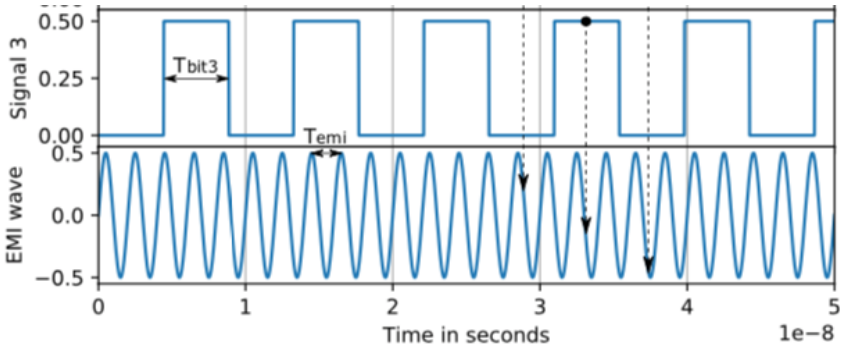
Hardware and Software Techniques and Measures to Effectively Manage EMI Functional Safety Risks



Keith Armstrong, Davy Pissoort and colleagues discuss the effectiveness of different hardware and software based techniques and measures used to reduce risks related to electromagnetic disturbances in mission- or safety-critical systems.

Concerns about the possibly serious consequences of Electromagnetic Interference (EMI) in mission- and safety-critical applications started about two decades ago. At first, the general belief was that all that was needed was a more solid application of the classical "hardware-only" EMI mitigation (i.e. grounding, filtering, shielding, etc.) combined with more severe testing (i.e. increased test levels). However, recent literature [1]-[3] has shown that no feasible and economically affordable EMI test plan can ever prove the high (equivalent) mean-time-to-dangerous-failures required within mission- or safety-critical applications. Indeed, an enormous amount of testing (i.e. multiple decades of continuous testing) would be required to duplicate all possible combinations of the many simultaneous types of EMI that an electronic system may encounter over its lifetime in its operational environment, while also covering all possible states of both hardware and software. Because digital systems are non-linear, no subset of testing can prove that the whole is safe and/or dependable enough.

More recently [4], insight has grown and indicates that the only cost-effective approach is the one in which the classical EMI mitigation techniques are complemented with a thorough EMI risk analysis, as well as appropriate risk reduction techniques and measures (T&Ms) that are typical in the discipline of Functional Safety. These T&Ms can be applied both in hardware as well as in software. The aim is to develop systems that are inherently resilient

to EMI. In case of disturbance, the applied T&Ms should make the system fault-tolerant for EMI so that the system either continues to work as intended in a safe manner or switches itself into a safe-state. This approach is described in general terms in the IET Code of Practice on EMI for Electromagnetic Resilience [4][5] and is also included in the IEEE Standard on Managing Risk due to EMI [6]. Although IEC 61508, the mother standard on Functional Safety, describes a broad set of T&Ms that over the years have become well understood, well-proven and widely used, these T&Ms were not originally developed to deal with EMI, nor were they ever studied in detail with respect to EMI. As EMI has become a major safety concern, these T&Ms need to be improved and adapted such that they effectively cope with EMI.

Hardware based T&Ms: Electromagnetic (EM) Diverse Redundancy

A typical T&M applied for mission- or safety-critical functions is to have two or more identical sets of hardware and software with the same inputs and performing the same operations on them. A few examples are:

- Multiple sensors sensing the same parameters
- Multiple copies of data stored
- Multiple communication channels carrying the same data
- Multiple processors processing the same data.

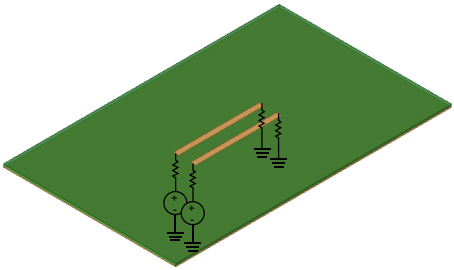
When a malfunction occurs in one of these 'parallel channels', a comparator/voter detects that their outputs no longer agree and triggers appropriate actions to maintain safety. Unfortunately, the malfunctions that EMI creates in identical channels can easily be so similar that the comparator/voter cannot tell that there was a problem at all. To be effective against EMI, the parallel paths should exhibit a different behaviour when subjected to the same EMI ("EM-diversity"). Options include, but are not limited to:

- Inversion of data on otherwise identical channels
- Spatial diversity where the placement of the parallel channels is chosen such that the likeliness of being disturbed by exactly the same EMI is reduced
- Time redundancy where the parallel channels work in different time windows
- Frequency redundancy where the parallel channels work at different frequencies.

