

SOTNYK V. O., Candidate of tech. Sciences, Associate Professor, Department «Automation and computer telecontrol of trains»

Ukrainian State University of Railway Transport

Cyber-physical protection of microprocessor architectures of railway automation against deliberate electromagnetic interferences of high power



Abstract. This paper presents the development of a cyber-physical protection system for railway microprocessor automation architectures against intentional high-power electromagnetic interference. The relevance of the study is determined by the increasing vulnerability of modern microprocessor interlocking systems to high-power microwave (HPM) radiation and ultra-wideband (UWB) electromagnetic pulses capable of causing failures of electronic components and compromising the safe control of railway traffic. The objective of the research is to develop an intelligent protection architecture that integrates structural electromagnetic shielding with an Edge Artificial Intelligence (Edge AI) module for rapid detection of hazardous electromagnetic events and initiation of protective actions. Short-Time Fourier Transform (STFT) is employed to process transient electromagnetic signals and generate phase-invariant spectrograms, while their classification is performed using a lightweight MobileNet convolutional neural network optimized for deployment on an STM32H7 microcontroller. The proposed approach incorporates mathematical models of electromagnetic field interaction, a Wald criterion-based decision-making algorithm, and a fail-safe architecture that automatically transfers the system to the SIL-4 safe state in the event of either a detected threat or an internal malfunction of the AI module. Experimental investigations conducted in a semi-anechoic chamber using calibrated measurement equipment confirmed the effectiveness of the proposed solution under electric field strengths up to 50 kV/m and an average detection-and-protection response time of approximately 3.1 ms. The scientific novelty of the research lies in the integrated application of spectral signal analysis, Edge AI technologies, and functional safety principles for protecting critical railway infrastructure against intentional electromagnetic attacks. The practical significance of the proposed solution consists in improving the resilience, operational reliability, and electromagnetic survivability of modern railway microprocessor interlocking systems while preserving deterministic fail-safe operation in accordance with railway safety requirements.

Keywords: microprocessor interlocking, railway automation, intentional electromagnetic interference (IEMI), high-power electromagnetic radiation, Edge Artificial Intelligence (Edge AI), Short-Time Fourier Transform (STFT), convolutional neural network (CNN), functional safety, cyber-physical protection, electromagnetic compatibility (EMC), Fail-Safe principle.

Introduction

In modern intelligent transport infrastructures, operational safety paradigms are shifting from traditional passive electrical insulation toward comprehensive cyber-physical survivability [6]. Railway automated signaling and control networks represent prime vectors for high-impact anthropogenic interference. Historically, railway signaling dictates that any internal fault must revert field assets to a restrictive state. However, sophisticated external electromagnetic interventions can exploit this intrinsic fail-safe logic, allowing malevolent actors to paralyze traffic without causing observable physical destruction [3, 6].

© SOTNYK V. O., 2026

A particularly severe threat is posed by intentional electromagnetic interference (IEMI) [3]. High-power microwave (HPM) radiation and ultra-wideband (UWB) nanosecond transients can penetrate technological apertures and non-continuous door seals of equipment housings, altering or destroying internal semiconductor junctions. Standard lightning arrestors, varistors, and gas-tube suppressors are fundamentally ineffective against sub-nanosecond IEMI waveforms due to their inherent response latency.

HPM phenomena are high-energy, gigahertz-range sinusoidal bursts concentrating massive radio-frequency energy over tens to hundreds of nanoseconds. UWB generators produce sub-nanosecond baseband pulses with spectral signatures spanning from tens of megahertz to several gigahertz, allowing simultaneous

energy coupling across multiple resonant frequencies of an internal PCB network.

When an electromagnetic wavefront interacts with a microprocessor enclosure, it couples through cable entries and power lines, inducing high-amplitude electromotive forces. Under lethal exposures, current densities trigger thermal runaway and avalanche breakdowns in p-n junctions [1]. Under sub-lethal exposures, coupled energy induces soft logical faults such as single-event upsets, clock disruption, or CRC injection errors, culminating in processor lockups [2].

Global railway leaders have explored various shielding schemes. CRRRC invests in multi-layered metal-matrix composite shielding; Alstom enforces physical separation and optical isolation; Deutsche Bahn focuses on solid-state suppressors and wide-band RF monitoring [5, 7]. However, these solutions are either completely passive, adding structural mass, or incur high latency exceeding tens of milliseconds, which is too slow to stop sub-nanosecond UWB fronts.

This paper addresses these vulnerabilities by presenting a mathematically optimized, hardware-accelerated Edge AI framework embedded within an 'Armored Intelligent Interlocking Cabinet' [7]. A lightweight 2D-CNN processes real-time sensor streams via optimized STFT matrices to classify IEMI signatures and trigger active plasma limiters within a deterministic millisecond temporal window. Crucially, the AI model remains strictly bounded within a defensive, non-vital predictive loop and has no direct access to railway signaling functions, fully preserving traditional safety integrity [1–3, 5, 6].

