Resilience of Reed-Solomon Codes Against Harsh Electromagnetic Disturbances: Influence of Over-Voltage Detection

Pejman Memar
Department of Computer Science
KU Leuven, Bruges Campus
Bruges, Belgium
pejman.memar@kuleuven.be

Jens Vankeirsbilck
Department of Computer Science
KU Leuven, Bruges Campus
Bruges, Belgium
jens.vankeirsbilck@kuleuven.be

Dries Vanoost
Department of Electrical Engineering
KU Leuven, Bruges Campus
Bruges, Belgium
dries.vanoost@kuleuven.be

Tom Holvoet
Department of Computer Science
KU Leuven
Leuven, Belgium
tom.holvoet@kuleuven.be

Jeroen Boydens
Department of Computer Science
KU Leuven, Bruges Campus
Bruges, Belgium
jeroen.boydens@kuleuven.be

***Abstract*—Communication networks are the backbone of the modern safety-critical systems. Thus, it is crucial to protect these error-prone networks against electromagnetic disturbances in ever more polluted electromagnetic environments. One major vulnerability in communication networks, even the networks which are armed with Error Detection and Correction Codes, is undetected incorrect data, also known as false negatives. From the safety viewpoint, false negatives must be mitigated to an as low as reasonably practicable level. This paper presents the influence of over-voltage detection on the behavior of primitive Reed-Solomon Codes under harsh single-frequency electromagnetic disturbances. In this regards, three different threshold pairs are employed. Our simulations show that by choosing an appropriate range, over-voltage detection could substantially decrease the number of false negatives. Furthermore, it is found that this improvement in the electromagnetic resiliency of Reed-Solomon Codes has been obtained at a cost: decreasing the availability. Nevertheless, this study takes advantage of this trade-off to provide a more resilient system in a safety-critical environment, as is the aim of this paper.**

***Index Terms*—Communication Channel, Electromagnetic Disturbance, Reed-Solomon Codes, Over-Voltage Detection, Resilience.**

I. INTRODUCTION

COMMUNICATION networks have become more vulnerable in increasingly electromagnetic (EM) polluted environments. Furthermore, due to the evolution in safety critical electrical, electronic and programmable electronic (E/E/PE) devices in which wired networks are taking over mechanical and hydraulic connections, the demand for reducing the associated safety-related risks has become of the utmost importance.

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Grant Agreement No 812.790 (MSCA-ETN PETER). This publication reflects only the authors' view, exempting the European Union from any liability. Project website: http://etn-peter.eu/

Unfortunately, owing to the design characteristics of these modern E/E/PE devices, such as smaller feature size and smaller voltage levels, they become inherently more vulnerable to electromagnetic disturbances (EMD) [1].

In a communication network, EMD can generate bit-flips in the transmitted data by inducing additional noise voltages onto the channel. To limit the effect of transmission errors, Error Detection and Correction codes (EDCC) have been developed and used to protect the communication networks against such external sources [2]. EDCCs encode the original data by adding redundant information to it on the producer side and use this information to detect or correct the possibly corrupted data at the consumer side.

However, one common drawback in all EDCCs is their inability to deal with false negatives, i.e. undetectable corrupted data since those data bits are turned into other valid code words. From a safety perspective, this type of error must be mitigated as it can result in severe harm to users, bystanders and the environments. In our previous study the effectiveness of primitive Reed-Solomon Codes (RSCodes) under harsh single-frequency EMD was investigated [3]. In that study, we have shown that the majority of false negatives in the primitive RSCodes are one-symbol-value code words (i.e. all symbols in a code word are identical) and by reducing this type of false negatives, RSCodes become more resilient against EMD. Accordingly, this study uses those findings to improve the EM-resiliency of primitive RSCodes under harsh single-frequency EMD. In accordance with the favorable impact of the over-voltage detection mechanism on the Hamming and the Triplication codes [4], this paper assesses the effect of this detection mechanism on the behavior of primitive RSCodes.

