https://doi.org/10.54361/ajmas.269913

Original article

A Risk-Based Regulatory Framework for EMC and EMI Management in Internet of Things Applications

Walid Hasan[1]*, Albahlool Abood[2], Zakaria Alforjnai[3], Ezzeddin Bendaw[4]

[1]National Authority for Scientific Research, Tripoli, Libya
[2]University of Gharyan, Gharyan, Libya
[3] Libyan Academy, Tripoli, Libya
[4]Ministry of Technical and Vocational Education, Libya
Email.Waleed82ly@gmail.com

Abstract
The rapid growth of Internet of Things (IoT) applications has increased the number of connected devices operating in shared wireless environments. IoT systems rely on sensors, actuators, embedded electronics, software, and internet connectivity to collect, exchange, and process data across sectors such as smart homes, healthcare, transportation, industrial systems, energy systems, and public infrastructure. However, the dense deployment of wireless IoT devices can create significant Electromagnetic Compatibility (EMC) challenges, especially when multiple transmitters and receivers operate in proximity or within the same or adjacent frequency bands. These conditions may lead to Electromagnetic Interference (EMI), which can degrade communication performance, reduce device reliability, and affect safety in critical environments. This study uses a regulatory review and conceptual framework development, drawing on literature synthesis, regulatory requirement extraction, analytical classification, regulatory mapping, and risk-based EMC categorisation. It identifies key EMC and EMI challenges in IoT applications, particularly in dense wireless and low-power communication environments. It analyses immunity requirements in critical sectors such as vehicular networks, healthcare, industry, and public infrastructure. It also develops a regulatory framework that defines stakeholder roles and classifies IoT connection methods, application areas, and device structures to support safer deployment and reduce interference risks.
Keywords. Internet of Things, Electromagnetic Compatibility, Electromagnetic Interference, Regulatory Framework.

Introduction

The Internet of Things (IoT) is a networked environment in which physical and virtual objects are interconnected through information and communication technologies. These interconnected objects can collect, exchange, and process data to support intelligent services, automation, monitoring, and decision-making across different application domains [1]. In general, IoT applications include physical devices, vehicles, buildings, sensors, actuators, and other smart objects that are connected to the internet to collect, exchange, and process data [2,3]. IoT systems rely on embedded electronics, software, and internet connectivity to collect, exchange, and process data [4]. These systems are increasingly used in various areas, including smart homes, healthcare, industrial automation, transportation, energy systems, smart cities, and public infrastructure, where wireless communication and supporting functions such as localization and position estimation enable flexible, mobile, and connected IoT services [5-7].
In the coming years, IoT is expected to support communication among tens of billions of devices and information systems [8,9]. This large-scale connectivity will integrate web-based services, mobile applications, cloud platforms, and automated systems [10]. As a result, IoT can improve operational efficiency, support intelligent interaction between people and machines, and connect a wide range of computing technologies, from servers and personal computers to small smart devices [11,12]. IoT applications use different technologies and components, including sensors, actuators, Radio Frequency Identification (RFID) tags, Vehicular Ad Hoc Networks (VANETs), and Low-Power Wide Area Networks (LPWANs) [13]. These technologies support various applications, including industrial monitoring, building control, e-health, smart energy grids, vehicle performance monitoring, and home automation [14]. The collected data can be transmitted through wireless, wired, or hybrid networks to backend servers, cloud platforms, or integration systems, where it is processed and converted into meaningful information [15]. However, as IoT systems move from closed, isolated networks to public internet-based environments, new technical challenges arise [16].
One important challenge is Electromagnetic Compatibility (EMC), especially when many wireless devices operate in proximity [17]. In dense IoT environments, multiple transmitters and receivers may operate simultaneously across a wide range of frequency bands, while emerging wireless communication systems are also extending toward frequencies above 100 GHz [18]. This can increase the possibility of Electromagnetic Interference (EMI), which may reduce communication reliability, degrade device performance, or interrupt critical services [19]. Traditional EMC testing usually focuses on individual devices. However, this approach may not fully consider the combined effect of multiple IoT devices operating together in the same environment. The simultaneous operation of many transmitters and receivers can create unintended interference, which may affect the intended receiver and reduce the reliability of the communication link. For example, LPWAN technologies are widely used because they provide long-range communication with low power consumption and low cost. Nevertheless, unexpected interference may negatively affect their communication range, data transmission reliability, and overall system performance. Therefore, EMC and EMI issues should be considered as important technical

Received: *02-07-2026 -* ***Accepted:*** *01-09-2026 -* ***Published:*** *07-09-2026*

and regulatory requirements for IoT applications, especially in critical environments such as healthcare, intelligent transportation, industrial automation, and public infrastructure.

A clear regulatory framework is needed to support safe IoT deployment, define stakeholder responsibilities, classify IoT technologies and applications, and reduce risks associated with electromagnetic interference. Existing EMC standards and IoT regulatory approaches generally focus on individual equipment compliance, communication requirements, or specific application domains. However, they do not provide a unified risk-based approach that links EMC and EMI risks with application criticality, device characteristics, stakeholder responsibilities, deployment conditions, and post-deployment monitoring. This limitation becomes more important in dense and safety-critical IoT environments, where the consequences of electromagnetic interference can differ greatly between consumer, industrial, healthcare, transportation, and public infrastructure applications. Therefore, this study addresses this gap by proposing an integrated risk-based regulatory framework that combines technical EMC/EMI considerations with application risk levels and appropriate regulatory responsibilities.

The main objectives of this paper are as follows:

1) Identification of the major EMC and EMI challenges associated with the rapid growth of IoT applications, particularly in dense wireless environments where many devices operate in proximity.
2) Analysis of IoT immunity requirements in critical environments, including vehicular networks, healthcare systems, industrial automation, and public infrastructure, where interference may affect safety and service reliability.
3) Development of a regulatory framework for IoT applications that defines stakeholder responsibilities, connection methods, application categories, and device classifications to support safe and reliable IoT deployment.

The remainder of this paper is organized as follows. Section 2 reviews related work on IoT regulation, EMC testing, and interference analysis. Section 3 presents the methodology adopted to construct the proposed regulatory framework. Section 4 explains the concept of electromagnetic compatibility and its main components. Section 5 discusses IoT immunity in critical environments. Section 6 identifies the main EMC challenges in IoT devices. Section 7 describes the IoT value chain. Section 8 presents the proposed regulatory framework, including its alignment with international references, operational model, implementation mechanism, connection methods, application classification, device classification, risk-based EMC classification, and EMC/EMI relevance. Finally, Section 9 concludes the paper and outlines future research directions.