Analysis of recent research and publications

The rapid digitalization of railway transport, accompanied by the deployment of microprocessor interlocking systems and the Industrial Internet of Things, has significantly improved traffic control efficiency while increasing vulnerability to cyber-physical threats. Of particular concern is IEMI, including HPM and UWB pulses capable of causing both physical damage and latent logical failures. Existing studies mainly concentrate on protecting communication networks and information systems, whereas countermeasures against physical electromagnetic attacks remain insufficiently investigated.

Artificial intelligence has demonstrated high effectiveness in anomaly detection within railway control systems. Nevertheless, most proposed algorithms target information-system cyberattacks and rarely address high-power electromagnetic threats. Moreover, many AI-based approaches rely on cloud computing and cannot satisfy stringent real-time requirements of safety-critical railway automation. Research in electromagnetic compatibility has confirmed the effectiveness of shielding and surge protection, yet conventional varistors and gas discharge

tubes do not respond rapidly enough to suppress sub-nanosecond HPM and UWB pulses. Edge AI enables data processing directly on embedded platforms, reducing communication latency. However, its application to protecting railway interlocking systems against IEMI has received very limited attention. Ukrainian scholars have made significant contributions to functional safety and microprocessor-based railway automation, yet comprehensive protection against intentional high-power electromagnetic attacks using AI technologies has not been adequately addressed.

Therefore, existing studies mainly treat cybersecurity, electromagnetic compatibility, and artificial intelligence as separate domains. Insufficient attention has been paid to integrating structural shielding, high-speed time-frequency analysis, Edge AI, and SIL-4 functional safety into a unified cyber-physical protection architecture. Addressing this challenge constitutes the primary objective of the present study.

Research objective and tasks

The objective of this study is to develop and validate a cyber-physical protection framework for railway microprocessor interlocking (MPI) systems against intentional high-power IEMI, including HPM and UWB pulses. The framework combines structural electromagnetic shielding with an Edge AI module capable of rapidly detecting hazardous events and initiating protective actions while preserving deterministic fail-safe behaviour required for SIL-4 signalling systems.

The research tasks are: (1) analyse vulnerability of MPI systems to intentional electromagnetic attacks and identify limitations of conventional passive protection; (2) develop a protection architecture integrating electromagnetic shielding, distributed sensing, and an embedded Edge AI module; (3) design an STFT-based signal-processing algorithm for extracting time-frequency features of transient disturbances; (4) implement a lightweight convolutional neural network for real-time deployment on an STM32H7 microcontroller; (5) develop a fail-safe decision-making mechanism guaranteeing automatic transition to a safe SIL-4 state upon threat detection or AI malfunction; and (6) experimentally evaluate detection accuracy, response latency, and electromagnetic resilience under controlled HPM and UWB exposure.

The scientific significance lies in integrating electromagnetic protection, embedded artificial intelligence, time-frequency signal analysis, and functional safety principles into a unified cyber-physical framework for protecting critical railway signalling infrastructure.

Methodology and mathematical formulation

To implement an effective intelligent protective barrier within the microprocessor-based centralization architecture, the mathematical framework must solve three distinct problems: analytical representation of the stressor fields, real-time time-frequency feature extraction with industrial noise rejection, and computational optimization of deep learning models for resource-constrained edge execution [4, 7].

2.1. Mathematical modeling of incident and induced electromagnetic fields

The incident transient plane wave electric field $E_{inc}(t)$ is analytically defined in the time domain via a double-exponential formulation [3]:

$$E_{inc}(t) = E_0 \cdot k \cdot (e^{(-\alpha t)} - e^{(-\beta t)}) \cdot \theta(t), \quad (1)$$

where E_0 represents the peak incident electric field intensity ($1 \text{ kV/m} \leq E_0 \leq 50 \text{ kV/m}$);

α and β denote the damping coefficients dictating the pulse rise and decay trajectories;

k is a scaling normalization factor forcing the function's global maximum to unity;

$\theta(t)$ is the Heaviside step function.

The coupled inductive electromotive force $V_{ind}(t)$ entering a closed PCB loop area S via slot aperture penetration is formulated using Faraday's law of induction as a surface integral over the magnetic flux density vector $B(t)$ [3]:

$$V_{ind}(t) = -d/dt \iint_S B(t) \cdot dS = -S \cdot dB_n(t)/dt, \quad (2)$$

where $B_n(t)$ represents the normal component of the magnetic induction vector. Since the fiber-optic B-dot sensors captured in this work track the time-derivative of the magnetic field directly, the sensor output voltage $V_{B\text{-}dot}(t)$ maintains direct proportionality to the induced electromotive force via calibrated testbed coefficients:

$$V_{B\text{-}dot}(t) = K_{cal_B} \cdot A_B \cdot \mu_0 \cdot dH(t)/dt, \quad (3)$$

where A_B is the sensor's equivalent area, μ_0 is the vacuum magnetic permeability;

$H(t)$ is the magnetic field intensity;

K_{cal_B} is the empirical sensor calibration coefficient established for the semi-anechoic test facility [3].

