12th INTERNATIONAL SCIENTIFIC CONFERENCE ON DEFENSIVE TECHNOLOGIES
OTEH 2026
Serbia, Tara, 21 - 24 October 2026

PREVENTIVE EM MEASUREMENTS: COST-EFFECTIVE SOLUTION FOR AWARENESS OF EMERGING TEMPEST THREATS

DRAGAN KONDIĆ
Applied Mathematics and Electronics Centre, Belgrade, dragan.kondic@vs.rs

BORKO DJAKOVIĆ
Applied Mathematics and Electronics Centre, Belgrade, borko.djakovic@vs.rs

MILENA GRDOVIĆ
Applied Mathematics and Electronics Centre, Belgrade, milena.grdovic@vs.rs

NENAD STEFANOVIĆ
Applied Mathematics and Electronics Centre, Belgrade, nenad.stefanovic@vs.rs

Abstract: *Emerging TEMPEST threats are gaining relevance due to increasing availablity of open platforms and publicly software that facilitate electromagnetic (EM) side-channel experimentation. Most commercial off-the-shelf and industrial-grade devices, as potential targets, do not address these vulnerabilities, while awareness of associated risks remains limited. Conversely, procurement of TEMPEST resistant devices, structures and facilities often requires heavy budget strains. Preventive EM measurements of protected entities are therefore essential for assesing exposure and identifying vulnerabilities. However, such measurements can be costly and resource-intensive, and unlike electromagnetic compatibility testing, where pre-compliance frameworks exist to reduce risk and cost, TEMPEST evaluation currently lacks formal intermediate assesment stages. As a result, organizations face significant uncertainty and potential expense if measurement processes are not properly structured. This paper proposes a hybrid methodology that integrates engineering-level pre-compliance EMSEC measurements with physical security measures, including shielding effectiveness (SE) assesment and EM security zoning. The approach leverages publicly available ITU-T Recommendations K.81, K.84, and K.87 to provide a systematic, repeatable and extensible framework for early-stage risk assesment and mitigation. By combining measurement-driven evaluation with spatially structured protective measures, the methodology bridges the gap between open-standard practices and classified TEMPEST requirements.*

Keywords: *side-channels, EMSEC, TEMPEST, zoning, shielding, profiling.*

1. INTRODUCTION

In an era where spectrum dominance dictates cross-domain security, mitigating data leakage via compromising electromagnetic emanations (CE) has become a critical priority at the convergence of cyber and physical warfare, Figure 1. Traditionally, exploiting such vulnerabilities required highly specialized equipment and expertise, limiting practical attacks to well-funded state actors or advanced laboratories. However, the threat landscape is rapidly evolving due to the increasing availability of open platforms and publicly accessible software tools that facilitate EM side-channel experimentation [1]. Recent comprehensive research surveys on EM information leakage [2] is followed by an on-line available tool to conduct some tests. Beyond phreaking video signals from monitors, recently published report describes similar leakage from cameras as well, including free tools for signal reconstruction [3]. Other give more general degrees of freedom creating more specific reconstruction templates [4]. Other closed-tool publications report on succsessfull recovering of other classes of emanations such as from touchscreens, smartphones [5], serial cables and broad list of other physical asserts. Furthermore, novel class of available threats is usage of sending informations over unintended emissions from electronic devices with activity of simple unprivileged code [6], showing increased risk that CE carry. However, in order to procure TEMPEST resistant devices, structures and facilities, expose high costs if not structured properly. Finally, to challenge the common assumption that compromising emanations are confined to short-range effects, recent studies on so-called *"screaming channels"* have demonstrated that sensitive information can couple onto RF carriers and propagate over significantly longer distances [7].

In this context, the paper proposes a hybrid EMSEC pre-compliance framework derived from publicly available ITU-T recommendations and extended through analytical propagation and probabilistic compromise models.

The proposed approach combines intrusion-zone-oriented assessment, shielding evaluation, and receiver-oriented measurement interpretation to support systematic early-stage EMSEC evaluation. The objective of proposed framework is not to replace formal TEMPEST evaluation, but to provide a structured engineering methodology for preliminary EMSEC assestment and mitigation planning.

Corresponding author: N. Stefanović;
E-mail: nenad.stefanovic@vs.rs

DOI: 10.5937/OTEH26081K

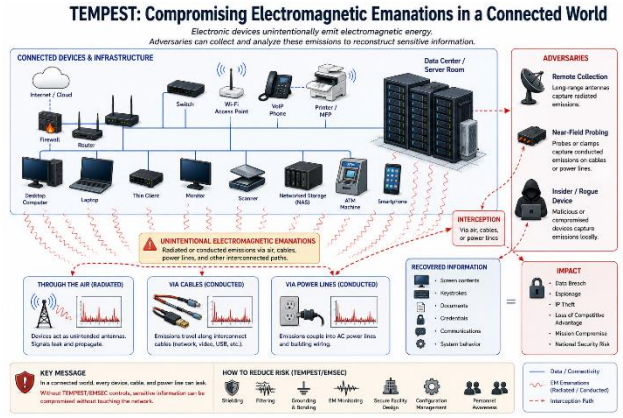


Figure 1. Overall description of CE threats

The paper contributions are:

- Interpretation of ITU-T K.84 through a propagation-oriented EMSEC threat model.
- Introduction of an engineering-level EMSEC pre-compliance workflow inspired by EMC pre-compliance practices.
- Development of a probabilistic compromise model linking emanation level, shielding, propagation distance and receiver capability.
- Extension of intrusion zones from geometric boundaries into probability-based exposure regions.
- Demonstration of measurement-driven mitigation optimization through illustrative examples.

