

Article

The Issue of Operating Security Systems in Terms of the Impact of Electromagnetic Interference Generated Unintentionally

Krzysztof Jakubowski ¹, Jacek Paś ²  and Adam Rosiński ^{3,*} 

¹ National Cyber Security Centre, Gen. Buła 1, 05-119 Legionowo, Poland; krzysztof.jakubowski.wel@gmail.com

² Division of Electronic Systems Exploitations, Faculty of Electronics, Institute of Electronic Systems, Military University of Technology, 2 Gen. S. Kaliski St, 00-908 Warsaw, Poland; jacek.pas@wat.edu.pl

³ Division Telecommunications in Transport, Faculty of Transport, Warsaw University of Technology, 75 Koszykowa St, 00-662 Warsaw, Poland

* Correspondence: adam.rosinski@pw.edu.pl

Abstract: This article discusses issues regarding electromagnetic interference generated unintentionally by transport telematics systems and electronic security systems (ESS) located within a railway area. These systems should operate correctly, since they ensure the safety of both vehicles and passengers. The electronic devices they use are exposed to electromagnetic interference that may lead to incorrect ESS functioning. In order to determine the impact of electromagnetic interference on ESS, the authors measured unintentional low-frequency electromagnetic field generated by MV—15 and 30 kV—power lines. This enabled determining the areas with maximum values of electromagnetic interference. The next stage of the research was to develop an ESS operating process model that takes into account the impact of unintentionally generated electromagnetic interference on the operating process. Introducing the electromagnetic interference impact coefficient enables a rational selection of solutions aimed at protecting against electromagnetic interference through the application of technical and organizational measures.

Keywords: electronic security system; electromagnetic interference; operation



Citation: Jakubowski, K.; Paś, J.; Rosiński, A. The Issue of Operating Security Systems in Terms of the Impact of Electromagnetic Interference Generated Unintentionally. *Energies* **2021**, *14*, 8591. <https://doi.org/10.3390/en14248591>

Academic Editors: Anna Richelli and Stanisław Duer

Received: 5 November 2021

Accepted: 14 December 2021

Published: 20 December 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Transport telematics systems and electronic security systems (ESS) located in a metal container on a railway route are considered to be the “State’s critical infrastructure items” [1–3]. Their most important task is to ensure the security of vehicle movement on railway routes [4,5]. They are located in a special, structurally reinforced metal container and are protected against the action of external and internal destructive factors. ESS elements can also be found inside buildings and in a publicly available external environment, where they are exposed to variable environmental parameters—temperature [6], humidity, etc., as well as the unintentional low-frequency electromagnetic field generated by medium voltage—15, 30 kV—power lines. These lines are a supply source for the aforementioned systems (Figure 1) [7].

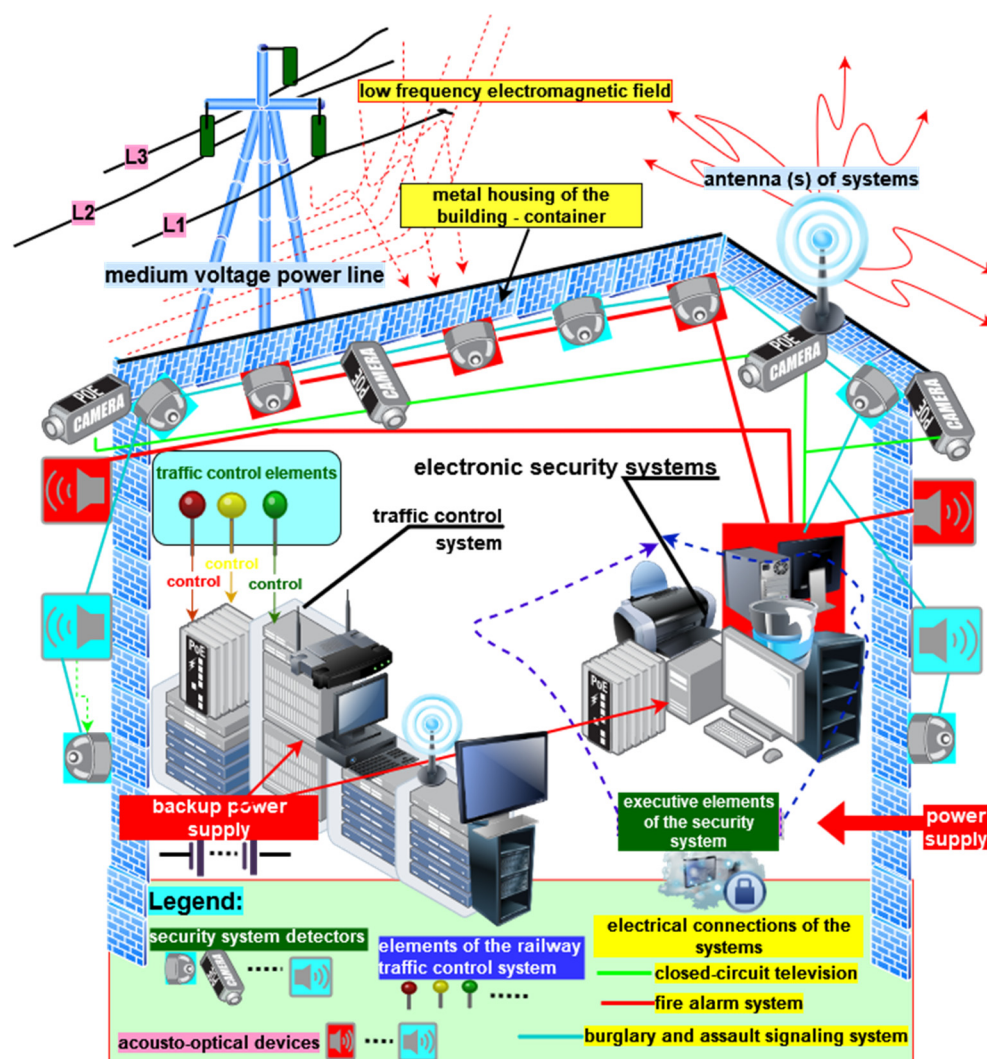


Figure 1. Arrangement of electronic security systems in a metal container due to their important functions within the State’s communication structure. Designations: L1, L2, L3—individual voltage phases found in the overhead power line supplying electricity to transport telematics systems and electronic security systems. The power is supplied from the MV grid and from backup power sources (battery banks for electronic security systems and UPSs for rail transport telematics systems due to the rated power demand).

Transport telematics systems and electronic security systems are supplied from the 15 kV or 30 kV medium-voltage grid. The overhead power line is 5 or 10 m away from the container where the aforementioned electronic systems are located, in accordance with applicable national standards that apply to ensuring protection against the impact of unintentional electromagnetic field on living and inanimate organisms. A transformer located outside the container ensures an appropriate voltage level—230 V electronic power supplies. Backup power supply in the form of battery banks for electronic security systems is provided in order to guarantee the high reliability of telematics systems and ESS in the container. It consists of a fire alarm system (FAS) [8,9], an intrusion detection system (IDS), and closed-circuit television (CCTV). Battery banks should exhibit sufficient capacity that is determined in accordance with applicable standards (taking into account detection and alarm currents that should be ensured for a specified operation period of these systems). Due to the higher consumption of working currents by telematics systems, the backup power supply is provided within such a technical facility by UPS devices. Both battery banks and UPS devices are technically organized in a manner sufficient for the purposes of

guaranteeing an adequate operational safety level by providing power supply continuity. In order to ensure an adequate power supply reliability level, designers use, e.g., redundancy—cold, warm, and hot reserve or the so-called “failsafe” principle. Electronic security system elements are operated inside the structurally and mechanically reinforced metal container, where an air-conditioning system located outside the structure provides a strictly defined temperature and humidity. In order to secure appropriate protection against external actions that may impact the technical facility in question, selected ESS elements are placed on the container walls. These include, among others, cameras, IDS detectors, fire detectors, and signaling and acoustic devices. These signaling and audio devices are distinctive, separately announcing a fire and intrusion alarm. IDS and CCTV systems are integrated in order to maintain an appropriate security level. The FAS is not subject to integration with the a/m systems due to the legislation applicable in Poland. Information on all breaches, alarms, damage, activations, deactivations, etc. related to all safety or fire zones is saved in the nonvolatile memory of the alarm control units of the aforementioned devices. Furthermore, the information is sent to a remote receiving center (ARC) via two independent telecommunication routes—hardwired and radio [10–12]. In addition, the FAS has a separate, standalone alarm and damage signal transmission device (ADSTD), where the alarm signal is forwarded to the State Fire Service (PSP). All security systems, because of the function performed within a critical infrastructure facility, have backup alarms and damage signal transmitter. There are no people in the container who are responsible for service and repairs, and who are on continuous duty—24 h per day. Information on alarm and damage is sent to an ARC for security systems, whereas, in the case of transport telematics systems, it is sent to a separate technical point, which monitors the operating process involving a given railway route section. The container’s layout and position in the vicinity of medium-voltage power lines necessitates including the impact of unintentional low-frequency electromagnetic radiation in the ESS operating process. Due to the methodology of the low-frequency measurements, two separate electromagnetic field components—E electric field strength and B magnetic field induction—need to be taken into account separately. An electromagnetic field unintentionally generated by an MV power line may adversely impact the operating process of the aforementioned electronic systems. A variable unintentional electric or magnetic field may lead to the generation of interference inside such electronic systems (individual elements—detectors, control or power modules, alarm control units, etc.), as well as power, signal, or control cables, transmission buses, and detection circuits in the case of FAS [13–15].