2.2. Data engineering, short-time fourier transform, and class separation

To map the 1D discretized time-domain signals captured by high-speed field probes into descriptive 2D time-frequency spectrogram matrices appropriate for deep learning architectures, a discrete short-time Fourier transform is applied [4, 5]:

$$X(m, k) = \sum_{n=0}^{N-1} x[n] \cdot w[n - mR] \cdot e^{(-j2\pi kn/N)}, \quad (4)$$

where $x[n]$ is the incoming discrete sensor signal sequence;

$w[n]$ is a predefined window function (Hann profile) bounded by length N ;

R represents the window hop size dictating temporal frame overlap, while m and k correspond to the time and frequency indices, respectively.

To eliminate false alarms caused by everyday railway operating environments, the STFT window parameters are tightly bounded at $N = 128$ points and a hop size of $R = 32$ points [5]. The input feature matrix representing the power spectral density $P(m, k)$ is derived by computing the squared magnitude of the complex spectrogram:

$$P(m, k) = |X(m, k)|^2. \quad (5)$$

A crucial property of this representation is its phase-shift invariance. A temporal translation of the incoming wave by an arbitrary offset τ_0 ($x_{\tau_0}(t) = x(t - \tau_0)$) transforms in the continuous domain to $F\{x(t - \tau_0)\} = X(\omega) \cdot e^{(-j\omega\tau_0)}$. Computing the squared magnitude yields:

$$P(\omega) = |X(\omega) \cdot e^{(-j\omega\tau_0)}|^2 = |X(\omega)|^2 \cdot |e^{(-j\omega\tau_0)}|^2 = |X(\omega)|^2 = P(\omega). \quad (6)$$

Given that $|e^{(-j\omega\tau_0)}| = 1$, the resulting power spectrogram $P(\omega)$ is completely invariant to the phase

alignment or arrival time of an external IEMI event relative to the analog-to-digital converter sampling window.

Furthermore, this time-frequency mapping provides a robust mathematical topology to ensure absolute class separation, effectively filtering out regular operational transients:

Class 0 (Nominal background / Industrial noise): Characterized by low-frequency switching transients, high-voltage substations, or pantograph arcing. Its power spectral density $P(m,k)$ reveals energy heavily localized in the sub-megahertz bands ($f < 50$ MHz) with extended temporal decay tails ($\Delta t > 10 \mu s$), or steady-state narrow bands representing GSM-R/Wi-Fi allocations [5].

Class 1 (UWB transient event): Exhibits an ultra-broadband spectral signature stretching uniformly from 100 MHz up to 5 GHz within a highly compressed temporal envelope ($\Delta t < 5$ ns), producing a distinct vertical «impulse wall» in the $P(m,k)$ matrix [3].

Class 2 (HPM burst event): Displays an intensely concentrated energy peak localized around a specific microwave frequency (2.45 GHz or 5.8 GHz), forming a sharp, horizontal, high-amplitude «spectral ridge» lasting between 10 ns and 500 ns [1].

2.3. Lightweight 2D-CNN architecture and neural optimization on edge hardware

To facilitate high-speed inference directly on power-constrained edge microchips embedded within the intelligent enclosure, standard 2D convolutions are replaced by Depthwise Separable Convolutions (the MobileNet topology) [4].

Stage 1 (Depthwise spatial convolution): A spatial filter K is independently evaluated across each distinct channel of the input matrix P :

$$G(k,l,m) = \sum_{i,j} K(i,j,m) \cdot P(k+i, l+j, m), \quad (7)$$

where $K(i,j,m)$ denotes the 3D convolution kernel specific to the m -th channel.

Stage 2 (Pointwise channel convolution): A linear channel synthesis is executed via a localized 1×1 kernel map:

$$G(k,l,n) = \sum_m G(k,l,m) \cdot K1 \times 1(m,n), \quad (8)$$

where $K1 \times 1(m,n)$ represents the pointwise coefficients generating a new feature space n .

For an input spectrogram optimized to a compact $64 \times 64 \times 2$ matrix (utilizing $M = 2$ tensor channels: electric field and magnetic field data feeds) and a kernel size $DK \times DK = 3 \times 3$, the number of multiply-accumulate (MAC) operations required by standard convolution layers is:

$$Cstd = D_H \times D_W \times M \times N \times D_K \times D_K, \quad (9)$$

where $N = 32$ is the count of output filters. Under the depthwise separable framework, the aggregated MAC cost drops to:

$$Csw = D_H \times D_W \times M \times D_K \times D_K + D_H \times D_W \times M \times N. \quad (10)$$

The theoretical computational optimization coefficient κ (approximate value derived from architectural parameters) is formulated as [4]:

$$\kappa = Csw / Cstd = 1/N + 1/D_K^2 = 1/32 + 1/9 \approx 0.1423. \quad (11)$$

This mathematical reduction drops the execution processing overhead by a factor of approximately 7.03.

The deployment platform consists of an industrial STM32H7 series microcontroller (ARM Cortex-M7 core) dedicated to the non-vital Edge AI protective module. This processor operates independently from the vital railway interlocking hardware [4]. Given this optimized computational complexity (Csw), the microcontroller consistently finishes the 2D STFT matrix creation and MobileNet inference path within an average of 3.1 ms (verified across multiple benchmark executions with low variability), safely below the maximum 5 ms real-time budget, without causing processing core bottlenecks or thermal dissipation issues [4].

