

Dependable Wireless Communications

In Smart Cities, with a focus on safety-critical applications?

Dr. Tim Claeys

What can go wrong?



What can go wrong?



What can go wrong?

Mobileye self-driving car runs red light during public demo

SEAN SZYMKOWSKI MAY 22, 2018 3 COMMENTS

Companies continue to race at lightspeed to bring self-driving cars to market, but along the way, the robo cars have had their fair share of incidents.

The latest error occurred in Jerusalem. While Mobileye showed off its latest self-driving car prototype, the vehicle ran a red light during a press demonstration.

Bloomberg reported on the incident on Tuesday and Mobileye has since declared onboard television cameras interfered with the car's own camera system. The self-driving car reportedly identified the red light, but electromagnetic interference cut the signal, and the car crept through the intersection instead.

Mobileye's safety driver let the car move through the intersection, likely as a valuable learning experience.



“It was a very unique situation,” he said, referring to the camera crew. “We’d never anticipated something like this.” Shashua said Mobileye was also modifying the hardware designed to shield the car’s computers from electromagnetic interference in order to prevent similar incidents in the future. Mobileye’s Jerusalem fleet has continued to operate and the company hasn’t received any complaints from automakers, Shashua said.

Let us have a look at wireless communications under electromagnetic disturbances!

What does the European Law say about immunity testing of wireless communication?

The Radio Equipment Directive

- What are the essential requirements
 1. Radio equipment shall be constructed so as to ensure:
 - (a) the protection of health and safety of persons and of domestic animals and the protection of property, including the objectives with respect to safety requirements set out in Directive 2014/35/EU, but with no voltage limit applying;
 - (b) an adequate level of electromagnetic compatibility as set out in Directive 2014/30/EU.
 2. Radio equipment shall be so constructed that it both effectively uses and supports the efficient use of radio spectrum in order to avoid harmful interference.
 3. Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements:

The Radio Equipment Directive: EMC testing for radios => the EMC Directive

Article 6

Essential requirements

The equipment shall meet the essential requirements set out in Annex I.

1. General requirements

Equipment shall be so designed and manufactured, having regard to the state of the art, as to ensure that:

- (a) the electromagnetic disturbance generated does not exceed the level above which radio and telecommunications equipment or other equipment cannot operate as intended;
- (b) it has a level of immunity to the electromagnetic disturbance to be expected in its intended use which allows it to operate without unacceptable degradation of its intended use.

The Radio Equipment Directive: ETSI EN 301 489-1

ETSI EN 301 489-1 V2.2.3 (2019-11)



**ElectroMagnetic Compatibility (EMC)
standard for radio equipment and services;
Part 1: Common technical requirements;
Harmonised Standard for ElectroMagnetic Compatibility**

The Radio Equipment Directive: ETSI EN 301 489-1

9.2.2 Test method

The test method shall be in accordance with CENELEC EN 61000-4-3 [3], clauses 6, 7 and 8.

The following requirements and evaluation of test results shall apply:

- the test level shall be 3 V/m (measured unmodulated). The test signal shall be amplitude modulated to a depth of 80 % by a sinusoidal audio signal of 1 000 Hz. If the wanted signal is modulated at 1 000 Hz, then an audio signal of 400 Hz shall be used;
- the test shall be performed over the frequency range 80 MHz to 6 000 MHz with the exception of the exclusion band for transmitters, receivers and duplex transceivers (see clause 4.3), as appropriate;
- for receivers and transmitters the stepped frequency increments shall be 1 % frequency increment of the momentary used frequency;
- the dwell time of the test phenomena at each frequency shall not be less than the time necessary for the EUT to be exercised and to be able to respond;

NOTE: Dwell time is product dependent.

- the frequencies selected and used during the test shall be recorded.

The Radio Equipment Directive: Efficient use of the spectrum

ETSI EN 300 220-1 V3.1.1 (2017-02)



**Short Range Devices (SRD) operating
in the frequency range 25 MHz to 1 000 MHz;
Part 1: Technical characteristics and
methods of measurement**

The Radio Equipment Directive: EN 300220

Emissions	Immunity	Other
Effective radiated power	Receiver saturation at adjacent channel	RX sensitivity level
Maximum effective radiated power	Spurious response rejection	
Duty cycle	blocking	Behavior at high wanted signal level
Occupied bandwidth	Adjacent channel selectivity	Polite spectrum access
Frequency error		Bi-directional operation verification
TX out of band emissions		
Unwanted emissions in the spurious domain		
Transient power		
Adjacent channel power		
TW behavior under low voltage conditions		
Adaptive power control		

