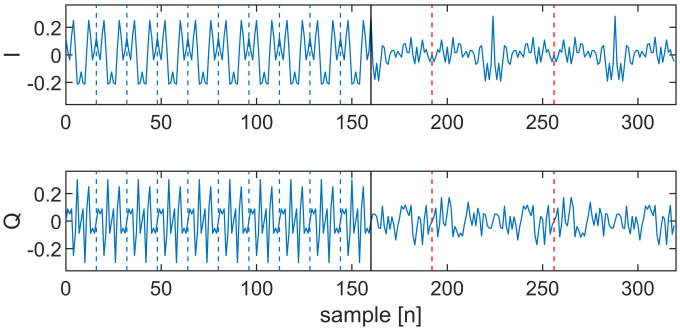

Figure 4. Example of Wi-Fi preamble. First half is LSTF and second half is LLTF. The short sequence boundaries are marked with blue dotted lines and the long sequence boundaries are marked with red dotted lines.

To intuitively expand on these ideas a bit further, Fig. 4 shows an example preamble from a IEEE802.11a frame in baseband. Notice the two distinct halves to this preamble, the left half is the LSTF and the right halve is the LLTF. Notice the repeating sequences in both parts. The LSTF is constructed of 10 identical repeating sequences, and the LLTF is constructed of 2 longer repeating sequences which are prepended by a cyclic prefix, i.e. the end of the sequence is copied to the beginning. This design allows the Wi-Fi receiver to reliably

synchronize to the frame in systems which are only affected by AWGN and frequency selective fading.

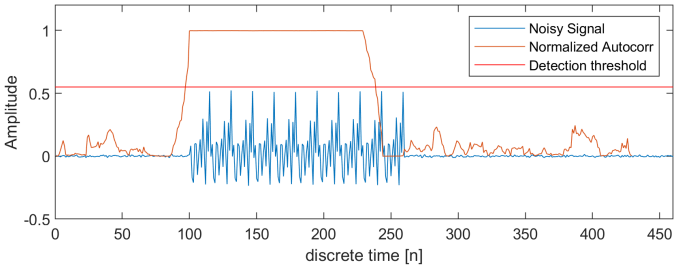

Figure 5. Autocorrelation of LSTF. SNR = 30 dB. Only the In-Phase component of the noisy signal is shown for simplicity.

Let us look at one of the ways synchronization takes places in Wi-Fi systems using this preamble design, namely packet detection. This is performed through an auto-correlation on the received signal from the RF front-end system. For this, the correlation is taken between a section of length L, the length of one sequence in the LSTF, of the received signal and of a time delayed copy of the received signal, with the time delay also equal to L. This auto-correlation searches for self-similarity within the received signal and will thus maximize when the received signal contains the LSTF of a Wi-Fi frame. An example of this is shown in Fig. 5, for a Signal to Noise Ratio (SNR) of 30 dB, where the LLTF of the preamble was omitted for simplicity. Notice that this auto-correlation was normalized and that it produces a plateau because of repeating short sequences in the LSTF. This auto-correlation is then checked with a detection threshold, 0.55 in these simulations, to make a decision about packet detection.

B. Influence of a Continuous Wave NBI on auto-correlation based packet detection

Let us now analyze how OFDM frame synchronization is vulnerable to NBI. For this case study, we will look at what happens to the previously explained OFDM packet detection procedure when it is being influenced by a specific type of NBI, a Continuous Wave (CW) interference. The EMD for this type of NBI can be modelled in baseband according to Eqs. (1) and (2). Here, n is the discrete time, A is the CW amplitude, φ is the CW phase expressed in radians with $\varphi \in \mathbb{R} : 0 \leq \varphi < 2\pi$, and $d + \alpha$ is the CW frequency relative to the amount of OFDM system subcarriers K, with $d \in \mathbb{Z} : -\frac{K}{2} \leq d \leq \frac{K}{2} - 1$ and $\alpha \in \mathbb{R} : 0 \leq \alpha < 1$. The CW frequency is expressed as a sum of d, a subcarrier frequency, and α, an offset to that subcarrier frequency. P_i is the interference power, P_s is the power of the signal being interfered with, and SIR is the Signal to Interference Ratio.

$$CW[n] = Ae^{j(2\pi(d+\alpha)\frac{n}{K}+\varphi)} \tag{1}$$

$$A = \sqrt{P_i} = \sqrt{\frac{P_s}{10^{\mathrm{SIR}/10}}} \tag{2}$$

Let us look at what happens when we inject the noisy signal from Fig. 5 with a CW according to the model in Eqs. (1) and (2) with parameters: $d + \alpha = 5.5$, $K = 64$, $\varphi = \frac{2\pi}{10}$ and a SIR of 7 dB. The result of this is shown in Fig. 6. It is clearly visible that the normalized auto-correlation of this signal is greatly impacted. During the LSTF the auto-correlation no longer reaches the threshold for packet detection and, thus, the packet detection fails in the Wi-Fi system. Also notice that the auto-correlation function exceeds the detection threshold in regions outside of the LSTF, or more precisely in regions without any signal. This makes sense as a NBI has a high auto-correlation. Depending on the Wi-Fi system implementation, this continuous triggering of the packet detection, when no valid packet is actually detected, can cause an unnecessary increase in resource usage and thus a waste of energy. While this increase might be negligible, it is still worth noting.