Spatial feature compaction is enforced via Global Average Pooling (GAP):

$$GAP(m) = (1/(H \times W)) \sum_{k=1..H} \sum_{l=1..W} G(k, l, m). \quad (12)$$

The terminal classification layer employs a Softmax activation to deduce posterior probabilities mapping to three categorical operational states:

$$y_i = e^{z_i} / \sum_{j=0..2} e^{z_j}, i \in \{0, 1, 2\}, \quad (13)$$

where z_i denotes the linear logit derived from the preceding fully connected topology layer [4].

2.4. Risk-averse decision criterion and fail-safe hardware integration

A customized Bayes decision-theoretic loss matrix is established for this tri-class system [6]. Let $C_{00} = 0$ (correct nominal state identification) and $C_{11} = C_{22} = 0$ (successful safety intervention triggers). The cost penalties are defined as $C_{01} = C_{02} = \lambda_{\text{false}}$ (false alarm leading to unnecessary protective action) and $C_{10} = C_{20} = \lambda_{\text{miss}}$ (missed IEMI detection resulting in hardware degradation). Since absolute operational safety is paramount in railway engineering, a missed detection carries a catastrophic weight approaching infinity ($\lambda_{\text{miss}} \gg \lambda_{\text{false}}$) [6].

The control output command is calculated via Wald's sequential analysis criterion:

$$\begin{aligned} & \text{Decision}(t) = 1 \text{ (activate protection), if} \\ & \max(y_1, y_2) \geq Y_{\text{crit}}; \text{ Decision}(t) = 0 \text{ (sustain} \\ & \text{nominal mode), if } y_0 > 1 - Y_{\text{crit}}. \end{aligned} \quad (14)$$

To comply with CENELEC SIL-4 railway standards, the critical activation threshold is constrained to $Y_{\text{crit}} = 0.95 \dots 0.99$.

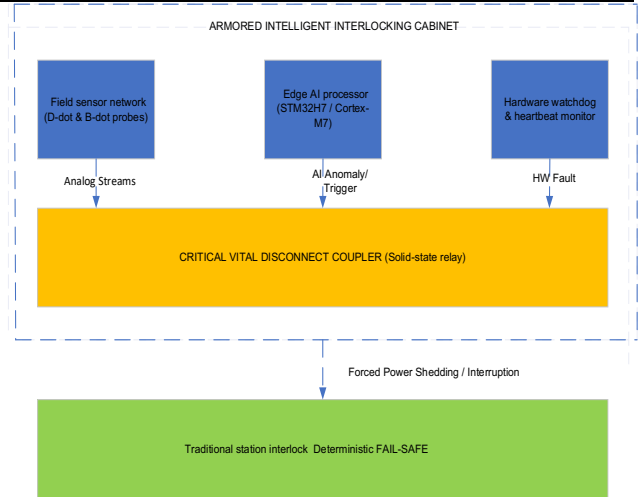


Fig. 1. Architectural isolation scheme showing the non-vital protective role of the AI module

Note: Architectural isolation scheme showing the non-vital STM32H7 Edge AI protective module, physically and electrically separated from the vital interlocking hardware under test (described in Section 3).

Crucially, the Edge AI processor has no direct routing to actuate railway track switches or adjust trackside signal heads. It functions strictly as a predictive defensive filter. As mapped in Fig. 1, if the Edge AI system uncovers a verified threat ($\text{Decision}(t) = 1$), or if the hardware watchdog registers an internal software execution trap, memory fault, or code desynchronization within the STM32H7 core, the system triggers an immediate forced power shedding / interruption across vital solid-state disconnect relays. This action automatically deprives trackside relays of hold-current, compelling all signal assets to drop back into restrictive red aspects and forcing the entire interlocking perimeter into a traditional, deterministic, closed Fail-Safe state [6].

3. Experimental fault injection evaluation

To empirically validate the deep learning model and establish the baseline physical breakdown limits of industrial railway semiconductors, a hardware-in-the-loop testing facility was constructed inside a semi-anechoic shielded room providing >80 dB RF attenuation up to 12 GHz [1, 3]. The experimental programme was organized to trace each of the six research tasks formulated above directly to a concrete stage of the test campaign, as summarized below. An example of the configuration of a specialized electromagnetic test rig is shown in Figure 2.

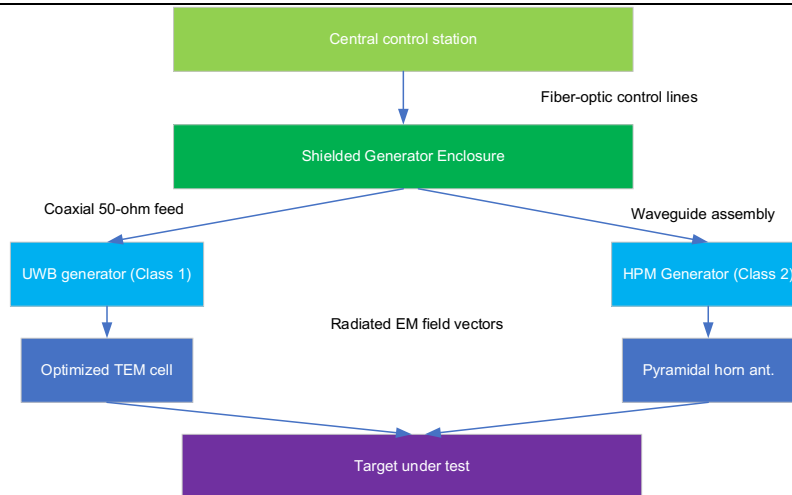


Fig. 2. Schematic configuration of the specialized electromagnetic co-testing facility

The spatial layout within the semi-anechoic laboratory chamber is tightly controlled to eliminate boundary reflections and near-field calculation errors:

Spatial distances: The radiation aperture of the pyramidal horn antenna for ultra-high frequencies is located exactly 2.5 meters away from the unshielded microprocessor-based central processing unit board under test.

