DOI: 10.2478/sbeef-2025-0016

MITIGATING COMPROMISING ELECTROMAGNETIC EMANATIONS IN TEMPEST-COMPLIANT EQUIPMENT DESIGN: A REVIEW OF STANDARDS, CERTIFICATION, AND ENGINEERING COUNTERMEASURES

Ciprian-Iulian Talîmbă-Mengu[1], Marilena Stănculescu[2], Emil Cazacu[2], Mihai Maricaru[2], Horia Andrei[3]
[1]Doctoral School of Electrical Engineering, POLITEHNICA Bucharest
[2]Electrical Engineering Faculty, POLITEHNICA Bucharest, Romania
[3]University Valahia of Targoviste
talimbaciprian@gmail.com, marilena.stanculescu@upb.ro, emil.cazacu@upb.ro, mihai.maricaru@upb.ro, hr_andrei@yahoo.com

Abstract. ***Compromising electromagnetic emanations (CEME) represent a practical side-channel through which information processed by electronic equipment may be inferred from unintended radiated or conducted emissions. Modern digital systems—characterized by dense interconnections, switching power converters, and high-speed I/O—create a broad spectrum of emission mechanisms that are difficult to predict and control late in the design cycle. This paper provides an engineering review of the TEMPEST threat model, the standards and certification ecosystem used in governmental environments, and countermeasures spanning architecture, layout, shielding, bonding and grounding, and filtering. Emphasis is placed on mapping mitigation strategies to dominant coupling paths through zoning, RED/BLACK separation, and interface hardening. A practical verification workflow is proposed to link early design decisions to test evidence***.

Keywords: TEMPEST, compromising emanations, electromagnetic compatibility, mitigation strategies.

1. INTRODUCTION

Electronic information is rarely confined to its intended interfaces. Any time-varying voltage or current generates electric and magnetic fields, and real interconnections behave as distributed impedances and antennas. Consequently, information-bearing activity can leak outside the physical boundary of a device as radiated emissions or as conducted disturbances on cables, power lines, and shared metallic structures [1].

In classical electromagnetic compatibility (EMC) engineering, the goal is to prevent interference and ensure compliance with emission and immunity limits intended to protect radio services and equipment. In the TEMPEST context, the goal is different: emissions are evaluated as an information channel. The relevant question becomes whether an adversary can reconstruct processed data (text, images, cryptographic keys, or protocol state) from those emissions [2].

Compromising emanations are well documented [3-10]. Early demonstrations showed recovery of video content from RF radiation of display systems, and subsequent work extended the concept to keyboards, printers, and other peripherals [3-7]. With the rise of high-speed serial links, switching regulators, and compact embedded platforms, leakage mechanisms have multiplied while the cost of capable receivers has decreased due to software-defined radio technology.

This paper is an engineering-oriented synthesis intended to support early design decisions for equipment that must meet TEMPEST requirements. It does not reproduce controlled limit values; instead, it consolidates publicly discussable concepts: how leakage arises, what standards families exist, and how countermeasures can be organized so that verification becomes tractable.

2. TEMPEST OVERVIEW AND THREAT MODEL

TEMPEST is not a physical phenomenon but a security discipline that defines technical and procedural controls intended to limit the exploitation of compromising emanations. In this paper, the focus is on electromagnetic compromising emanations (CEME), which represent the physical side-channel exploited by an adversary [11].

In this paper, the focus is electromagnetic leakage, often referred to as compromising electromagnetic emanations. The adversary model is typically passive: the attacker observes emissions with a receiver and suitable antennas or probes, and applies signal processing to recover a representation of sensitive information (the "RED" data).

A useful mental model is an unintentional communication system formed by (i) a source that modulates a carrier, (ii) a coupling path through the environment, and (iii) an unintended receiver.

Switching activity creates wideband spectra; the information is embedded as a structured modulation or correlation. Recoverability depends on bandwidth, SNR, and the availability of side information such as timing of video lines or protocol framing. A system can be noisy from an EMC perspective yet still leak if a coherent component is present and can be isolated with narrowband filtering or synchronous processing [12-15].

TEMPEST requirements are often operationalized through controlled zones. A controlled zone specifies separation distance and/or construction constraints so that emissions at the boundary do not enable exploitation with a defined receiver class. The standoff is not universal: it depends on equipment category, sensitivity of processed information, and site environment (attenuation, reflections, and ambient noise). Zoning is used both for facility planning and to drive product design trade-offs [16-18].