In this regard, the developed fault model by [5] is employed to simulate the incoming single-frequency EMD in reverberant

Table I: Reed-Solomon Codes Setup Parameters

Symbol Size (r)	Field Size (q)	Block Length (n)	Message Length (k)	Correction Capability (s)	Hamming Distance (d)
3	8	7	1	3	7
3	8	7	3	2	5
4	16	15	1	7	15
4	16	15	3	6	13

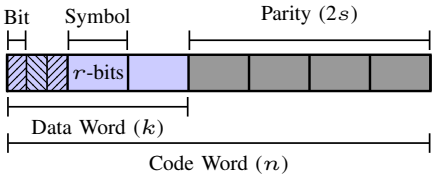

Figure 1: The structure of the RSCodes' code word

environments. Correspondingly, this paper analyzes the EM-resilience of RSCodes armed with over-voltage detection and compares the output results with our previous study as a baseline under the same condition and setup parameters.
The remainder of this paper is organized as follows. Section II details the mathematical concepts of RSCodes. Section III describes the experimental setup, followed by the impact of over-voltage detection in Section IV. Finally, conclusions and future works are covered in Section V

II. REED SOLOMON CODES

Reed-Solomon codes (RSCodes) are a subset of non-binary Bose–Chaudhuri–Hocquenghem (BCH) codes and are linear block-based cyclic EDCCs [6]. A primitive RSCode (n, k) is defined over a finite field $GF(P^r)$, where $q = P^r$ and $n = q-1$. This means that an RSCode has a message or data word length of k symbols, and block or code word length of n symbols. Furthermore, r denotes the symbol size in which the number of available bits in each symbol is defined. Fig. 1 shows the structure of the generated code word by RSCodes.
As stated in [6], [7], P is always a prime number, and r is a positive integer, i.e. $\mathbb{N}_1$. A forward error correction (n, k) RSCode has the capability of correcting s symbol errors, and detecting up to $2s$ symbol errors, where $n - k = 2s$. In this regard, an RSCode encoder adds extra information as parity symbols to the data word at the producer side and generates a code word. Accordingly, the encoder generates a dictionary of q^k valid code words. Later, these parity symbols will be used by the decoder to detect and to recover the possibly corrupted code word, and to extract the original data word at the consumer side.
As the transmitted code words in this study are in the form of binary sequences, finite fields with base 2 (i.e. $\mathbb{F} = GF(2^r)$) will be used throughout this paper. Furthermore, all simulations will be conducted based on the parameters specified in Table I.

A. Reed Solomon Codes Encoder

In the finite finite $\mathbb{F}$ with $q = 2^r$ elements, parity information is generated through the polynomial $g(x)$. Equation (1) uses the cyclic characteristic of the multiplicative group of a finite field [6] to construct the polynomial $g(x)$. It should be noted that α is used as a primitive element of this field which indicates that each non-zero element of $GF(q)$ is describable in the form of α^i for some integer i.

$$g(x) = \Pi_{i=fcr}^{fcr+2s-1}(x - \alpha^i) \tag{1}$$

Here, s is the desired number of symbol errors to be corrected, and fcr is the the power of the first consecutive root of the finite field $\mathbb{F}$. In this study, fcr is equal to 1 which indicates that the first consecutive root and the primitive element are both equal to α. As shown in Equation (2), systematic coding is used to encode the data words. This coding scheme embeds the data word within the generated code word.

$$c(x) = x^{2s} \cdot m(x) - [x^{2s} \cdot m(x) \ mod \ g(x)] \tag{2}$$

In Equation (2), the data word polynomial and the generated code word polynomial are indicated by $m(x)$ and $c(x)$, respectively. Moreover, x^{2s} is used to shift the data word to higher order to prevent the overlapping between the data word and the parity information.