A previous study [16] presented issues associated with the use of PV module energy in rail transport and its storage in order to supply vehicles. Such solutions are ecofriendly, but require the use of electrical and electronic devices, which also impact electronic security systems. For this reason, the analysis of the applied solutions aimed at improving resistance to electromagnetic interference is important.

Moreover, the issues regarding radio transmission are significant for the correct functioning of electronic security systems. The authors of [17] described the issue associated with high-strength electromagnetic fields generated by high-power pulse transmitters. This may severely affect electrical and electronic systems, unless rational solutions improving the strength and resistance of ESS to such interference are applied.

The location of the electromagnetic interference source is also important. Issues in this field were discussed in [18]. The authors suggested an innovative localization technique based on the time-reversal cavity (TRC) concept. This is an interesting approach; nevertheless, due to the measurement specificity and the available devices for measuring electromagnetic fields, the authors applied a traditional approach for two MV power lines in this article.

The authors of [19] described the problem of energy recovery upon train braking with regard to electromagnetic compatibility (more precisely—the interference between generated current harmonics and the rail signaling system). The conducted simulations enabled suggesting an asymmetric brake control in order to reduce current harmonics.

The issue regarding the impact of electromagnetic interference on the functioning of electronic rail transport devices is of particular importance in the case of high-speed railway. A previous study [20] presented an original approach to assessing the impact of electromagnetic interference on radio transmission that is based on common EMI characteristics. The application of radio transmission using local coding enables maintaining correct communication parameters.

The authors of [21] also addressed the interactions actions of the electromagnetic environment on high-speed railway. A graph model was developed in order to analyze the impact of electromagnetic interference on the operation of electronic railway equipment. It enables a more detailed reflection of the relationships for individual subsystems in the context of electromagnetic compatibility.

Despite the presented various approaches, the electromagnetic compatibility analysis involving electronic devices lacks studies that would link reliability and operational modeling of electronic railway equipment with resistance to electromagnetic interference. For this purpose, the authors of this article studied the issues in this field.

The issue of powering transport telematics systems and electronic security systems is characterized at the beginning of the paper. Particular attention is paid to the reliability and operational aspects, and the impact of unintentional low-frequency electromagnetic radiation. Next, the authors present the results of tests involving the electromagnetic environment surrounding medium-voltage lines supplying a container security system. This was used as a base to conclude that it was justified to apply solutions resulting in mitigated low-frequency electromagnetic field impact on the systems in question. Another stage of the deliberations by the authors was the analysis of the security system operating process in terms of the impact of unintentionally generated electromagnetic interference. The determined relationships enable rationally selecting solutions aimed at protecting systems against electromagnetic interference.

2. Study of the Electromagnetic Environment Surrounding Medium-Voltage Lines Supplying a Container Security System

The study was conducted for two medium-voltage (15 kV and 30 kV) power lines that supplied a metal container housing transport telematics systems and electronic security systems. The aforementioned containers were located near a railway communication route; however, the significant distance (over 250 m) from the overhead contact line allowed the authors to discard unintentional, nonstationary electromagnetic interference generated by the moving electric locomotives [22,23]. Operating electrical or electronic devices that are powered by electricity leads to generating electromagnetic, electric, or magnetic fields. A field generated artificially, intentionally or unintentionally by humans, deforms the natural electromagnetic environment. Most often, humans encounter in their nearest surroundings (their workplace or residence) unintentional electromagnetic radiation sources that are primarily of the low-frequency range. Power transmission lines are one of the main sources of unintentional electromagnetic radiation. Due to their coverage (overhead lines in particular), they emit electromagnetic radiation over a large area. Two frequency subranges for field meters were introduced in the measurement methodology involving the issues associated with diagnosing low-frequency electromagnetic fields, e.g., sources with a frequency of 50 Hz that are generated by power lines. The first range included extremely low frequencies (ELF)—from 5 Hz to 2 kHz, while the second involved very low frequencies (VLG)—from 2 kHz to 100 kHz. The space around the medium-voltage lines was diagnosed within these frequencies, pursuant to the applicable regulations on the measurement methodology. In order to investigate the impact of medium-voltage lines on the electromagnetic environment inside and outside the container with installed transport telematics systems, the authors measured the distribution of electromagnetic field components under three power lines supplying technical facilities, i.e., a 30 kV line and two different 15 kV lines. The measurements were taken at a positive outside temperature 20–21 °C and humidity 38–42%. The so-called “electromagnetic field background measurements” were conducted prior to commencing the measurements covering the

electromagnetic field generated by the studied power lines. They were taken in places where the natural electromagnetic field of the Earth is undistorted. The results are listed in Table 1.

Table 1. Mean magnetic field induction B and electric field strength E values in the ELF and VLF frequency ranges near the studied lines—field background measurement.

	30 kV Line	15 kV Line No. 1	15 kV Line No. 2
Mean magnetic field induction B, ELF range	0.02 μ T	0.02 μ T	0.015 μ T
Mean magnetic field induction B, VLF range	0.6 nT	0.4 nT	0.4 nT
Mean electric field strength E, ELF range	46 V/m	26 V/m	23 V/m
Mean electric field strength E, VLF range	2.2 V/m	2.3 V/m	2.2 V/m

Studies involving the impact of unintentional electromagnetic field on the external and internal environment of a container housing telematics and security systems were conducted in accordance with Figure 2.

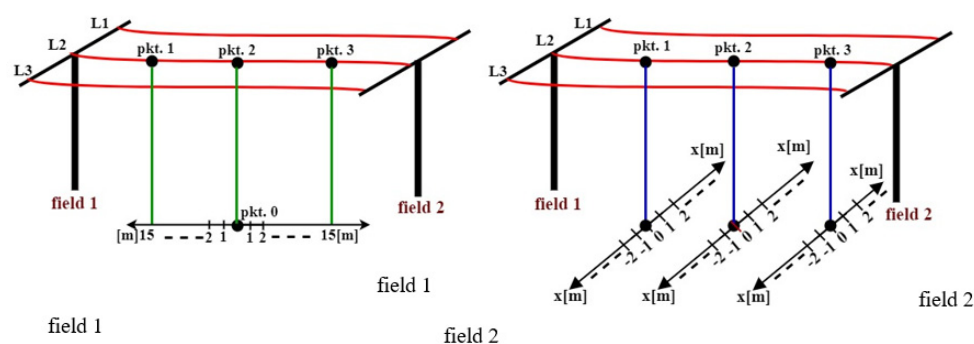


Figure 2. Diagram of a test stand for measuring electromagnetic field components along the line's phase conductors, and across the medium-voltage power line.

The presented characteristic curve (Figure 3) shows a significant decline in magnetic field induction B with increased distance from the studied lines. Magnetic field induction B reaches a field background level at a distance of 17–19 m from point 0 in the case of the 15 kV power line No. 1, whereas, for the 15 kV power line No. 2 and the 30 kV line, this distance is 7–9 m from point 0, with the measurement conducted in accordance with Figure 2. Disproportions between the maximum and minimum magnetic field induction B, depending on the measurement location, can be noticed when analyzing the resulting distribution. According to the Biot–Savart law, magnetic field induction B is proportional to the value of the flowing current and inversely proportional to the distance of the measuring point from the field source. Higher voltage of a transmission line supplying a container does not necessarily mean the presence of higher magnetic field induction B values. This is confirmed by the characteristic curves in Figure 3. The values of magnetic field induction B components B_x , B_y , and B_z are shown in Figure 4 for measuring point No. 2 (Figure 2), due to the fact that it provided the highest magnetic field induction B values.

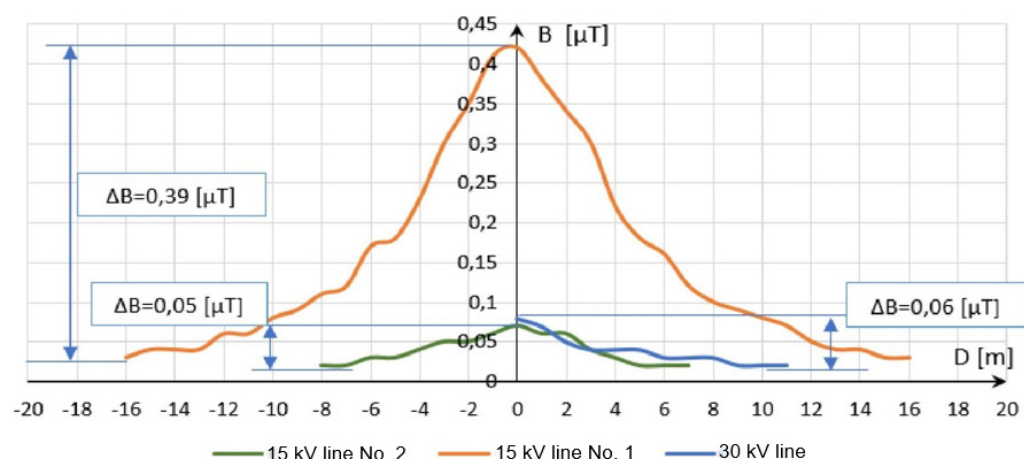


Figure 3. Distribution of magnetic field induction B across the line, for measuring point No. 1 and the ELF frequency range (induction measuring methodology as in Figure 2).