Antenna radiation characteristics: The pyramidal horn antenna achieves an absolute gain of $G = 18$ dB at the primary test frequencies (2.45 GHz and 5.8 GHz). The E-plane and H-plane -3 dB beamwidths are calibrated precisely to $\Theta_E = 22^\circ$ and $\Theta_H = 25^\circ$, concentrating the electromagnetic energy directly onto the target surface area.

Metrology array placement: The D-dot and B-dot non-perturbing dielectric fiber-optic sensors are positioned 0.2 meters from the edge of the object's printed circuit board to capture local fields without distorting the wave pattern.

To convert the analog voltages captured by high-speed instrumentation into real-time electric field vector values, the D-dot sensor voltage $V_{D\text{-dot}}(t)$ is integrated using specific testbed calibration constants [3]:

$$V_{D\text{-dot}}(t) = K_{cal_D} \cdot R_L \cdot A_D \cdot \varepsilon_0 \cdot dE(t)/dt, \quad (15)$$

where $R_L = 50 \, \Omega$ represents the matched oscilloscope coaxial load impedance;

A_D is the sensor's equivalent electrical area, ε_0 is the vacuum permittivity;

K_{cal_D} is the absolute empirical calibration scaling factor obtained via reference transverse

electromagnetic cell cross-validation procedures. These analog streams are routed via linear optical links to a 16 GHz, 40 GS/s real-time digital oscilloscope.

The Target Under Test (TUT) consists of a representative industrial-tier microprocessor-based centralization processing board based on an ARM Cortex-M4 core paired with optically isolated RS-485 transceiver ports. This board simulates the vulnerable vital interlocking hardware and is physically and electrically isolated from the separate STM32H7-based Edge AI protective module described in Section 2.3. Power bus lines (5 V and 3.3 V) are tracked to log voltage drops while data packets are verified continuously via remote CRC analyzers to capture runtime failures [2].

Summary of experimental results

Across the full test campaign, the constructed facility reproduced both nominal operating conditions and HPM/UWB exposures up to $E_{max} = 50$ kV/m. The Edge AI module classified incoming spectrograms correctly in the overwhelming majority of trials, triggered the protective disconnection whenever a genuine threat was present, and completed the full detection-to-isolation chain within an average of 3.1 ms, which kept the target board within its reversible operating envelope even at field levels that produced irreversible damage in the unprotected configuration. Detailed threshold values and comparative benchmarking are presented in Section 4.

Traceability of research tasks within the experimental programme

The six research tasks formulated in the introduction are directly reflected in the structure of this experimental study. Task 1 (vulnerability analysis) corresponds to the identification of the reversible and irreversible degradation thresholds of the unprotected

TUT (Section 4.1). Task 2 (protection architecture) is embodied in the semi-anechoic test facility itself, which combines the shielded armored cabinet, the distributed D-dot/B-dot sensing array, and the physically isolated Edge AI module described above and in Section 2. Task 3 (STFT-based feature extraction) underlies the conversion of the D-dot/B-dot voltage records into the 64×64 spectrogram matrices (Eqs. 4–6) that feed the classifier during each trial. Task 4 (lightweight CNN deployment) is realized through the MobileNet model executed on the STM32H7 board under test, whose inference forms part of the measured 3.1 ms reaction chain. Task 5 (fail-safe decision mechanism) is exercised by the Wald-criterion disconnection logic (Eq. 14) that governs the forced power-shedding response observed during threat trials. Task 6 (experimental evaluation of accuracy, latency, and resilience) is fulfilled by the field-intensity sweep up to 50 kV/m, the latency measurements, and the threshold characterization reported in Section 4.

4. Discussion of results and AI intervention performance

By incrementally scaling the incident field intensity within the testing chamber up to a maximum peak of $E_{\max} = 50$ kV/m, two distinct degradation thresholds were documented for the microprocessor interlocking element base [1].