2.1 Measurement perspective

From a measurement standpoint, TEMPEST evaluation differs from typical EMC compliance in three ways [19, 21].

First, the measurement bandwidth and frequency range may be extended to include frequencies where information components appear. Second, detectors and analysis methods are selected based on recoverability, not solely on amplitude. Besides peak and quasi-peak detection, evaluators may use demodulators (AM/FM), time-domain recording, and correlation with known timing.

Third, the measurement configuration is tied to the threat model. Antenna type, polarization, standoff distance, and the presence of representative cables or peripherals can change the result dramatically. For conducted paths, current probes and line-impedance stabilization networks provide repeatable coupling, while for near-field assessment, small E-field and H-field probes can localize sources at board level.

The implication for designers is that pre-compliance should include both spectral scans and time-locked observation. For example, a spur that is barely visible in a wideband scan may become clearly correlated with keystrokes when the receiver bandwidth is narrowed and the time series is aligned to events.

2.2 RED/BLACK separation principles

A foundational TEMPEST concept is the separation of "RED" and "BLACK" domains. RED refers to circuits, conductors, and spaces that carry unencrypted or otherwise sensitive information. BLACK refers to areas where such information is not present, including encrypted domains or public interfaces. The purpose is to prevent direct coupling from RED to BLACK, because BLACK infrastructure (cables, racks, building wiring) often extends beyond the controlled zone and can carry leakage farther than anticipated.

In product design, RED/BLACK separation is implemented as a combination of physical partitioning and controlled transitions [22]. Sensitive processing and its associated internal interconnects should be kept within a defined volume that can be shielded and bonded as a unit. Transitions such as power entry, network links, and maintenance ports become boundary controls with dedicated filtering, shielding termination, and sometimes isolation or encryption. Separation must also be preserved mechanically so routine maintenance does not inadvertently compromise the boundary [23, 23].

A common design error is mixing return paths. If RED and BLACK share uncontrolled chassis bonds or cable-shield connections, common-mode currents can bridge domains even when signal conductors appear separated. Therefore, RED/BLACK allocation should include signal conductors, shields, chassis connections, and power returns.

From an engineering standpoint, TEMPEST can therefore be treated as a special case of electromagnetic compatibility in which the performance metric is information recoverability rather than interference level.

3. STANDARDS AND CERTIFICATION LANDSCAPE

Documents used for TEMPEST programs are typically controlled because they describe limits, test methods, and approved countermeasures for specific threat assumptions. Nevertheless, the ecosystem can be summarized. In NATO contexts, the SDIP-27 series is widely referenced for protection against compromising emanations, while in the United States guidance is associated with the National Security Agency (NSA) and the Committee on National Security Systems (CNSS). Many countries operate national TEMPEST authorities that interpret baselines, accredit facilities, and manage equipment approval lists [24].

Figure 1 summarizes the practical equivalence between protection levels and deployment zones used in military zoning procedures. As the assumed interception distance increases (or as the building attenuation improves), the emission limits become progressively less restrictive from Level A to Level C.

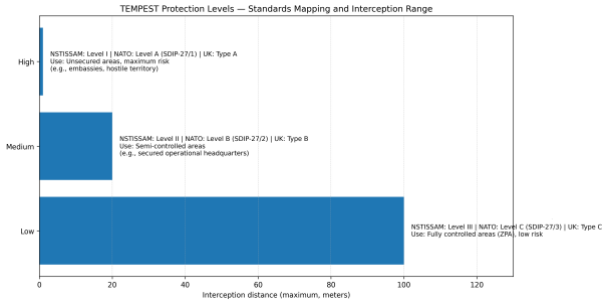

Figure 1. Tempest protection levels

As the assumed interception distance increases (or as the building attenuation improves), the emission limits become progressively less restrictive from Level A to Level C (figure 2).

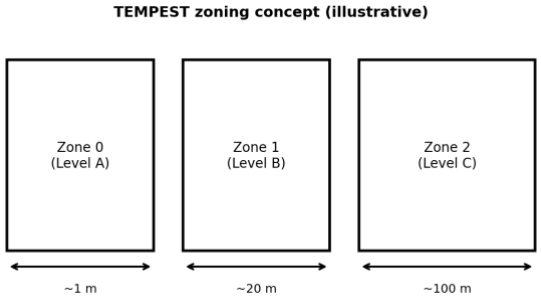

Figure 2. TEMPEST zoning concept (illustrative).