2. EMSEC THREAT MODEL

2.1. Compromising Emanation Threat Landscape

Electromagnetic security assessment defined in ITU-T K.84 is fundamentally based on the relationship between the spatial intrusion threat model and the measurable compromising emanations generated by information processing equipment, Figure 2. Unlike conventional EMC testing, the purpose of EMSEC measurements is not regulatory compliance but evaluation of information reconstruction feasibility at different intrusion zones. The recommendation implicitly defines a spatially dependent threat model where the electromagnetic field strength at the attacker location depends on the original emanation level, equipment countermeasures, building shielding, propagation distance and receiver sensitivity.

Consequently, the measurement methodology must be adapted to the assumed intrusion zone and attacker capabilities.

The measurement methodology is directly linked to the assumed intrusion zone, table 1. Lower intrusion zones correspond to shorter attacker distances and therefore require evaluation of higher received field strengths and wider receiver capabilities.

Conversely, higher intrusion zones are dominated by propagation attenuation and shielding effects, making narrow-band spectral detection more suitable for evaluating residual leakage components.

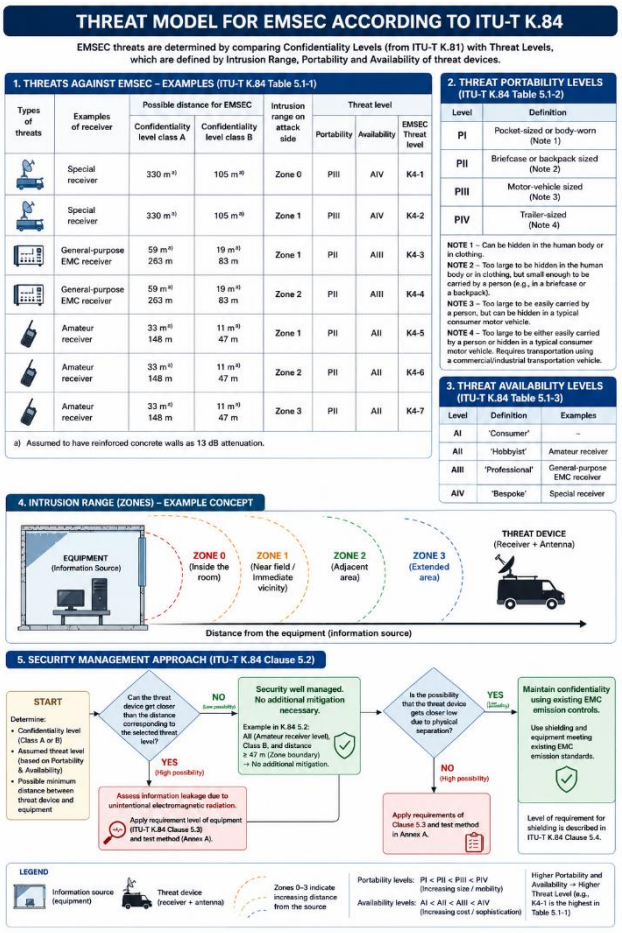


Figure 2. Modeling threats acording to ITU-T K.84

ITU-T K.84 implicitly separates EMSEC evaluation into two complementary dimensions:

1. Spatial threat evaluation through intrusion zones and propagation attenuation;
2. Spectral leakage evaluation through wideband and narrow-band measurement techniques.

Table 1. Intrusion EMSEC zones

Intrusion Zone	Dominant threat	Preferred measurement meth.	Objective
Zone 0	Direct reconstruction	*Wideband*	*Image reconstruction capability*
Zone 1	Adjacent room leakage	*Wideband + Narrowband*	*Reconstruction + spectral analysis*
Zone 2	Boundary leakage	*Narrowband*	*Leakage frequency identification*
Zone 3	Extended perimeter	*Narrowband*	*Residual spectral detectability*

The combination of these approaches forms a practical framework for estimating the feasibility of electromagnetic information compromise under realistic operational conditions.

Recommendation identifies several possible mechanisms for compromising electromagnetic emanation acquisition, including free-space radiated interception using antennas, conductive coupling through metallic structures and

leakage acquisition through power-supply lines.

2.2 Wideband and Narrow-Band EMSEC Measurements

ITU-T K.84 practically introduces two different measurement paradigms, table 2.