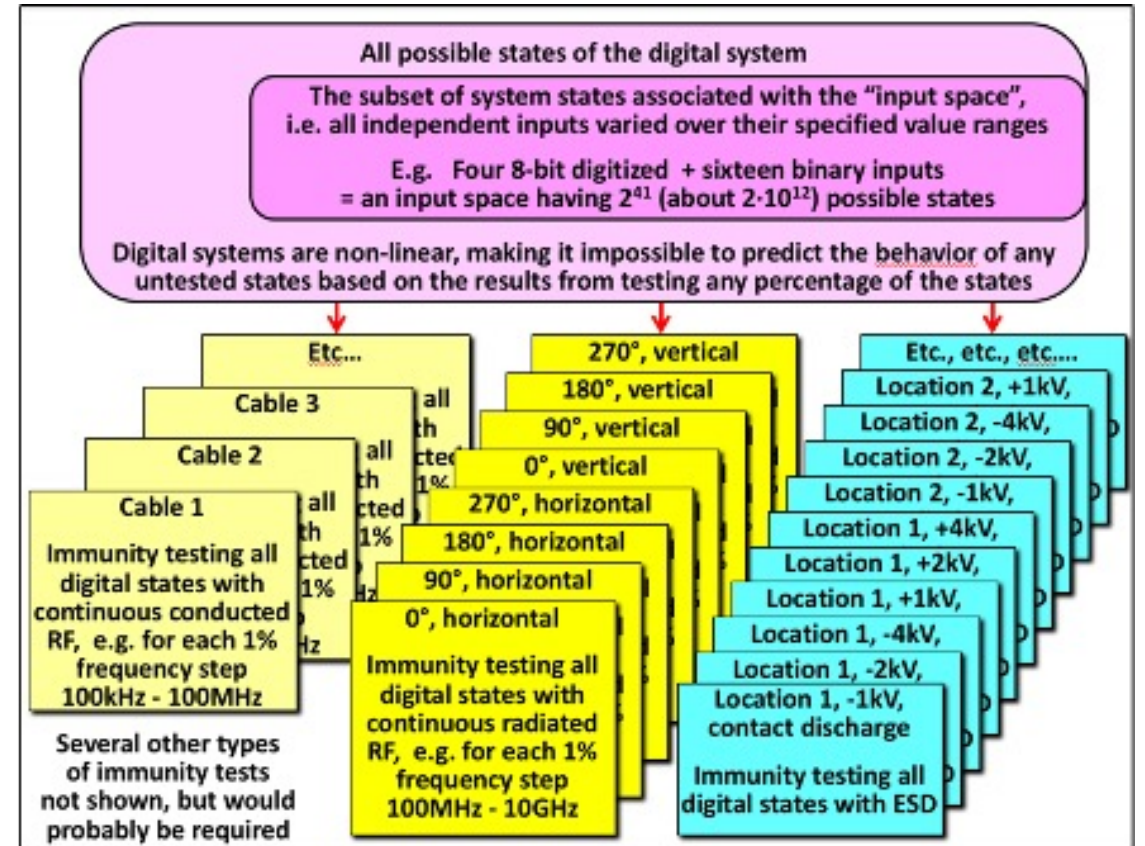
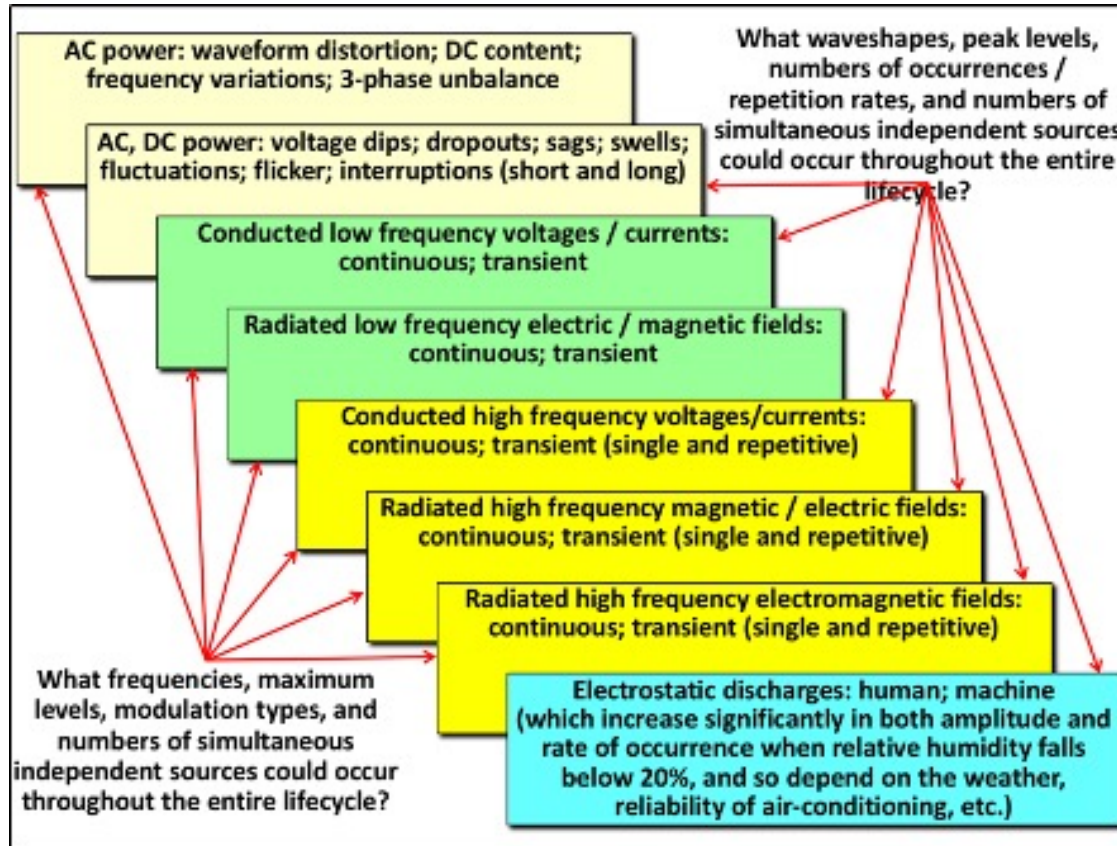
The Radio Equipment Directive:



What about in-band testing?

If we would have an in-band testing standard,
will the wireless communications be safe then?

The exploding test plan



Can we use the EMC risk-based approach for wireless communications?

Risk-Based Approach

- Follows a thorough **systems-engineering approach**
- Assessment of:
 - the expected actual EM environment
 - immunity and emission characteristics of equipment
- Then: Implement necessary measures (incl. non-technical)
- Some parts/equipment will be hardened more, some others less compared to the “rule-based EMC-approach”

Risk based approach

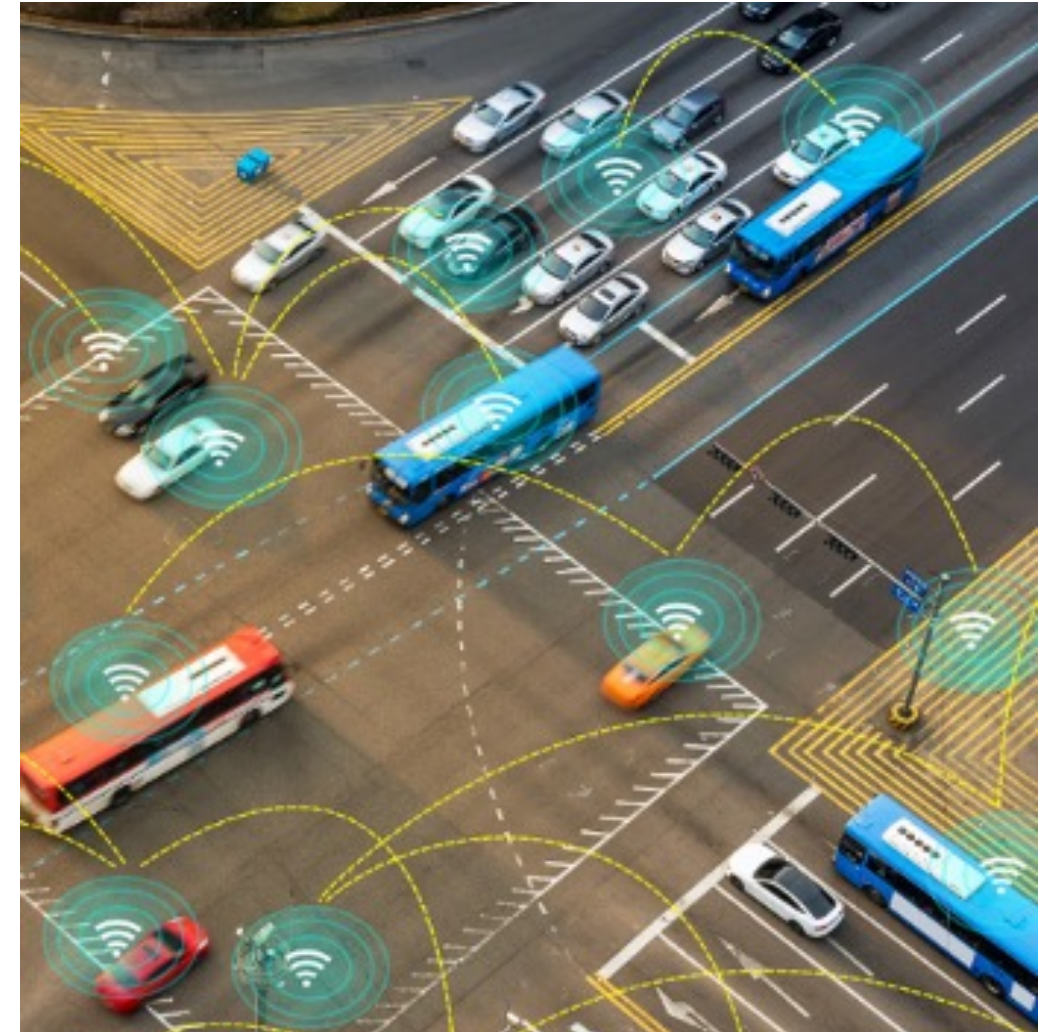
- Not new, this is well known
- Goal is to make sure your device works for the given environment, not more, not less!