B. Reed Solomon Codes Decoder

After receiving the code word, the RSCode decoder calculates the syndrome components as the first step. In this step, the calculated syndrome determines whether the received code word is valid or not. In the case when the syndrome is zero, the received code word is valid and no further calculation is required. However, in this case either the original data is received or the data is corrupted in a way that resulted in an another valid code word. The latter is undetectable and is called a false negative. The data word is eventually stripped from the code word in this case.
A nonzero syndrome, however, indicates the presence of faults, and it demands further steps to recover the data word. In such a case, the decoder tries to find an error locater polynomial. This paper uses the Berlekamp-Massey algorithm [8] for this purpose. Thereafter, RSCode finds the error locations by calculating the error locater polynomial's roots. The Chien search algorithm [9] is used in this study to find the roots. Subsequently, the error values are calculated using the Forney's algorithm [10] based on the calculated roots and syndrome components. Ultimately, the RSCode decoder constructs the data word using the aforesaid parameters.

III. EXPRIMENTAL SETUP

This paper has employed the in-house software-based simulation framework which was previously used in [3]–[5]. However, to assist the readers in understanding of the remainder of this paper, we repeat Sections III-A, III-B and III-C of [3].

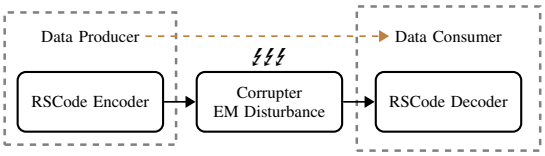

Figure 2: Conceptual overview of the simulation setup

A. The Producer-Consumer Overview

The conceptual overview of the simulation setup is illustrated in Fig. 2. A data producer generates data words. The RSCode encoder then encodes them and puts the resulting code words onto the communication channel. The channel transmits the code words to the data consumer while being exposed to the electromagnetic disturbance. The RSCode decoder at the data consumer side decodes the received code words to data words. In order to investigate the effectiveness of the considered RSCode, the decoded data word is compared to the original transmitted data word.

B. EMD Effect Simulation Setup

As already stated, the communication channel is subjected to harsh single-frequency electromagnetic disturbances. The representation of the simulated disturbances is given in Equation (3).

$$\begin{cases} U(i) = A \cdot \sin[(2\pi \cdot f_{\text{emd}} \cdot t_i) + \phi] \\ t = \dfrac{i}{f_{\text{bit}}} \\ i \in [0, N-1] \\ N = \text{block length } (n) \times \text{symbol size } (r) \end{cases} \tag{3}$$

Within Equation (3), multiple parameters are specified. $U(i)$ denotes the induced voltage at a certain time. A and ϕ represent the amplitude and phase, respectively. Other characteristics are the disturbance frequency f_{emd} and bit frequency f_{bit}. Finally, counter i indicates the bit to be sampled. In total, there are N bits of information in a code word.

Within this framework, the logical 0s and 1s in the code word are converted to voltages using the Non-Return-to-Zero-Level encoding, i.e, a logical '0' is converted to 0 V and a logical '1' to 1 V. The disturbances are then added to the corresponding voltages to simulate the EMD effect. In order to convert back the altered voltages to logical '0' and '1', a fixed threshold (V_{THLD}) is considered. Accordingly, any voltages less than $V_{\text{THLD}} = 0.5$ V are converted to logical '0', and voltages greater than or equal to $V_{\text{THLD}} = 0.5$ V are converted to logical '1'. Note that all data points (i.e. voltages) are sampled in the middle of the bit period.

In our experiments, four specific parameters must be set initially: f_{emd}, f_{bit}, A, and N. These values are given in Equation (4). It should be noted that amplitude values less than 0.5 are excluded from the simulation due to their incapability in generating bit-flips.