Table 2. EMSEC measurement approaches

Method	Purpose	Security interpretation
Wideband	Reconstruction capability	*Can attacker reconstruct information?*
Narrowband	Spectral leakage detection	*Which frequencies carry compromising information?*

The wideband method attempts to emulate the operational conditions of a realistic compromising emanation receiver capable of reconstructing video information. The measurement process approximates the operational capability of advanced EMSEC threat receivers described in higher threat classes. The wideband method preserves the energy distribution of compromising emanations over a broad frequency interval, enabling estimation of reconstructed information quality rather than isolated spectral components.

The narrow-band method focuses on identification of discrete spectral components correlated with assumed information patterns. Frequencies exhibiting significant amplitude differences between static and time-varying patterns are identified as potential compromising emanation carriers. Consequently, the narrow-band method represents a frequency-domain leakage localization technique rather than a direct reconstruction method.

The minimum electromagnetic field level [dBμV/m], necessary for successful information reconstruction is expressed as:

$$E_{min} = V_{min} + SN + A_f \quad (1)$$

where: V_{min} [dBμV] denotes minimum detectable receiver voltage, SN [dB] denotes the signal-to-noise ratio required for reconstruction, and $A_f[dB]$ denotes the antenna factor. This formulation directly links electromagnetic propagation to information reconstruction feasibility. Consequently, successful EMSEC interception requires careful optimization between receiver bandwidth, amplifier gain, noise figure and spectral filtering.

The recommendation categorizes interception receivers into three operational classes: amateur receivers, professional EMC receivers and specialized EMSEC receivers. These categories correspond to progressively improved sensitivity, signal processing capability, bandwidth and reconstruction performance. The interception problem may therefore be interpreted as a competition between propagation attenuation, shielding attenuation and receiver sensitivity enhancement. This interpretation directly motivates the use of probabilistic compromise models, described later in section 4.2.

3. EMSEC PRE-COMPLIANCE FRAMEWORK

3.1 Cost-Effective Measurement-Driven EMSEC Assessment

EMSEC protection mechanisms such as facility shielding, filtered infrastructure, protected zoning, and TEMPEST-certified equipment may introduce substantial financial and operational costs if implemented without prior leakage characterization. Unlike conventional EMC mitigation, where compliance limits are standardized and well understood, EMSEC protection depends strongly on equipment-specific compromising emanation profiles, installation geometry, building materials, cable routing and attacker positioning relative to the protected asset. Consequently, the effectiveness of countermeasures cannot be reliably estimated without measurement-driven assessment.

In practical environments, compromising emanations are rarely uniformly distributed across the spectrum or spatial environment. Certain frequency bands may exhibit significantly elevated leakage levels due to internal clock harmonics, display synchronization frequencies, cable resonances, power conversion stages or unintended antenna structures formed by connected conductors.
Similarly, electromagnetic leakage paths are highly dependent on physical installation conditions. Openings, windows, ventilation structures, cable penetrations, and conductive building elements may create localized reductions in shielding effectiveness (SE), enabling disproportionate propagation toward specific intrusion zones.

As a result, implementation of generalized shielding measures without prior measurements may produce excessive shielding costs, unnecessary infrastructure modifications, overestimation of threat exposure, or insufficient protection against dominant leakage mechanisms.

The measurement methodology defined in ITU-T K.84 therefore serves not only as a security evaluation procedure, but also as an engineering optimization mechanism for determining dominant leakage frequencies, effective propagation directions, critical intrusion zones and required attenuation margins. Wideband measurements enable estimation of practical information reconstruction feasibility, while narrow-band measurements identify dominant spectral leakage components. Their combined application supports prioritization of mitigation measures according to measurable compromise potential rather than purely theoretical assumptions.

3.2 Facility-Oriented Workflow

The proposed analytical propagation framework further extends this concept by enabling preliminary estimation of compromise distance, shielding requirements and intrusion-zone exposure before deployment of expensive TEMPEST-oriented infrastructure modifications.
The conceptual facility-oriented assessment shown in Figure 3 illustrates how EMSEC pre-compliance

evaluation may be integrated into realistic operational environments. Instead of treating compromising emanations as purely device-level phenomena, the proposed approach considers the combined influence of equipment leakage characteristics, building geometry, SE, intrusion-zone proximity and propagation-oriented measurement positioning.

Wideband and narrow-band measurements are strategically positioned according to expected attacker locations and dominant propagation paths. The resulting measurements are then incorporated into the proposed analytical propagation framework to estimate residual compromise probability across the protected facility. This interpretation enables targeted deployment of shielding and filtering countermeasures only where measurements indicate elevated compromise potential, thereby reducing unnecessary infrastructure hardening and minimizing over-engineering costs.

3.3 Proposed Pre-Compliance Methodology

The proposed framework may be interpreted as a staged EMSEC pre-compliance methodology intended to reduce uncertainty prior to expensive TEMPEST-oriented mitigation deployment.

Unlike conventional TEMPEST evaluation procedures, which are typically performed only after infrastructure deployment or during formal certification stages, the proposed methodology introduces intermediate engineering-level assessment phases derived from publicly available ITU-T recommendations.