Applicable to wireless communications?

Let us have a look at “EMC for functional safety” or
“EM Resilience”

Vehicle-to-X Communication

- Car-to-car
- Car-to-infrastructure
- Car-to-pedestrian
- Etc.
- **Robust wireless communication (5G) is key element!**



What is EM Resilience

- “A system is resilient if it can adjust its functioning prior to, during, or following events (changes, disturbances, and opportunities), and thereby sustain required operations under both expected and unexpected conditions.”
 - Erik Hollnagel, author of the book “Resilience Engineering”
- Resilience of a safety-related system = the ability of the system to remain acceptably safe despite unforeseeable events
- Electromagnetic resilience is the term given to the new functional safety risk-management discipline that describes how to use techniques and measures to manage functional safety risks as regards of electromagnetic disturbances

So for us....



Risk-Based EMC

EM Resilience

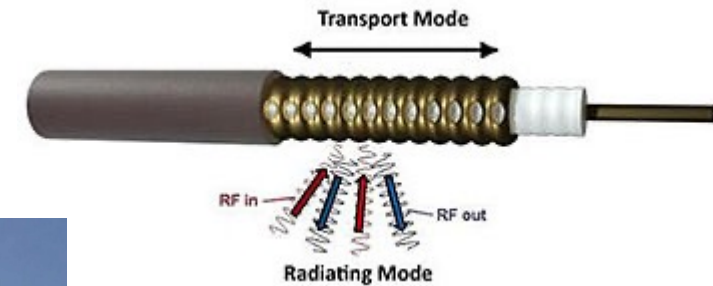
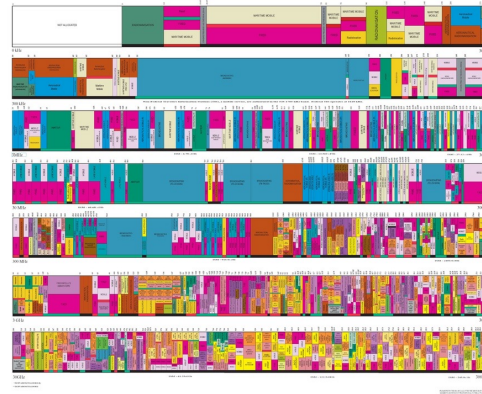
IEEE 1848 for wireless communications?

IEEE 1848 A.3.25: Careful use of wireless (radio) data communications

- Continuous transmission wireless communications
 - Is TDMA enough?
 - Can we use NOMA
- Co-existence testing and its lack thereafter in the EMC standards
- The use of heart beats
- EM diverse redundant channels
- The ANSI C63.27 co-existence standard and the AAMI TIR 69-2017 guide

What can be added?

- Spectrum management
- Use of near-fields
- Antenna arrays
- Wireless protocol diversity
- The use of specific interference avoidance techniques



guus.leenders@kuleuven.be

Waves: Core Research and Engineering
(WaveCore), Technologiccampussen Gent en
Aalst

Gebroeders De Smetstraat 1
9000 Gent

[KU Leuven kaart](#)

lokaal: 02.B221

tel. +32 9 331 65 47

What do we do @ KU Leuven campus Bruges?

Dynamic avoidance of interference in Bluetooth Low Energy



Article

Bluetooth Low Energy Interference Awareness Scheme and Improved Channel Selection Algorithm for Connection Robustness

Bozheng Pang^{1,*}, Kristof T'Jonck¹, Tim Claeys², Davy Pissoort², Hans Hallez¹ and Jeroen Boydens¹

- ¹ M-Group, DistriNet, Department of Computer Science, KU Leuven Bruges Campus, 8200 Bruges, Belgium; kristof.tjonck@kuleuven.be (K.T.); hans.hallez@kuleuven.be (H.H.); jeroen.boydens@kuleuven.be (J.B.)
² M-Group, WaveCoRE, Department of Electrical Engineering, KU Leuven Bruges Campus, 8200 Bruges, Belgium; tim.claeys@kuleuven.be (T.C.); davy.pissoort@kuleuven.be (D.P.)
* Correspondence: bozheng.pang@kuleuven.be

Abstract: Bluetooth Low Energy (BLE) is a popular wireless communication protocol heavily used in Internet of Things applications. Nowadays, robustness is considered a key requirement in wireless communication. However, radio interference from various sources may affect the performance of BLE devices, leading to channel congestion. Therefore, there is a broadly recognized need of methodologies capable of sensing and avoiding interference. In this paper, two improvements at the data link layer for interference detection and channel selection are proposed to enhance the BLE connection robustness. This paper also presents a wide range of experimental evaluations aiming at validating the improvements and providing insights on both these improvements. Particularly, the communication performance of the BLE link layer is assessed in terms of channel usage distribution, supervision timeout ratio (STR) and packet loss rate (PLR) under different interference environments. Results from these experiments (reliability over 97% and 99% under two different harsh environments) highlight the effects of both improvements on the BLE robustness. Meanwhile, the authority of scheduling the whole mechanism is given to the link layer and even the higher application layer. This paper provides a set of solutions for BLE confronting interference in link layer.