The effectiveness of these four types of EM diversity is studied in more detail below, for the case where the EMI comprises a strong, continuous EM field ("plane wave)". To get statistically meaningful results, a very large set of plane-waves is considered, with each of the plane-waves having a random angle-of-incidence, polarization and phase.

Effectiveness of inversion

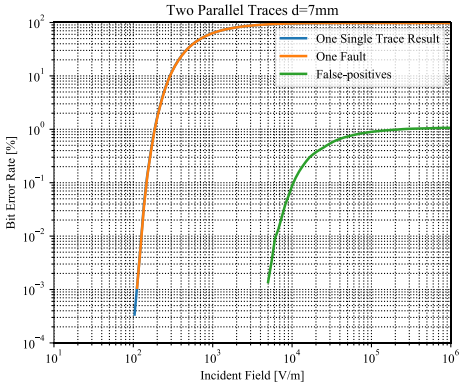
The figure shows the geometry considered for the study of the effectiveness of inversion [7]. It comprises a two-channel redundant system formed by two parallel traces on a simple Printed Circuit Board (PCB). The PCB is an FR4 substrate of 10cm by 16cm and 1.6mm thickness. All traces have a width of 3mm and a length of 5cm. The

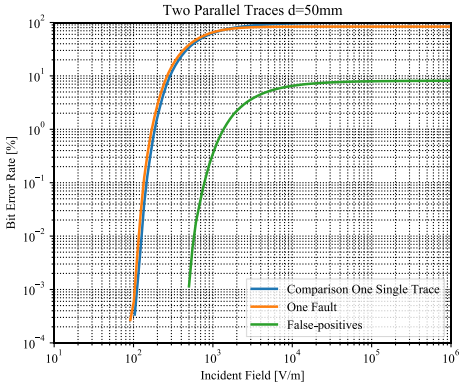


traces are terminated in 50 Ohm loads, i.e. the characteristic impedance of the traces, at both ends. Over the traces, a large random set of bits is transmitted from one end to the other of each trace. At the same time, the PCB is disturbed with a strong continuous EM field ("plane wave)", as explained above.

For the encoding and decoding, Unipolar Non-Return-to-Zero-Level was used, with the following metrics. For encoding, the voltage levels for a '0' and a '1' at an input sides of the traces are 0V and 1V, respectively. For the decoding, the thresholds used to differentiate between a '0' or a '1' are set to 1/3rd and 2/3^{rds} of the theoretical output voltage, respectively. If the voltage is below the 1/3rd threshold, then a '0' is seen. The same goes when the voltage is above the 2/3^{rds} threshold, at which moment a '1' will be read. For any values in between the thresholds, the bit is seen as faulty, to create a worst-case result. For easier processing, a decoding technique is used where we don't look at the transient behaviour of the received bit patterns, but only at the middle of each received bit. So, our analysis does not use any special detection techniques (eg. Schmitt-trigger). The Bit-Error-Rate (BER) is used as the metric to assess the effectiveness of inversion. The BER is defined as the ratio between the number or bits that are decoded incorrectly at the output side versus the total number of bits that were considered.

With inversion, the bit patterns on the two traces are opposite to each other. This means that on one trace a '1' is represented by a high voltage, while on the other a '1' is represented by a low voltage. At the end of the two traces an ideal voter is assumed. This voter compares the bit patterns of both traces. If at one moment in time, the received bits at the end of the two traces are not the same (taking into account that for one trace these were inverted), then the voter flags that an error must have occurred and can trigger that the Equipment Under Control (EUC) puts itself into a safe-state. However, dangerous failures can occur when both bits at the end of the traces are wrong at the same time ('false positive'). In that case, the voter would assume wrongly that there is no error at all, and would not trigger the EUC to put itself into a safe-state and would continue with the wrong data. Such a "two faults"-situation or "false-positive" can happen when the induced voltages on the two microstrips have a phase difference that is sufficiently large. In that case, the induced voltage can cause both decoded bits to be wrong. Another possibility is that the induced voltages levels fall between the thresholds, so that the decoder also detects a faulty bit (a voltage level between both thresholds was always considered faulty in this study). The probability