The workflow consists of five sequential stages:

1. **Initial Threat Profiling**. Identification of critical assets, expected attacker capabilities, operational frequencies, and applicable intrusion zones according to ITU-T K.84.
2. **Preliminary Spectral Leakage Assessment.** Narrow-band measurements are performed to identify dominant compromising frequencies, harmonics, cable resonances, and propagation-sensitive spectral regions.
3. **Reconstruction-Oriented Evaluation.** Wideband measurements are performed for selected high-risk frequencies and operational modes to evaluate practical information reconstruction feasibility.
4. **Spatial Propagation and Intrusion-Zone Analysis.** Measured emanation levels are incorporated into the proposed propagation model to estimate compromise probability across intrusion zones while considering shielding attenuation, building geometry, and receiver sensitivity.
5. **Targeted Mitigation Optimization.** Shielding reinforcement, zoning adaptation, filtering deployment, and equipment hardening are prioritized according to the measured compromise contribution of individual leakage paths.

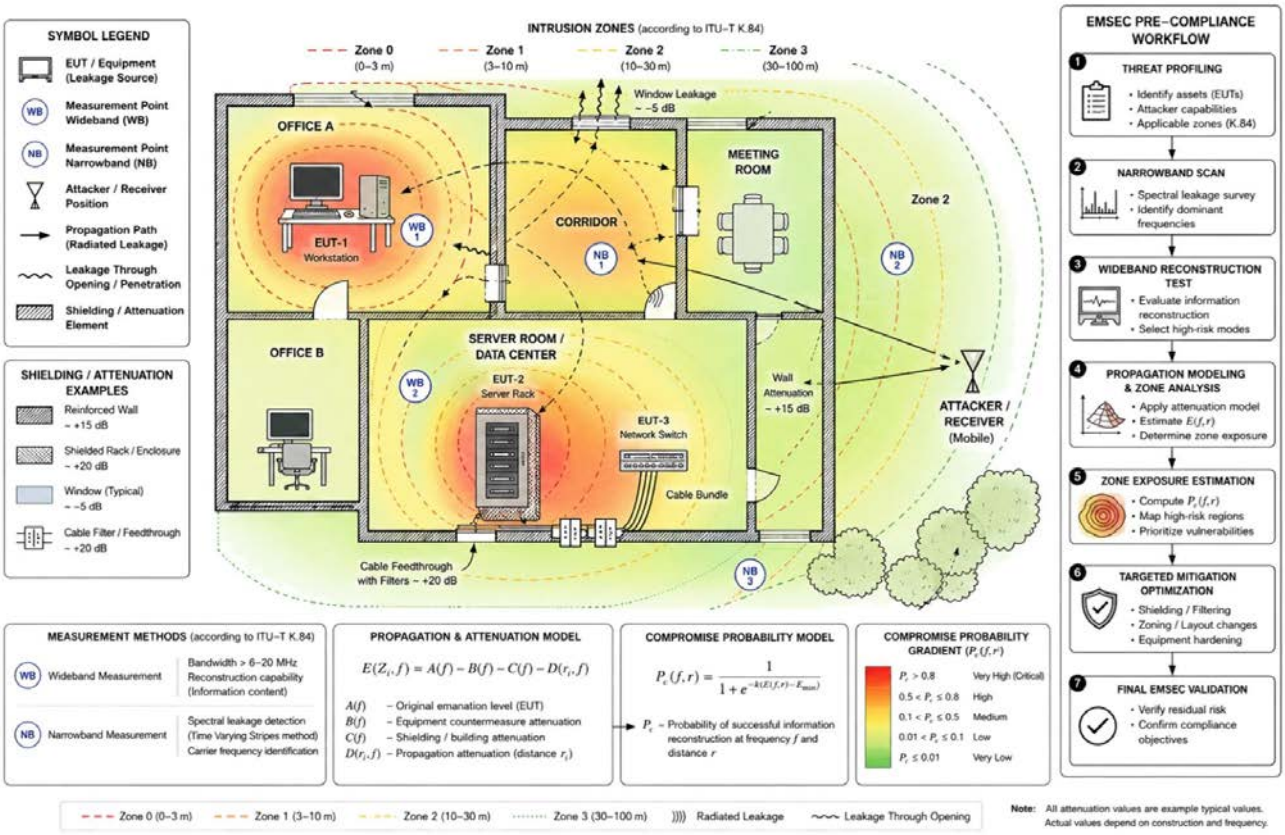


Figure 3. Example facility-oriented EMSEC pre-compliance assessment workflow integrating intrusion-zone analysis, propagation-oriented leakage measurements, shielding evaluation, and targeted mitigation optimization derived from ITU-T K.84 and related recommendations.

The proposed staged approach enables iterative EMSEC hardening where mitigation measures are guided by measurable compromise potential rather than worst-case assumptions alone. Consequently, the methodology supports cost-effective deployment of EMSEC protections while preserving compatibility with formal TEMPEST-oriented evaluation procedures.