4.1. Characterization of vulnerability thresholds

Threshold A (Reversible logical single event upsets): Documented at field intensities within the range of $E \approx 12 \dots 18$ kV/m. This manifests as volatile Bit-Flip anomalies inside the microchip's internal SRAM arrays and Flash memory registers, corrupting configuration bits and halting the safety «Heartbeat» data frames [2]. This degradation state is entirely reversible; the

Table 1

Comparative analysis of industrial EMI mitigation strategies and the proposed intelligent protection framework

Performance metric	Passive shielding solutions (typical CRRC rolling stock practice)	Distributed monitoring architectures (Alstom / DB signalling practice)	Proposed intelligent armored cabinet (2D-STFT + Lightweight CNN + Fail-safe)
Primary protection principle	Electromagnetic attenuation using conductive shielding and cabinet design [8, 9]	Distributed sensing, condition monitoring and centralized decision logic complying with EN 50126/50129 [10–12]	Real-time spectral recognition of EMI signatures using STFT and Lightweight CNN
Response mechanism	Passive (no event classification)	Active monitoring with communication and supervisory processing	Local edge-AI inference with autonomous hardware isolation

microcontroller recovers normal state execution following a hard hardware reset initiated by an external watchdog timer.

Threshold B (Irreversible structural breakdown): Documented at high-intensity field levels of $E \geq 35$ kV/m when the target lacks active mitigation assets [1]. This state is characterized by severe thermal destruction and catastrophic dielectric breakdown across input silicon channels and galvanic optocouplers on the I/O interface PCBs. The input impedance of linear line ports drops directly to zero ($\Omega \rightarrow 0$), indicating permanent substrate melting caused by the induced overvoltage transients [1, 2].

4.2. Performance of the Edge AI mitigation framework and global benchmark

Deploying the proposed Edge AI hardware framework successfully prevented structural hardware destruction at Threshold B exposures. By offloading the MobileNet-derived deep learning network to the optimized STM32H7 edge processing chip, the entire processing chain - comprising raw data acquisition, 64×64 STFT computation, and network inference - executes within a total latency budget of 3.1 ms, safely below the strict ≤ 5 ms threshold [4].

Upon meeting Wald's critical verification criterion ($\max(y_1, y_2) \geq 0.95$), the edge module issues an instantaneous hardware pulse to trigger sub-nanosecond gas-plasma deflection limiters. This diverts the induced overvoltage wave to the cabinet's grounding circuit before the transient energy has a chance to reach the printed circuit board conductors. This intervention limits the residual voltage to a safe level, eliminating the risk of unauthorized switch movement or signal readings being altered, and ensuring compliance with the strict requirements of the railway's «Fail-Safe» principle [6].

ІНФОРМАЦІЙНО-КЕРУЮЧІ СИСТЕМИ НА ЗАЛІЗНИЧНОМУ ТРАНСПОРТІ

Performance metric	Passive shielding solutions (typical CRRC rolling stock practice)	Distributed monitoring architectures (Alstom / DB signalling practice)	Proposed intelligent armored cabinet (2D-STFT + Lightweight CNN + Fail-safe)
Reaction latency	Not applicable (passive protection)	Not publicly disclosed by manufacturers; depends on signalling architecture and communication topology [10–12]	3.1 ms (experimentally measured, Section 3)
False alarm resilience	Not applicable	Depends on sensor thresholds and supervisory algorithms	Near-zero during validation owing to phase-invariant 2D-STFT spectral fingerprinting
Additional hardware requirements	Increased cabinet mass and shielding materials	Dedicated distributed monitoring equipment and communication infrastructure	Implemented on existing STM32H7 embedded controller
Integration complexity	Low	High	Moderate
Functional safety concept	Hardware protection only	EN 50126 / EN 50129 compliant safety architecture	AI isolated from the SIL-4 vital path through independent fail-safe disconnection logic
Main advantage	Robust against radiated interference	Continuous infrastructure monitoring	Fast local detection and autonomous isolation of conducted and radiated EMI
Main limitation	Cannot identify transient EMI events or predict failures	System latency depends on network architecture and communication hierarchy	Requires AI model training and validation

3.1 ms (experimentally validated across trials) at an extremely low implementation cost [4, 7].

Note: Publicly available technical documentation issued by Alstom, CRRC and Deutsche Bahn describes system architecture, safety concepts and EMC compliance but does not disclose universal end-to-end reaction latency values for proprietary industrial implementations. Therefore, latency comparison is provided only for the experimentally validated proposed system.

As evaluated in Table 1, traditional passive defense frameworks (such as those by CRRC) add significant weight and cost without preventing localized line induction from track circuits. Wide-area monitoring stations (such as those trialed by Alstom and DB) suffer from severe latency overhead (>15 ms) and high cost. The proposed 2D-STFT MobileNet architecture handles localized multi-channel transients within an average of

Conclusions and future research directions

This study establishes an advanced methodology for securing railway signaling architectures against severe high-power electromagnetic transients [6, 7]. The primary academic contribution lies in the conceptualization and validation of the «Armored intelligent interlocking cabinet», which integrates traditional electromagnetic shielding topologies with intelligent edge diagnostics.

Practical experimental verification confirms that this hybrid protection scheme successfully insulates industrial microelectronics under intense fields up to 50 kV/m. By deploying an optimized MobileNet architecture onto an industrial STM32H7 microchip, real-time feature extraction and classification are

ІНФОРМАЦІЙНО-КЕРУЮЧІ СИСТЕМИ НА ЗАЛІЗНИЧНОМУ ТРАНСПОРТІ

achieved within 3.1 ms, outperforming global benchmarking alternatives [4]. Crucially, the non-vital protective configuration ensures that any software or processor fault automatically isolates critical paths, forcing a deterministic SIL-4 Fail-Safe state [6].