Keywords: Bluetooth Low Energy (BLE); link layer; interference; channel selection algorithm; reliability; robustness



Citation: Pang, B.; T'Jonck, K.; Claeys, T.; Pissoort, D.; Hallez, H.; Boydens, J. Bluetooth Low Energy Interference Awareness Scheme and Improved Channel Selection Algorithm for Connection Robustness. *Sensors* **2021**, *21*, 2257. <https://doi.org/10.3390/s21072257>



bozheng.pang@kuleuven.be

Gedistribueerde en Veilige Software
(DistriNet), Campus Brugge

Spoorwegstraat 12

8200 Sint-Michiels

[KU Leuven kaart](#)

tel. +32 50 66 49 72

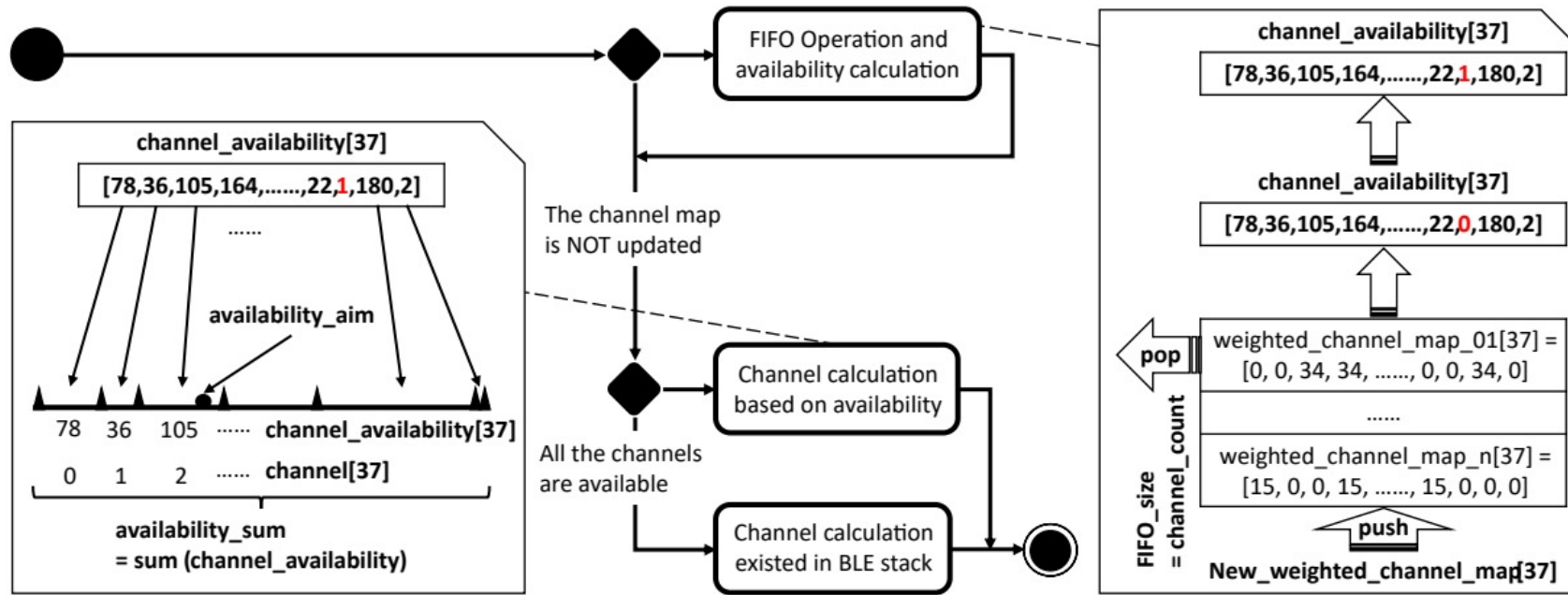


Figure 5. The main logic for the improved CSA.






Table 3. The results of STR and PLR under different conditions (the * represents no data tested for that condition).

		CSA #1	CSA #2	Improved CSA
fixed controlled Wi-Fi interference (after 10,000 connection events)	STR	2.73%	3.27%	0.78%
	PLR	2.73%	3.26%	0.74%
random controlled Wi-Fi interference (after 100,000 connection events)	STR	*	5.65%	2.78%
	PLR	*	5.65%	2.80%
uncontrolled Wi-Fi interference (after 100,000 connection events)	STR	*	4.51%	0.76%
	PLR	*	4.13%	0.72%

A Novel Method of Removing the Influence of Continuous Electromagnetic Wave Disturbances in OFDM Systems

IEEE TRANSACTIONS ON ELECTROMAGNETIC COMPATIBILITY

A Novel Method of Removing the Influence of Continuous Electromagnetic Wave Disturbances in OFDM Systems

Aleksandr Ovechkin , Student Member, IEEE, Tim Claeys , Member, IEEE, Dries Vanoost , Member, IEEE, Guy A. E. Vandebosch , Fellow, IEEE, and Davy Pissoot , Senior Member, IEEE

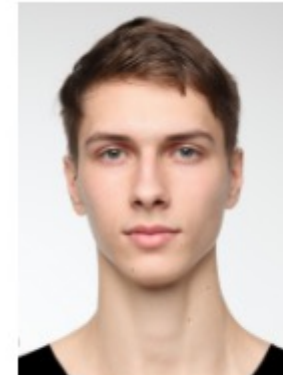
Abstract—This article describes a novel technique for removing the influence of a continuous wave (or narrowband) electromagnetic disturbance in orthogonal frequency division multiplexing (OFDM) systems with quadrature amplitude modulation or phase-shift keying modulation schemes. The technique relies on a mathematical derivation of how a continuous wave electromagnetic disturbance induces spectral leakage in the OFDM system. Using this derivation, an algorithm is obtained that aims to cancel the continuous wave electromagnetic disturbance by estimating its frequency, retrieving its amplitude and phase from the corrupted OFDM frame. Note that the algorithm does not require any prior information about the disturbance. The proposed algorithm is validated through thorough simulations, covering different modulations, noise variations, and spectral leakage cases, and compared with standard OFDM performance without the algorithm. Through our experimentation, it has been demonstrated that for a disturbance frequency not equal to one of the OFDM subcarriers, the algorithm can estimate the disturbance frequency with high precision, resulting in a gain of more than 80 dB when compared to the case without the algorithm. For a disturbance frequency equal to one of the OFDM subcarriers, a simple coding technique such as Hamming & interleaving enables the user to remove the disturbance.

Index Terms—Continuous wave (CW) noise, electromagnetic disturbance (EMD), narrowband interference, noise cancellation, orthogonal frequency division multiplexing (OFDM).

into autonomous systems including automobiles. Within the automotive sector, there are six levels of automation [1]. The sixth level does not require any supervision or a human-in-the-loop that presents significant engineering challenges, including, among other things, electromagnetic compatibility (EMC), reliability, and safety. The IEEE 802.11bd and 5G New Radio (NR) protocols are seen as the most probable ones to be used in autonomous vehicles [2]. The communication basis for these protocols is orthogonal frequency division multiplexing (OFDM) [3].