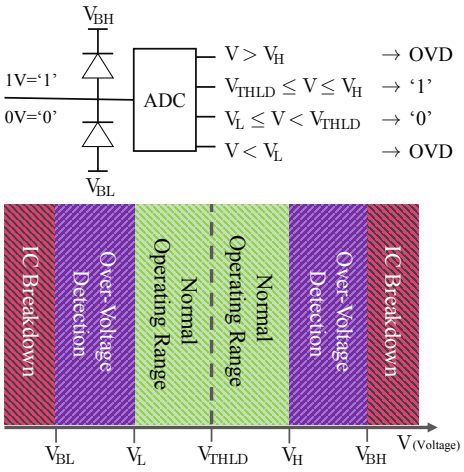

Figure 3: Distribution of the decoding voltages thresholds.

$$\begin{cases} f_{\text{emd}} \in [1 \text{ MHz} : 1 \text{ GHz}];\ \Delta f_{\text{emd}} = 1 \text{ MHz} \\ f_{\text{bit}} = 200 \text{ Mbps} \\ A \in [0.5 : 10]\, V;\ \Delta A = 0.02V \\ N = [21, 60] \text{ bits} \\ \phi \in [0 : 359];\ \Delta\phi = 1 \text{ degree} \end{cases} \tag{4}$$

C. Over-Voltage Detection

It is a good engineering practice to protect the consumer side against over-voltages, specifically for safety-critical purposes. In this regard, several thresholds must be considered while decoding a received voltage to a logical '1' or '0' [5]. This process is depicted in Fig. 3.

V_{L} and V_{H} denote the low and high ends of the normal operating voltage range and they the required voltages to create bit-flip. In this region, voltages are converted to logical '1' or '0' based on the specified threshold in Section III-A (i.e. $V_{\text{THLD}} = 0.5$) .The Over-Voltage Detection (OVD) is triggered in the ranges of V_{BL} to V_{L} and V_{H} to V_{BH}. Voltages less than V_{BL} or greater than V_{BH} would result in Integrated Circuits (IC) break-down. Thus, it is crucial to avoid IC break-down through over-voltage detection mechanisms. These mechanisms help to ensure the overall safety of the considered system by clamping the voltage and keeping it within the purple region in Fig. 3.

In this paper, three thresholds pairs of over-voltage detection, namely $\{V_{\text{L}} = -0.5, V_{\text{H}} = 1.5\}$, $\{V_{\text{L}} = -0.75, V_{\text{H}} = 1.75\}$ and $\{V_{\text{L}} = -1, V_{\text{H}} = 2\}$, have been used. Greater distance between V_{L} and V_{H} indicates that more bit-flips are allowed to occur during the transmission. Note that both V_{BL} and V_{BH} are determined by the characteristics of the used IC.

D. Fault Categorization

In accordance to the different outputs of the simulation, six distinct categories are considered. These are labeled with distinct colors in Figs. 4 and 5 of this paper.

1) Correct Data without Correction: The decoded data is correct without any correction. The code word has not

been affected by the interference, and thus, no correction at all had to be made. This is the normal behavior and is labeled in blue.

2) Correct Data with Correction: The decoded data is correct, but only after the correction procedure. The RSCode was able to detect the errors and correct them since the number of errors was in the RSCode correcting capability. This category is desired and labeled in green. However, although this category is desired, the system receives a warning that something was wrong.
3) RSCodes Inherent Detection: There is no decoded data. The RSCode was able to detect the errors. However, in this case either the number of errors is beyond the RSCode correcting capability or it is in the RSCode correcting capability, but in a way that there are more than one valid code words with the same minimum symbol distance (i.e. number of symbol-wise differences between two code words) to the corrupted code word. In both cases, RSCode stops the operation. This category is acceptable and labeled in yellow. The system detects that something was wrong and has to switch to a minimum-risk state.
4) False Data with Correction: the decoded data is incorrect. The RSCode was able to detect the errors but the code word remained faulty after the correction. In this case, there is only one valid code word with a minimum symbol distance to the corrupted code word. However, this valid code word differs from the original one, and thus the corrupted code word is mis-corrected to a wrong valid code word. This category is undesired and labeled in orange. However, the system still receives a warning that something was wrong.
5) False Data without Correction: the decoded data is incorrect, but the RSCode did not even detect the errors since it turned to another valid code word, and RSCode assumed that all is right; this category is also known as a false negative. In such a case, the system is unaware that the received data word is incorrect, and thus no countermeasures can be taken. Consequently, this undetected category could result in critical failures. Accordingly, this category is considered detrimental to the overall system safety and is, therefore, labeled in red.
6) Over-Voltage Detection: the over-voltage detector is triggered to ensure the overall safety of the system. Accordingly it stopped the transmission to the consumer side and transfer the system to a minimum-risk state. This category is desired and labeled in purple.