Literature Review

Michalak and Szafrańska [20] examined electromagnetic compatibility issues associated with the rapid growth of IoT-related equipment. Their study highlighted that large numbers of connected devices often operate in proximity, which may create EMC problems in real deployment environments. They also explained that individual EMC compliance does not necessarily guarantee reliable operation when several IoT devices coexist within the same environment. In addition, the authors discussed classical EMC testing, real-time measurement, PCB-like testing, and system-level testing approaches. Dionísio, Lolic, and Torres [21] analysed radio interference in Industrial IoT environments using SEAMCAT simulation. Their work investigated coexistence between legacy industrial wireless systems, including Wi-Fi, Bluetooth, and WirelessHART, and 5G systems in factory environments. The study considered interference scenarios, propagation models, interference-to-noise analysis, and the impact of radio interference on industrial wireless communication performance. Noor-A-Rahim *et al*. [22] presented a comprehensive review of wireless communication technologies for smart manufacturing and Industrial IoT. Their study examined industrial wireless protocols, machine-to-machine communication, smart factory uses cases, 5G, 6G, and future industrial communication requirements. The authors also discussed key challenges related to reliability, latency, interoperability, radio propagation, power consumption, and electromagnetic interference in manufacturing environments. Li, Maiti, and Fei [23] reviewed regulatory technology and its application in Industrial IoT and non-financial sectors. Their work explained how IoT, artificial intelligence, machine learning, cloud computing, and data analytics can support compliance, supervision, monitoring, reporting, and regulatory decision-making. They also discussed the roles of producers, regulators, and supervisors in technology-supported compliance systems.

Shilpa, Gupta, Jha, and Hashmi [24] reviewed interference issues in LoRa-based dense IoT networks. They covered LPWAN technologies, especially LoRa, and discussed challenges such as interference, scalability, reliability, and security. They also classified different types of LoRa interference and reviewed solution approaches for improving LoRa network performance. Hwata et al. [25] proposed an Internet of Things-based electromagnetic compatibility monitoring architecture for biomedical devices. Their study focused on the need for continuous EMC monitoring in healthcare environments, where biomedical devices may be affected by electromagnetic disturbances generated by wireless communication systems and nearby electronic equipment. The proposed architecture highlights the importance of real-time observation, interference detection, and reliable monitoring mechanisms to support the safe operation of medical IoT and biomedical systems.

Existing studies have examined EMC testing, industrial IoT interference, wireless communication technologies, regulatory technologies, LPWAN interference, and biomedical EMC monitoring. However, these studies are mostly fragmented because each one focuses on a specific technology, application domain, or interference scenario. They do not provide a unified regulatory perspective that connects EMC and EMI risks with IoT application categories, connection methods, device structures, stakeholder responsibilities, and post-deployment monitoring requirements.

Received: *02-07-2026 -* ***Accepted:*** *01-09-2026 -* ***Published:*** *07-09-2026*

In addition, limited attention has been given to risk-based EMC classification for IoT applications, although the consequences of interference differ significantly between consumer applications, industrial systems, healthcare environments, transportation networks, and public infrastructure. Therefore, a structured regulatory framework is needed to support safer IoT deployment by linking technical EMC requirements with regulatory control mechanisms and the operational responsibilities of IoT stakeholders.

Methodology

This study uses a regulatory review and conceptual framework development approach to formulate a regulatory framework for IoT applications under EMC and EMI constraints. The method is based on reviewing relevant academic studies, standards, and regulatory documents, identifying key EMC and EMI requirements, and organising these findings into application, device, and regulatory categories. The aim is not to conduct laboratory experiments or simulations, but to develop a practical framework that links EMC and EMI concerns with regulatory requirements for IoT deployment. The source-identification process considered academic studies and authoritative regulatory and standards documents relevant to IoT, EMC, EMI, wireless coexistence, device immunity, critical IoT applications, and regulatory compliance. Academic literature was identified using Google Scholar, covering the period [January 2015 to August 2026]. The main search terms included combinations of "Internet of Things," "IoT," "Industrial IoT," "electromagnetic compatibility," "EMC," "electromagnetic interference," "EMI," "wireless interference," "immunity," "coexistence," "regulation," and "standards." Official standards and regulatory documents relevant to the proposed framework were also considered, particularly material from IEC, ETSI, and ITU.

Sources were included when they addressed at least one aspect directly relevant to the development of the framework, including IoT communication technologies, EMC/EMI behaviour, interference or coexistence, device immunity, critical IoT applications, stakeholder responsibilities, regulatory requirements, or EMC-related standards. Sources that had no direct relevance to IoT-related EMC/EMI or regulatory issues, duplicated information already represented by a more authoritative source, or did not provide sufficient information for framework development were excluded. The methodological workflow followed in this study is illustrated in Fig. 1. The workflow begins with the synthesis of relevant literature and proceeds through requirement extraction, analytical classification, regulatory mapping, and risk-based EMC categorisation. These stages collectively support the formulation of the proposed regulatory framework by connecting electromagnetic compatibility concerns with practical governance requirements for IoT deployment.

Electromagnetic Compatibility

EMC refers to the ability of electrical and electronic equipment or systems to operate satisfactorily within their electromagnetic environment without generating, propagating, or receiving electromagnetic disturbances that could cause malfunction, performance degradation, or physical damage to other equipment [26]. The main objective of EMC is to ensure that different devices and systems can operate correctly and safely when sharing the same electromagnetic environment [27]. EMC generally involves three main aspects: emissions, susceptibility or immunity, and coupling. Emissions refer to the electromagnetic energy generated by a device, either intentionally or unintentionally, and released into the surrounding environment. EMC studies aim to identify these unwanted emissions and apply suitable countermeasures to reduce their impact. Electromagnetic Susceptibility (EMS) describes the tendency of a device or system to malfunction when exposed to unwanted electromagnetic disturbances, commonly referred to as RFI.

In contrast, immunity refers to the ability of equipment to continue operating correctly in the presence of such interference. Improving immunity, or hardening the equipment, is therefore an important part of EMC design. The third aspect, coupling, describes the path or mechanism through which electromagnetic interference is transferred from the source to the affected device [28,29]. Electromagnetic emissions can be classified into conducted and radiated emissions. Conducted emissions occur when unwanted electromagnetic energy is transferred through physical conductors, such as power cables or signal wires. Radiated emissions, on the other hand, occur when electromagnetic energy is released into the air and propagates as electromagnetic fields [30]. Therefore, effective interference mitigation can be achieved by controlling the source of interference, reducing or blocking the coupling paths, and improving the immunity of the affected equipment. These measures collectively support the achievement of electromagnetic compatibility in complex electrical and electronic systems.

Received: *02-07-2026 -* ***Accepted:*** *01-09-2026 -* ***Published:*** *07-09-2026*

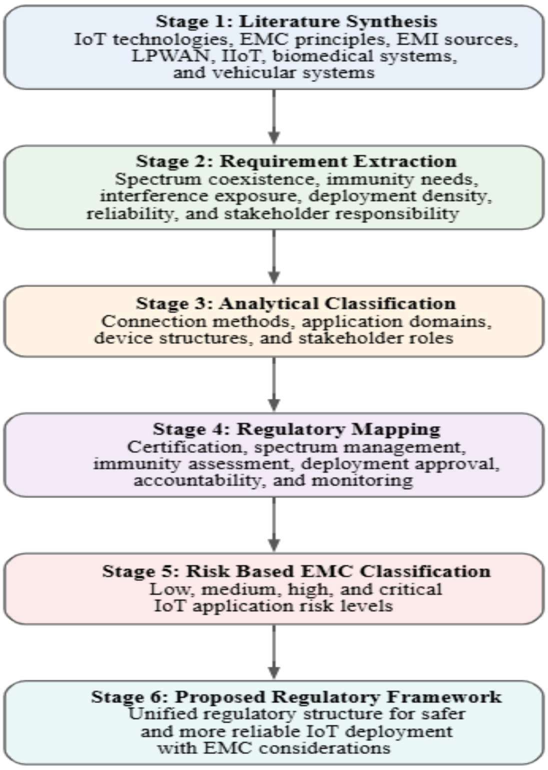

Figure 1. Methodological workflow for constructing the proposed IoT regulatory framework