OFDM divides its bandwidth into multiple subcarriers orthogonal to each other, allowing to eliminate guard intervals between subcarriers (which are used in frequency division multiplexing) and increase the bandwidth efficiency. By introducing orthogonal subcarriers, an OFDM system can reduce the intersymbol interference due to multipath fading to a bare minimum [3]. However, despite all its advantages, OFDM is not flawless and has drawbacks such as sensitivity to Doppler shift and frequency synchronization, high peak-to-average-power ratio, and a decrease in efficiency due to the implementation of guard intervals [3].

The two new previously mentioned communication protocols (IEEE802.11bd and 5G NR) will be used in vehicle-to-everything (V2X) communication. Their main fea-



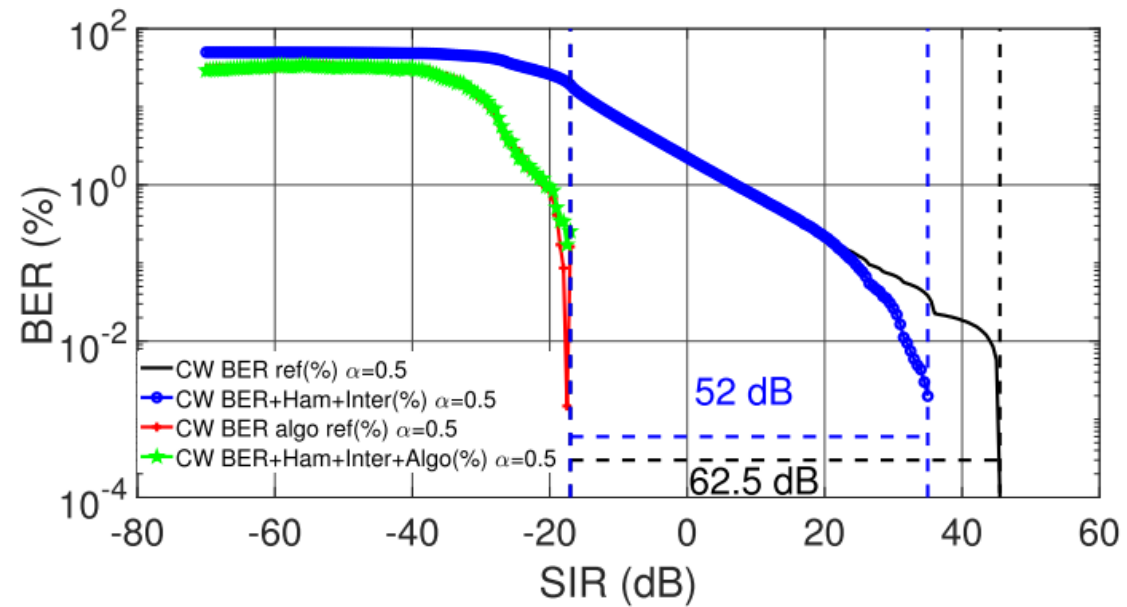
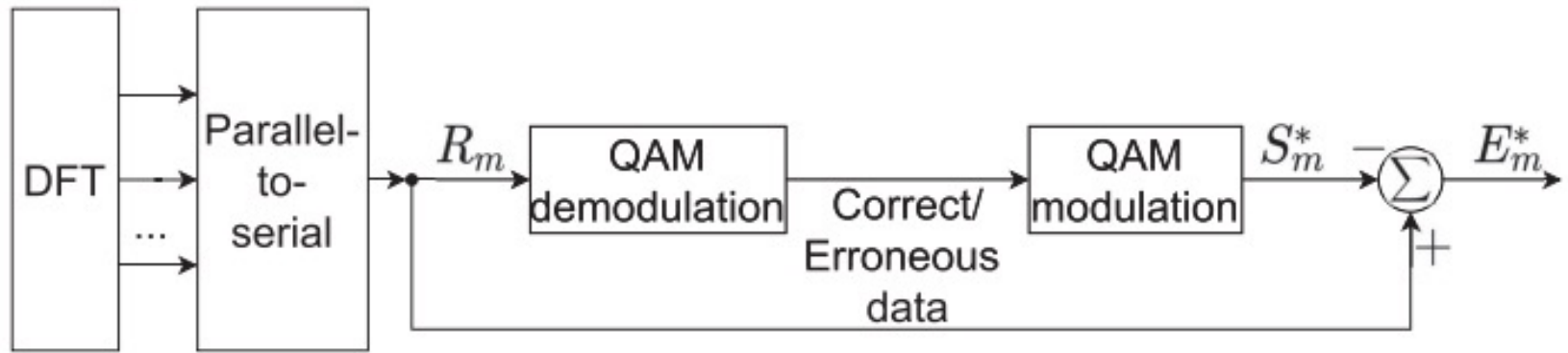
aleksandr.ovechkin@kuleuven.be

**Waves: Core Research and Engineering
(WaveCore), Campus Brugge**

Spoorwegstraat 12
8200 Sint-Michiels

[KU Leuven kaart](#)

tel. [+32 50 66 49 66](tel:+3250664966)



And many more...

The Need for and How To Evaluate Continuous Wave Immunity of Wireless Systems used in V2X Applications

Tim Claes
M-Group
KU Leuven Bruges Campus
8200 Bruges, Belgium
tim.claes@kuleuven.be

Aleksandr Ovechkin
M-Group
KU Leuven Bruges Campus
8200 Bruges, Belgium
aleksandr.ovechkin@kuleuven.be

Dries Vanooost
M-Group
KU Leuven Bruges Campus
8200 Bruges, Belgium
dries.vanooost@kuleuven.be

Guy A. E. Vandebosch
ESAT-Telemic
KU Leuven
3000 Leuven, Belgium
guy.vandebosch@kuleuven.be

Davy Pissoot
M-Group
KU Leuven Bruges Campus
8200 Bruges, Belgium
davy.pissoort@kuleuven.be

Characterizing the Robustness of Wi-Fi and Bluetooth against Continuous Wave EM Disturbances inside a Reverberation Chamber

Aleksandr Ovechkin
ESAT-WaveCore, M-Group
KU Leuven Bruges Campus
Bruges, Belgium
aleksandr.ovechkin@kuleuven.be

Tim Claes
ESAT-WaveCore, M-Group
KU Leuven Bruges Campus
Bruges, Belgium
tim.claes@kuleuven.be

Dries Vanooost
ESAT-WaveCore, M-Group
KU Leuven, Bruges Campus
Bruges, Belgium
dries.vanooost@kuleuven.be

Guy A. E. Vandebosch
ESAT-WaveCore
KU Leuven
Leuven, Belgium
guy.vandebosch@kuleuven.be

Davy Pissoot
ESAT-WaveCore, M-Group
KU Leuven
Bruges, Belgium
davy.pissoort@kuleuven.be