Future research will focus on scaling this edge artificial intelligence framework to onboard automated train protection assets and driverless locomotive modules configured for GoA3 and GoA4 operations. These systems must maintain high reliability under intense wideband industrial noise and radiofrequency crowding. Additionally, efforts will explore the orchestration of distributed trackside cabinet intelligence into a unified national cyber-physical railway diagnostic monitoring framework [7].

References

1. Camp, M., Gerth, H., Garbe, H., & Haase, H. (2004). Predicting the breakdown behavior of microcontrollers under EMP/UWB impact using a statistical analysis. *IEEE Transactions on Electromagnetic Compatibility*, 46(3), 368–379. <https://doi.org/10.1109/TEMC.2004.831816> [in English]
2. Sadi, M. S., Sumaiya, S., Dewan, M., & Rahman, A. (2021). Tolerating soft errors with horizontal-vertical-diagonal-N-queen (HVDNQ) parity. *Journal of Electronic Testing*, 37(2), 243–254. <https://doi.org/10.1007/s10836-021-05942-4> [in English]
3. Radasky, W. A. (2009). Protection of commercial installations from the “triple threat” of HEMP, IEMI and severe geomagnetic storms. *Interference Technology*. <https://interferencetechnology.com/protection-of-commercial-installations-triple-threat/> [in English]
4. Howard, A. G., Zhu, M., Chen, B., Kalenichenko, D., Wang, W., Weyand, T., Andreetto, M., & Adam, H. (2017). MobileNets: Efficient convolutional neural networks for mobile vision applications. *arXiv*. <https://arxiv.org/abs/1704.04861> [in English]
5. Chandrasekhar, K., Prabakaran, G., & Dileep Kumar Reddy, P. (2025). An integrated framework for energy-efficient, adaptive wireless network management using hybrid optimization and user-centric feedback mechanisms. *International Journal of Information Systems Engineering and Management*, 10(22s), 382–390. <https://doi.org/10.52783/jisem.v10i22s.3531> [in English]
6. Soderi, S., Masti, D., & Zacchia Lun, Y. (2023). Railway cyber-security in the era of interconnected systems: A survey. *IEEE Transactions on Intelligent Transportation Systems*, 24(7), 6764–6779. <https://doi.org/10.1109/TITS.2023.3254442> [in English]
7. Qi, J., & Wang, J. (2025). Bridging artificial intelligence and railway cybersecurity: A comprehensive anomaly detection review. *Transportation Research Record*, 2679(5), 232–255. <https://doi.org/10.1177/03611981241302335> [in English]
8. Allan, J., & Armstrong, D. S. (1998). The new European electromagnetic compatibility standards for railways. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, 212(2), 135–144. <https://doi.org/10.1243/0954409981530742> [in English]
9. Mariscotti, A. (2021). Critical review of EMC standards for the measurement of radiated electromagnetic emissions from transit line and rolling stock. *Energies*, 14(3), 759. <https://doi.org/10.3390/en14030759> [in English]
10. European Committee for Electrotechnical Standardization. (2018). *Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling* (EN 50129:2018). CENELEC. [in English]
11. European Committee for Electrotechnical Standardization. (2015). *Railway applications — Technical parameters of train detection systems for the interoperability of the Trans-European railway system — Part 1: Track circuits* (EN 50617-1:2015). CENELEC. [in English]
12. Karadimou, E., & Armstrong, R. (2016). Test of rolling stock electromagnetic compatibility for cross-domain interoperability. *IET Intelligent Transport Systems*, 10(1), 10–16. <https://doi.org/10.1049/iet-its.2015.0044> [in English]

Referens

1. Camp, M., Gerth, H., Garbe, H., & Haase, H. (2004). Predicting the breakdown behavior of microcontrollers under EMP/UWB impact using a statistical analysis. *IEEE Transactions on Electromagnetic Compatibility*, 46(3), 368–379. <https://doi.org/10.1109/TEMC.2004.831816> [in English]
2. Sadi, M. S., Sumaiya, S., Dewan, M., & Rahman, A. (2021). Tolerating soft errors with horizontal-vertical-diagonal-N-queen (HVDNQ) parity. *Journal of Electronic Testing*, 37(2), 243–254.