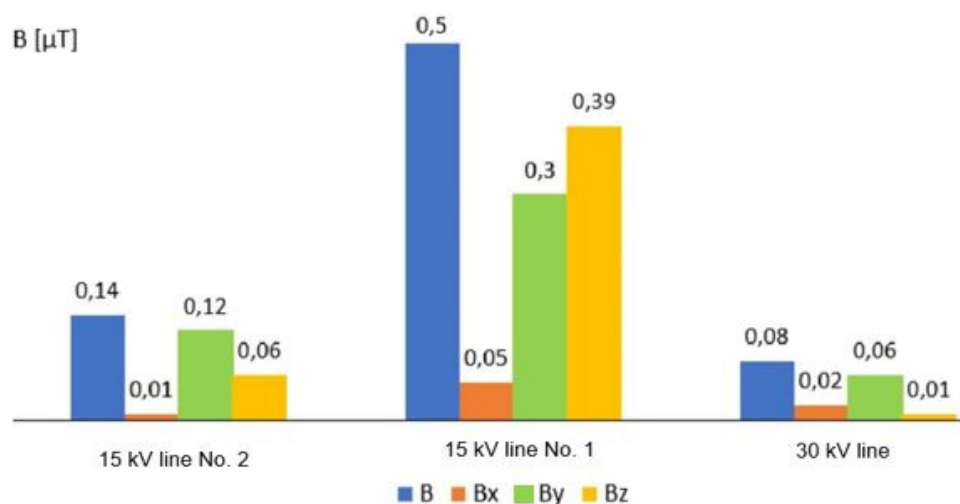


Figure 4. The value of magnetic field induction B and its components B_x , B_y , B_z at the point of maximum cable sag in the power line supplying the container with telematics and security systems. Maximum magnetic field induction B under MV lines for the ELF range was recorded at measuring point No. 2.

Magnetic induction in the VLF range was also measured at measuring point No. 2 (Figure 2). The results are shown in Figure 5.

The maximum magnetic field induction B for the VLF range under the 30 kV line was 2.2 nT, which was achieved at a distance of 5 m from point 0 (measurement in accordance to Figure 2). In contrast, the maximum magnetic field induction B was 0.9 nT for 15 kV line No. 1 and 0.7 nT for 15 kV line No. 2. Figures 6 and 7 show the measurement of magnetic induction along phase conductors of the container supply lines for the ELF range and two supply voltages—15 and 30 kV. The measurement procedure is shown in Figure 2.

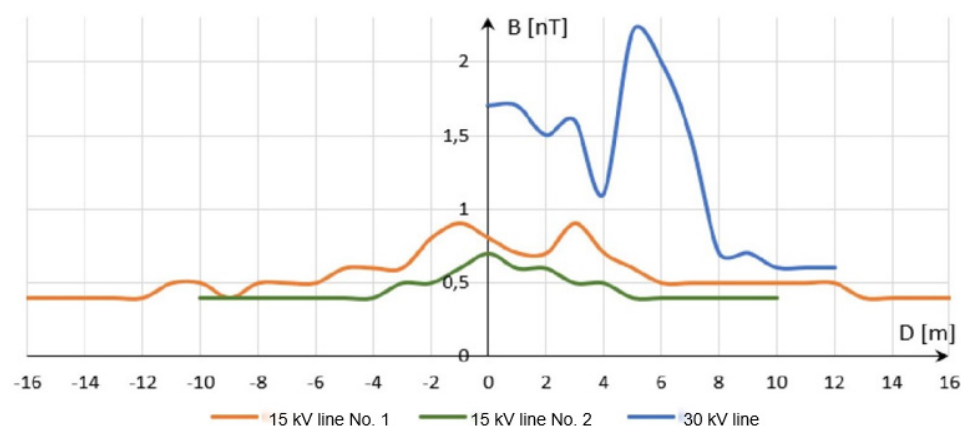


Figure 5. Distribution of magnetic field induction B across the line for measuring point No. 2, and the VLF frequency range (induction measuring methodology as in Figure 2).

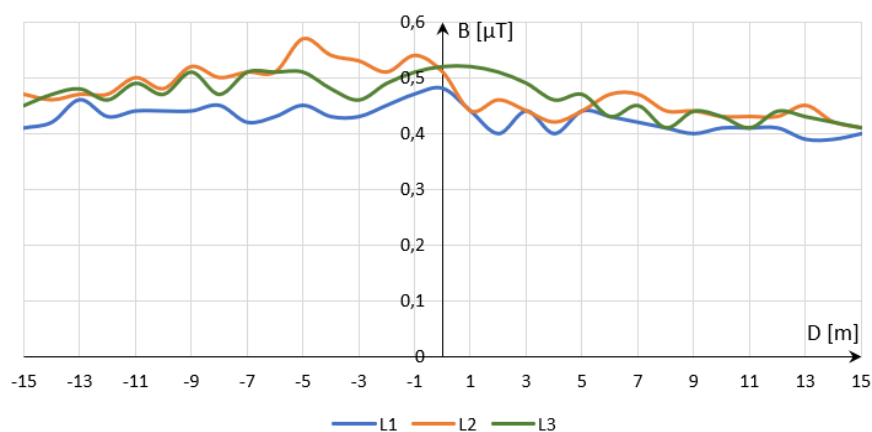


Figure 6. Distribution of magnetic field induction B along L1, L2, L3 phase conductors of the 15 kV power line No. 1, ELF frequency range.

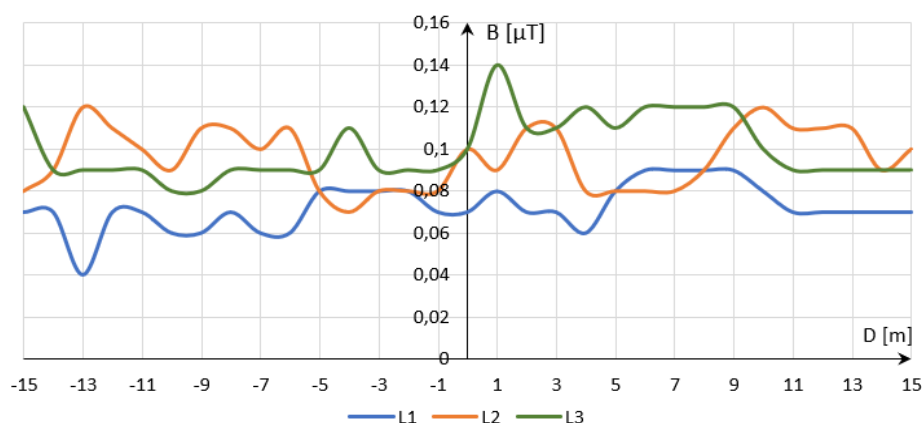


Figure 7. Distribution of magnetic field induction B along L1, L2, L3 phase conductors of the 30 kV power line No. 1, ELF frequency range.

The maximum magnetic field induction B measured along the phase conductors for the ELF range was identified under the central L2 conductor of the 15 kV line No. 1 and amounted to $0.57 \mu\text{T}$, while the value under the 30 kV line was equal to $0.14 \mu\text{T}$. Figures 8 and 9 show the magnetic field induction B along phase conductors for the VLF phase (measurement methodology shown in Figure 2). Upon observing the changes in the magnetic field induction B along the phase conductors over the VLF range, it can be noted that the 30 kV supplying the container was distinguished by higher values relative to both

15 kV lines. There were also significant differences between the maximum and minimum magnetic field induction B value depending on the rated voltage of the line supplying the container with telematics and security systems.

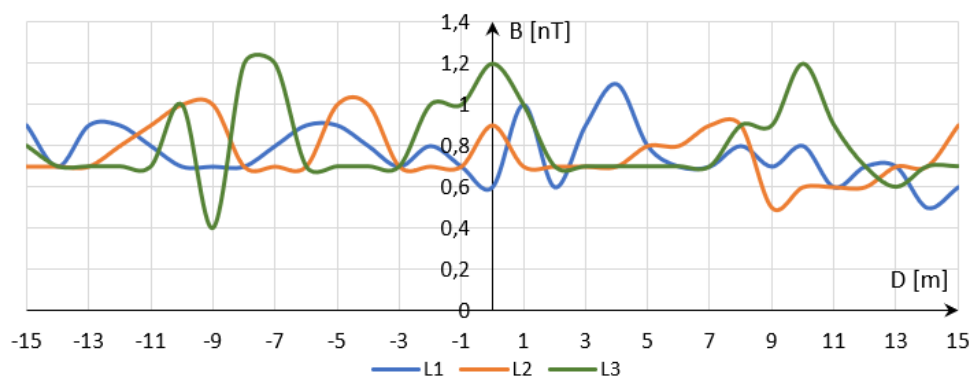


Figure 8. Distribution of magnetic field induction B along L1, L2, L3 phase conductors of the 15 kV container power line No. 1, VLF frequency range.