4. ANALYTICAL PROPAGATION AND COMPROMISE MODEL

The intrusion zones defined in ITU-T K.84 directly determine the required measurement configuration. As the intrusion distance increases from Zone 0 toward Zone 3, the received field strength decreases due to propagation attenuation and shielding effects.

4.1 Spatial propagation model

For each intrusion zone Z_i, the measurable threat level can be expressed as:

$$E(Z_i, f) = A(f) - B(f) - C(f) - D(r_i, f) \quad (2)$$

where: $E(Z_i, f)$ is the received electric field strength at intrusion zone Z_i and frequency f, $A(f)$ denotes the original compromising emanation spectrum generated by the EUT, $B(f)$ denotes equipment countermeasure attenuation, $C(f)$ represents shielding attenuation, $D(r_i, f)$ represents propagation attenuation associated with attacker distance r_i.

The security criterion becomes:

$$E(Z_i, f) \leq E_{th}(f) \quad (3)$$

which establishes $E_{th}(f)$ the maximum acceptable emanation level for each intrusion zone - the minimum detectable electromagnetic field required for information reconstruction.

Substituting the propagation model yields:

$$A(f) - B(f) - C(f) - D(r_i, f) \leq E_{th}(f) \quad (4)$$

which can be rearranged into:

$$B(f) + C(f) + D(r_i, f) \geq A(f) - E_{th}(f) \quad (5)$$

This expression defines the total required attenuation budget necessary to preserve confidentiality at intrusion zone Z_i. The maximum compromise distance can be derived from the security condition. Solving for distance yields:

$$r_{max}(f) = 10^{\frac{A(f) - B(f) - C(f) - E_{th}(f)}{20}} \quad (6)$$

The obtained value represents the maximum intrusion radius at which compromising information remains detectable.

4.2 Probabilistic Reconstruction Model

Because information reconstruction quality improves gradually rather than instantaneously, EMSEC compromise may be represented using a probabilistic model. The probability of successful information reconstruction is approximated as:

$$P_c(f, r) = \frac{1}{1 + e^{-k(E(f,r) - E_{min})}} \quad (7)$$

where: P_c denotes compromise probability, k controls transition sharpness, $E(f, r)$ represents received field strength, E_{min} represents the minimum reconstruction threshold.

This formulation enables continuous estimation of EMSEC exposure rather than binary secure/insecure classification. The wideband and narrow-band measurement methods defined in ITU-T K.84 may now be interpreted within the proposed propagation framework.

The wideband method evaluates practical information reconstruction capability, temporal signal integrity and real compromise feasibility. Conversely, the narrow-band method evaluates spectral leakage localization, carrier frequency identification and frequency-selective propagation characteristics.

5. ILLUSTRATIVE APPICATIONS

5.1 Protection Optimization Concept

The conceptual model shown in Figure 4 illustrates that mitigation strategies implemented without prior leakage characterization may result in excessive shielding complexity and unnecessary infrastructure modifications. In contrast, measurement-driven assessment enables prioritization of dominant leakage paths and frequency components, thereby reducing overall protection cost while maintaining acceptable EMSEC risk levels. The residual compromise probability illustrated in Figure 4 conceptually corresponds to the probabilistic compromise function defined in Equation (7), where mitigation measures progressively reduce the received field strength below the reconstruction threshold. The “Potential Over-Engineering” region illustrates that EMSEC countermeasures implemented without prior leakage characterization may produce disproportionately high shielding and infrastructure costs while yielding only marginal reductions in residual compromise probability. This directly emphasizes the necessity of measurement-driven assessment, since realistic propagation analysis and intrusion-zone evaluation enable optimization of protection measures according to actual electromagnetic exposure rather than worst-case assumptions.

5.2 Spatial-Frequency Exposure Surface

The probabilistic compromise model introduced in Equation (7) can be further extended into a spatial-frequency exposure metric representing the residual EMSEC risk over the operational bandwidth of the compromising emanation. Instead of evaluating information reconstruction feasibility at a single frequency component, practical EMSEC compromise depends on the cumulative contribution of multiple spectral components propagating through the environment.

Accordingly, the average residual compromise probability at distance r may be expressed as:

$$P_{avg}(r) = \frac{1}{BW} \int_{f_1}^{f_2} P_c(f, r) df \quad (8)$$

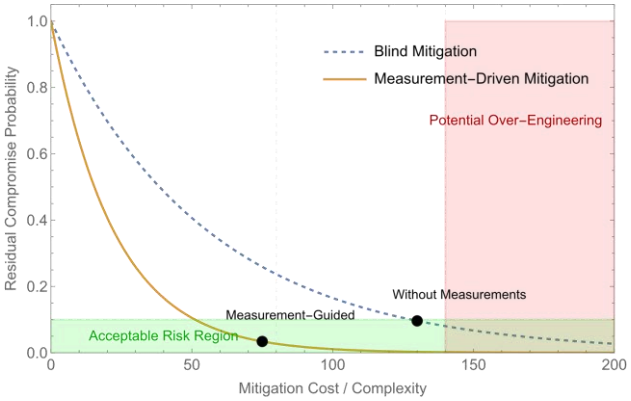


Figure 4. Conceptual comparison between blind EMSEC mitigation and measurement-driven protection optimization.

where: $BW = f_2 - f_1$ denotes the observed frequency bandwidth,

$P_c(f,r)$ represents the probabilistic compromise function,

and $P_{avg}(r)$ expresses the cumulative reconstruction feasibility across the measured spectral interval.