An important focus of this paper is to improve the resiliency of RSCodes under harsh EMD by reducing the rate of false negatives indicated with the red label.

IV. Influence of Over-Voltage Detection

Based upon the very favorable impacts of the over-voltage detection on the Triplication and Hamming codes [4], this study investigates the influence of this uncomplicated technique on RSCodes.

Using the setup parameters shown in Table I, several graphs were generated of which the most important ones are presented here. It should be noted that due to the periodicity of the applied single-frequency disturbances, all graphs contain one period only. Figs. 4 and 5 demonstrate the fault category distribution of the considered setup for the symbol size of 3 and 4, respectively. Each row contains 4 graphs which represent the results for two data word lengths (i.e. $k = 1$ and $k = 3$) and two amplitudes (i.e. $A = 0.6$ V and $A = 1$ V). Graphs (*a-d*) depict the normal behavior of RSCodes under harsh EMD without over-voltage detection and act as a baseline which was investigated in our previous study [3]. Graphs (*e-h*) show the influence of over-voltage detection when $V_{\mathrm{L}} = -0.5$ and $V_{\mathrm{H}} = 1.5$. Likewise, graphs (*i-l*) and (*m-p*) manifest the corresponding results for the thresholds pairs of $\{V_{\mathrm{L}} = -0.75, V_{\mathrm{H}} = 1.75\}$ and $\{V_{\mathrm{L}} = -1, V_{\mathrm{H}} = 2\}$, respectively.

A. Impact of the Specified Over-Voltage Detection Ranges

In [3], we showed that the majority of false negatives are one-symbol-value code words (i.e. all symbols in a code word are identical). This type of false negatives occurs at specific frequencies [3], as presented in Equation (5).

$$f_{\text{false negative}} = \frac{j}{r} \cdot f_{\text{bit}},\ j \in \mathbb{N}^{+} \tag{5}$$

Accordingly, there are 4 false negative peaks for the symbol size of 3, and 5 false negative peaks for the symbol size of 4 in the presented graphs. Mitigating this specific type of false negative would significantly increase the EMI-resiliency of RSCodes. Note that any other visible false negatives in the graphs are generated from multi-symbol-value code words.

As can be seen in Figs. 4 (*e-h*) and 5 (*e-h*), the ratio of false negative peaks at harmonics (i.e. 200 MHz and 400 MHz) are at least reduced to half. This decrease is more noticeable when $k = 3$ in which the false negative peaks are reduced from values above 30% to around 0.1% for the symbol size of 3 and around 0.2% for the symbol size of 4. Furthermore, as can be observed in Figs. 4 (*h* and *l*), over-voltage detection could catch all the false negatives which were generated by multi-symbol-value code words (i.e. all other code words except the one-symbol-value code words).

Compared to the $\{V_{\mathrm{L}} = -0.5, V_{\mathrm{H}} = 1.5\}$ range, Figs. 4 (*i-p*) and 5 (*i-p*) show that increasing the OVD range could make this mechanism ineffective or provide limited benefits at its best, i.e. slight reduction in false negatives in Figs. 4 (*j* and *l*) as well as 5 (*j* and *l*).