IoT Immunity in Critical Environments

Vehicular ad hoc networks (VANETs) enable vehicle-to-vehicle (V2V) and vehicle-to-roadside (V2R) communication. Roadside access points, often called Roadside Units (RSUs), support the exchange of traffic, safety, and environmental information. Intelligent VANET systems commonly employ wireless communication technologies such as Wi-Fi based on IEEE 802.11p and WiMAX based on IEEE 802.16 to support communication among vehicles in highly dynamic mobility environments [31], [32]. These technologies can provide effective mechanisms for vehicle tracking, traffic monitoring, and cooperative transportation services [33]. Connected vehicles and intelligent transportation systems rely on several sensing, navigation, and communication technologies, including GPS-enabled devices, roadside sensors, and V2V/V2I communication systems. The data collected from these systems can support traffic monitoring, route guidance, and real-time decision-making [34]. However, the increasing number of electronic and wireless systems inside and around vehicles introduces new EMI challenges.

EMI sources in automotive environments may be either unintentional or intentional. Unintentional sources include internal electronic components, external radio-frequency noise, lightning, and background electromagnetic noise. Intentional sources may include ZigBee sensors, cellular signals, Wi-Fi devices used by passengers, and V2V and V2R communication systems. More generally, radio-frequency interference from active transmitters is a recognised concern in transportation environments [35]. The carrier frequencies used in these systems may be similar or different depending on the communication protocols involved. In addition, modern vehicles perform intensive data-processing tasks, including digital signal processing, visual data analysis, and authentication processes to verify the reliability of received traffic information. These operations may contribute to the overall electromagnetic noise environment, although their impact is often overlooked in traditional analysis because they may have limited influence on the detection of intended signals under normal conditions. Nevertheless, EMI cannot be ignored in IoT-based critical environments. Electromagnetic disturbances may affect sensors, electronic control units, and communication links within connected vehicles, particularly V2V and V2R communication. Any failure or degradation in these systems may have serious safety consequences. Similar concerns apply to other critical environments, such as hospitals, where wireless IoT devices are increasingly used for remote patient monitoring and healthcare services. In such environments, strong EMC requirements and reliable immunity testing are essential to ensure safe and dependable operation of IoT systems [36].

EMC Challenges in IoT devices

Several challenges can affect the electromagnetic compatibility (EMC) performance of IoT devices. These challenges are mainly related to the increasing number of connected devices, the use of higher operating frequencies, operation in licensed and unlicensed frequency bands, and the characteristics of low-power wide area networks.

Received: *02-07-2026 -* ***Accepted:*** *01-09-2026 -* ***Published:*** *07-09-2026*

https://doi.org/10.54361/ajmas.269913

The number of devices

As the density of IoT devices increases within a specific geographical area, the physical separation between devices decreases. This results in a crowded electromagnetic environment where many wireless and wired devices, such as IoT sensors, smartphones, tablets, laptops, and personal computers, operate in proximity. Such crowding increases the risk of radio-frequency interference and may reduce the EMI immunity of nearby devices. In dense deployments, the interference power generated by one or more transmitting devices may exceed the noise threshold of a receiver, leading to degraded communication performance or device malfunction [37,38]. Recent quantitative studies confirm the effect of device density on interference in IoT networks. For example, a 2025 simulation study of LoRaWAN and IEEE 802.11ah coexistence considered LoRa deployments ranging from 10 to 8000 nodes and reported that increasing LoRa traffic could reduce IEEE 802.11ah throughput by up to 31% and increase packet loss to as much as 79% [39]. These results demonstrate that increasing IoT device density can have a substantial measurable impact on communication reliability in shared-spectrum environments.

Higher frequency of operation

Future IoT and wireless systems have been anticipated to use substantially higher frequency ranges, with visions extending to approximately 30 GHz for outdoor environments and 90 GHz for indoor applications [40]. ITU-T K.136 addresses radiated electromagnetic-field measurements over a broad frequency range; however, conventional CISPR-based measurement instrumentation is generally applied up to 18 GHz, with alternative measurement procedures used at higher frequencies [41]. Therefore, the continued expansion of IoT operating frequencies requires corresponding development of EMC measurement and assessment methods.

Licensed and Unlicensed Frequency Bands

IoT applications may use either licensed or unlicensed frequency bands for data collection and exchange. Licensed bands are usually regulated and coordinated by national authorities, while unlicensed bands can be used without individual permission. Although unlicensed bands provide flexibility and reduce deployment costs, they also pose EMC challenges, as multiple devices may operate in the same frequency range without coordination. The electromagnetic environment in these bands can vary significantly between locations, depending on device density and usage levels. Heavy use of unlicensed bands may result in signal disruption, increased latency, packet loss, and reduced communication reliability [42,43]. Real-world measurements also demonstrate that interference in unlicensed IoT spectrum can be substantial. Measurements of LoRaWAN operation in the 868 MHz ISM band reported probabilities of interfering signals ranging from 13.2% to 97.3% in mandatory uplink channels and from 4.8% to 54% in downlink channels [44].

Low-Power Wide Area Networks

IoT systems commonly use both short-range low-power communication technologies and Low-Power Wide Area Networks (LPWANs). While LPWAN technologies are useful for long-range communication with low energy consumption, their low transmission power can make them more vulnerable to electromagnetic interference. In areas where many low-power devices are co-located, the overall interference level may increase, which can reduce the signal-to-noise ratio and affect communication reliability [45,46]. Therefore, dense LPWAN deployments require careful EMC consideration, particularly in critical applications where communication failure may lead to safety, operational, or economic consequences. Recent LoRa evaluations of networks with 100–2000 nodes showed that interference-aware channel access can significantly improve packet delivery in dense deployments, with about a 20-percentage-point improvement at 2000 nodes compared with standard CSMA/CA [47].

IoT Value Chain

The IoT value chain, illustrated in (Figure 2), consists of several interconnected layers that collectively enable the delivery of IoT services. Each layer performs a specific function, starting from data generation at the device level and ending with service delivery to the final user. The first layer is the smart module layer, which includes IoT-enabled devices such as smart home appliances, connected vehicles, industrial machines, and sensors used in smart city applications. These devices are responsible for sensing, collecting, and sometimes processing data from the physical environment. The second layer is the gateway layer. This layer collects data or signals from connected devices and may perform basic processing, filtering, or protocol conversion before forwarding the data to the network. The third layer is the connectivity layer, which provides the communication link between the gateway and the IoT platform. This connection may be established through wireless, wired, cellular, satellite, or low-power wide area network technologies, depending on the application requirements. The fourth layer is the platform or server layer, where the collected data is stored, processed, and analysed.