In practice, two document classes appear: (1) policy and management guidance (zoning, separation rules, handling procedures, accreditation processes), and (2) technical standards for equipment evaluation (limit values, test setups, receiver characteristics, and reporting). Equipment is categorized by acceptable exploitation

distance and by sensitivity level of processed information. In procurement, this becomes an explicit requirement: devices must be sourced from an approved product list or evaluated by an authorized laboratory.

Although TEMPEST is distinct from EMC, the disciplines overlap. EMC standards define radiated and conducted emission limits intended to reduce unintentional interference; TEMPEST adds an information-security perspective and often demands lower leakage, different measurement bandwidth, and exploitation-aware analysis. A device may pass civilian EMC limits yet still exhibit exploitable correlation with displayed or processed data.

For engineering teams, the key implication is that certification should not be treated as a final "black box" test. A successful program requires explicit environment and zone assumptions, design rules aligned with typical TEMPEST findings (seams, apertures, cable entries, mixed-domain bonding), and verification items such as emission scans, near-field maps, and interface transfer-function measurements (Table 1). These items allow the design to converge before formal evaluation and provide traceability from requirements to implementation.

Table 1. Conceptual mapping between protection intent and controlled-zone boundary.

Protection intent	Example controlled-zone boundary
High assurance / close-in threat	Within room or adjacent space
Medium assurance / building perimeter	Outside building envelope
Basic assurance / local perimeter	Site boundary or defined standoff

From requirements to test evidence:

A recurring challenge is translating high-level policy into engineering evidence. Requirements are typically expressed as a combination of sensitivity of processed information, intended site zoning, and equipment category (e.g., workstation, peripheral, communication device). Engineering evidence must show that the implemented design—enclosure, interfaces, and internal architecture—reduces leakage sufficiently under the applicable test conditions.

Evidence packages that have proven useful include: interface inventories with RED/BLACK allocation and a description of each boundary control (filter type, location, shielding termination); mechanical drawings showing gasket locations, seam strategy, and cable-entry details; PCB-level artifacts such as return-path analysis, near-field heatmaps, and differential-to-common-mode conversion checks at high-speed connectors; and measurement records with before/after comparisons for mitigations and calibration traces for probes and receivers.

This approach aligns certification with normal engineering iteration. Instead of discovering a problem at the end, teams can isolate root causes early—such as a cable shield terminated with a long pigtail, a filter placed far from the boundary, or a seam that behaves as a slot antenna—and fix them before the design is frozen.

4. SOURCES AND COUPLING MECHANISMS

Digital systems produce wideband spectra because edges contain harmonics well into the GHz range. Even with modest clock frequency, rise and fall times, ringing, and simultaneous switching noise extend the emission bandwidth. Switching-mode power supplies add additional spectral lines and broadband noise through high di/dt loops and non-linear device capacitances [25].

Leakage sources can be grouped into functional signal paths, power distribution networks, and structural paths. These sources couple to the outside world through conducted, capacitive, inductive, and radiated mechanisms (figure 3). In practice, multiple mechanisms are active simultaneously, and the goal is to identify the dominant one for the intended environment [26].

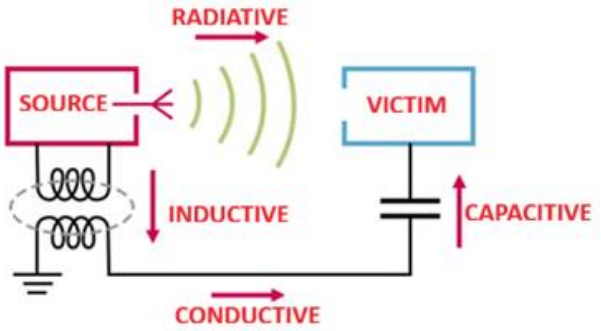

Figure 3. Graphical representation of coupling mechanisms

Common-mode conversion is central. Differential signals are expected to be confined between a pair of conductors, but asymmetry in impedance, return paths, connectors, or routing converts part of the differential energy into common-mode currents. Those currents readily excite cables and chassis, producing efficient radiation. Apertures and seams behave as slot antennas when illuminated by internal fields.