This formulation enables interpretation of EMSEC exposure as a continuous spatial-frequency risk distribution rather than a discrete threshold phenomenon. Consequently, the compromise probability becomes dependent not only on distance and shielding attenuation, but also on the spectral distribution of the emanation source and receiver sensitivity over the operational bandwidth. The proposed model is particularly suitable for visualization through three-dimensional propagation surfaces and intrusion-zone probability maps, Figure 5.
Such visualization enables measurement-driven optimization of shielding deployment, intrusion-zone geometry, receiver-oriented threat assessment and pre-compliance EMSEC mitigation strategies.
The probabilistic compromise surface may additionally be interpreted through intrusion-zone thresholds derived from ITU-T K.84. Instead of representing intrusion zones solely as fixed physical distances, the proposed framework associates each zone with a compromise probability interval over the spatial-frequency propagation surface, Figure 6. Instead of defining intrusion zones only through physical separation distances, the proposed framework associates each zone with a characteristic compromise probability interval derived from the propagation model.

Accordingly, intrusion zones may be represented as:

$$Z_i \equiv \{(f,r) | P_c(f,r) \in \Omega_i\}$$

where: Ω_i denotes the compromise probability interval associated with intrusion zone Z_i and $P_c(f,r)$ represents the probability of successful information reconstruction at frequency f and distance r.

An example interpretation may be expressed as:

– Zone 0: high-confidence reconstruction region ($P_c > 0.8$),

– Zone 1: partial reconstruction region ($0.5 < P_c \leq 0.8$),

– Zone 2: detectable spectral leakage region ($0.1 < P_c \leq 0.5$),

– Zone 3: residual detectability region ($P_c \leq 0.1$).

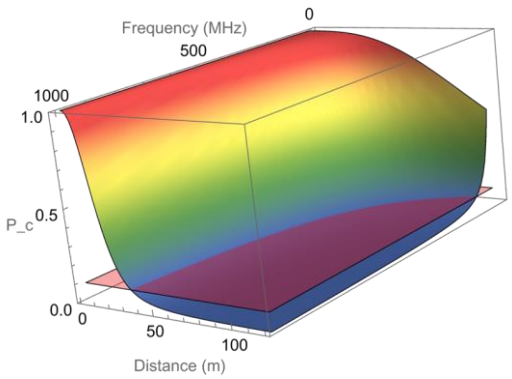


Figure 5. Three-dimensional spatial-frequency representation of probabilistic EMSEC exposure derived from the proposed propagation and reconstruction model. The red plane represents an acceptable residual compromise probability threshold.

This interpretation transforms intrusion zones into measurable propagation-dependent security regions whose boundaries vary according to SE, receiver sensitivity, propagation attenuation and emanation spectral distribution. Consequently, intrusion-zone boundaries are no longer fixed architectural distances, but dynamically depend on the electromagnetic characteristics of the protected environment and attacker capabilities.

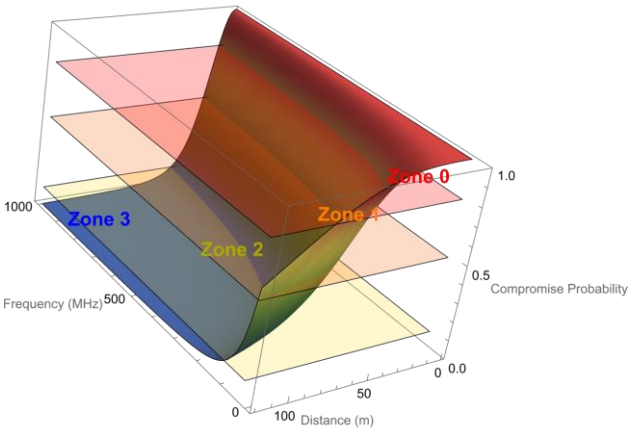


Figure 6. Spatial-frequency EMSEC Exposure with Intrusion Zone thresholds derived from the proposed compromise model.

This representation transforms the intrusion-zone concept into a dynamic propagation-oriented EMSEC assessment model suitable for measurement-driven pre-compliance analysis.

5.3 Intrusion-Zone Exposure versus Shielding

Figure 7 illustrates the relationship between intrusion distance, SE, and the probability of successful electromagnetic information reconstruction. The model assumes an emanation level of 62.2 dBμV/m at the reference distance and a reconstruction threshold of 15 dBμV/m representing the minimum field strength required by the adversary's receiving system. The probability curves are generated using the proposed logistic compromise model, where the parameter k=0.166 controls the transition

between successful and unsuccessful reconstruction regions.