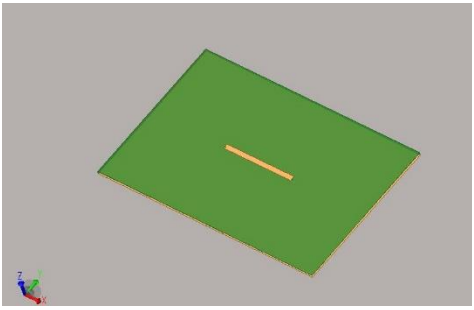
that this happens becomes greater with increasing distance between the traces. The figures on the previous page illustrate this for a bit frequency of 200MHz and a disturbance frequency of 500MHz respectively. Hence, for inversion to work properly, both traces should be completely identical and as close as possible to each other.

Effectiveness of spatial diversity

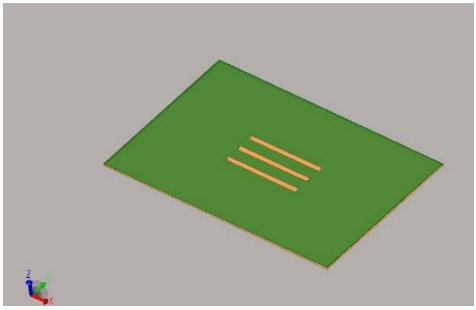
To study the effectiveness of spatial diversity [8][9], four different geometries have been considered:

- A single PCB with a single trace (top left figure). This is the reference situation (non-redundant system)
- A single PCB with three parallel, identical traces (6mm spacing between the traces) (top right)
- A single PCB with three identical, but differently oriented traces (bottom left)
- Three identical, but differently oriented PCBs (bottom right)

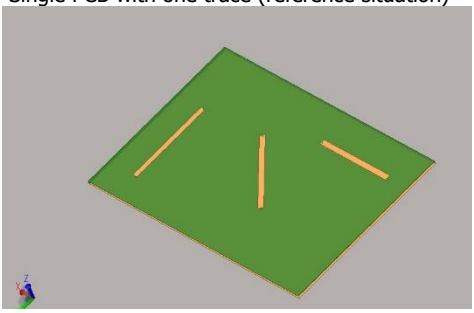
All of the redundant systems are 2oo3 systems. This means that after the (ideal) voter, a bit error will only occur if the bit error occurs for at least 2 of the redundant paths. Note that there is a significant difference with respect to what can be obtained with a 2oo3 system compared to a 2-channel redundant system as studied in the previous section on inversion. Indeed, with a 2oo3 system one can use majority voting to obtain fault-tolerant behaviour. In contrast, with a 2-channel system, one can only detect that an error has occurred (when both channels have a different outcome) upon which one can trigger an appropriate action (e.g. transition to a fail-safe state).



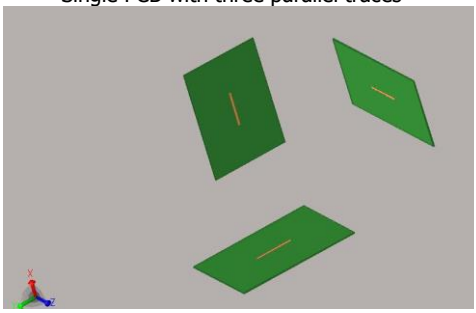
Single PCB with one trace (reference situation)



Single PCB with three parallel traces

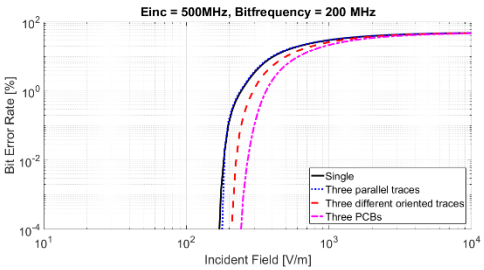


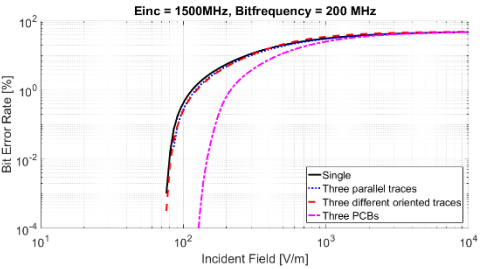
Single PCB with three differently oriented traces