4.1 Field regions and distance scaling

The coupling mechanism often changes with distance. Close to a source (near field), electric and magnetic fields can be analyzed separately, and the dominant component depends on whether the source is voltage- or current-driven. A common boundary between near- and far-field regions is $r \approx \lambda/(2\pi)$, where λ is wavelength. At 100 MHz the boundary is roughly 0.5 m; at 1 GHz it is about 5 cm.

In the reactive near field, field strength can decay faster than $1/r$ (often $1/r^2$ or $1/r^3$). In the far field, radiated field components decay approximately as $1/r$, so reductions in common-mode current translate into meaningful improvements at standoff distances.

This distinction explains why shielding and filtering must be treated together. A shield reduces internal near-field coupling to seams and apertures, while a properly

bonded cable shield reduces far-field radiation by suppressing common-mode currents on long conductors.

4.2 Conducted paths and common impedance

Conducted leakage occurs when information-bearing currents appear on external conductors: power leads, signal lines, or shields. Even when information is present as differential signaling, imperfect balance and return-path discontinuities generate a common-mode component measurable with current probes. Another contributor is common-impedance coupling: circuits share part of the return path (ground, chassis, cable shield), so the voltage drop produced by one circuit is observed by another. At high frequency, the inductive part of the impedance dominates, making bond length and geometry critical.

The design objective is to control return paths so that high-frequency currents close locally, rather than flowing on external conductors. This is the rationale behind bulkhead filters, 360° shield termination at the boundary, and avoiding long pigtail connections.

4.3 Typical exploitation examples

Video displays are a canonical case because pixel timing creates strong periodic structure. A receiver that captures a narrowband component correlated with the video signal can reconstruct the displayed image when synchronized to frame and line timing. Modern flat panels reduce some analog leakage but introduce high-speed serial links (LVDS/eDP) and internal switching supplies that can radiate or conduct correlated components [27].

Keyboards and printers can leak through both radiated and conducted channels. Keystrokes create distinct burst patterns and timing signatures; the data path can couple onto peripheral cables or onto the chassis. For printers, emissions may carry information about raster lines and motor control [28].

Air-gap and covert-channel research demonstrates that ordinary interfaces may be repurposed as transmitters. Modulating USB traffic (figure 4) [29], CPU load, or GPU activity can intentionally create detectable emissions, illustrating that structured modulation can exist even when a device is not designed as a radio.

Figure 4. Unmodified USB device (memory stick) (A) transmits information to a nearby receiver (B) via electromagnetic waves emitted by the bus [29].

4.4 Skin depth and material considerations (illustrative)

For conductive materials, attenuation is related to skin depth:

$$\delta = \sqrt{\frac{2}{\omega\mu\sigma}} \quad (1)$$

where ω is angular frequency, μ is permeability, and σ is conductivity.

A common approximation for the attenuation is:

$$A_{dB} \approx 8.69\frac{t}{\delta} \quad (2)$$

where t – is the thickness.

Table 2 lists indicative skin-depth values for common materials. Actual performance depends on thickness, seams, and mechanical implementation; the table is included to build intuition about frequency scaling.

Table 2. Illustrative skin depth values (steel assumes high relative permeability).

Material	Frequency	Skin depth (approx.)
Copper	100 MHz	6.6 µm
Copper	1 GHz	2.1 µm
Aluminum	100 MHz	8.5 µm
Aluminum	1 GHz	2.7 µm
Steel (low-carbon)	100 MHz	2.1 µm
Steel (low-carbon)	1 GHz	0.6 µm

5. ENGINEERING COUNTERMEASURES

Mitigation is most effective when countermeasures are aligned with the dominant coupling path and applied early. TEMPEST engineering can be viewed as layered defense:

(1) reduce emission at the source,

(2) reduce coupling to external structures, and

(3) reduce receiver recoverability through zoning and facility measures.

Source reduction includes controlling edge rates and minimizing current-loop areas. Series resistors, controlled-impedance routing, and spread-spectrum clocking can reduce discrete spectral components. In power electronics, compact high di/dt loops, shielded inductors, and careful placement of input/output capacitors reduce both radiated and conducted components.