IoT service providers use this layer to transform raw data into useful information that can support monitoring, automation, and decision-making. The fifth layer is the applications and services layer, which provides the final IoT services to users. These services may include remote monitoring, control, alerts, analytics, reporting, and automation functions. The final layer is the customer layer, which represents the end users of IoT services. Customers may include individuals, private organisations, government agencies, public authorities, or industrial operators. It should be noted that the complete value chain is not required in all IoT deployments. In some cases, IoT devices may connect directly to the platform or server

Received: *02-07-2026 -* ***Accepted:*** *01-09-2026 -* ***Published:*** *07-09-2026*

without using a separate gateway. This depends on the device capability, communication technology, network architecture, and service requirements.

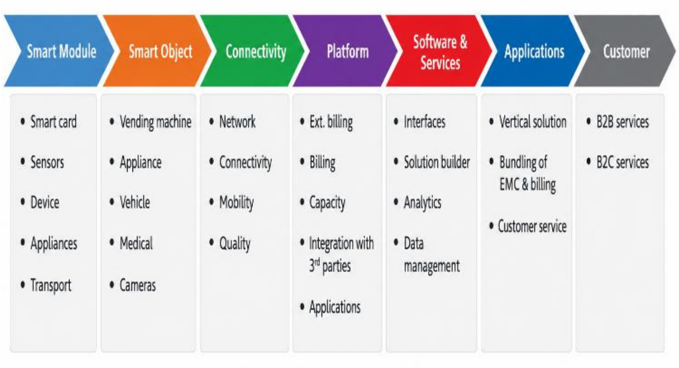

Figure. 2. IoT Value Chain

The Regulatory Framework

The proposed regulatory framework aims to establish rules and controls for the use of communication technologies that support IoT services, including mobile networks, low-power wide area non-cellular networks, satellite networks, wireless networks, and fixed wired connections. The framework is intended to support safe, reliable, and compliant IoT deployment by defining the responsibilities of the main stakeholders involved in IoT service provision. As illustrated in (Fig. 3), the operational model consists of three main parties: the IoT Network Operator, the IoT Service Provider, and the End User.

Alignment with International EMC and IoT Regulatory References

The proposed framework is not intended to replace established EMC standards or international IoT recommendations. Rather, it provides a complementary regulatory structure that connects technical EMC compliance with IoT application classification, stakeholder responsibility, deployment context, and risk level. International EMC references, particularly the IEC 61000 family [48], provide essential foundations for electromagnetic compatibility assessment, including environmental considerations, emission control, immunity requirements, and testing procedures. IEC also indicates that generic EMC standards are used for products operating in a defined EMC environment when no specific product EMC standard exists. More recently, IEC 61000-6-3:2026 extended the generic EMC emission requirements for residential environments to explicitly include equipment with radio functions. The revised edition also introduces magnetic-field emission requirements, including wireless power transfer functions, and extends low-voltage AC mains emission requirements over the 9 kHz–150 kHz range. These developments are particularly relevant to IoT devices deployed in residential and smart-environment applications and demonstrate the continuing evolution of EMC requirements for connected equipment [49].

Similarly, the ETSI EN 301 489 series provide EMC requirements for radio equipment and associated ancillary equipment, which is highly relevant to wireless IoT systems operating over cellular, short-range wireless, and low-power communication technologies. ETSI documents describe EN 301 489 as a multipart EMC standard for radio equipment and radio services, with different parts addressing specific categories of radio equipment [50]. Recent European regulatory developments further demonstrate the importance of risk-aware EMC assessment for wireless equipment. Commission Implementing Decision (EU) 2025/893 includes several EN 301 489 standards relevant to IoT communication technologies, including EN 301 489-3 V2.3.2 for short-range devices, EN 301 489-17 V3.3.1 for broadband and wideband data transmission systems, and EN 301 489-52 V1.3.1 for cellular communication equipment. The Decision also identifies limitations in some harmonised standards, including incomplete treatment of emissions below 9 kHz and restrictions associated with the use of certain performance criteria. These developments reinforce the need for regulatory assessment that considers deployment conditions and risk rather than relying only on basic equipment conformity [51].

From an IoT perspective, ITU-T Y.2060, also known as ITU-T Y.4000, provides a broad conceptual reference for the Internet of Things by defining its scope, fundamental characteristics, high-level requirements, reference model, ecosystem, and business models [52]. However, such international references are generally not designed to provide an integrated regulatory classification that links EMC and EMI risks with IoT application sectors, device communication structures, connection methods, stakeholder responsibilities, deployment approval, and post-deployment monitoring. Recent development within the ITU-T Y.4000 series is also demonstrated by ITU-T Y. Sup85 (2025), which presents IoT-based smart aquaculture use cases and illustrates the continuing expansion of IoT applications into specialised operational environments [53]. The proposed framework builds on these international references by linking EMC requirements with IoT application risk, deployment conditions, and regulatory controls. Low-risk consumer devices may require basic EMC compliance, while healthcare, transportation, industrial, and public-infrastructure applications may require stronger immunity assessment, spectrum coordination, deployment approval, and monitoring. To position the proposed framework against established international references, (Table 1) provides a concise comparison with widely used EMC and IoT references.

***Received:** 02-07-2026 - **Accepted:** 01-09-2026 - **Published:** 07-09-2026*

https://doi.org/10.54361/ajmas.269913

Table 1. Positioning of the proposed framework in relation to international EMC and IoT references

Reference	Main focus	Corresponding element in proposed framework
IEC 61000 family	EMC environment, emissions, immunity, and testing.	Device certification, immunity assessment, risk-based EMC classification.
ETSI EN 301 489 series	EMC requirements for radio equipment.	Wireless-device compliance, spectrum/coexistence assessment.
ITU-T Y.4000 or Y.2060	IoT architecture, ecosystem and requirements.	Stakeholder roles, connection methods, application classification
Proposed framework	EMC/EMI regulatory governance for IoT	Integrates technical compliance with risk level, deployment approval, and monitoring

(Table 1) shows how the proposed framework relates to the main international references. IEC 61000 supports emission and immunity assessment, ETSI EN 301 489 addresses EMC requirements for radio equipment, and ITU-T Y.4000/Y.2060 provides the broader IoT architecture and stakeholder context. The proposed framework combines these elements with application risk, stakeholder responsibility, deployment approval, and post-deployment monitoring. Recent European regulation also demonstrates that regulatory requirements for connected radio equipment are expanding beyond conventional EMC compliance. Under the EU Radio Equipment Directive, cybersecurity requirements apply to relevant internet-connected radio equipment, including requirements related to network protection, privacy, and protection from fraud [54]. Although these requirements address cybersecurity rather than EMC, they illustrate the broader regulatory trend toward risk-based and lifecycle-oriented governance of connected devices.

Operational Model

The proposed IoT service delivery model involves three primary stakeholders: the IoT network operator, IoT service provider, and end user. Other parties may include equipment manufacturers, system suppliers, application developers, platform providers, regulatory authorities, and utility providers. Recent ITU-T frameworks also recognise the importance of service providers and broader stakeholder participation in IoT deployment [55]. Within the Internet of Things (IoT) ecosystem, three primary stakeholders can be distinguished. The IoT network operator is responsible for establishing, operating, and maintaining the telecommunications infrastructure that enables IoT connectivity. This infrastructure may encompass cellular networks, low-power wide-area networks (LPWAN), satellite links, wireless systems, or fixed wired communication platforms. The IoT service provider delivers IoT services to end users in exchange for a fee. These users may include individuals, companies, organizations, or public authorities.