Abstract—This paper describes a detailed test setup and procedure to characterize the robustness of Wi-Fi and Bluetooth 4.2 against continuous wave electromagnetic disturbances inside a reverberation chamber. Bluetooth 4.2 robustness was also characterized by continuous broadband noise. These experiments aim to reveal the susceptibility of commonly used wireless communication protocols against continuous wave noise. Results show that Wi-Fi has an abrupt rise in the packet error rate (up to $\approx 100\%$) when the continuous wave noise overlaps with the Wi-Fi working frequency. Bluetooth 4.2 is robust against continuous wave noise, even when the frequency hopping technique, but fails against broadband noise.

vehicles topped 18.2 billion in 2020 [2]. Note that there are other wireless technologies, which are also widely used (LoRa, Sigfox, Zigbee, LTE, 5G NR, etc.). With such a big increase in devices, the allocated working bandwidth for each device can overlap what leads to Electromagnetic Interference (EMI). EMI itself can be either intentional or unintentional. This paper focuses on the latter. Unintentional EMI may occur due to the use of different communication protocols within the same allocated bandwidth. For example, in [3] the author clearly shows that in different parts of the world the aforementioned wireless communication protocols can work within the same frequency range which significantly increases the chances of EMI.

Index Terms—Electromagnetic interference, EMI, Electromagnetic disturbances, EMI, Continuous Wave noise, CW, Narrowband interference, Broadband interference, IEEE 802.11g, Bluetooth

EMI unavoidably happens from time to time. According to [1], interference can be classified into three categories:

Abstract—This paper describes an initial study of the susceptibility to EMI of wire-vehicle technologies which are or will be used in Intelligent Transportation Systems (ITS). In starting frequency-coverage between the two most recent Radio Access Technologies (RATs) IEEE802.11ad and NR-V2X are related to appear. Yet some of them consider single/multi-frequency EMI as a possible interference despite the fact that these can and will appear in reality. In this paper two simulation methods and a real-life test method, in a reverberation chamber, are proposed to evaluate the reliability of the RATs under these interferences. Single-frequency CW interference evaluation is possible for a limited number of combinations using simulation, but multi-frequency CW simulations are nearly impossible to evaluate due to the large amount of possible combinations. Solutions are proposed to use a smaller test set of combinations. Evaluation of the RATs using simulation can be very useful, but will never reveal the full story how the RAT will react to interference. Therefore, a real-life test method in a reverberation room, or MIMO antenna measurement system, is proposed to try to cover the full RAT protocol for a smaller set of test combinations.

Index Terms—NR-V2X, IEEE802.11ad, Reverberation room, immunity characterization, simulation



Development of an EMI Detector Based on an Inverted Data Pair with Reduced Number of False Negatives

Hasan Habib
M-Group
KU Leuven Bruges Campus
8200 Bruges, Belgium
hasan.habib@kuleuven.be

Tim Claes
M-Group
KU Leuven Bruges Campus
8200 Bruges, Belgium
tim.claes@kuleuven.be

Dries Vanooost
M-Group
KU Leuven Bruges Campus
8200 Bruges, Belgium
dries.vanooost@kuleuven.be

Guy A. E. Vandebosch
ESAT-Telemic
KU Leuven
3000 Leuven, Belgium
guy.vandebosch@kuleuven.be

Davy Pissoot
M-Group
KU Leuven Bruges Campus
8200 Bruges, Belgium
davy.pissoort@kuleuven.be

Abstract—This paper proposes a design of an EMI detector, based on an inverted data pair, for the detection of unwanted electromagnetic disturbances on a wired communication channel with the aim to reduce the overall safety risks related to bit errors on such a communication channel. The EMI detector can detect unwanted electromagnetic (EM) disturbances and generate a warning, which can help the system to follow a precautionary procedure. The performance of the EMI detector is analysed by simulating a random pattern of transmitted bits through a wired channel in the presence of (continuous wave) EMI with varying amplitude, phase, frequency and phase difference between the lines in the inverted data pair. This performance itself is determined by two main metrics: (I) false positives, the number of generated warnings when there is no bit error and, (II) false negatives, the number of bit errors without any warning given by the detector. An ideal EMI detector would have zero false positives and zero false negatives. In this paper, the goal is mainly to reduce the number of false negatives. The EMI detector can be made by using low-cost electronics. It works quite effectively in most of the cases and works better than other detectors presented in the literature.

Index Terms—EMI Sensors, EMI Risk management, EMC, functional safety

for sophisticated and safe electronic devices is continuously rising for mission-critical applications. Electromagnetic interference (EMI) can affect performance, corrupt the information, and at the extreme, cause a fatal failure of the system [1]. For the same reason, Electro-Magnetic Compatibility (EMC) Engineering and System Safety Engineering are both gaining importance.

In many electronic devices, safety-related risks due to errors in communication channels are critical, especially as we are moving towards e.g. autonomous systems. For decades, wired channels have played a pivotal role in the communication networks and still represent one of the essential mediums for electronic data transfer. The probability of disturbance in wired channels due to EMI is continuously rising [2]. The increase in the demand for sophisticated and safe transmission channels, leads to the desire for the development of EMI resilient communication networks. A number of techniques have been proposed in the recent past to protect the data from EMI [3]. Conventional methods used for the protection of systems from EMI include shielding, filtering and grounding,

Risk Management of Wireless Communications with regards to Electromagnetic Disturbances, An Addition to IEEE1848 or a New Guide?

Tim Claes
ESAT-WaveCoRE
KU Leuven Bruges Campus
Bruges, Belgium
tim.claes@kuleuven.be

Abstract—This paper discusses the suggestions on risk management with regards to electromagnetic disturbances for the careful use of wireless communication systems in the IEEE1848 standard. The suggestions serve as a good base for risk management with regards to electromagnetic disturbances when using wireless communications. The suggestions are continuous transmission wireless communications, Co-existence testing, heart beats and diversity. Yet, a lot more techniques can be implemented and used to increase the general dependability of the communication link under electromagnetic interference. A set of techniques like spectrum management, antenna arrays, etc. is discussed. All these techniques are summarized and elucidated. The radio equipment directive (RED) is also shortly discussed with its regards to safety. This paper has as a goal to show that a lack exists in risk management for wireless communication with regards to electromagnetic disturbances and in-band standardized interference testing.