Shielding and enclosure engineering are decisive (figure 5). A continuous conductive enclosure provides attenuation, but real products have seams, fasteners, vents, and cable penetrations. Bonding between panels must be low impedance over frequency; conductive gaskets, suitable surface finishes, and proper fastener spacing maintain continuity. Where ventilation is required, waveguide-below-cutoff structures and honeycomb vents reduce leakage compared to open slots. For low-frequency magnetic fields, high-permeability

materials and increased separation from loop sources are more effective than thin conductive foils.

Figure 5. Shielding solutions for discontinuities in metal enclosures (ventilation slots, inspection windows, etc.).

5.1 Filtering and boundary placement

Cables are the most common leakage vector because they form efficient antennas and provide long conducted paths (figure 6). Filtering is most effective when placed at the boundary between RED and BLACK domains. Bulkhead feedthrough capacitors and filtered connectors reduce parasitic inductance by referencing directly to the enclosure wall. When filtering is placed deep inside the enclosure, the cable segment between wall and filter can still radiate.

Practical filter performance is dominated by parasitics [30, 31]. Component self-resonance, lead inductance, and PCB layout can turn a nominal LC network into a poor attenuator at high frequency.

For TEMPEST-relevant bands, they focus on short and wide reference connections, minimizing loop area around the filter, using multi-stage filtering with separation, and validating with insertion-loss measurements rather than relying on datasheets.

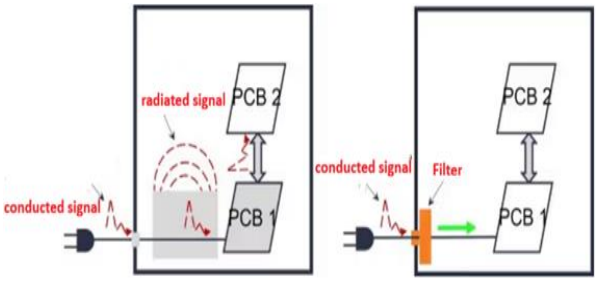

Figure 6. The fundamental difference between an unfiltered system (left) and a filtered system (right) [40]

For TEMPEST-oriented projects, passive vs. active filtering can be compared in terms of stability, complexity and potential self-emissions.

Table 3 consolidates the comparative analysis from the source report.

Table 3. Comparative analysis of passive vs. active filters

Criterion	Passive filters	Active filters
Generated EMI	Inexistent	Possible high
Reliability	high	Variable
Stability in time	Excellent	Depending on medium/functioning conditions
TEMPEST certifiable	Da	Practically never
Applications in TEMPEST	Standard	Avoided completely

5.2 Cable shields and terminations

A frequent root cause of poor performance is improper cable-shield termination. A 360° termination at the connector (conductive backshell or clamp) provides a low-impedance path for high-frequency shield currents and reduces common-mode radiation. A pigtail connection adds inductance that is negligible at DC but large at tens or hundreds of MHz, forcing shield currents to flow on the cable and radiate.

Shield terminations should be paired with a clear bonding strategy and with strain relief that preserves contact pressure over time. In environments where corrosion or vibration is expected, material pairing and surface treatment become part of the security design, not only a mechanical concern.

Figure 7 presents a comparative analysis of three different cable shielding solutions.

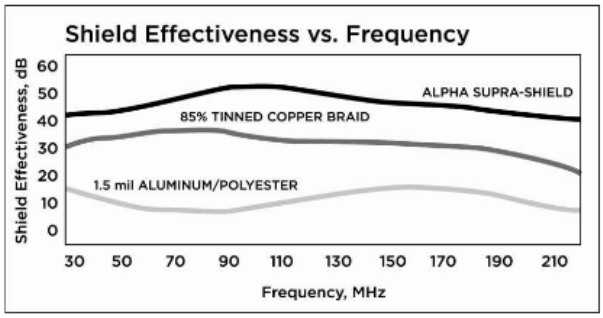

Figure 7. Frequency-domain analysis of various shielding solutions [32].

In a shielded system, shielding effectiveness is determined by the weakest-shielded component.

A high-quality cable is compromised by a low-quality connector. Similarly, an excellent connector cannot compensate for the shortcomings of a poor cable.

Table 4 presents the countermeasures mapped to dominant coupling paths.

Table 4. Countermeasures mapped to dominant coupling paths.