Service providers typically rely on networks established by licensed IoT network operators and may contract with additional partners to support specific layers of the IoT system, such as the application or platform layer. Despite these collaborations, the service provider retains ultimate responsibility for the quality, reliability, and compliance of the services delivered. Finally, the end user is the individual or legal entity that contracts with the IoT service provider to obtain services. End users may range from private individuals and companies to government bodies, public institutions, and industrial organizations. Their role is central, as they define the demand and practical applications that drive IoT service development and deployment. Broader stakeholder engagement is particularly important in smart-city and public-infrastructure environments. ITU-T Y. Sup34 identifies stakeholders such as governments, utility providers, telecommunications operators, industry organisations, citizens, and standards bodies [56]. Recent ITU-T work also demonstrates the role of IoT-based communication and ICT infrastructure in supporting coordinated public-health emergency management [57]. Therefore, effective implementation of the proposed framework requires cooperation among network operators, service providers, end users, manufacturers, regulators, and other relevant stakeholders, particularly for compliance, spectrum management, deployment approval, monitoring, and corrective action.

Received: *02-07-2026 -* ***Accepted:*** *01-09-2026 -* ***Published:*** *07-09-2026*

https://doi.org/10.54361/ajmas.269913

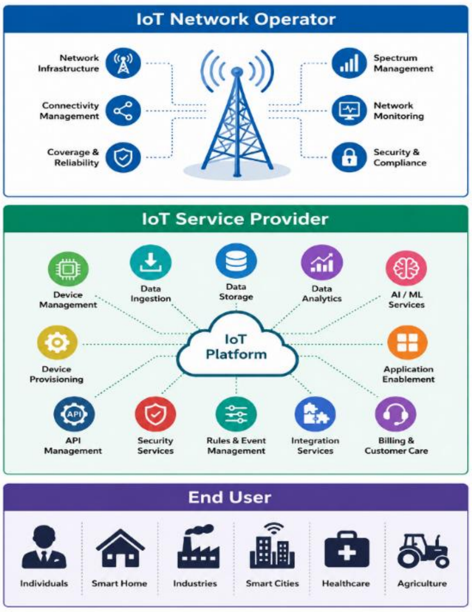

Figure 3. Operational model of the proposed regulatory framework

Regulatory Implementation Mechanism

The proposed framework can be implemented through a staged regulatory mechanism that begins before device deployment and continues throughout the operational lifetime of the IoT service. This mechanism is intended to ensure that EMC and EMI risks are considered not only during device certification, but also during network planning, service operation, and post-deployment monitoring. In the first stage, IoT devices should be assessed according to their communication technology, operating frequency, transmitter and receiver structure, intended application domain, and expected deployment environment. This stage supports early identification of potential interference risks and determines whether basic EMC compliance is sufficient or whether additional immunity assessment is required. In the second stage, the IoT service provider and network operator should define the deployment conditions, including spectrum use, device density, communication range, coexistence with nearby wireless systems, and the sensitivity of the target environment. This stage is particularly important in healthcare facilities, industrial sites, transportation systems, and public infrastructure, where electromagnetic interference may affect service reliability or safety.

In the third stage, regulatory authorities may apply differentiated approval requirements according to the EMC risk level of the application. Low-risk consumer IoT applications may only require standard device certification, while high-risk and critical applications may require deployment approval, spectrum coordination, immunity verification, and documented operational procedures. In the fourth stage, post-deployment monitoring should be used to detect interference conditions that may not appear during laboratory testing. Monitoring may include periodic inspection, interference reporting, service reliability analysis, and corrective actions when EMI affects device performance or communication quality. This stage is essential because dense IoT environments are dynamic, and interference behaviour may change as more devices are added or as wireless usage patterns evolve. The four stages link technical assessment with stakeholder responsibilities, deployment approval, and post-deployment monitoring. This allows EMC and EMI risks to be considered throughout the lifetime of an IoT deployment rather than only during initial device certification.

Methods of Connecting IoT Devices

IoT devices can be connected through several communication methods, each selected according to application requirements, coverage area, power consumption, cost, reliability, and data-rate needs. Broadly, these methods can be classified into five categories. The first category comprises mobile networks, which include traditional cellular systems such as 3G, 4G, and 5G, where IoT connectivity is provided via mobile data SIM cards. In addition, specialized cellular IoT technologies—such as Extended Coverage GSM (EC-GSM), LTE Machine-Type Communication (LTE-M), and Narrowband IoT (NB-IoT)—have been developed to support wide coverage, low power consumption, and large-scale device connectivity. The second category is low-power wide area networks (LPWANs), which are widely used for devices requiring long-range communication, low energy consumption, and low data rates. LPWAN technologies are particularly suited for sensors and monitoring devices deployed in smart cities, agriculture, environmental monitoring, and utility services. The third category involves satellite networks, which provide wide-area coverage in remote regions, rural areas, maritime environments, and across multiple countries.

Satellite IoT enables sensor connectivity via satellite links, with recent innovations such as Satellite NB-IoT expanding opportunities where terrestrial networks are unavailable. The fourth category consists of wireless networks, particularly short-range Wireless Personal Area Networks (WPANs) such as Bluetooth, Bluetooth Low Energy, ZigBee, and Z-Wave, which are common in smart homes and low-power applications. Wireless Local Area Networks (WLANs), such as Wi-Fi, provide broader coverage and higher data rates, making them suitable for smart TVs, smart speakers, industrial monitoring,

***Received**: 02-07-2026 - **Accepted**: 01-09-2026 - **Published**: 07-09-2026*

https://doi.org/10.54361/ajmas.269913

and office environments. Finally, fixed wired lines remain important in IoT systems requiring high reliability, low latency, and stable connectivity. Ethernet-based technologies are often preferred in industrial environments due to their resistance to wireless interference and predictable performance. While wireless IoT technologies continue to expand rapidly, wired communication is expected to remain critical in many industrial and mission-critical applications.

IoT application classification

IoT applications can be broadly classified into five categories according to their nature of use. The first category is consumer IoT applications, which encompass wearable devices, smart home systems, home automation, energy and water management solutions, and intrusion detection systems. These applications are primarily designed to enhance user comfort, convenience, safety, and energy efficiency. The second category is commercial IoT applications, including transportation services, fleet management, surveillance and monitoring systems, asset tracking, and connected-vehicle services operated in commercial contexts. Their primary role is to support business operations, improve monitoring, and enable more informed decision-making. The third category is industrial IoT applications, which involve digital industrial control systems, smart agriculture, equipment monitoring, predictive maintenance, and process automation. These systems monitor parameters such as temperature, oxygen levels, gas flow, and equipment condition, while also supporting automatic fault detection, diagnosis, control, and emergency response. The fourth category is infrastructure IoT applications, commonly deployed in smart city systems. Examples include traffic monitoring, environmental sensing, pollution detection, irrigation control, smart lighting, parking management, and waste management. These applications enhance the efficiency, sustainability, and reliability of public infrastructure. Finally, governmental IoT applications provide services directly to citizens, such as e-health, utilities (water, electricity, gas), transportation, education, emergency response, and public service delivery. These applications are particularly significant because they are closely tied to community welfare and public service provision.