The results demonstrate that increasing shielding attenuation shifts the compromise-probability curves downward and compresses the effective interception range. Without shielding, the probability of successful reconstruction remains relatively high even within extended intrusion zones, whereas shielding levels of 20–30 dB substantially reduce the compromise probability before the Zone 2 and Zone 3 boundaries are reached. This observation supports the central premise of measurement-driven EMSEC assessment: the required protection level is strongly dependent on the actual emanation characteristics and intrusion-zone geometry rather than on generic worst-case assumptions.

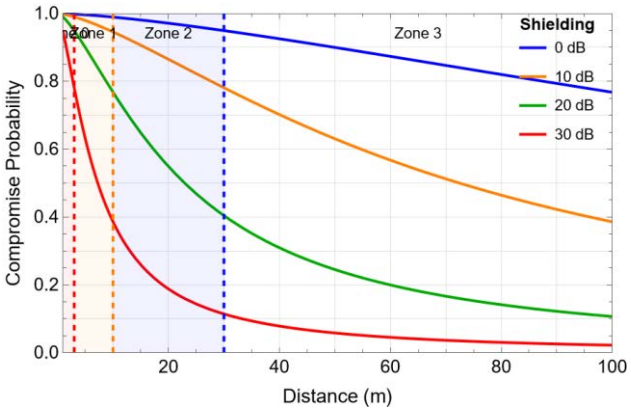


Figure 7. Intrusion-Zone EMSEC Exposure versus Shielding

The selected emanation level (62.2 dBμV/m) approximately corresponds to a leakage source that already satisfies conventional EMC emission requirements, illustrating that EMC compliance alone does not necessarily imply electromagnetic security. The reconstruction threshold (15 dBμV/m) represents the minimum electromagnetic field strength required for meaningful signal recovery by the assumed receiver class, hile the probability sharpness parameter (k = 0.166) models the gradual degradation of reconstruction quality observed in practical EMSEC scenarios. Rather than producing a strict secure/insecure boundary, the model reflects the realistic transition from reliable reconstruction to partial recovery and finally to residual detectability.

The figure highlights that intrusion-zone boundaries alone are insufficient for EMSEC assessment; identical facilities may exhibit substantially different exposure profiles depending on the measured emanation level and SE, thereby justifying the need for pre-compliance EMSEC measurements prior to implementation of costly countermeasures.

5.4 Frequency-Selective Leakage Characterization

In contrast to the spatial propagation analysis presented previously, narrow-band EMSEC measurements focus on identification of spectral components that carry compromising information. As described in ITU-T K.84, specific frequencies may exhibit significantly higher leakage levels due to deterministic electronic processes occurring inside the equipment under test.

The conceptual spectrum shown in Figure 8 models three representative leakage mechanisms frequently encountered in practical systems: clock harmonic, cable resonance and switching noise. Each mechanism contributes differently to the overall compromising emanation profile and therefore requires different mitigation strategies.

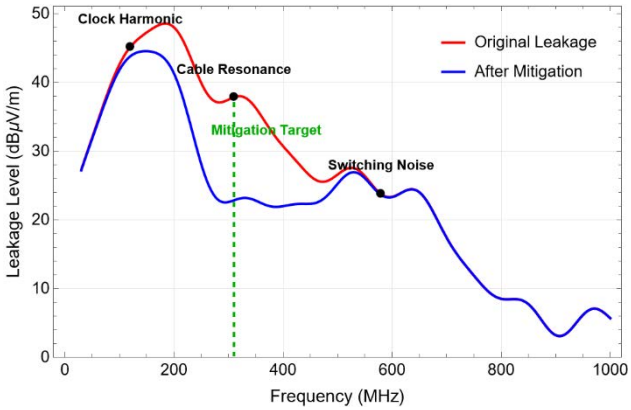


Figure 8. Frequency-Selective EMSEC Leakage Analysis

The resulting leakage spectrum may be approximated as:

$$S(f) = S_{clk}(f) + S_{cab}(f) + S_{sw}(f) \quad (9)$$

where, $S_{clk}(f)$ represents leakage generated by internal clock harmonics, $S_{cab}(f)$ represents resonant amplification caused by connected cables or conductive structures, and $S_{sw}(f)$ represents broadband emissions produced by switching power electronics and digital circuitry. A mitigation function $M(t)$ is then applied around a selected dominant leakage frequency, producing a residual spectrum

$$S_{mit}(f) = S(f) + M(f) \quad (10)$$

which models the effect of shielding, filtering, cable treatment, or redesign actions.