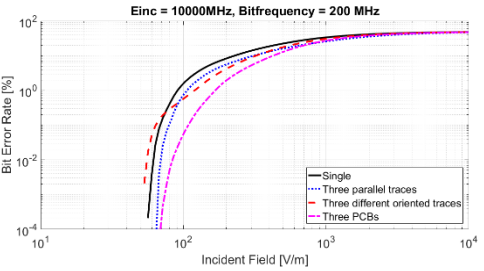


Three differently oriented PCBs

The resulting BER (i.e. after the ideal voting) vs the amplitude of the incident field is shown in the following figures for a disturbance at 500MHz, 1.5GHz, and 10GHz, respectively. In all cases, the bit frequency is 200 MHz.



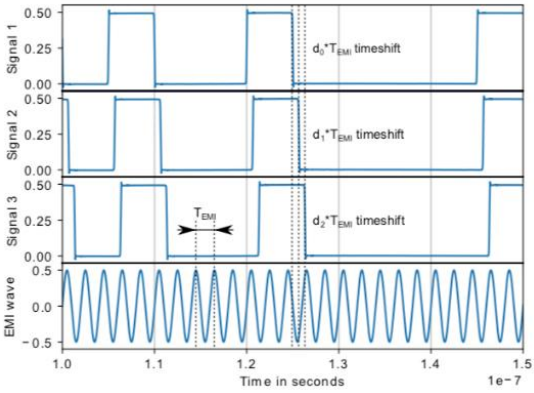




As expected, the situation with the redundant system comprising only a single PCB with three parallel traces doesn't give much benefit compared to the non-redundant system. Only when the frequency goes up such that the distance between the traces becomes "electrically" large, the BER of the situation with three parallel traces behaves (slightly) better than the non-redundant system.

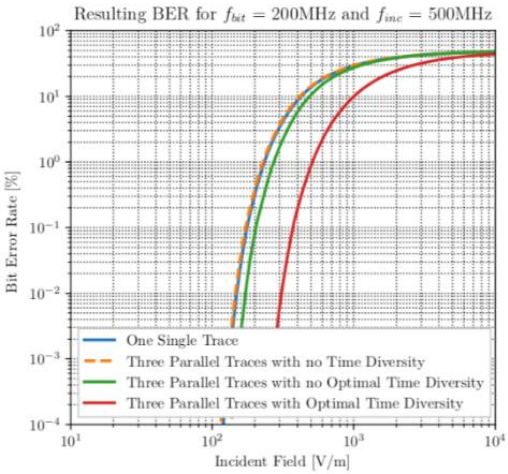
The single PCB with three differently oriented traces behaves somewhat better at some of the frequencies. However, at other frequencies, its benefit is only limited or even worse compared to the single trace. A possible cause might be that two of the three paths are located more closely to the edge of the PCB where they are more sensitive to an incoming plane wave. Only the case of three different PCBs results in a consistent reduction of the BER.

Effectiveness of time diversity



In this situation, the diversity property is created by changing the timing according to the redundant channel data being transmitted [10]. The reasoning behind time diversity is that the data is sampled at a constant rate (the bit frequency), and that point in time never changes. This means that for all three redundant channels, where the voltage induced because of EMI is nearly the same, the sampled value will be nearly the same every time. If we could change that point in time where the three different channels are sampled, a different value from the disturbance will be sampled, and this would create a straightforward EM-diverse system. This principle is shown in the figure above where the timeshift is represented by a percentage of the period of the frequency of the disturbance.

The following figure shows the BER in function of the strength of the EMI disturbance for a non-redundant system and a 2oo3 system (parallel traces as shown earlier) with and without the application of time diversity. Once again, the disturbance frequency was 500 MHz and the bit frequency 200 MHz. It is seen that the performance of time diversity heavily depends on the timeshift.