IoT Device Classification

IoT devices can also be classified according to the complexity of their transmitter and receiver structures. Based on this classification, IoT and cyber-physical devices can be divided into three main classes:

1) Single Transmitter and Receiver Pair Devices: These devices have simple communication structures and include examples such as GPS receivers and RFID tags.
2) Single Input Single Output Devices: Single input single output devices use one transmit and one receive path. Examples include Bluetooth, Bluetooth Low Energy, ZigBee, and Narrowband IoT devices.
3) Multiple Input Multiple Output Devices: More advanced IoT devices may use multiple input multiple output structures to improve communication performance, reliability, and capacity. Examples include Wi-Fi, 4G-LTE, 5G and beyond, and WiMAX-based devices.

Risk-Based IoT EMC Classification

To strengthen the proposed regulatory framework, IoT applications can be classified by their EMC and EMI risk levels. Since IoT applications have different safety and reliability requirements, a risk-based EMC classification is necessary. Low-risk applications may only require basic EMC compliance and device certification, while high-risk and critical applications may require stricter EMC immunity testing, spectrum coordination, deployment approval, and post-deployment monitoring. (Table 2) presents the proposed risk-based IoT EMC classification. The table categorises IoT applications into low, medium, high, and critical risk levels based on the application area, possible EMI impact, and recommended regulatory requirements. This classification helps regulatory authorities apply suitable EMC control measures according to the potential safety, operational, and service reliability risks caused by electromagnetic interference. The proposed risk assessment considers two dimensions: consequence severity and interference exposure. Consequence severity represents the potential impact of EMI on safety, service continuity, equipment operation, and public welfare, and is primarily determined by the IoT application category and its operational criticality. Interference exposure represents the likelihood that an IoT deployment will experience significant electromagnetic interference. It is assessed from deployment-specific factors, including device density, operation in licensed or unlicensed spectrum, coexistence with nearby wireless systems, communication technology, and device immunity characteristics. Therefore, applications within the same general category may receive different final EMC risk levels when they operate under different electromagnetic and deployment conditions.

Table 2. Risk-based EMC classification of IoT applications

IoT application area	Examples	Possible EMI impact	Risk level	Recommended regulatory requirement
Consumer IoT	Smart lighting, smart speakers, smart-home appliances, wearable devices	Temporary service interruption or reduced user convenience	Low	Basic EMC compliance and device certification

***Received**: 02-07-2026 - **Accepted**: 01-09-2026 - **Published**: 07-09-2026*

Commercial IoT	Fleet management, commercial surveillance, asset tracking, commercial monitoring	Data delay, packet loss, or reduced service reliability	Medium	EMC compliance, spectrum-use control, and coexistence assessment
Industrial IoT	Factory monitoring, oil and gas sensors, industrial control systems, smart agriculture	Sensor malfunction, process disruption, incorrect data, or interruption of industrial operations	High	EMC immunity testing, deployment approval, spectrum/coexistence assessment, and periodic inspection
Infrastructure IoT	Smart traffic infrastructure, smart lighting, environmental monitoring, parking systems, public-infrastructure sensors	Disruption of infrastructure monitoring/control or degradation of essential services	High	Enhanced EMC immunity assessment, spectrum coordination, deployment approval, and post-deployment monitoring
Governmental IoT	E-health and wireless patient monitoring, public utilities, emergency-response systems, and safety-critical transportation/V2V/V2R services	Failure of critical services, incorrect safety information, medical device/communication malfunction, or risk to public safety	Critical	Strict EMC/immunity testing, spectrum coordination, critical-environment approval, and continuous/post-deployment monitoring

Table 3. EMC risk determination matrix

Impact of EMI	**Low**	**Medium**	**High**
Low Impact	Low	Low	Medium
Medium Impact	Low	Medium	High
High Impact	Medium	High	Critical
Critical Impact	High	Critical	Critical

Illustrative Framework Application and Validation Considerations

To illustrate how the proposed framework can support regulatory decision-making beyond simple application classification, consider a smart-meter LPWAN deployment on a hospital campus. Smart meters would normally be associated with a smart-city or infrastructure application and may initially be considered to have a medium level of consequence. However, the final EMC risk can change when the actual deployment conditions are taken into account. In this scenario, a large number of smart meters operate within a dense hospital environment using shared unlicensed spectrum. The same environment also contains wireless patient-monitoring devices, biomedical equipment, Wi-Fi systems, and other radio-based services. These conditions increase the likelihood of interference because of high device density, shared-spectrum operation, and coexistence with several wireless systems. The interference exposure can therefore be assessed as High. Using the proposed EMC risk assessment matrix, the combination of Medium EMI impact and High interference exposure results in a High EMC risk level. The regulatory treatment should therefore be stronger than would be suggested by the application category alone. Appropriate controls may include coexistence assessment, immunity evaluation, spectrum-use control, deployment approval, and post-deployment monitoring. The final EMC risk is therefore not determined by application type alone.

Deployment-specific interference exposure also affects the assigned risk level and the regulatory controls that should be applied. This is important because two deployments involving similar IoT devices may require different levels of regulatory attention when they operate in different electromagnetic environments. The practical implementation of the framework may also introduce challenges. Additional EMC assessment, certification, and post-deployment monitoring can increase compliance costs for manufacturers and IoT service providers. Regulatory authorities may require suitable testing facilities, technical expertise, and trained personnel to assess dense and complex IoT environments. Effective implementation also requires coordination among equipment manufacturers, network operators, service providers, regulators, and end users, particularly where responsibility for interference management is shared. This case shows how application characteristics and deployment-specific interference exposure can be combined to determine a final risk level and corresponding regulatory controls. However, the case is illustrative rather than an independent empirical validation. Further expert evaluation, stakeholder consultation, and real-world pilot application are required to validate and refine the proposed framework.

Received: *02-07-2026* - ***Accepted:*** *01-09-2026* - ***Published:*** *07-09-2026*

https://doi.org/10.54361/ajmas.269913

EMC and EMI Relevance of the Proposed Regulatory Framework

The regulatory framework should not only define stakeholders and connection methods but also explain how each regulatory element contributes to reducing EMC and EMI risks. (Table 4) presents the EMC and EMI relevance of the proposed regulatory framework. It links key regulatory elements, such as device certification, spectrum management, EMC immunity testing, application classification, device structure classification, stakeholder responsibilities, deployment approval, and post-deployment monitoring, with their role in reducing interference risks. This connection is important because regulatory control should not be limited to licensing or service provision only. It should also ensure that IoT devices and systems operate safely in real electromagnetic environments, particularly when many devices operate together in dense or critical environments.