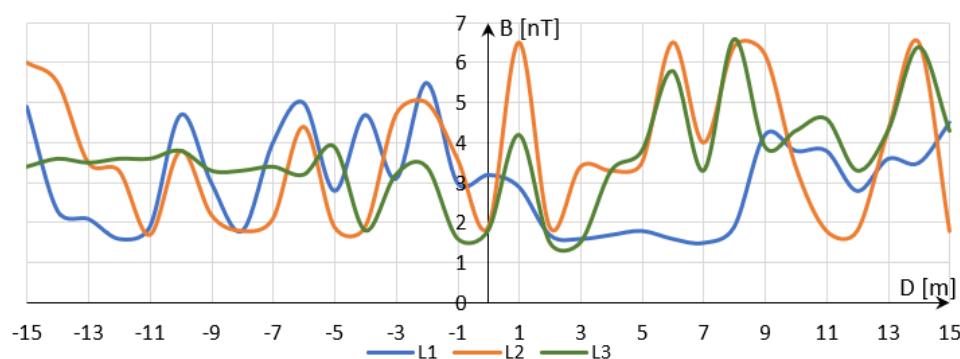


Figure 9. Distribution of magnetic field induction B along L1, L2, L3 phase conductors of the 30 kV container power line, VLF frequency range.

Changes in the magnetic field induction B over time were also measured. The measurements were taken in the location where the highest values were recorded. The magnetic field induction B value was read every minute for 15 min. Measurement results are shown in Figure 10. On comparing the magnetic field induction B values obtained over time, it can be concluded that they remained on average at a constant level. It was $0.53 \mu\text{T}$ for the 15 kV line No. 1 and $0.08 \mu\text{T}$ for the 30 kV and 15 kV No. 2 lines.

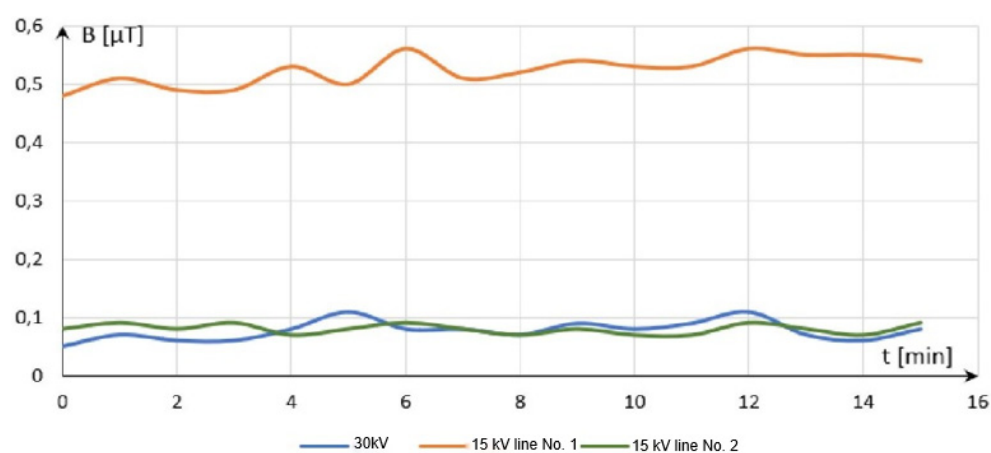


Figure 10. Magnetic field induction B change fluctuations under medium-voltage lines for the ELF range.

Figures 11 and 12 show the distribution of electric field strength E across MV power lines supplying the container with transport telematics system and ESS, at two measuring points, in accordance with Figure 2.

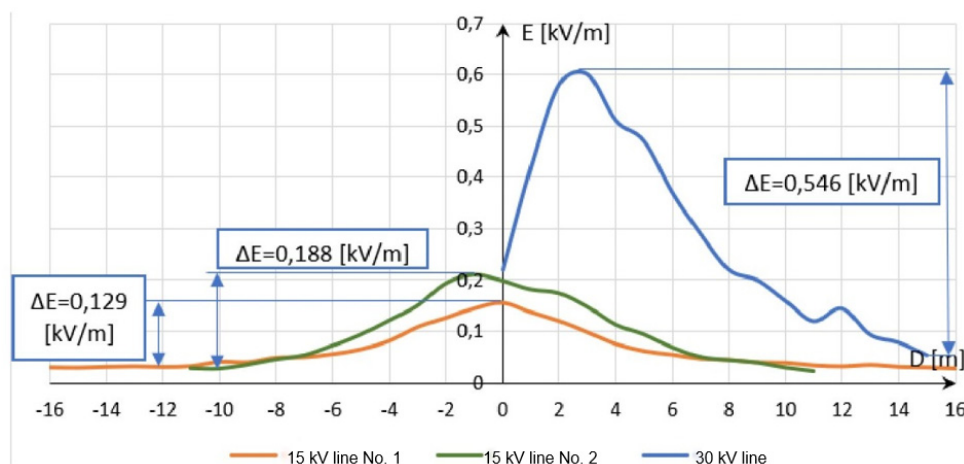


Figure 11. Distribution of electric field strength E across the line, for measuring point No. 1 and the ELF frequency range (induction measuring methodology as in Figure 2).

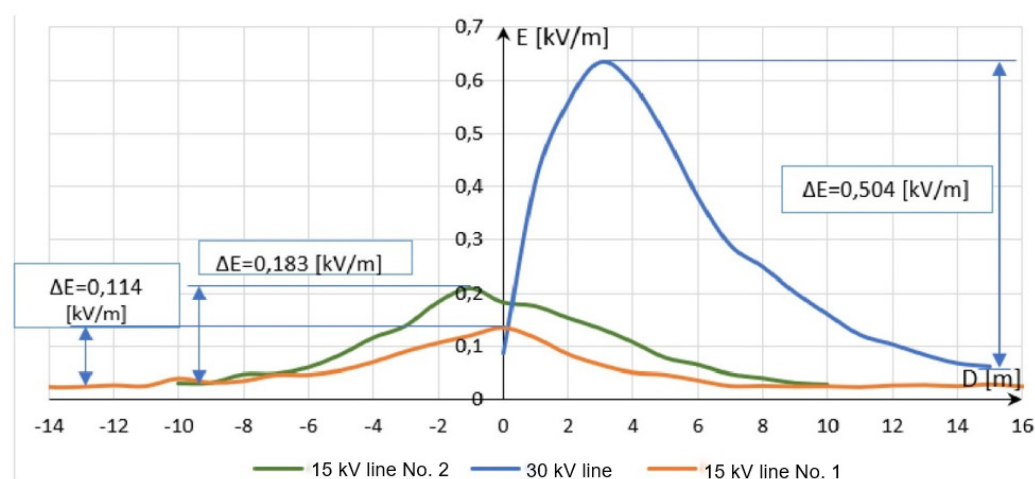


Figure 12. Distribution of electric field strength E across the line, for measuring point No. 3 and the ELF frequency range (induction measuring methodology as in Figure 2).

Electric field strength E decreased with increasing distance from point 0 and reached a background value at a distance of 11–13 m for the 15 kV power line and 15–16 m for the 30 kV line. As in the case of the magnetic field induction B , the electric field strength E also reached the highest values at measuring point No. 2. The 30 kV power line, however, achieved significantly higher electric field strength E values. Along with the increase of the line voltage, the electric field strength E also increased.

The electric field strength E was also measured in terms of the VLF range for measuring point No. 2 (measurement methodology as in Figure 2). Measurement results are shown in Figure 13.

In the course of analyzing the characteristic curves, it can be concluded that 15 kV lines produced virtually no electric field strength E component over the VLF range. The changes in the values over the entire measuring range fluctuated from 2.1 to 2.3 V/m, which corresponded to the values of the measured electric field background. The changes in the electric field strength E along the phase conductors of container-supplying MV power lines were also analyzed. The results of these tests are shown in Figures 14 and 15.

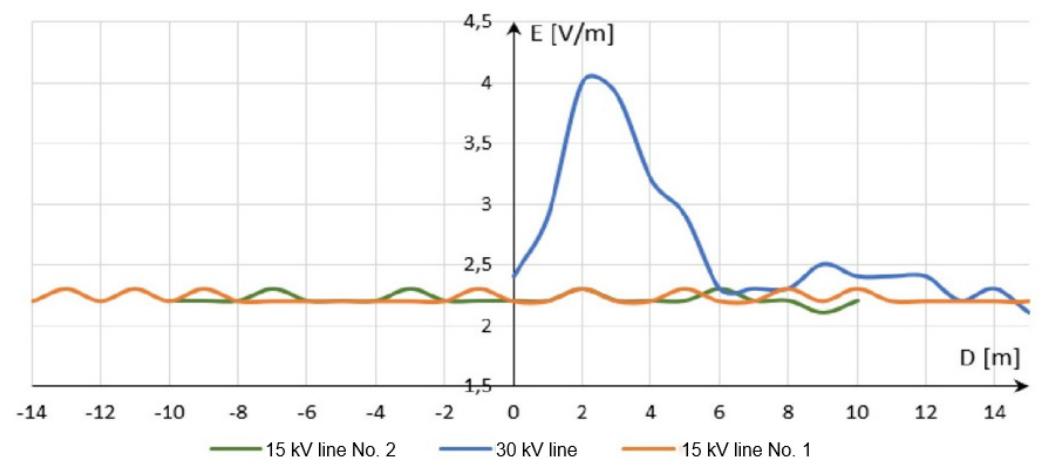


Figure 13. Distribution of electric field strength E across the line, for measuring point No. 2 and the VLF frequency range (induction measuring methodology as in Figure 2).