Index Terms—com-pb

the requirement of less errors than 10^{-9} per hour to a safety-critical network [6]. Specifically for safety-critical networks in industrial networks, IEC61784-3 [7] has been written to reach the Safety Integrity Level(SIL) 3 with, in most cases, a black box approach and with the added countermeasures of a Cyclic Redundancy Check (CRC), Numbering and Timestamping messages [6]. In [6], Pesarico et al. introduced a first step of implementing the IEC61784-3 approach on an industrial Internet of Things (IIoT). Although successfully implemented, the wireless communications cannot deliver the performance needed to fully enable safety-critical networks via wireless communications yet. There have been many other implementations and research on industrial networks via wireless communications [81-101] on the topics of its reliability

Combining 2oo3 Voting and Hamming Error Correction to Reduced the Occurrence of False Negatives in Wired Communication Lines under Continuous-Wave Electromagnetic Disturbances

Mohammad Kameli
ESAT-WaveCore
KU Leuven Bruges Campus
Bruges, Belgium
mohammad.kameli@kuleuven.be

Tim Claes
ESAT-WaveCore
KU Leuven Bruges Campus
Bruges, Belgium
tim.claes@kuleuven.be

Davy Pissoot
ESAT-WaveCore
KU Leuven Bruges Campus
Bruges, Belgium
davy.pissoort@kuleuven.be

Abstract—In this paper, a multi-layer scheme to increase the safety of wire communication lines against electromagnetic interference is evaluated. The multi-layer approach consists of a voter based on three wired communication lines which are or are not optimally time diverse. On a second layer, Hamming encoding and decoding is implemented. Each separate technique and possible multi-layer approach is evaluated in simulation under a wide range of single-frequency electromagnetic disturbances. A new way of combining both layers is introduced, i.e. using warnings of the first layer in the second layer is presented. The results show an increase in the safety of the communication system (i.e. reducing the number of false negatives) when combining multiple layers. As a bonus, the availability of the communication system can also be increased by combining multiple layers, if one chooses to.

Index Terms—Electromagnetic Interference (EMI), EMI-resilience, EMI detector/corrector

I. INTRODUCTION

It goes without doubt that advancements in electronic systems inevitably leads to more complex electromagnetic environments and, as such, to more opportunities and increased likelihood of Electromagnetic Interference (EMI) between electronic systems [1]. At the same time, electronic systems are being used more and more for or within safety- or mission-critical systems [2].

In a TMR system, the same data is sent over three parallel traces. While TMR with 2oo3 voting has proven its advantages for coping with random failures of components due e.g. vibrations or ageing [5], it struggles with coping with the systematic failures that are caused by electromagnetic disturbances leading to EMI interferences (EMI). At the same time, all E/E/PE devices generate electromagnetic disturbances. EMI can corrupt the signal, and in extreme cases, it can cause fatal errors. In order to keep the devices in a safe operation especially in harsh electromagnetic (EM) environments, a focus on managing safety risks due to EM disturbances is gaining more and more importance [1].

Advanced applications of smart devices are significantly dependent on the communication channel between the different devices and/or the outside world. The robustness and resilience of the communication channel depends on many

Effectiveness of a Matched Filter to Cope With Harsh Phase and Amplitude Modulated EMI

Jonas Lannoo, Tim Claes, Dries Vanooost, Jonas Van Waes, Student Member, IEEE, Jeroen Boydens, Member, IEEE, and Davy Pissoot, Senior Member, IEEE

Abstract—This article investigates the effectiveness of a matched filter to cope with continuous wave electromagnetic disturbances that are phase and amplitude modulated from wireless systems, e.g., binary phase shift keying and quadrature amplitude modulation. A wired communication channel between sender and receiver that uses nonreturn-to-zero-level data encoding is disturbed by those nearby wireless systems. A matched filter is used on the wired communication channel to filter out the additional unwanted wireless disturbance. The bit-error rate (BER) is calculated after filtering and decoding the received voltages and is used as a metric to compare different kinds of disturbances and different levels of sampling frequency. The results show that the matched filter is very effective when the carrier frequency of the disturbance is equal to an integer multiple of the bit frequency and when not equal to the sampling frequency. This sampling frequency is determined by the bit rate of the desired signal and the oversampling factor on which the matched filter is based. Finally, the filter gain at a BER of 0.1 % is determined. This gain shows that an oversampling of 4 times per bit and using a matched filter already results in an average filter gain of 10–15 dB.

Index Terms—Bit-error rate (BER), digital signal processing, electromagnetic interference (EMI) risk management, matched filter.

where safety is of utmost importance like autonomous robots and cars, co-bots and hospitals nowadays comprise a huge set of sensors and wireless electronics that have to work in a safe and safety-critical manner. With the contemporary knowledge, one would think that this is an easy task, but the reality is misleading and disappointing. All these devices have to work seamlessly together in an increasingly polluted electromagnetic (EM) environment, which is indeed not an easy task. Additionally, not only the interference and coupling mechanism [which could be (near)far field coupling of EM waves depending on the distance between victim and source] of innocent wireless devices but also other types of interference such as intentional-EMI interference are important, where the goal is to disturb a system intentionally. This is often done in malicious practices or for warfare purposes where hundreds or thousands of volts per meter are used to disrupt a system. The approach of adding a matched filter at the receiver of susceptible communication channels could improve the bit-error rate (BER) significantly, keeping in mind that other hardware parts are necessary to protect the physical hardware (gates/transistors/junctions/capacitors) [1].

To create a system that is able to work perfectly in an EM environment and that can perform safety-critical operations, the

Comparative Study on AFH Techniques in Different Interference Environments

Bo-Zheng Pang¹, Tim Claes², Davy Pissoot², Hans Hallez² and Jeroen Boydens¹
¹Department of Computer Science, M-Group, KU Leuven Bruges Campus
²Department of Electrical Engineering, M-Group, KU Leuven Bruges Campus
Sporroewegstraat 12, 8200 Bruges, Belgium
{Bozheng.Pang | Tim.Claes | Davy.Pissoot | Hans.Hallez | Jeroen.Boydens}@kuleuven.be

Abstract— In this paper the use of Adaptive Frequency Hopping (AFH) as a solution to interference problems caused by the proximity and simultaneous operation of radio systems in the 2.4 GHz band is discussed. The main algorithms for AFH that attempt to avoid frequency collisions are considered. A comparative analysis of their respective performance is conducted. The trends and trade-offs for different interference levels are discussed. Performance is analyzed in terms of collision frequency and channel usage distribution frequency.

Keywords— Bluetooth Low Energy, Frequency Hopping, Channel Selection, Interference, Robustness

I. INTRODUCTION

In recent years, the concept of IoT (Internet of Things) has become more and more popular. It is expected to be a revolutionary update for information transfer in multiple dimensions. Smart devices would be allowed to connect, transfer and even make autonomous decisions on behalf of people. This new technology is called ‘connectivity for anything’ [1], which is defined as ‘to be able to connect anywhere, anytime and anything.’