Coupling path	Typical symptom	Primary mitigations
Conducted (cables)	High common-mode current; correlated lines	Bulkhead filtering, feedthrough capacitors, CM chokes, 360° shield terminations
Capacitive (E-field)	Hotspots near fast nodes; trace coupling	Guard traces, spacing, shielding, controlled edge rates

Inductive (H-field)	Loop-to-loop coupling	Loop minimization, return-path control, magnetic shielding, separation
Radiated (far-field)	Aperture radiation; cable as antenna	Enclosure continuity, gasketed seams, controlled apertures, cable management

5.3 Verification and pre-compliance workflow

Formal TEMPEST evaluation is resource-intensive, so projects benefit from a repeatable pre-compliance workflow that screens major leakage paths and documents design rationale. A practical workflow combines requirement interpretation, design rules, and measurements that approximate the official setup.

Pre-compliance typically includes near-field scans over PCBs and around cable entries, bulk-current probe scans on cables to identify common-mode peaks, and radiated scans in bands where structured components appear. These measurements are most valuable when performed comparatively—before and after a mitigation—so that root causes can be isolated and improvements quantified.

Shielding effectiveness (SE) is commonly expressed as:

$$SE = 20 \cdot \log_{10}\left(\frac{E_{protected}}{E_{unprotejat}}\right)[\text{dB}]. \quad (3)$$

In high-security electromagnetic enclosures, shielding effectiveness values on the order of 60–80 dB or higher are commonly targeted, depending on frequency and threat model.

Figure 8 presents a TEMPEST-oriented workflow from requirements to evidence.

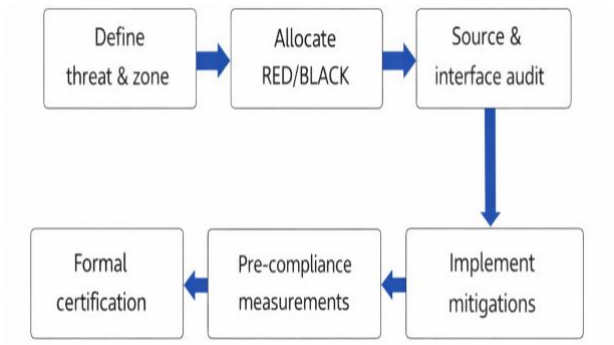

Figure 8. TEMPEST-oriented workflow from requirements to evidence.

Workflow description

- Define threat model and controlled-zone assumptions (receiver class, standoff, and site attenuation).
- Allocate RED/BLACK domains and list all cross-domain interfaces (power, I/O, maintenance, structural bonds).
- Perform a source audit (clocks, converters, high-speed links) and identify likely hotspots (connectors, seams, long traces).
- Implement mitigations with testability (bulkhead filter locations, removable panels with reliable gaskets, documented bonds).
- Run pre-compliance scans (near-field, bulk current, radiated) and keep before/after records for each change.
- Assemble an evidence package linking mitigations, drawings, and measurements to requirements.

5.4 Facility and operational mitigations

Even well-designed equipment can be undermined by an unsuitable installation. Facility measures complement product measures and often determine whether the controlled-zone boundary is realistic. Common controls include dedicated equipment rooms with controlled access, separation of RED cabling from building infrastructure, and use of shielded conduits or raceways for cables that must exit the controlled area.

Power and grounding deserve special attention. Shared power networks can provide a conducted path that bypasses distance. Depending on the threat model, installations may use dedicated power transformers, power-line filters at room entry, and carefully managed bonding networks to avoid long shared-impedance paths. The intent is not only to reduce emissions, but also to prevent the building wiring from acting as a large antenna.

Operational procedures preserve the integrity of technical controls. Examples include controlling maintenance ports, prohibiting unapproved peripherals, and requiring that cable assemblies, shield terminations, and gaskets be inspected and replaced on a defined schedule. When equipment is moved between rooms with different zone assumptions, re-accreditation may be required because standoff distance, wall attenuation, and cable routing all affect recoverability.

Table 5. Example pre-compliance checklist to reduce common findings.