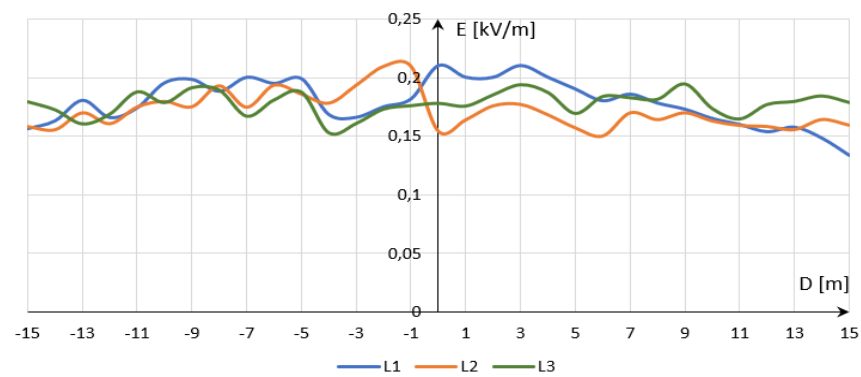


Figure 14. Distribution of electric field strength E along L1, L2, L3 phase conductors of the 15 kV container power line, ELF frequency range (measurement methodology as in Figure 2).

Figure 16 shows changes in the electric field strength E under MV lines supplying the container, for the ELF range. In the case of both 15 kV lines, the electric field strength could be considered constant, and its mean value was 0.19 kV/m and 0.21 kV/m for 15 kV lines No. 1 and No. 2, respectively. In the case of the 30 kV line, the electric field strength ranged from 0.53 kV/m to 0.73 kV/m.

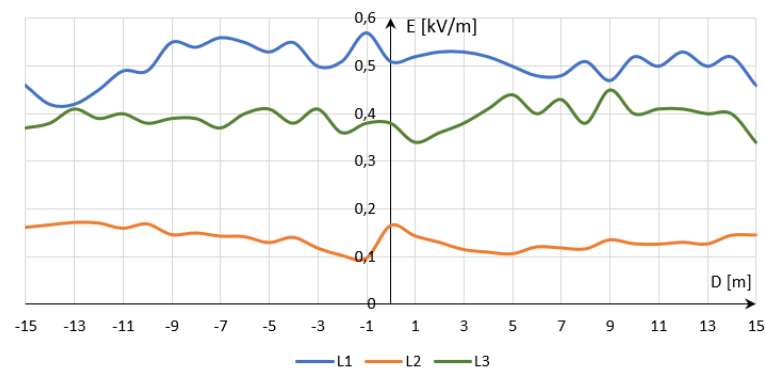


Figure 15. Distribution of electric field strength E along L1, L2, L3 phase conductors of the 30 kV container power line, ELF frequency range (measurement methodology as in Figure 2).

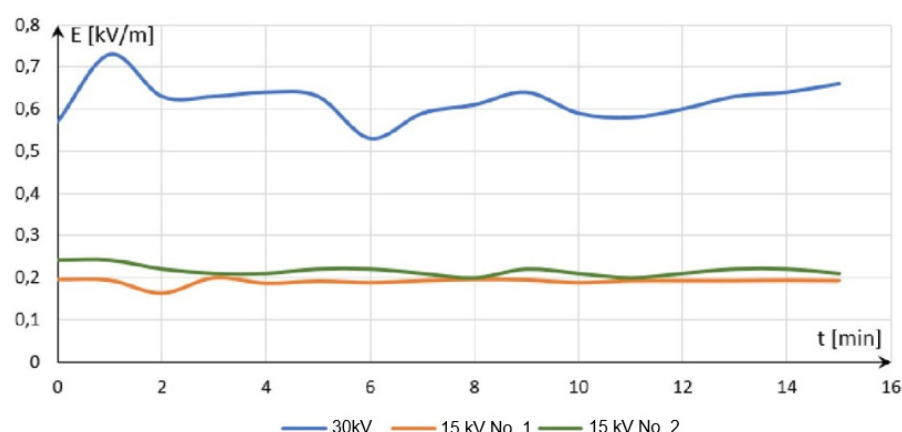


Figure 16. Electric field strength E fluctuations under MV lines supplying the container, for the ELF range (measurement methodology as in Figure 2).

When analyzing the obtained measurement results for all power lines supplying the container, it can be concluded that the highest magnetic field induction B was recorded under the 15 kV line No. 1 and amounted to $0.57 \mu\text{T}$. In contrast, the maximum electric field strength E component value was at a level 0.64 kV/m , which was achieved near the 30 kV line.

3. Metal Container Housing: Determining the Shielding Effectiveness for a Low-Frequency Electromagnetic Field

When constructing and operating electronic, transport telematics, or security equipment and systems, it is required to protect a given technical facility against the impact of undesirable electromagnetic interference over a wide spectrum range [24,25]. Appropriately manufactured guards, usually metallic, called shields are used in such cases in accordance with the electromagnetic compatibility pyramid [26–28]. An electromagnetic shield is always a conductive shield that separates two areas. One is the source, e.g., of an unintentional electromagnetic field, i.e., MV power lines supplying the container in this case. The other does not contain the source, i.e., it is the container interior. This separation applies not only to fields, but also to fault currents. A shield also provides a potential reference for cables routed from the container housing and for electronic circuits located inside the metal container. The most important parameter that characterizes shielding execution is the so-called “shield effectiveness S coefficient”. It is a ratio of the shield attenuation determined on the basis of field residual strength (electric, magnetic, or electromagnetic field) measured in the presence of a shield and the field strength measured without the shield. The shielding effectiveness S coefficient is a dimensionless value. Shield attenuation S is most usually expressed in dB, as per Equation (1).

$$S = 20 \cdot \log \cdot (P_{be}/P_{ze}), \quad (1)$$

where P_{be} is the unshielded field strength, and P_{ze} is the shielded field strength.

Shield attenuation is defined in relation to an electrical (Equation (2)), magnetic (Equation (3)), or coupled field. Shield effectiveness relative to the electrical or magnetic field is expressed by Equations (2) and (3), respectively.

$$S_E = 20 \cdot \log \cdot (E_{be}/E_{ze}), \quad (2)$$

$$S_H = 20 \cdot \log \cdot (H_{be}/H_{ze}), \quad (3)$$

where E_{be} , H_{be} are, respectively, unshielded electric and magnetic strengths, and E_{ze} , H_{ze} are, respectively, shielded electric and magnetic strengths.

A positive attenuation values is expressed in dB and means a reduction in field strength. A negative attenuation implies a strength increase. In any given electronic device,

at various frequency ranges, poorly executed shielding may behave like a directional antenna. Shielding effectiveness is a function with numerous variables and depends on parameters such as frequency, shield geometric structure, location within the shield where the field is determined, type of shielded field—electric, magnetic, or electromagnetic, incidence direction, and wave polarization. The total shielding effectiveness of the material used to manufacture the container where the telematics and security systems are operated is equal to the total relative measures of attenuation losses A , deflection losses R , and the correction factor B . The correction factor B takes into account the so-called “numerous deflections in thin shields” (Figure 17). In such a case, the total shielding effectiveness of a metal container can be expressed using Equation (4).

$$S[dB] = A + R + B. \quad (4)$$

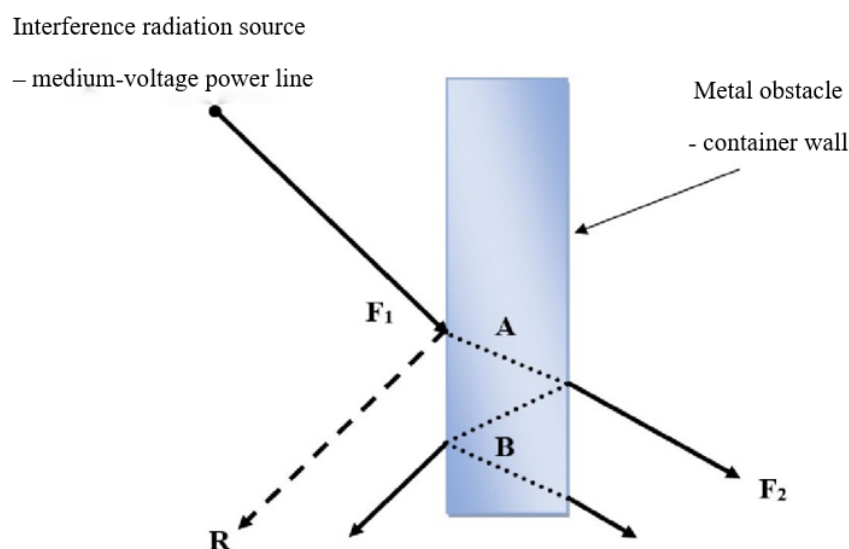


Figure 17. Principle of shielding an electromagnetic wave generated by an MV power line through a metal obstacle constituting the container.