Table 4. EMC and EMI relevance of the proposed regulatory framework

Regulatory element	Purpose in IoT regulation	EMC and EMI relevance
Device certification	Ensures that IoT devices meet minimum technical and safety requirements before deployment.	Reduces the risk of non-compliant devices causing electromagnetic interference.
Spectrum management	Controls the use of licensed and unlicensed frequency bands.	Reduces interference between devices operating in the same or adjacent frequency bands.
EMC immunity testing	Verifies that devices can operate correctly in the presence of electromagnetic disturbances.	Improves device reliability in dense and critical environments.
Application classification	Categorises IoT applications according to use, such as consumer, industrial, healthcare, and infrastructure.	Helps identify applications that require stricter EMC requirements.
Device structure classification	Classifies devices according to Tx and Rx complexity, such as single pair, SISO, and MIMO structures.	Supports suitable testing procedures based on device complexity.
Stakeholder responsibilities	Defines the roles of network operators, service providers, manufacturers, regulators, and end users.	Clarifies responsibility for compliance, monitoring, safe operation, and corrective action.
Deployment approval	Requires approval before using IoT systems in sensitive environments.	Protects hospitals, transport systems, industrial sites, and public infrastructure from unmanaged EMI risks.
Post-deployment monitoring	Monitors IoT systems after installation and during operation.	Detects EMI problems that may not appear during laboratory testing.

Conclusion and Future Work

This paper examined the regulatory implications of electromagnetic compatibility and electromagnetic interference in Internet of Things applications. The study argued that EMC and EMI issues in IoT should not be treated only as individual device compliance matters, but as system-level regulatory concerns that involve devices, networks, services, stakeholders, deployment environments, and operational monitoring. This perspective is increasingly important as IoT devices become more densely deployed across smart homes, healthcare systems, transportation networks, industrial automation, energy systems, smart cities, and public infrastructure. The main contribution of this paper is the development of a structured regulatory framework for IoT applications under EMC and EMI constraints. The framework integrates stakeholder responsibilities, IoT connection methods, application categories, device communication structures, and risk-based EMC classification within a unified regulatory perspective. It also clarifies how regulatory elements such as device certification, spectrum management, immunity assessment, deployment approval, stakeholder accountability, and post-deployment monitoring can contribute to reducing interference risks and improving service reliability.

The proposed framework also shows that IoT applications should not be regulated uniformly. Low-risk consumer applications may require basic EMC compliance and device certification, whereas industrial, healthcare, transportation, and public infrastructure

applications require stricter regulatory treatment because electromagnetic interference in these environments may affect operational continuity, safety, public services, and human well-being. Therefore, risk-based EMC classification provides a practical basis for differentiated regulatory control according to the severity of possible EMI consequences. Future work should validate the proposed framework in national regulatory contexts, particularly in Libya, through sector-based pilot studies in healthcare, transportation, industrial sites, smart-city infrastructure, and public utilities. Expert and stakeholder evaluations should also be carried out with regulators, telecommunications operators, IoT service providers, manufacturers, and critical-infrastructure stakeholders. Quantitative interference measurements, coexistence simulation,

Received: *02-07-2026 -* ***Accepted:*** *01-09-2026 -* ***Published:*** *07-09-2026*

spectrum-use analysis, and operational reliability indicators could then be used to refine the proposed risk levels and regulatory requirements.

Conflict of interest. *NIL*

References

1. Rose K, Eldridge S, Chapin L. The internet of things: an overview. Internet Soc (ISOC). 2015;80(15):1–53.
2. Abood AM, Hasan WK, Khaled H. 6LoWPAN-technical features and challenges in IoT: a review. In: 2024 IEEE 4th International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA). IEEE; 2024. p. 476–481.
3. Hasan WK, Abood AM, Habbal M. A review of blockchain-based on IoT applications (challenges and future research directions). In: 2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA). IEEE; 2020. p. 1–7.
4. Hasan WK, Alraddad A, Ashour A, Ran Y, Alkelsh MA, Ajele RA. Design and implementation smart transformer based on IoT. In: 2019 International Conference on Computing, Electronics & Communications Engineering (iCCECE). IEEE; 2019. p. 16–21.
5. Zargelin OA, Lashhab FM, Hasan WK. Localization methods based on error analysis and modeling in one dimension. In: 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). IEEE; 2020. p. 0674–0683.
6. Zargelin OA, Lashhab FM, Hasan WK. Localization methods based on error analysis and modeling in two dimensions. In: 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). IEEE; 2020. p. 0690–0699.
7. Hasan WK, Ran Y, Agbinya J, Tian G. A survey of energy efficient IoT network in cloud environment. In: 2019 Cybersecurity and Cyberforensics Conference (CCC). IEEE; 2019. p. 13–21.
8. Cheikh I, Roy S, Sabir E, Aouami R. Energy, scalability, data and security in massive IoT: current landscape and future directions. IEEE Internet Things J. 2026;13(6):10127–10163.
9. Shefer O, Myhal S. A method for developing support networks for high-density internet of things through the integration of SDN and MEC technologies. Adv Inf Syst. 2025;9(4):66–74.
10. Saban M, et al. A smart agricultural system based on PLC and a cloud computing web application using LoRa and LoRaWan. Sensors. 2023;23(5):2725.
11. Hu Y, et al. Industrial internet of things intelligence empowering smart manufacturing: a literature review. IEEE Internet Things J. 2024;11(11):19143–19167.
12. Rehman Z, Tariq N, Moqurrab SA, Yoo J, Srivastava G. Machine learning and internet of things applications in enterprise architectures: solutions, challenges, and open issues. Expert Syst. 2024;41(1):e13467.
13. Mousavi SM, Khademzadeh A, Rahmani AM. The role of low-power wide-area network technologies in Internet of Things: a systematic and comprehensive review. Int J Commun Syst. 2022;35(3):e5036.
14. Minoli D, Occhiogrosso B. Internet of things applications for smart cities. In: Internet of Things A to Z: technologies and applications. 2025. p. 297–326.
15. Bansal S, Kumar D. IoT ecosystem: a survey on devices, gateways, operating systems, middleware and communication. Int J Wireless Inf Networks. 2020;27(3):340–364.
16. Mahapatra SN, Singh BK, Kumar V. A survey on secure transmission in internet of things: taxonomy, recent techniques, research requirements, and challenges. Arab J Sci Eng. 2020;45(8):6211–6240.
17. Hossain K. Study on electromagnetic interference (EMI) and electromagnetic compatibility (EMC): sources and design concept for mitigation of EMI/EMC. J Liberal Arts Humanit. 2023;4(8):68–96.
18. Jornet JM, Knightly EW, Mittleman DM. Wireless communications sensing and security above 100 GHz. Nat Commun. 2023;14(1):841.
19. Wiklundh KC. Understanding the IoT technology LoRa and its interference vulnerability. In: 2019 International Symposium on Electromagnetic Compatibility - EMC EUROPE. IEEE; 2019. p. 533–538.
20. Michalak MP, Szafrańska ME. EMC in IoT world. Przegl Elektrotechniczny. 2018;94(2):50–53. doi: 10.15199/48.2018.02.12.
21. Dionísio R, Lolić T, Torres P. Electromagnetic interference analysis of industrial IoT networks: from legacy systems to 5G. In: 2020 IEEE Microwave Theory and Techniques in Wireless Communications (MTTW). Vol 1. IEEE; 2020. p. 41–46.
22. Noor-A-Rahim M, et al. Wireless communications for smart manufacturing and industrial IoT: existing technologies, 5G and beyond. Sensors. 2022;23(1):73.
23. Li J, Maiti A, Fei J. Features and scope of regulatory technologies: challenges and opportunities with industrial internet of things. Future Internet. 2023;15(8):256.
24. Shilpa B, Gupta HP, Jha RK, Hashmi SS. LoRa interference issues and solution approaches in dense IoT networks: a review. Telecommun Syst. 2024;87(2):517–539.
25. Hwata C, et al. Internet of Things-Based Electromagnetic Compatibility Monitoring (IEMCM) architecture for biomedical devices. Appl Sci. 2025;15(22):12337.
26. Wu J, et al. Review of the EMC aspects of Internet of Things. IEEE Trans Electromagn Compat. 2020;62(6):2604–2612.
27. Zhang H, Zhang Y, Huang C, Yuan Y, Cheng L. Spacecraft electromagnetic compatibility technologies. Springer; 2020.
28. Boyer A, Sicard E. Basis of electromagnetic compatibility of integrated circuits. Toulouse, France: Presses Universitaires du Midi; 2017.
29. Kumar K. Study and control of electromagnetic compatibility (EMC) and electromagnetic interference (EMI) in printed circuit boards. SSRN. 2025. Available from: https://ssrn.com/abstract=5501900.
30. Mariscotti A. Critical review of EMC standards for the measurement of radiated electromagnetic emissions from transit line and rolling stock. Energies. 2021;14(3):759.