A quite brute-force method was used to find out what combination of timeshifts is the most optimal. This was done by creating a long list of random bits, and encoding them to voltages. A sine-wave with the desired EMI frequency is used to simulate the incoming disturbance.

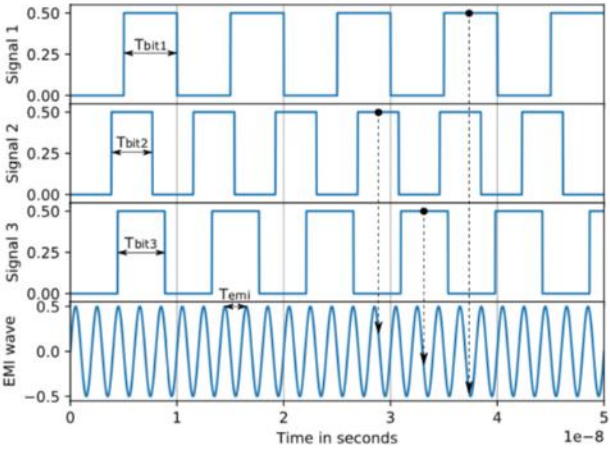
The time delay between the bit patterns is swept for two of the three trace inputs, one input is fixed at 0% or no time delay. The profile of the sweep is from 0%-40% of the period of the bit-frequency, which is equal to 0%-100% of the period of the EMI frequency. The results of this study showed that for a 2oo3 system, a timeshift of 0, 1/3 and 2/3 times the period of the incoming EMI disturbance has the best performance. When we look at a sinewave and take three sample points that are shifted 120° at all times, one notices that those points are the most different when comparing to other combinations of timeshifts.

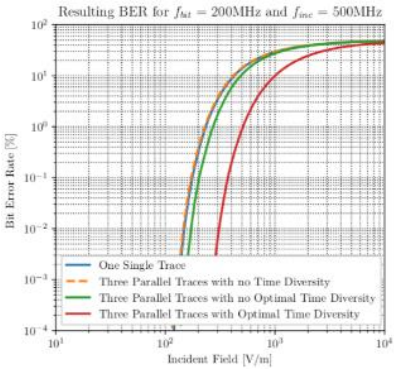
It was confirmed that these results can be extrapolated to more general NooM systems. For example, for a 3oo5 system, the optimum timeshift is 1/5th of the period of the EMI disturbance.

Effectiveness of frequency diversity

The goal of frequency diversity is to use three different frequencies for the data transmission.

This will change the position in time where the bits will be sampled at the output, and thus change the value of the induced voltage that will be measured by the output as shown in the figure opposite.





The figure shows the BER in function of the strength of the EMI disturbance for a non-redundant system and a 2oo3 system (parallel traces as shown earlier) with and without the application of frequency diversity. Once again, the disturbance frequency was 500 MHz. It is seen that the performance of frequency diversity heavily depends on the choice of the three frequencies f_1, f_2 and f_3. It can be proven (but the mathematical analysis falls outside of the scope of this contribution) that an ideal combination is (assuming that f_1 is given and that the frequency f_{EMI} of the disturbance is known): f_1, $f_2 = f_1 + f_{EMI}/3$, and $f_3 = f_1 + 2f_{EMI}/3$.

Software based T&Ms: Error Detection and Correction Codes

In order to protect communication channels from bit errors, Error Detection and Correction Codes (EDCCs) have been developed and used since the 1950s. Such EDCCs add redundant information (bits) to the actual data in order to enable the receiver to detect or even correct corrupted information. Cyclic Redundancy Checks (CRC), Hamming Codes and Data Triple Modular Redundancy (TMR), also called Triplication, are well known examples. Below, we discuss the effectiveness of these codes to cope with strong, continuous EMI disturbances. An important concern is whether or not false negatives can occur, i.e. whether corrupted and, hence, incorrect data could be seen as correct.

In all sections below, the geometry under study is the PCB with a single trace – the reference situation discussed earlier. At the input side of the trace, a data producer generates data words, encodes them (either with or without an EDCC) and puts these code words onto the communication channel (the PCB trace in this case). The channel then transmits the code words to the data consumer at the output side of the trace. The data consumer decodes the received code words to data words. The entire communication subsystem is subjected to a continuous EMI disturbance. In order to check the effectiveness of the considered EDCCs, the decoded data word is compared to the original data word that was sent.