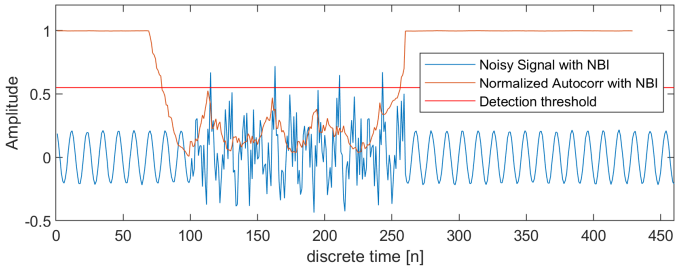

Figure 6. Autocorrelation of LSTF with CW. SNR = 30 dB, SIR = 7 dB and CW parameters: $d + \alpha = 5.5$, $\varphi = \frac{2\pi}{10}$. Only the In-Phase component of the signal is shown for simplicity.

To analyse this further, let us define a rule for valid packet detection. If the normalized auto-correlation exceeds the detection threshold anywhere within the expected range under normal conditions, thus anywhere during the first 8 repeating sequences of the LSTF, we can say a packet is detected correctly. This is of course not an entirely realistic metric, but rather a convenient one for simulations, and can be considered a best case scenario for packet detection. If we now simulate the scenario of Fig. 6 with varying SNR and SIR levels, again with a CW with constant parameters: $d+\alpha = 5.5$ and $\varphi = \frac{2\pi}{10}$, and then calculate the detection error rate based on 1000 observations for each SNR and SIR level, we get the graph from Fig. 7.

This graph shows some interesting phenomena. Firstly, if the SIR is very high, i.e. there is virtually no interference, the detection error rate starts increasing when the SNR is around 4 dB. From this, one can draw the conclusion that the communication systems requires at least a SNR of 4 dB to work correctly. This is in line with the recommended SNR (around 5 dB) for the lowest Modulation Coding Scheme (MCS) in the WiFi standard [14]. On the other hand, when the SNR becomes large, and thus the effect of noise becomes negligible, one can clearly see that the detection error rate starts rising when the SIR is around 11 dB. From this it can be concluded that when the SIR is lower than 11 dB, correct operation of the communication is no longer possible. Depending on the noise level, this SIR threshold can be even higher. For example, at an SNR of 6 dB, which is near the

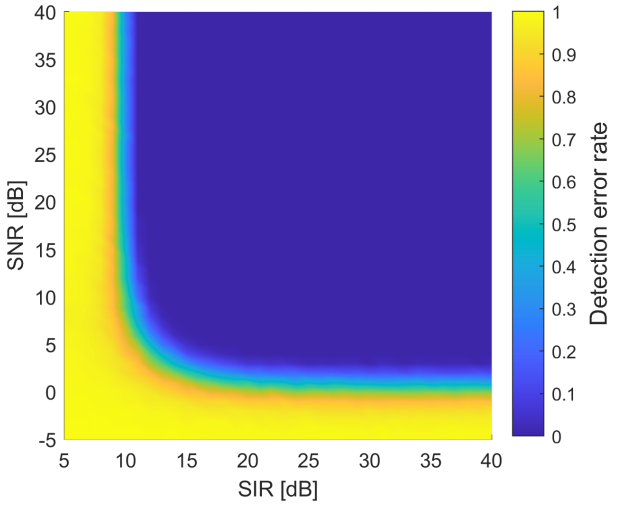

Figure 7. Detection error rate for autocorrelation based frame detection with a detection threshold of 0.55 and with CW parameters: $d+\alpha = 5.5$, $\varphi = \frac{2\pi}{10}$

bare minimum for the correct operation without any EMI, the detection error rate starts going up at an SIR of around 15 dB.

Comparing the minimum SNR and SIR needed for correct operation, around 4dB and 11dB respectively, one can see a clearly higher sensitivity, of about 7 dB, towards a CW EMI than towards AWGN for OFDM packet detection.