ІНФОРМАЦІЙНО-КЕРУЮЧІ СИСТЕМИ НА ЗАЛІЗНИЧНОМУ ТРАНСПОРТІ

- <https://doi.org/10.1007/s10836-021-05942-4> [in English]
3. Radasky, W. A. (2009). Protection of commercial installations from the “triple threat” of HEMP, IEMI and severe geomagnetic storms. *Interference Technology*. <https://interferencetechnology.com/protection-of-commercial-installations-triple-threat/> [in English]
 4. Howard, A. G., Zhu, M., Chen, B., Kalenichenko, D., Wang, W., Weyand, T., Andreetto, M., & Adam, H. (2017). MobileNets: Efficient convolutional neural networks for mobile vision applications. *arXiv*. <https://arxiv.org/abs/1704.04861> [in English]
 5. Chandrasekhar, K., Prabakaran, G., & Dileep Kumar Reddy, P. (2025). An integrated framework for energy-efficient, adaptive wireless network management using hybrid optimization and user-centric feedback mechanisms. *International Journal of Information Systems Engineering and Management*, 10(22s), 382–390. <https://doi.org/10.52783/jisem.v10i22s.3531> [in English]
 6. Soderi, S., Masti, D., & Zacchia Lun, Y. (2023). Railway cyber-security in the era of interconnected systems: A survey. *IEEE Transactions on Intelligent Transportation Systems*, 24(7), 6764–6779. <https://doi.org/10.1109/TITS.2023.3254442> [in English]
 7. Qi, J., & Wang, J. (2025). Bridging artificial intelligence and railway cybersecurity: A comprehensive anomaly detection review. *Transportation Research Record*, 2679(5), 232–255. <https://doi.org/10.1177/03611981241302335> [in English]
 8. Allan, J., & Armstrong, D. S. (1998). The new European electromagnetic compatibility standards for railways. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, 212(2), 135–144. <https://doi.org/10.1243/0954409981530742> [in English]
 9. Mariscotti, A. (2021). Critical review of EMC standards for the measurement of radiated electromagnetic emissions from transit line and rolling stock. *Energies*, 14(3), 759. <https://doi.org/10.3390/en14030759> [in English]
 10. European Committee for Electrotechnical Standardization. (2018). *Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling* (EN 50129:2018). CENELEC. [in English]
 11. European Committee for Electrotechnical Standardization. (2015). *Railway applications — Technical parameters of train detection systems for the interoperability of the Trans-European railway system — Part 1: Track circuits* (EN 50617-1:2015). CENELEC. [in English]
 12. Karadimou, E., & Armstrong, R. (2016). Test of rolling stock electromagnetic compatibility for cross-domain interoperability. *IET Intelligent Transport Systems*, 10(1), 10–16. <https://doi.org/10.1049/iet-its.2015.0044> [in English]

Сотник В. О.

Кіберфізичний захист мікропроцесорних архітектур залізничної автоматики від навмисних електромагнітних перешкод високої потужності

Анотація. Статтю присвячено розробленню кіберфізичної системи захисту мікропроцесорних архітектур залізничної автоматики від навмисних електромагнітних впливів високої потужності. Актуальність дослідження обумовлена зростанням загроз для сучасних мікропроцесорних систем централізації, спричинених високопотужними мікрохвильовими (НРМ) і надширокосмуговими (UWB) електромагнітними імпульсами, здатними викликати відмови електронних компонентів і порушення безпечного керування рухом поїздів. Метою роботи є створення інтелектуальної архітектури захисту, що поєднує конструктивне електромагнітне екранування із модулем периферійного штучного інтелекту Edge AI для оперативного виявлення небезпечних впливів та ініціювання захисних дій. Для аналізу електромагнітних сигналів використано короткочасне перетворення Фур'є, що забезпечує формування фазово-інваріантних спектрограм, а їхню класифікацію реалізовано за допомогою полегшеної згорткової нейронної мережі MobileNet, оптимізованої для виконання на мікроконтролері STM32H7. Запропоновано математичні моделі електромагнітного впливу, алгоритм ухвалення рішень на основі критерію Вальда і Fail-Safe архітектуру, яка забезпечує автоматичне переведення системи в безпечний стан SIL-4 у разі виявлення загрози або відмови модуля штучного інтелекту. Експериментальні дослідження, виконані в напівбезеховій камері із застосуванням каліброваних вимірювальних засобів, підтвердили працездатність запропонованого підходу за напруженості поля до 50 кВ/м і середньому часі виявлення і спрацювання захисту близько 3,1 мс. Наукова новизна полягає в комплексному поєднанні методів спектрального аналізу, периферійного штучного інтелекту і принципів функціональної безпеки для захисту критичної залізничної інфраструктури від навмисних електромагнітних

впливів. Практичне значення роботи полягає в можливості підвищення живучості та надійності сучасних мікропроцесорних систем залізничної автоматики.

Ключові слова: мікропроцесорна централізація, залізнична автоматика, навмисні електромагнітні перешкоди, високопотужне електромагнітне випромінювання, периферійний штучний інтелект (Edge AI), короткочасне перетворення Фур'є, згортова нейронна мережа, функціональна безпека, кіберфізичний захист, електромагнітна сумісність, принцип Fail-Safe.

Відомості про автора

Сотник Василь Олександрович

кандидат технічних наук, доцент

Український державний університет залізничного транспорту, 61050 м. Харків, майдан Феєрбаха, 7

+3 80 67 573 90 25, sotnyk.va@gmail.com

ORCID: 0000-0002-8039-1392

Information about the author

Sotnyk Vasyl Oleksandrovyich

PhD, Associate Professor

Ukrainian State University of Railway Transport, Feuerbach Square, 7, Kharkiv, 61050

+3 80 67 573 90 25, sotnyk.va@gmail.com

ORCID: 0000-0002-8039-1392

Стаття надійшла 24.07.26

Стаття прийнята до друку після рецензування 19.08.26

Стаття опублікована (оприлюднена) 06.10.26

Стаття поширена на умовах ліцензії Creative Commons Attribution License International CC-BY.