Cyclic Redundancy Checks (CRC)

A data word is initialized at the data producer, and its CRC [11] is calculated and added to the data word before sending all bits over the communication. The CRC is in essence the remainder after a bit-wise division. Both the sender and receiver use the same divisor, called the polynomial. In this study, data words consisted of 32-bits, whereby the first 16 bits are data and the second 16 bits are its CRC value. For the 16-bit CRC-CCITT method, the following divisor is used: $x^{16} + x^{12} + x^5 + 1$. At the receiver side, the data consumer, the main function is to check the data for errors. When an error is detected, the data can be discarded and a retransmission can be requested. The data is considered correct at receiver side when the calculated CRC is equal to the one that was sent with the data. However, this leaves room for false negatives. A false negative arises when the data, at receiver side, is considered correct by its CRC, but the data is not equal to the original data sent by the data producer. This situation arises when the disturbance of the signal is such that both the data

and the CRC are corrupted in such a way that the disturbed CRC matches the disturbed data.

When studying CRC in the way described above, it was noted that no false negatives occurred, except in the specific cases where the disturbance frequency is an integer multiple of the bit frequency. However, in that case, the likelihood of a false negative is 50% for very strong EMI disturbances. The reason for this is that a very strong EMI disturbance pushes all sampled voltages above or below the threshold for a '1' or a '0'. This causes the output to be all ones or zeros, respectively. Unfortunately, in CRC, a data word comprising of all zeroes is considered correct, leading to a false negative. Adding a fixed offset to the CRC such that original data comprising all zeroes doesn't lead to an all-zero CRC helps to overcome the occurrence of false positives.

Hamming Codes

The Hamming Code [12][13] is a linear, Single Error Correction (SEC) code. It is one the most efficient SEC codes and was designed by R. W. Hamming in the 1950s to protect his calculations from random single bit errors. Whilst very efficient and used in many different applications, little to no attention has been paid to the effectiveness of the original Hamming Code to cope with EMI disruptions. In [12] and [13], we studied the performance of Hamming Code in the same way as described above for CRC. Specifically, we focused again on the possible occurrence of false negatives. Our research showed that for a Hamming Code there is always a certain likelihood of false negatives, but that this likelihood significantly increases when the disturbance frequency and the bit frequency are related by:

$$f_{\text{BIT}} = \frac{2f_{\text{EMI}}}{2n+1}, \text{ with n=0,1,2,...}$$

The reason for this is specific repetitiveness that can be found in valid Hamming Code words, like alternating groups of single, double,... ones or zeroes. Applying an odd parity to the Hamming Code avoids many of those repetitive patterns and decreased the likelihood of false negatives.

Triplication

Triplication [13][14] is a fault-masking technique whereby the data is sent three times over the communication channel. Once again, we investigated the effectiveness of triplication with the method described above. Four triplication variants were considered in our study. The first variant - simple triplication - is denoted as TEC, since it sends the data three times (Triplication), without inversion (Equal), bit by bit (Close together). When the data bits are interleaved within the code word, the technique is called TED, since it sends the data three times (Triplication), without inversion (Equal), with interleaving (Dispersed). Trading interleaving for inversion, the methodology is called TDC, since it sends the data three times (Triplication), with inversion (Diverse data bits), bit by bit (Close together). Finally, the last variant can use both inversion and bit interleaving. Following the same name-giving the technique becomes TDD: since it sends the data three times (Triplication), with inversion (Diverse data bits), with interleaving (Dispersed).

TEC(ABCD) = [AAA BBB CCC DDD]

TDC(ABCD) = [A$\bar{A}$A B$\bar{B}$B C$\bar{C}$C D$\bar{D}$D]

TED(ABCD) = [ABCD ABCD ABCD]

TDD(ABCD) = [ABCD $\bar{A}\bar{B}\bar{C}\bar{D}$ ABCD]

Again, we focused on the occurrence of false negatives. Our study revealed that for triplication, the overall rate of false negatives is low. However, as was the case with Hamming, specific bit rates show an increased rate of false negatives. Also, here, related to repetitiveness within valid triplication code words. Our current research focuses on improved triplication codes for which the likelihood of false negatives under strong, continuous EMI disturbances is as low as possible.