Area	Checklist items (examples)
Enclosure	Seams gasketed; fastener spacing consistent; vents waveguide-like; no uncontrolled apertures.
Cables & connectors	Shield bonded 360°; filter at boundary; controlled routing; avoid pigtails.
PCB layout	Minimize loop areas; continuous return plane; controlled impedance; avoid stubs at high speed.
Power	Converter loops compact; input/output filtering; CM choke where needed; shielded magnetics.
Bonding	Low-impedance bonds; avoid long straps; intentional DC bonds; corrosion control for long term.

6. CONCLUSIONS

Compromising electromagnetic emanations remain a relevant security risk for systems that process sensitive information, especially where an adversary can deploy capable receivers and antennas. Unlike conventional EMC, TEMPEST engineering targets the recoverability of information, which depends on both amplitude and

structure. Practical mitigation therefore requires a coupling-path mindset: identify where information is modulated, determine how it can leave the device, and apply layered controls at the source, at domain boundaries, and in the facility environment.

Across standards families, common themes emerge: controlled-zone assumptions, rigorous test setups, and an emphasis on cable interfaces and enclosure integrity. For designers, the central lesson is that TEMPEST compliance is achieved through architecture and disciplined implementation rather than through a single component. Early allocation of RED/BLACK boundaries, careful management of common-mode currents, and verification using near-field mapping and interface measurements improve the likelihood of passing formal evaluation.

Future work will focus on correlating repeatable pre-compliance measurements with controlled-zone performance, enabling faster iteration during product development while maintaining traceability to certification requirements.

7. REFERENCES

[1] V. Antic, D. Protic, M. Stankovic, R. Prodanovic, M. Manic, G. Ostojic, S. Stankovski și D. Kucevic, *Protecting Data at Risk of Unintentional Electromagnetic Emanation: TEMPEST Profiling*, Applied Sciences, vol. 14, nr. 11, art. 4830, 2024.

[2] G. Hortopan, *Principii și tehnici de compatibilitate electromagnetică*, Editura Tehnică, București, 1998

[3] T. Kitazawa, S. Matsumoto and Y. Hayashi, *"Pixel Level Character Reconstruction by Background Profiling Against TMDS Emanations"* 2025 IEEE International Symposium on Electromagnetic Compatibility, Signal & Power Integrity (EMC+SIPI), Raleigh, NC, USA, 2025, pp. 60-65.

[4] Y. Zhang, F. Du, X. Chi and Z. Lv, "USB Catcher: Detection of Controlled Emissions via Conducted Compromising Emanations," *2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Sanya, China, 2024, pp. 1296-1303.

[5] J. Guo, Y. Xu, M. Zhang, W. Huang and H. Guo, *"Behavior Recognition and Anomaly Detection Utilizing Memory Electromagnetic Emanation"* MILCOM 2024 - 2024 IEEE Military Communications Conference (MILCOM), Washington, DC, USA, 2024, pp. 530-535.

[6] A. -M. Vizitiu, L. Dobrescu, C. Molder, B. Sebacher, B. C. Trip and V. F. Butnariu, *"Detection of TEMPEST audio compromising signal using artificial intelligence"* 2024 15th International Conference on Communications (COMM), Bucharest, Romania, 2024, pp. 1-6

[7] Y. Zhang, H. Li, Q. Ye, J. Hu, Y. Han and Z. Lv, *"A Conducted Compromising Emanations Method on High-Speed USB Devices via USB Hubs,"* 2024 IEEE Symposium on Computers and Communications (ISCC), Paris, France, 2024, pp. 1-8

[8] B. Liu, Y. Xu, W. Huang and S. Guo, *"Detecting USB Storage Device Behaviors by Exploiting Electromagnetic Emanations,"* ICC 2022 - IEEE International Conference on Communications, Seoul, Korea, Republic of, 2022, pp. 4980-4985

[9] E. Lee, D. -H. Choi, T. Nam and J. -G. Yook, *"A Quantitative Analysis of Compromising Emanation From TMDS Interface and Possibility of Sensitive Information Leakage,"* in IEEE Access, vol. 10, pp. 73997-74011, 2022

[10] W. Huang, Z. Feng, Y. Xu and N. Zhang, *"A Novel Method for Malicious Implanted Computer Video Cable Detection via Electromagnetic Features,"* 2021 IEEE Wireless Communications and Networking Conference (WCNC), Nanjing, China, 2021, pp. 1-6.