The following materials are sufficient for the shielding of the low-frequency electromagnetic fields that are generated by MV power lines:

- thin, highly conductive materials, 20 to 50 μm thick, since they guarantee high losses related to deflection of electric waves;
- several millimeter thick materials, when shielding a magnetic field. This is brought about by the poor attenuation that is associated with waves deflecting from the shield surface; hence, it must provide high absorption losses if the shield is to be effective (shielding fields with a frequency up to 500 kHz requires the application of a magnetically soft material, e.g., iron with relative conductivity $\mu_r = 200$ or Alu-metal with a thickness >0.5 mm).

The simplest way to reduce the impact of an electromagnetic radiation source on a given electronic device or element is placing it as far from the source as possible—in this case, away from the medium-voltage supply lines. This will enable locating it in areas where the unintentionally generated electromagnetic field exhibits low values. However, it is impossible to always apply this principle. In such a case, a solution is to mitigate the impact of an electromagnetic field by shielding the source or a selected space around the MV power lines. Shield effectiveness was measured for a metal housing of a container made of sheet metal with thickness $h = 1.5$ mm. The results of shielding effectiveness measurements for the ELF and VLF ranges are shown in Table 2. Figure 18 shows the shielding effectiveness of a 1.5 mm thick steel material for magnetic field induction B and electric field strength E over the ELF and VLF ranges. The shielding effectiveness

value should be taken into account when determining operating process safety indices for security and telematics systems operated inside any metal container.

Table 2. Magnetic field induction B and electric field strength E shielding effectiveness over the described ELF and VLF ranges for individual shields (shield is the metal container housing, with a sheet thickness $h=1.5$ mm).

Shielding Effectiveness S	S (dB)			
	Magnetic Field Induction B		Electric Field Strength E	
Frequency range	ELF	VLF	ELF	VLF
Shield made of steel sheet, thickness $h = 1.5$ mm	8.26	13.5	3.57	8.1

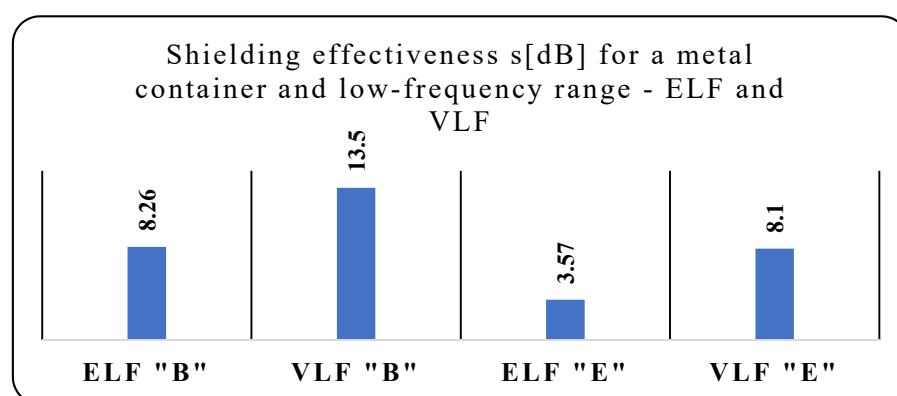


Figure 18. Shielding effectiveness for a metal material with a thickness $h = 1.5$ mm, for magnetic field induction B and electric field strength E, over the ELF and VLF ranges.

4. Analysis of the Security System Operating Process in Terms of the Impact of Unintentionally Generated Electromagnetic Interference

The impact of use [29], operation and power supply [30,31] conditions, including the impact of unfavorable external [32–35], and internal [36] environmental factors (e.g., low-frequency electromagnetic field) on electronic telematics [37–40] and security systems can be described through, e.g., a change in the intensity of damage to λ components making up a specific system [41,42]. Telematics and security systems and equipment operated in the container contain a large number of active and passive elements. These elements exhibit various margins of resistance to different interference, e.g., electromagnetic, environmental, electrical, thermal, and mechanical, generated in a container in an intentional or unintentional manner. The resistance value undergoes constant change impacted by various environmental factors, e.g., electromagnetic interference, temperature, humidity, and precipitation. Therefore, it is essential to develop an operating process model that takes into account the resistance to electromagnetic interference.

A functional analysis of an electronic security system located in a metal container, taking into account the impact of unintentionally generated electromagnetic interference, enables illustrating the relations therein from the reliability and operational perspective, as demonstrated in Figure 19.

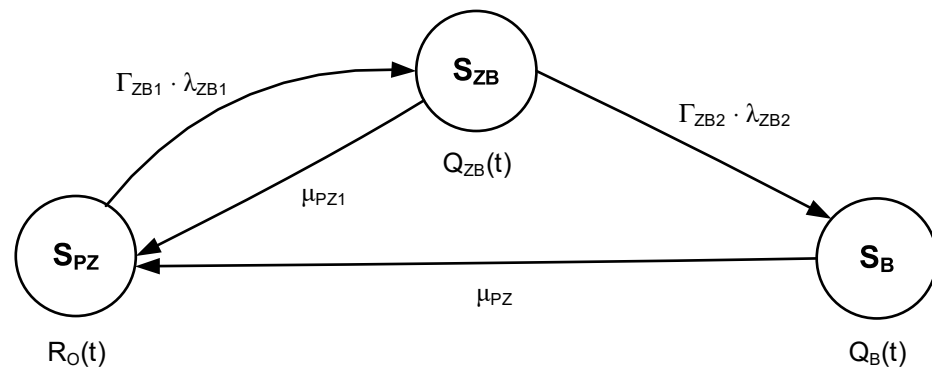


Figure 19. Functional relations within an electronic security system, taking into account the impact of unintentionally generated electromagnetic interference. Designations in Figure: $R_0(t)$ —probability function for an ESS to stay in state S_{PZ} ; $Q_{ZB}(t)$ —probability function for an ESS to stay in state S_{ZB} ; $Q_B(t)$ —probability function for an ESS to stay in state S_B ; λ_{ZB1} —intensity of transitions from state S_{PZ} to state S_{ZB} ; μ_{PZ1} —intensity of transitions from state S_{ZB} to state S_{PZ} ; λ_{ZB2} —intensity of transitions from state Q_{ZB} to state Q_B ; μ_{PZ} —intensity of transitions from state Q_B to state S_{PZ} ; Γ_{ZB1} and Γ_{ZB2} —electromagnetic interference impact coefficients.

The state of full fitness S_{PZ} is a state in which an electronic security system operates correctly. The state of security hazard S_{ZB} is a state in which an ESS operates partially correctly. The state of security unreliability (failure) S_B is a state in which an ESS does not operate correctly.

In the event of the ESS staying in a state of full fitness S_{PZ} and the presence of unintentionally generated electromagnetic interference resulting in the inability to perform certain function, the system will shift to a state of security hazard S_{ZB} , with an intensity equal to the product of $\Gamma_{ZB1} \lambda_{ZB1}$.

An ESS in a state of security hazard S_{ZB} can move to a state of full fitness S_{PZ} , if the ability to implement all ESS functions is restored, or security unreliability Q_B , with an intensity equal to the product of $\Gamma_{ZB2} \lambda_{ZB2}$ in the event of electromagnetic interference, resulting in ESS's inability to perform its functions.

Transition from a state of security unreliability S_B to a state of full fitness S_{PZ} takes place when the ability to perform all ESS functions is restored.

The Γ_{ZB1} and Γ_{ZB2} coefficients quantify the impact of unintentionally generated electromagnetic interference, taking into account the applied countermeasures.