B. Trade-off Between Safety and Availability

From the safety viewpoint, both green (i.e. Correct Data with Correction) and orange (i.e. False Data with Correction) categories are untrustworthy as in a real communication network it is unattainable to distinguish between the corrected and mis-corrected data at this layer. On the other hand, higher ratio of blue category (i.e. Correct Data without Correction)

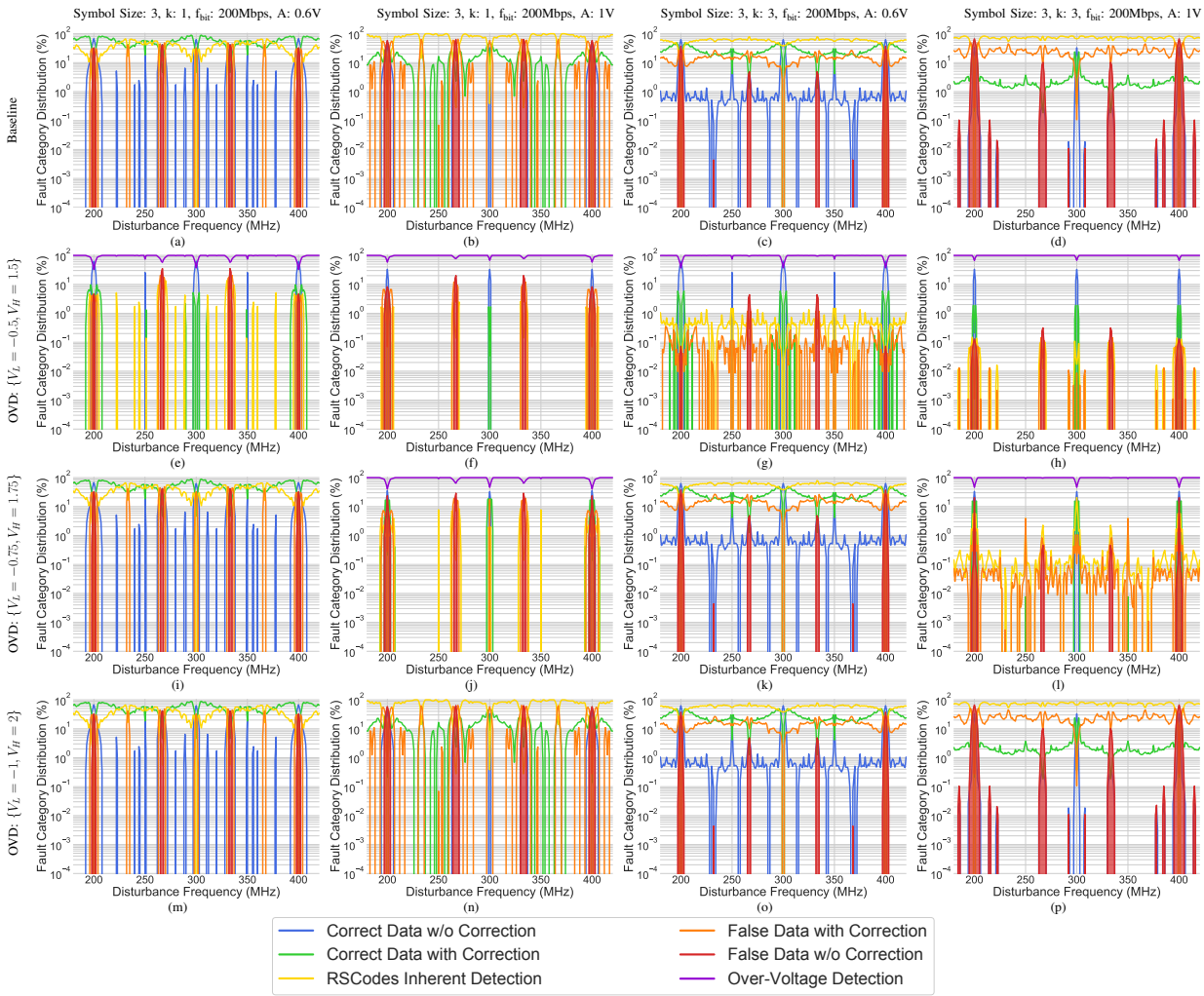

Figure 4: Reed-Solomon Codes Effectiveness under harsh electromagnetic disturbances for the symbol size of 3.

and very small ratio (or preferably none) of red category (i.e. False Data without Correction) are favorable targets for a safety-critical systems. Based upon this perspective, the output results are promising since there is a significant reduction in the red category while maintaining the blue categories mainly at the positive integer multiples of 100 MHz. Besides, a great portion of the remaining categories (above 95%) are caught by the over-voltage detection. Undoubtedly, these results are achieved at a cost, which is availability in this case.