[11] https://csrc.nist.gov/glossary/term/tempest, accessed December 2025

[12] IEC 61000-4-23, "Electromagnetic compatibility (EMC) Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test, Std., 2008

[13] IEEE Standard Method for Measuring the Effectiveness of Electromagnetic Shielding Enclosures, Std. IEEE Std 299–2006.

[14] Electromagnetic Compatibility (EMC)-Part 4-21: Testing and Measurement Techniques-Reverberation Chamber Testmethods, Std. *IEC* 61 000 - 4–21

[15] Mechanical Structures for Electrical and Electronic Equipment-Tests for IEC 60917 and IEC 60297 Series-Part 1: Environmental Requirements, *Test Setups and Safety Aspects, Std. IEC* 61 587–3.

[16] NATO Standard Allied Environmental Conditions and Tests Publication AECTP-500 Edition E Version 1, *"Electromagnetic Environmental Effects Tests and Verification,"* Dec. 2016

[17] Bulut, V. Solak and H. S. Efendioglu, *"A Novel Approach to Measure Shielding Effectiveness in TEMPEST-Protected Buildings,"* 2024 International Symposium on Electromagnetic Compatibility – *EMC Europe*, Brugge, Belgium, 2024, pp. 279-283

[18] *NATO Zoning Procedures, SDIP 28*, NATO Std., 2014.

[19] A. Kohling: TEMPEST - eine Einfuhrung und Ubersicht zu kompromittierenden Aussendungen, einem Teilaspekt der Informationssicherheit [TEMPEST - an introduction and overview on compromising emanations, one aspect of information security]. In H.R. Schmeer (Edit.): Elektromagnetische Vertraglichkeit/EMV'92, Stuttgart, pp. 97-104, VDE-Verlag, Berlin, 1992

[20] L. Jinming, J. Mao J. Zhang, L. Yongmei. *"The Designing of TEMPEST Security Testing Model."* TELKOMNIKA Indonesian Journal of Electrical Engineering 12, No. 2 (2014), pp. 866-871

[21] EMC testing for aerospace and defense, https://www.rohde-chwarz.com/solutions/aerospace-and-defense/land/emc-testing-for-aerospace-and-efense/emc-testing-for-aerospace-and-defense_255762.html, accessed on Nov. 2025

[22] https://www.majr.com/a-quick-guide-to-tempest-levels/, accessed December 2025

[23] https://cryptome.org/tempest-2-95.htm, accessed December 2025.

[24] Tempest NATO SDIP-27 - NATO AMSG - USA NSTISSAM – NATO, Zones https://www.interelectronix.com/tempest.html, accessed on sept 2025.

[25] Paul, Clayton R., Robert C. Scully, Mark A. Steffka *Introduction to electromagnetic compatibility.* John Wiley & Sons, 2022

[26] Henry W. Ott , Electromagnetic Compatibility Engineering, Wiley, 2009, ISBN: 978-0-470-18930-6

[27] M. Popescu, C. Morari, C. Popescu and E. -M. Badula, *"Innovative Method for TEMPEST Detection and Identification of Compromising Emission Generated by The Video Signal from a Laptop,"* 2025 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Chisinau, Moldova, Republic of, 2025, pp. 1-4

[28] H. -J. Choi, H. S. Lee, D. Sim, J. -G. Yook and K. Sim, *"Reconstruction of leaked signal from USB keyboards,"* 2016 URSI Asia-Pacific Radio Science Conference (URSI AP-RASC), Seoul, Korea (South), 2016, pp. 1281-1283

[29] M. Guri, M. Monitz, Y. Elovici, *USBee: Air-Gap Covert-Channel via Electromagnetic Emission from USB*, Ben-Gurion University of the Negev, 2016

[30] Y. Lai, S. Wang, Y. Yang, Q. Huang and Z. Ma, *"Review on Modeling and Emissions from EMI Filters in Power Electronics: Inductors,"* 2023 IEEE Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMC+SIPI), Grand Rapids, MI, USA, 2023, pp. 566-572.

[31] What is an EMI Filter, Spectrum Control, https://www.spectrumcontrol.com/products/emi-protection/what-is-an-emi-filter, accessed on May 2025

[32] *Understanding Shielded Cable – Technical Paper*, Alpha Wire ,https://www.alphawire.com, accessed on June 2025.

[33] Montrose, M. I., *EMC and the Printed Circuit Board*, IEEE Press, 2nd Ed., 2015.