Summary and conclusions

To achieve the necessary risk-reduction within mission- or safety-critical systems against EMI disturbances, EMI-resilience has to be built into the system such that it becomes fault-tolerant against harsh EMI. This can be achieved by using, in different phases of the design process, appropriate EMI-effective T&Ms. Most of the T&Ms align with the T&Ms from IEC 61508, but modified or adopted to be (more) effective for EMI. Care has to be taken when implementing these T&Ms in a practical design as was shown with a basic study of the effectiveness of (i) hardware T&Ms like inversion, spatial, time and frequency diversity and (ii) software T&Ms like CRC coding, Hamming codes, and triplication.

References

[1] K. Armstrong, "Why EMC Immunity Testing is Inadequate for Functional Safety", Proceedings of the IEEE 2004 International Symposium on EMC, Santa Clara, CA, USA, August 9-13, pp. 145-149

[2] K. Armstrong. "Why increasing immunity test levels is not sufficient for high-reliability and critical equipment", Proceedings of the IEEE 2009 International Symposium on EMC, Austin, TX, USA, August 17-21, pp. 30 – 35.

[3] D. Pissoort and K. Armstrong. "Why is the IEEE Developing a Standard on Managing Risks Due to EM Disturbances?" Proceedings of the IEEE 2016 International Symposium on EMC, Ottawa, Canada, pp. 78 – 83.

[4] K. Armstrong, "It's EMC Jim, but not as we know it", IN Compliance, July 2015, pp. 24-35

[5] "IET Code of Practice for Electromagnetic Resilience", 2017, ISBN: 978-1-78516-324-1

[6] IEEE Standards Association, project P1848, "Techniques and Measures to Manage Risks with Regard to Electromagnetic Disturbances"

[7] J. Lannoo, A. Degraeve, D. Vanoost, J. Boydens, D. Pissoort, "Effectiveness of Inversion Diversity to Cope with EMI within a Two-Channel Redundant System", in: 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), pp. 216-220)

[8] A. Degraeve and D. Pissoort, "Study of the Effectiveness of Spatially EM-Diverse Redundant Systems under Plane-Wave Illumination", in: Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC) 2016: vol. 1 (pp. 211-213)

[9] A. Degraeve and D. Pissoort, "Study of the Effectiveness of Spatially EM-Diverse Redundant Systems under Reverberation Room Conditions", in: IEEE 2016 International Symposium on Electromagnetic Compatibility (EMC) (pp. 374-378)

[10] J. Lannoo, J. Van Waes, A. Degraeve, D. Vanoost, J. Boydens, D. Pissoort, "Effectiveness of Time Diversity to Obtain EMI-Diverse Redundant Systems", in: 2018 International Symposium on Electromagnetic Compatibility (EMC Europe) (pp. 288-292)

[11] J. Van Waes, J. Lannoo, A. Degraeve, D. Vanoost, D. Pissoort, J. Boydens, "Effectiveness of Cyclic Redundancy Checks under Harsh Electromagnetic Disturbances", in: 2017 International Symposium on Electromagnetic Compatibility - EMC Europe (1-6)

[12] J. Van Waes, J. Lannoo, J. Vankeirsbilck, A. Degraeve, J. Peuteman, D. Vanoost, D. Pissoort, J. Boydens, "Effectiveness of Hamming Single Error Correction Codes under Harsh Electromagnetic Disturbances", in: IEEE International Symposium on Electromagnetic Compatibility Presented at the EMC Europe, Amsterdam, The Netherlands, Sept. 2018

[13] J. Van Waes, J. Lannoo, J. Vankeirsbilck, D. Vanoost, D. Pissoort, and J. Boydens, "Resilience of error correction codes against harsh electromagnetic disturbances: Fault mechanisms," IEEE Transactions on Electromagnetic Compatibility, 2019, submitted

[14] J. Van Waes, J. Vankeirsbilck, J. Lannoo , D. Pissoort, J. Boydens, "Effectiveness of Data Triplication in Harsh Electromagnetic Environments", in: 2018 International Symposium on Electromagnetic Compatibility - EMC Europe

Copyright of this article remains with the authors.