From the availability perspective, although there is a significant improvement in the EMI-resiliency of RSCode with regard to false negatives ratio, the overall performance has adversely been affected by the over-voltage detection. Most portion of the green category (i.e. Correct Data with Correction) is replaced by the purple category (i.e. Over-Voltage Detection). This indicates that when using over-voltage detection in an EM-polluted environment, a great portion of the transmitted code words will not be received at the consumer side. However, as demonstrated in baseline graphs, the ratio of the green categories are significantly higher. In other words, in an EM-polluted environment, over-voltage detection provides a better EMI-resiliency but it reduces the availability of RSCodes to a great extent. It should also be noted that under a similar setup, OVD resulted in a better availability for the Hamming and the Triplication Codes [4]. This rises from the length of the transmitted code words; the longer the code word length, the more detection occurs by the OVD mechanism. This behavior is clearly observable for the symbol size of 4, i.e. in Figs. 5 (*e-h*), in which the code word length increases from 21 bits (i.e. for the symbol size of 3) to 60 bits. Correspondingly, the results show that increasing the code word length would adversely impact the availability of RSCodes.

As this study has focused on the EMI-resiliency of RSCodes since the beginning, notably the ratio of false negatives, it is justified to say that over-voltage detection would provide an acceptable, but not a perfect, performance under harsh single-frequency EMD.

V. Conclusion

This paper presented the impact of the over-voltage detection mechanism on the primitive RSCodes behavior in harsh EM environments. Three ranges of OVD were applied for