From this case study it is clear that a further deep dive into the effects of NBI on OFDM frame synchronization is desirable to paint a clearer picture on this issue with the goal of achieving dependable URLLC under EMI. Analyzing the effect of NBI on carrier frequency offset, carrier phase offset, sampling frequency offset and timing offset estimation are all points of interest for future work. Additionally, the NBI model used in this paper was quite rudimentary, so the inclusion of broader or more sophisticated models in the further analysis is definitely advised.

IV. Conclusions

This paper discusses how Electromagnetic Risk Management (EMRM) principles can be used in wireless communications for mission and safety-critical applications, i.e. for Ultra-Reliable Low-Latency Communication (URLLC). Parallels between the EMRM and URLLC literature were presented, most notably the call for a risk based approach for dealing with EMI. The comparison showed a very significant overlap in the ideas being developed in both fields, which lead to the formulation of a combined vision of EMRM for wireless communication. A case study was presented to illustrate the usefulness of EMRM for wireless communications. The case study showed the significant vulnerability of OFDM auto-correlation based packet detection, a fundamental part of the wireless technology considered for mission and safety-critical applications, towards NBI and proposed further topics of research in this problem space.

References

[1] P. Schulz, M. Matthe, H. Klessig, M. Simsek, G. Fettweis, J. Ansari, S. A. Ashraf, B. Almeroth, J. Voigt, I. Riedel, A. Puschmann, A. Mitschele-Thiel, M. Muller, T. Elste, and M. Windisch, "Latency critical iot applications in 5g: Perspective on the design of radio interface and network architecture," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 70–78, 2017.

[2] P. Popovski, Stefanović, J. J. Nielsen, E. de Carvalho, M. Angjelichinoski, K. F. Trillingsgaard, and A.-S. Bana, "Wireless access in ultra-reliable low-latency communication (URLLC)," *IEEE Transactions on Communications*, vol. 67, no. 8, pp. 5783–5801, 2019.

[3] P. Popovski, J. J. Nielsen, C. Stefanovic, E. d. Carvalho, E. Strom, K. F. Trillingsgaard, A.-S. Bana, D. M. Kim, R. Kotaba, J. Park, and R. B. Sorensen, "Wireless access for ultra-reliable low-latency communication: Principles and building blocks," *IEEE Network*, vol. 32, no. 2, pp. 16–23, 2018.

[4] M. Bennis, M. Debbah, and H. V. Poor, "Ultrareliable and low-latency wireless communication: Tail, risk, and scale," *Proceedings of the IEEE*, vol. 106, no. 10, pp. 1834–1853, 2018.

[5] D. Pissoort, A. Degraeve, and K. Armstrong, "EMI risk management: A necessity for safe and reliable electronic systems!" in *2015 IEEE 5th International Conference on Consumer Electronics - Berlin (ICCE-Berlin)*, pp. 208–210.

[6] D. Pissoort and K. Armstrong, "Why is the IEEE developing a standard on managing risks due to EM disturbances?" in *2016 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, pp. 78–83.

[7] IEC, "electromagnetic interference - IEV ref 161-01-06," International Electrotechnical Vocabulary (IEV), 2018.

[8] B. Leeman and T. Claeys, "Analysis of MAUDE database for reports related to Wireless Communications/EMC/EMI/RFI/ESD issues," 02 2024. [Online]. Available: https://doi.org/10.48804/VV5PBF

[9] G. Naik, B. Choudhury, and J.-M. Park, "IEEE 802.11bd & 5G NR V2X: Evolution of Radio Access Technologies for V2X Communications," *IEEE Access*, vol. 7, pp. 70 169–70 184, 2019.

[10] R. Lowdermilk and F. Harris, "Interference mitigation in orthogonal frequency division multiplexing (OFDM)," in *Proceedings of ICUPC - 5th International Conference on Universal Personal Communications*, vol. 2, pp. 623–627 vol.2.

[11] K. M. Fors, K. C. Wiklundh, and P. F. Stenumgaard, "On the Mismatch of Emission Requirements for CW Interference Against OFDM Systems," *IEEE Transactions on Electromagnetic Compatibility*, vol. 60, no. 5, pp. 1555–1561, Oct. 2018.

[12] M. Marey and H. Steendam, "Analysis of the narrowband interference effect on ofdm timing synchronization," *IEEE Transactions on Signal Processing*, vol. 55, no. 9, pp. 4558–4566, 2007.

[13] T. Schmidl and D. Cox, "Robust frequency and timing synchronization for ofdm," *IEEE Transactions on Communications*, vol. 45, no. 12, pp. 1613–1621, 1997.

[14] GNS Wireless, "Signal to Noise Ratio WiFi — SNR WiFi Table," https://www.gnswireless.com/info/signal-to-noise-ratio-snr/, accessed: 03/05/2024.