The electronic security system presented in Figure 19 is described by the following Kolmogorov–Chapman system of equations:

$$\begin{aligned} R'_0(t) &= -\Gamma_{ZB1} \cdot \lambda_{ZB1} \cdot R_0(t) + \mu_{PZ1} \cdot Q_{ZB}(t) + \mu_{PZ} \cdot Q_B(t), \\ Q'_{ZB}(t) &= \Gamma_{ZB1} \cdot \lambda_{ZB1} \cdot R_0(t) - \mu_{PZ1} \cdot Q_{ZB}(t) - \Gamma_{ZB2} \cdot \lambda_{ZB2} \cdot Q_{ZB}(t), \\ Q'_B(t) &= \Gamma_{ZB2} \cdot \lambda_{ZB2} \cdot Q_{ZB}(t) - \mu_{PZ} \cdot Q_B(t). \end{aligned} \quad (5)$$

If we assume the following baseline conditions for further analysis:

$$\begin{aligned} R_0(0) &= 1, \\ Q_{ZB}(0) &= Q_B(0) = 0, \end{aligned} \quad (6)$$

and then apply the Laplace transform [43–45], we obtain the following set of linear equations:

$$\begin{aligned} s \cdot R_0^*(s) - 1 &= -\Gamma_{ZB1} \cdot \lambda_{ZB1} \cdot R_0^*(s) + \mu_{PZ1} \cdot Q_{ZB}^*(s) + \mu_{PZ} \cdot Q_B^*(s), \\ s \cdot Q_{ZB}^*(s) &= \Gamma_{ZB1} \cdot \lambda_{ZB1} \cdot R_0^*(s) - \mu_{PZ1} \cdot Q_{ZB}^*(s) - \Gamma_{ZB2} \cdot \lambda_{ZB2} \cdot Q_{ZB}^*(s), \\ s \cdot Q_B^*(s) &= \Gamma_{ZB2} \cdot \lambda_{ZB2} \cdot Q_{ZB}^*(s) - \mu_{PZ} \cdot Q_B^*(s). \end{aligned} \quad (7)$$

After further conversions, we acquire the symbolic (Laplace) probabilities for the ESS to stay in functional states.

$$\begin{aligned}
 R_0^*(s) &= \frac{s^2 + s \cdot \mu_{PZ} + s \cdot \mu_{PZ1} + s \cdot \Gamma_{ZB2} \cdot \lambda_{ZB2} + \mu_{PZ} \cdot \mu_{PZ1} + \mu_{PZ} \cdot \Gamma_{ZB2} \cdot \lambda_{ZB2}}{s^2 \cdot \mu_{PZ} + s^2 \cdot \Gamma_{ZB1} \cdot \lambda_{ZB1} + s^2 \cdot \mu_{PZ1} + s^2 \cdot \Gamma_{ZB2} \cdot \lambda_{ZB2} + s^3 +} \\
 &\quad + s \cdot \mu_{PZ} \cdot \Gamma_{ZB1} \cdot \lambda_{ZB1} + s \cdot \mu_{PZ} \cdot \mu_{PZ1} + \\
 &\quad + s \cdot \mu_{PZ} \cdot \Gamma_{ZB2} \cdot \lambda_{ZB2} + s \cdot \Gamma_{ZB1} \cdot \lambda_{ZB1} \cdot \Gamma_{ZB2} \cdot \lambda_{ZB2}, \\
 Q_{ZB}^*(s) &= \frac{s \cdot \Gamma_{ZB1} \cdot \lambda_{ZB1} + \mu_{PZ} \cdot \Gamma_{ZB1} \cdot \lambda_{ZB1}}{s^2 \cdot \mu_{PZ} + s^2 \cdot \Gamma_{ZB1} \cdot \lambda_{ZB1} + s^2 \cdot \mu_{PZ1} + s^2 \cdot \Gamma_{ZB2} \cdot \lambda_{ZB2} + s^3 +} \\
 &\quad + s \cdot \mu_{PZ} \cdot \Gamma_{ZB1} \cdot \lambda_{ZB1} + s \cdot \mu_{PZ} \cdot \mu_{PZ1} + \\
 &\quad + s \cdot \mu_{PZ} \cdot \Gamma_{ZB2} \cdot \lambda_{ZB2} + s \cdot \Gamma_{ZB1} \cdot \lambda_{ZB1} \cdot \Gamma_{ZB2} \cdot \lambda_{ZB2}, \\
 Q_B^*(s) &= \frac{\Gamma_{ZB1} \cdot \lambda_{ZB1} \cdot \Gamma_{ZB2} \cdot \lambda_{ZB2}}{s^2 \cdot \mu_{PZ} + s^2 \cdot \Gamma_{ZB1} \cdot \lambda_{ZB1} + s^2 \cdot \mu_{PZ1} + s^2 \cdot \Gamma_{ZB2} \cdot \lambda_{ZB2} + s^3 +} \\
 &\quad + s \cdot \mu_{PZ} \cdot \Gamma_{ZB1} \cdot \lambda_{ZB1} + s \cdot \mu_{PZ} \cdot \mu_{PZ1} + \\
 &\quad + s \cdot \mu_{PZ} \cdot \Gamma_{ZB2} \cdot \lambda_{ZB2} + s \cdot \Gamma_{ZB1} \cdot \lambda_{ZB1} \cdot \Gamma_{ZB2} \cdot \lambda_{ZB2},
 \end{aligned} \tag{8}$$

The determined relationships in Equation (8) enable calculating the probabilities of an electronic security system staying in the three distinguished states, taking into account the impact of unintentionally generated electromagnetic interference. The introduction of the Γ_{ZB1} and Γ_{ZB2} coefficients of electromagnetic interference in terms of impact on the ESS enables to rationally select solutions aimed at protecting against electromagnetic interference.

5. Conclusions

The issue of operating transport telematics and electronic security systems located within railway areas is extremely important. They ensure the safety of both vehicles and passengers. For this reason, the issue related to the impact of unintentionally generated electromagnetic interference on the ESS becomes one of particular importance. They can lead to a state of partial fitness of transport telematic systems and electronic security systems, whereby the ESS is unable to execute all of its functions.

In order to determine the impact of unintentionally generated electromagnetic interference on ESS, the authors measured the low-frequency electromagnetic field generated by MV—15 and 30 kV—power lines. The obtained results enable determining numerous characteristic curves that allowed defining points of particularly high magnetic and electric field strength values. An analysis of the solution in the form of a metal housing for a container containing transport telematics and electronic security system equipment was also conducted. It was found that such a structure reduced the impact of electromagnetic interference originating from medium-voltage power lines on the analyzed systems. Therefore, it is possible to increase shielding effectiveness for a low-frequency electromagnetic field.

The conducted security system operating process analysis in terms of the impact of unintentionally generated electromagnetic interference enabled determining mathematical relationships defining the probabilities for a system to stay in distinguished states. It also allowed numerically defining the impact of applied solutions aimed at protecting against electromagnetic interference. Therefore, it is possible to rationally select solutions (structural and organizational [46]) aimed at protecting systems against electromagnetic interference.

The next stage of the study was to develop an ESS operating process model that takes into account the impact of unintentionally generated electromagnetic interference. Introducing the electromagnetic interference impact coefficient enables a rational selection of solutions aimed at protecting against electromagnetic interference. This is a significant practical aspect of the conducted test and scientific studies discussed in this article, since it has application value. As further research, the authors are planning to determine the values of electromagnetic interference impact coefficients depending on the applied design solutions.

Author Contributions: Conceptualization, K.J., J.P. and A.R.; methodology, J.P. and A.R.; validation, K.J. and J.P.; formal analysis, K.J., J.P. and A.R.; investigation, J.P. and A.R.; resources, K.J. and J.P.; data curation, K.J. and J.P.; writing—original draft preparation, K.J., J.P. and A.R.; writing—review and editing, J.P. and A.R.; visualization, K.J. and J.P.; supervision, A.R.; project administration, A.R.;