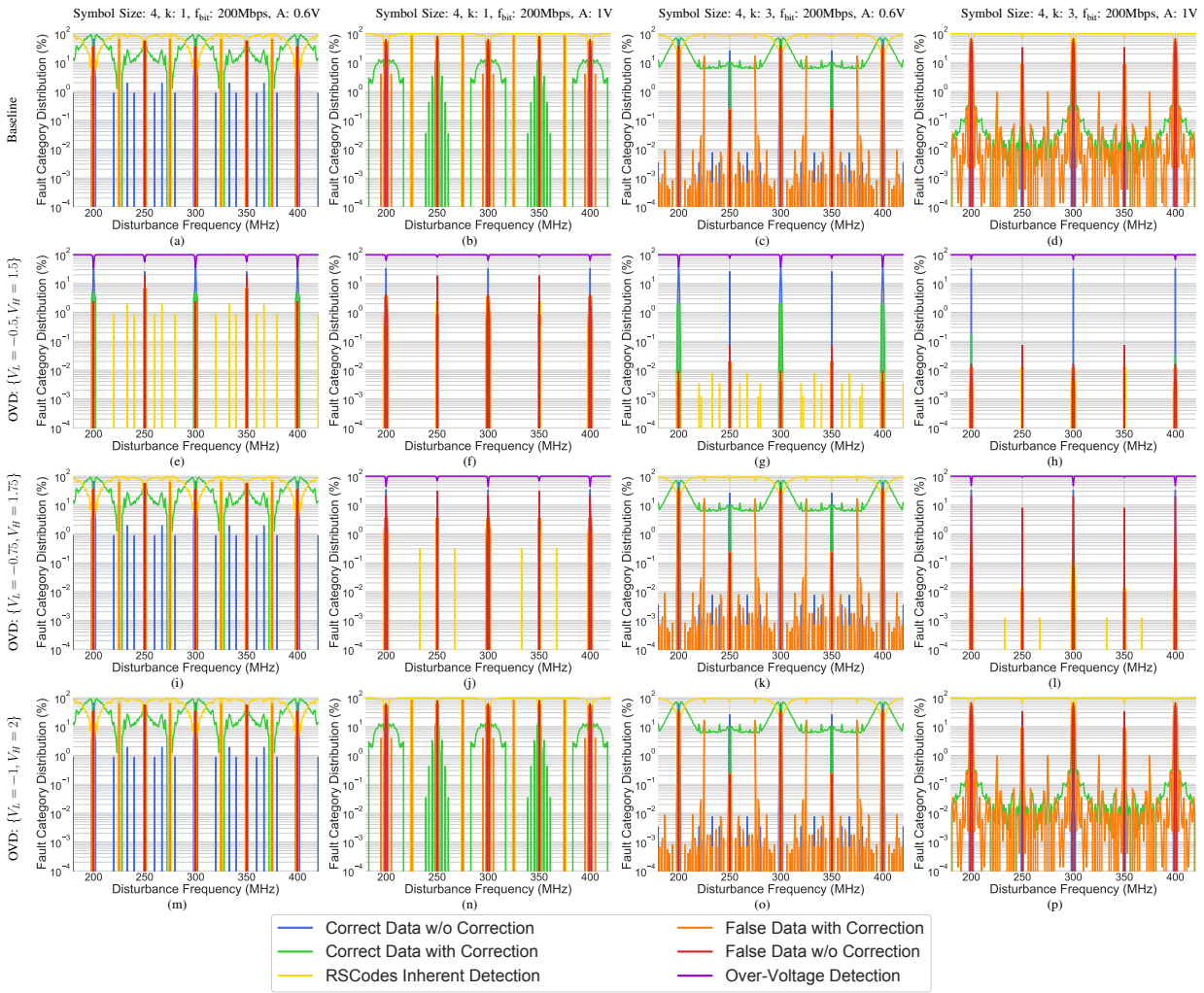

Figure 5: Reed-Solomon Codes Effectiveness under harsh electromagnetic disturbances for the symbol size of 4.

this purpose. It is found that for a proper threshold pairs, OVD can reduce the false negative ratios considerably and provide a safer communication. Moreover, this study showed that this reduction is obtained at a cost: a trade-off between safety and availability. The OVD mechanism significantly improved the EMI-resiliency of RSCodes in an EM-polluted environment while it reduced its availability at the same time. Accordingly, it is appropriate to say that the results of this study are promising for the safety-critical applications. However, for other applications in which the availability has a higher priority, OVD is not recommended since it adversely impacts the normal operation of RSCodes and reduces the overall performance.

In the future studies, more advanced bit and symbol manipulation techniques will be investigated to mitigate the false negatives while maintaining or preferably improving the availability of RSCodes.

References

[1] 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)*. IEEE, 2016, pp. 78–83.

[2] R. W. Hamming, "Error detecting and error correcting codes," *The Bell system technical journal*, vol. 29, no. 2, pp. 147–160, 1950.

[3] P. Memar, J. Vankeirsbilck, D. Vanoost, D. Pissoort, T. Holvoet, and J. Boydens, "Resilience of reed-solomon codes against harsh electromagnetic disturbances: Fault mechanisms," unpublished.

[4] J. Van Waes, D. Vanoost, J. Vankeirsbilck, J. Lannoo, D. Pissoort, and J. Boydens, "Resilience of error correction codes against harsh electromagnetic disturbances: Fault elimination for triplication-based error correction codes," *IEEE Transactions on Electromagnetic Compatibility*, 2020.

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

[6] W. A. Geisel, "Tutorial on reed-solomon error correction coding," 1990.

[7] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the society for industrial and applied mathematics*, vol. 8, no. 2, pp. 300–304, 1960.

[8] E. Berlekamp, "Algebraic coding theory mcgraw-hill," *New York*, vol. 8, 1968.

[9] R. Chien, "Cyclic decoding procedures for bose-chaudhuri-hocquenghem codes," *IEEE Transactions on information theory*, vol. 10, no. 4, pp. 357–363, 1964.

[10] G. Forney, "On decoding BCH codes," *IEEE Transactions on information theory*, vol. 11, no. 4, pp. 549–557, 1965.