In order to achieve the connectivity for anything, wireless communication is a must for IoT systems. This will introduce a large number of wireless communication protocols.

both of which help increase the performance of AFH [5]. Other frequency hopping algorithms, as shown in [6–8], developed by researchers from related domains also exist. This paper makes a comparison between CSA #1 and #2 in different interferences. It shows how both algorithms react to different environments. Our results will provide more information to help developers make a decision between CSA #1 and #2. This paper will offer some ideas to help for the future improvement of algorithms.

The paper is organized as follows. Section II presents the channel selection algorithms in AFH technology in BLE. Section III illustrates the experimental setup for the algorithm simulation. In Section IV, the results of the simulation experiments are demonstrated and analyzed, and some discussion about them are performed. Section V concludes the paper. Section VI proposes future work.

II. ADAPTIVE FREQUENCY HOPPING

In this section, two different AFH techniques, in use by BLE, are explained from a software algorithm point of view. Their results will be compared in section III.

A. Basic Concept and Logic

A System’s Perspective on the Use of EMI Detection and Correction Methods in Safety Critical Systems

Tim Claes
ESAT-WaveCoRE, M-Group
KU Leuven Bruges Campus
Bruges, Belgium
tim.claes@kuleuven.be

Hasan Tirmizi
ESAT-WaveCoRE, M-Group
KU Leuven Bruges Campus
Bruges, Belgium
hassan.tirmizi@kuleuven.be

Hasan Habib
ESAT-WaveCoRE, M-Group
KU Leuven Bruges Campus
Bruges, Belgium
hasan.habib@kuleuven.be

Dries Vanooost
ESAT-WaveCoRE, M-Group
KU Leuven Bruges Campus
Bruges, Belgium
dries.vanooost@kuleuven.be

Guy A.E. Vandebosch
ESAT-WaveCoRE
KU Leuven
Leuven, Belgium
guy.vandebosch@kuleuven.be

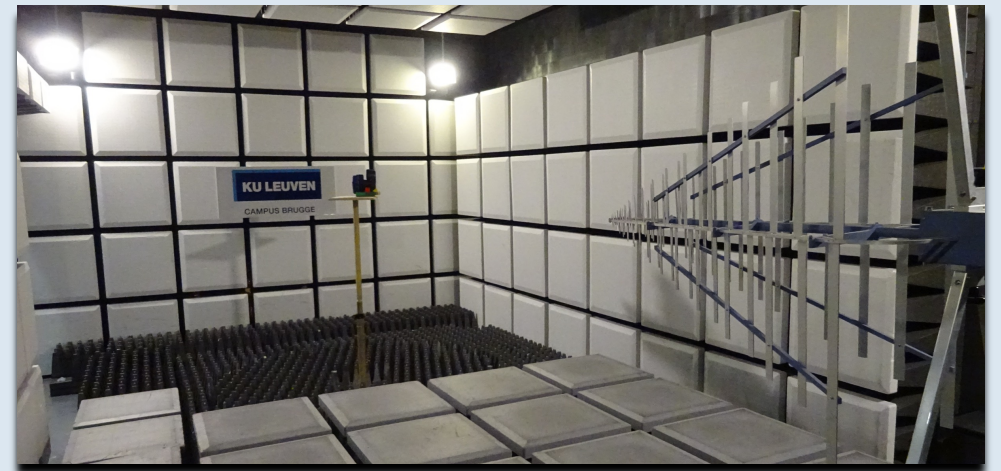
Davy Pissoot
ESAT-WaveCoRE, M-Group
KU Leuven Bruges Campus
Bruges, Belgium
davy.pissoort@kuleuven.be

Abstract—In this paper we discuss the condition assessment definitions previously used to analyse the effectiveness of ElectroMagnetic Interference (EMI) detectors/correctors. It is shown that these definitions do not resemble the correct condition and an expansion is needed. New expanded condition assessment definitions are presented and evaluated in comparison with the old ones for a two out of three majority voter system used in an Electro Magnetic (EM) diverse system. The new definitions provide a better insight into the effectiveness of EMI detectors on its own or in correctors. We also discuss the use of the new definitions in a multi-layer error detection and correction system.

Index Terms—EM resilience, EMC, Risk management, EMI detectors/correctors

Dependable Services @ FMEC

www.fmec.be





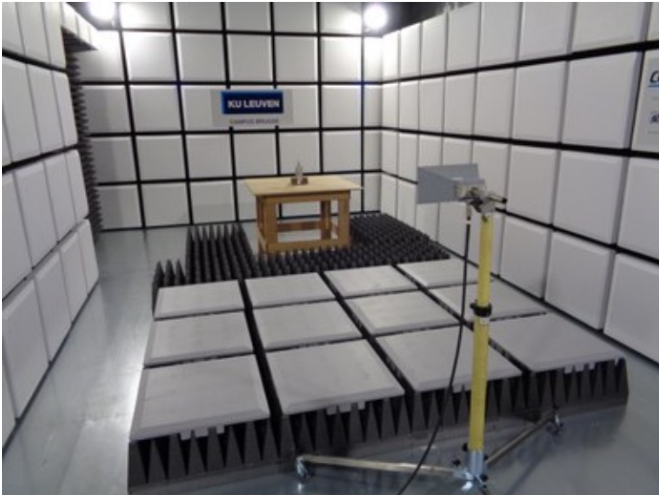
3m Semi-Anechoic Chamber (SAC)



High-end Power analysis system for harmonic emission and Flicker



Large 15 cm automotive stripline



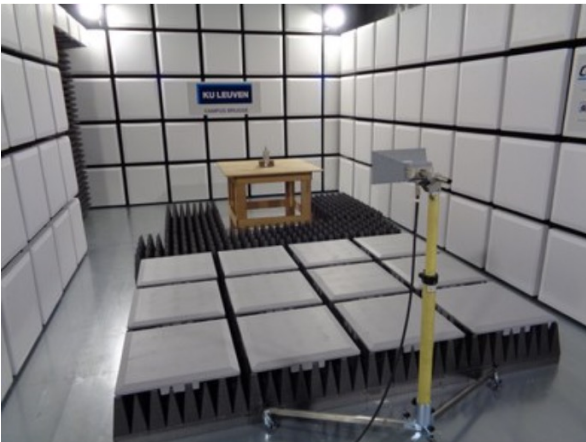
2 port 14 GHz Vector Network Analyzer

FMEC OFFERS CONSULTING RELATING TO

- EMC
- RED
- Functional safety
- Environmental testing
- ...



- High frequency update
 - Vector signal generator R&S SMM100A
 - 100KHz-44GHz
 - 500MHz baseband bandwidth
 - Multi carrier CW
 - IEEE802.11
 - OFDM
 - 5G NR
 - Vector signal analyzer R&S FSVA3000
 - 100KHz-44GHz
 - 2GHz baseband bandwidth
 - Vector signal analysis
 - IEEE802.11
 - OFDM
 - 5G NR



Research projects at European level





Questions?