funding acquisition, J.P. and A.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Government Security Center. National Critical Infrastructure Protection Programme in Poland. Available online: <https://www.gov.pl/attachment/ee334990-ec9c-42ab-ae12-477608d94eb1> (accessed on 18 August 2021).
2. Kołowrocki, K.; Soszyńska-Budny, J. Critical Infrastructure Safety Indicators. In Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bangkok, Thailand, 16–19 December 2018; pp. 1761–1764. [CrossRef]
3. Stawowy, M.; Perlicki, K.; Sumiła, M. Comparison of Uncertainty Multilevel Models to Ensure ITS Services. In *Safety and Reliability: Theory and Applications—Proceedings of the European Safety and Reliability Conference ESREL 2017, Portorož, Slovenia, 18–22 June 2017*; Cepin, M., Bris, R., Eds.; CRC Press/Balkema: London, UK, 2017; pp. 2647–2652. [CrossRef]
4. Gołębiowski, P.; Jacyna, M.; Stańczak, A. The Assessment of Energy Efficiency versus Planning of Rail Freight Traffic: A Case Study on the Example of Poland. *Energies* **2021**, *14*, 5629. [CrossRef]
5. Jacyna, M.; Żochowska, R.; Sobota, A.; Wasiak, M. Scenario Analyses of Exhaust Emissions Reduction through the Introduction of Electric Vehicles into the City. *Energies* **2021**, *14*, 2030. [CrossRef]
6. Stypułkowski, K.; Gołda, P.; Lewczuk, K.; Tomaszewska, J. Monitoring System for Railway Infrastructure Elements Based on Thermal Imaging Analysis. *Sensors* **2021**, *21*, 3819. [CrossRef] [PubMed]
7. Billinton, R.; Allan, R.N. *Reliability Evaluation of Power Systems*; Plenum Press: New York, NY, USA, 1996.
8. Klimczak, T.; Paś, J. *Basics of Exploitation of Fire Alarm Systems in Transport Facilities*; Military University of Technology: Warsaw, Poland, 2020.
9. Klimczak, T.; Paś, J. Reliability and operating analysis of transmission of alarm signals of distributed fire signaling system. *J. KONBiN* **2019**, *49*, 165–174. [CrossRef]
10. Polak, R.; Laskowski, D.; Matyszek, R.; Łubkowski, P.; Konieczny, Ł.; Burdzik, R. Optimizing the Data Flow in a Network Communication between Railway Nodes. In *Research Methods and Solutions to Current Transport Problems, Proceedings of the International Scientific Conference Transport of the 21st Century, Advances in Intelligent Systems and Computing, Ryn, Poland, 9–12 June 2019*; Siergiejczyk, M., Krzykowska, K., Eds.; Springer: Cham, Switzerland, 2020; Volume 1032, pp. 351–362. [CrossRef]
11. Krzykowska-Piotrowska, K.; Dudek, E.; Siergiejczyk, M.; Rosiński, A.; Wawrzyński, W. Is Secure Communication in the R2I (Robot-to-Infrastructure) Model Possible? Identification of Threats. *Energies* **2021**, *14*, 4702. [CrossRef]
12. Bednarek, M.; Dąbrowski, T.; Olchowik, W. Selected practical aspects of communication diagnosis in the industrial network. *J. KONBiN* **2019**, *49*, 383–404. [CrossRef]
13. Paś, J.; Rosiński, A.; Białek, K. A reliability-operational analysis of a track-side CCTV cabinet taking into account interference. *Bull. Pol. Acad. Sci. Tech. Sci* **2021**, *69*, e136747. [CrossRef]
14. Paś, J.; Rosiński, A.; Białek, K. A reliability-exploitation analysis of a static converter taking into account electromagnetic interference. *Transp. Telecommun.* **2021**, *22*, 217–229. [CrossRef]
15. Pas, J.; Rosinski, A.; Chrzan, M.; Bialek, K. Reliability-operational analysis of the LED lighting module including electromagnetic interference. *IEEE Trans. Electromagn. Compat.* **2020**, *62*, 2747–2758. [CrossRef]
16. RajaPriyanka, D.; ShanmugaPriya, G.; Sabashini, R.; Jacintha, V.M.E. Power generation and energy management in railway system. In Proceedings of the Third International Conference on Science Technology Engineering & Management (ICONSTEM), Chennai, India, 18 January 2017; pp. 949–954. [CrossRef]
17. Sunitha, K.; Thomas Joy, M. Effect of Soil Conditions on the Electromagnetic Field from an Impulse Radiating Antenna and on the Induced Voltage in a Buried Cable. *IEEE Trans. Electromagn. Compat.* **2018**, *61*, 990–997. [CrossRef]
18. Karami, H.; Azadifar, M.; Wang, Z.; Rubinstein, M.; Rachidi, F. Single-Sensor EMI Source Localization Using Time Reversal: An Experimental Validation. *Electronics* **2021**, *10*, 2448. [CrossRef]
19. Steczek, M.; Chudzik, P.; Szlag, A. Application of a Non-carrier-Based Modulation for Current Harmonics Spectrum Control during Regenerative Braking of the Electric Vehicle. *Energies* **2020**, *13*, 6686. [CrossRef]
20. Geng, X.; Wen, Y.; Zhang, J.; Zhang, D. A Method to Supervise the Effect on Railway Radio Transmission of Pulsed Disturbances Based on Joint Statistical Characteristics. *Appl. Sci.* **2020**, *10*, 4814. [CrossRef]
21. Li, M.; Wen, Y.; Wang, G.; Zhang, D.; Zhang, J. A Network-Based Method to Analyze EMI Events of On-Board Signaling System in Railway. *Appl. Sci.* **2020**, *10*, 9059. [CrossRef]

22. Wróbel, Z. The Electromagnetic Compatibility in Researches of Railway Traffic Control Devices. In *Analysis and Simulation of Electrical and Computer Systems*; Springer: Cham, Switzerland, 2018; pp. 275–287. [\[CrossRef\]](#)
23. Smolenski, R.; Lezynski, P.; Bojarski, J.; Drozd, W.; Long, L.C. Electromagnetic compatibility assessment in multiconverter power systems—Conducted interference issues. *Measurement* **2020**, *165*, 108119. [\[CrossRef\]](#)
24. Valouch, J. Technical requirements for Electromagnetic Compatibility of Alarm Systems. *Int. J. Circuits Syst. Signal Process.* **2015**, *9*, 186–191. Available online: <https://www.naun.org/main/NAUN/circuitssystemsignal/2015/a522005-196.pdf> (accessed on 1 October 2021).
25. Urbancokova, H.; Valouch, J.; Adamek, M. Testing of an intrusion and hold-up systems for electromagnetic susceptibility—EFT/B. *Int. J. Circuits Syst. Signal Process.* **2015**, *9*, 40–46.
26. Chmielińska, J.; Kuchta, M.; Kubacki, R.; Dras, M.; Wierny, K. Selected methods of electronic equipment protection against electromagnetic weapon. *Przegląd Elektrotechniczny* **2016**, *92*, 1–8. [\[CrossRef\]](#)
27. Lheurette, E. (Ed.) *Metamaterials and Wave Control*; ISTE and Wiley: London, UK, 2013.
28. Piersanti, S.; Orlandi, A.; de Paulis, F. Electromagnetic Absorbing materials design by optimization using a machine learning approach. *IEEE Trans. Electromagn. Compat.* **2018**, 1–8. [\[CrossRef\]](#)
29. Kozłowski, E.; Borucka, A.; Swiderski, A. Application of the logistic regression for determining transition probability matrix of operating states in the transport systems. *Eksplot. Niezawodn.–Maint. Reliab.* **2020**, *22*, 192–200. [\[CrossRef\]](#)
30. Hosseini, S.M.; Carli, R.; Dotoli, M. Robust optimal energy management of a residential microgrid under uncertainties on demand and renewable power generation. *IEEE Trans. Autom. Sci. Eng.* **2020**, *18*, 618–637. [\[CrossRef\]](#)
31. Tu, H.; Feng, H.; Srdic, S.; Lukic, S. Extreme Fast Charging of Electric Vehicles: A Technology Overview. *IEEE Trans. Transp. Electr.* **2019**, *5*, 861–878. [\[CrossRef\]](#)
32. Jakubowski, J.; Kuchta, M.; Kubacki, R. D-Dot Sensor Response Improvement in the Evaluation of High-Power Microwave Pulses. *Electronics* **2021**, *10*, 123. [\[CrossRef\]](#)
33. Tomczuk, P.; Chrzanowicz, M.; Jaskowski, P.; Budzynski, M. Evaluation of Street Lighting Efficiency Using a Mobile Measurement System. *Energies* **2021**, *14*, 3872. [\[CrossRef\]](#)
34. Tomczuk, P.; Chrzanowicz, M.; Jaskowski, P. Procedure for Measuring the Luminance of Roadway Billboards and Preliminary Results. *LEUKOS* **2020**, 1–19. [\[CrossRef\]](#)
35. Zieja, M.; Szelmanowski, A.; Pazur, A.; Kowalczyk, G. Computer Life-Cycle Management System for Avionics Software as a Tool for Supporting the Sustainable Development of Air Transport. *Sustainability* **2021**, *13*, 1547. [\[CrossRef\]](#)
36. Lewczuk, K.; Kłodawski, M.; Gepner, P. Energy Consumption in a Distributional Warehouse: A Practical Case Study for Different Warehouse Technologies. *Energies* **2021**, *14*, 2709. [\[CrossRef\]](#)
37. Jacyna, M.; Szczepański, E.; Izdebski, M.; Jasiński, S.; Maciejewski, M. Characteristics of event recorders in Automatic Train Control systems. *Arch. Transp.* **2018**, *46*, 61–70. [\[CrossRef\]](#)
38. Kornaszewski, M. Modelling of exploitation process of the railway traffic control device. *WUT J. Transp. Eng.* **2019**, *124*, 53–63. [\[CrossRef\]](#)
39. Watral, Z.; Michalski, A. Selected Problems of Power Sources for Wireless Sensors Networks. *IEEE Instrum. Meas. Mag.* **2013**, *16*, 37–43. [\[CrossRef\]](#)
40. Suproniuk, M.; Skibko, Z.; Stachno, A. Diagnostics of some parameters of electricity generated in wind farms. *Przegląd Elektrotechniczny* **2019**, *95*, 105–108. [\[CrossRef\]](#)
41. Caban, D.; Walkowiak, T. Dependability analysis of hierarchically composed system-of-systems. In Proceedings of the Thirteenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX, Brunów, Poland, 2–6 July 2018; Springer: Cham, Switzerland, 2019; pp. 113–120. [\[CrossRef\]](#)
42. Duer, S. Assessment of the Operation Process of Wind Power Plant's Equipment with the Use of an Artificial Neural Network. *Energies* **2020**, *13*, 2437. [\[CrossRef\]](#)
43. Klimczak, T.; Paś, J. Selected issues of the reliability and operational assessment of a fire alarm system. *Eksplotacja i Niezawodn.–Maint. Reliab.* **2019**, *21*, 553–561. [\[CrossRef\]](#)
44. Kołowrocki, K.; Soszyńska-Budny, J. *Reliability and Safety of Complex Technical Systems and Processes: Modeling–Identification–Prediction–Optimization*; Springer: London, UK, 2011. [\[CrossRef\]](#)
45. Grabski, F. *Semi-Markov Processes: Applications in System Reliability and Maintenance*; Elsevier: Amsterdam, The Netherlands, 2015.
46. Suproniuk, M.; Paś, J. Analysis of electrical energy consumption in a public utility buildings. *Przegląd Elektrotechniczny* **2019**, *95*, 97–100. [\[CrossRef\]](#)