Received: *02-07-2026* - ***Accepted***: *01-09-2026* - ***Published***: *07-09-2026*

https://doi.org/10.54361/ajmas.269913

31. Abbasi IA, Shahid Khan A. A review of vehicle to vehicle communication protocols for VANETs in the urban environment. Future Internet. 2018;10(2):14.
32. Naeem MA, et al. Vehicle to everything (V2X) communication protocol by using vehicular ad-hoc network. In: 2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP). IEEE; 2020. p. 384–388.
33. Sheikh MS, Liang J, Wang W. A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs). Sensors. 2019;19(16):3589.
34. Guerrero-Ibáñez J, Zeadally S, Contreras-Castillo J. Sensor technologies for intelligent transportation systems. Sensors. 2018;18(4):1212.
35. Malik A, Rao M. Radio frequency interference, its mitigation and its implications for the civil aviation industry. Electronics. 2025;14(12):2483.
36. Qi Y, Wu J, Gong G, Fan J, Orlandi A, Yu W, et al. Review of the EMC aspects of Internet of Things. IEEE Trans Electromagn Compat. 2018;60(5):1152–1160.
37. Masoudi M, Azari A, Yavuz EA, Cavdar C. Grant-free radio access IoT networks: scalability analysis in coexistence scenarios. In: 2018 IEEE International Conference on Communications (ICC). IEEE; 2018. p. 1–7.
38. Azari A, Stefanović Č, Popovski P, Cavdar C. Energy-efficient and reliable IoT access without radio resource reservation. IEEE Trans Green Commun Netw. 2021;5(2):908–920.
39. Tito-Lara M, Domínguez-Limaico HM, Maya-Olalla E, Cuzme-Rodríguez F. Inter-protocol interference impact of LoRaWAN on IEEE 802.11ah in a simulation environment. Sensors. 2025;25(22):6924.
40. Wiklundh K, Stenumgaard P. Internet of Things – future EMC challenges. Stockholm, Sweden: Swedish Defence Research Agency (FOI); 2018. Report No.: FOI-R--4550--SE.
41. International Telecommunication Union. Recommendation ITU-T K.136: electromagnetic compatibility requirements for radio telecommunication equipment. Geneva, Switzerland: ITU-T; Nov 2022.
42. Ismail NL, Kassim M, Ismail M, Mohamad R. A review of low power wide area technology in licensed and unlicensed spectrum for IoT use cases. Bull Electr Eng Inform. 2018;7(2):183–190.
43. Zhang H, Di B, Bian K, Song L. IoT-U: cellular Internet-of-Things networks over unlicensed spectrum. IEEE Trans Wireless Commun. 2019;18(5):2477–2492.
44. Harinda E, Wixted AJ, Qureshi A-U-H, Larijani H, Gibson RM. Performance of a live multi-gateway LoRaWAN and interference measurement across indoor and outdoor localities. Computers. 2022;11(2):25.
45. Ismail D, Rahman M, Saifullah A. Low-power wide-area networks: opportunities, challenges, and directions. In: Proceedings of the workshop program of the 19th International Conference on Distributed Computing and Networking. 2018. p. 1–6.
46. Ngwenyama PL, Webber-Youngman RC. Recent advances, challenges and future trends for the applications of low power wide area networks (LPWANs) technologies in underground mines. Int J Min Reclam Environ. 2025;39(8):547–599.
47. Cheng W, Cui H, Yu H. ILA-CSMA: hybrid sensing and adaptive fair backoff for large-scale LoRa networks. Sensors. 2026;26(11):3593.
48. International Electrotechnical Commission. IEC 61000 series: electromagnetic compatibility standards. Geneva, Switzerland: IEC; [cited 2026 Jun 7]. Available from: https://www.iec.ch/generic-emc-standards.
49. International Electrotechnical Commission. IEC 61000-6-3:2026, electromagnetic compatibility (EMC) – Part 6-3: generic standards – emission standard for equipment in residential locations. 4th ed. Geneva, Switzerland: IEC; Apr 2026.
50. European Telecommunications Standards Institute. ETSI EN 301 489-1 V2.2.3: electromagnetic compatibility standard for radio equipment and services, Part 1: common technical requirements. Sophia Antipolis, France: ETSI; 2019.
51. European Commission. Commission Implementing Decision (EU) 2025/893 of 14 May 2025 amending Implementing Decision (EU) 2022/2191 as regards harmonised standards for digital enhanced cordless telecommunications devices, short range devices, satellite systems, broadband and wideband data transmission systems, international mobile telecommunication systems, aeronautical and meteorological radars, 5 and 6 GHz WAS/RLAN equipment, wireless digital video links, and advanced surface movement guidance and control systems. Off J Eur Union. 2025 May 15;L 2025/893.
52. International Telecommunication Union. Recommendation ITU-T Y.4000/Y.2060: overview of the Internet of things. Geneva, Switzerland: ITU; 2012.
53. International Telecommunication Union. ITU-T Y.4000-series – use cases of Internet of Things (IoT)-based smart aquaculture. ITU-T Supplement 85. Geneva, Switzerland: ITU; Jan 2025.
54. European Commission. Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f). Off J Eur Union. 2022 Jan 12;L 7:6–10.
55. International Telecommunication Union. Recommendation ITU-T Y.4228: requirements and framework of industrial IoT (IIoT) infrastructure for smart manufacturing. Geneva, Switzerland: ITU-T; Aug 2024.
56. International Telecommunication Union. ITU-T Y.4000 series – smart sustainable cities – setting the stage for stakeholders' engagement. ITU-T Supplement 34. Geneva, Switzerland: ITU; Jul 2020.
57. International Telecommunication Union. Recommendation ITU-T Y.4233: information and communication technology implementation framework for smart public health emergency management in smart and sustainable cities. Geneva, Switzerland: ITU-T; Jan 2025.

Received*: 02-07-2026 -* ***Accepted****: 01-09-2026 -* ***Published****: 07-09-2026*