Figure 8 illustrates a representative narrow-band EMSEC measurement scenario derived from the concepts described in ITU-T K.84. The red curve represents the original leakage spectrum measured from an information-processing device, while the blue curve illustrates the residual leakage after application of a targeted mitigation measure. Three dominant leakage components can be observed. The first peak at approximately 120 MHz corresponds to a clock harmonic generated by internal digital timing circuits. The second peak at approximately 310 MHz is associated with cable resonance effects, where connected conductors behave as unintended radiating structures. The third peak at approximately 580 MHz represents switching-noise emissions originating from power conversion circuitry. The dashed line indicates a mitigation target frequency identified through spectral analysis. Application of a frequency-selective countermeasure reduces the leakage level around the dominant resonance, resulting in the mitigated spectrum shown in blue. The figure illustrates how narrow-band measurements can be used to identify dominant compromising frequencies and guide targeted EMSEC mitigation efforts. Instead of applying generalized

shielding measures over the entire spectrum, the proposed methodology uses measurement results to identify dominant leakage frequencies and prioritize mitigation efforts where they produce the greatest reduction in compromise potential. Examples of such mitigation techniques include selective shielding reinforcement, cable rerouting, ferrite suppression, filtering, grounding improvements, or equipment relocation.

Within the context of the proposed analytical framework, the mitigated spectrum corresponds to a reduction of the emanation term $A(f)$ in Equation (5), which directly decreases the maximum compromise distance and lowers the compromise probability defined by Equation (7). The figure therefore provides a practical interpretation of how narrow-band measurements can be translated into measurable reductions of EMSEC exposure and intrusion-zone risk.

6 CONCLUSION

The proposed analytical framework represents a simplified propagation-oriented approximation of practical EMSEC environments. Real electromagnetic leakage scenarios may additionally depend on multipath propagation, polarization mismatch, near-field coupling effects, non-linear leakage mechanisms and receiver-specific reconstruction algorithms. Consequently, the proposed framework should be interpreted primarily as an engineering-oriented pre-compliance assessment methodology intended to support early-stage EMSEC risk evaluation and mitigation prioritization rather than a replacement for formal TEMPEST certification procedures.

To be concluded, the proposed framework demonstrates how publicly available ITU-T recommendations can be combined with propagation-oriented analysis, intrusion-zone assessment, and measurement-driven mitigation planning to establish an engineering-level EMSEC pre-compliance methodology. Unlike traditional TEMPEST evaluation procedures, which are typically performed during certification stages, the proposed approach enables early identification of dominant leakage paths, estimation of compromise probability, and optimization of shielding and zoning strategies prior to expensive infrastructure modifications. However, it is not substitution for formal TEMPEST evaluation. The illustrative examples demonstrate how propagation modeling and spectral leakage characterization can support targeted mitigation while reducing the risk of over-engineered countermeasures.

Acknowledgements

This work resulted from part of research P1/26-28 and was supported by MoD of RS

References

[1] F. LARROCA, P. BERTRAND, F. CARRAU AND V. SEVERI.: *gr-tempest: an open-source GNU Radio implementation of TEMPEST*, 2022 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Singapore, Singapore, 2022, pp. 1-6, doi: 10.1109/AsianHOST56390.2022.10022149.

[2] C. LAVAUD, R. GERZAGUET, M. GAUTIER, O. BERDER, E. NOGUES, ET AL..: *Whispering devices: A survey on how side-channels lead to compromised information*, Journal Hardware and Systems Security, 2021, 5 (2), pp.143-168. ⟨10.1007/s41635-021-00112-6⟩. ⟨hal-03176249⟩.

[3] Y. LONG, Q. JIANG, C. YAN, T. ALAM, X. JI, W. XU, K. FU: *EM Eye: Characterizing Electromagnetic Side-channel Eavesdropping on Embedded Cameras*, Network and Distributed System Security Symposium, 2024, San Diego, CA, USA

[4] POHL,J., NOACK,A.: *Universal Radio Hacker: A Suite for Wireless Protocol Analysis*, IoTS&P '17: Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, Dallas Texas USA, 2017. https://doi.org/10.1145/3139937.3139951

[5] LIU Z., SAMWEL N., WEISSBART L., ZHAO Z., LAURET D., BATINA L., LARSON M. : *Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel,* Network and Distributed Systems Security (NDSS) Symposium 2021, Virtual, https://dx.doi.org/10.14722/ndss.2021.23021

[6] CAMURATI G., FRANCILLON A.: *Noise-SDR: Arbitrary Modulation of Electromagnetic Noise from Unprivileged Software and Its Impact on Emission Security*, IEEE Symposium on Security and Privacy (SP), 2022, San Francisco, USA, https://10.1109/SP46214.2022.9833767

[7] CAMURATI G., FRANCILLON A. and STANDAERT F.X.: *Understanding Screaming Channels: From a Detailed Analysis to Improved Attacks,* IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES), 2020, https://tches.iacr.org/index.php/TCHES/article/view/8594

[8] ITU-T K.84.: *Test method and guide for EMSEC*, International Telecommunication Union (ITU-T), Recommendation K.84, Geneva, Switzerland, January 2011.

[9] ITU-T K.81.: *High-power electromagnetic immunity guide for telecommunication systems*, International Telecommunication Union (ITU-T), Recommendation K.87, Geneva, Switzerland, August 2024.

[10] ITU-T K.87.: *Guide for the application of electromagnetic security requirements – Overview*, International Telecommunication Union (ITU-T), Recommendation K.87, Geneva, Switzerland, August 2024.