future internet

MDPI

Review

Overview of Protocols and Standards for Wireless Sensor Networks in Critical Infrastructures

Spyridon Daousis [1], Nikolaos Peladarinos [1], Vasileios Cheimaras [1], Panagiotis Papageorgas [1,2,*], Dimitrios D. Piromalis [1] and Radu Adrian Munteanu [2]

[1] Department of Electrical and Electronics Engineering, University of West Attica, 12244 Athens, Greece; sdaousis@uniwa.gr (S.D.); npeladarinos@uniwa.gr (N.P.); vcheimaras@uniwa.gr (V.C.); piromali@uniwa.gr (D.D.P.)
[2] Department of Electrotechnics and Measurements, Technical University of Cluj-Napoca, 400114 Cluj-Napoca, Romania; radu.a.munteanu@ethm.utcluj.ro
* Correspondence: ppapag@uniwa.gr

Abstract: This paper highlights the crucial role of wireless sensor networks (WSNs) in the surveillance and administration of critical infrastructures (CIs), contributing to their reliability, security, and operational efficiency. It starts by detailing the international significance and structural aspects of these infrastructures, mentions the market tension in recent years in the gradual development of wireless networks for industrial applications, and proceeds to categorize WSNs and examine the protocols and standards of WSNs in demanding environments like critical infrastructures, drawing on the recent literature. This review concentrates on the protocols and standards utilized in WSNs for critical infrastructures, and it concludes by identifying a notable gap in the literature concerning quality standards for equipment used in such infrastructures.

Keywords: critical infrastructures; wireless sensor networks; protocols; standards

Citation: Daousis, S.; Peladarinos, N.; Cheimaras, V.; Papageorgas, P.; Piromalis, D.; Munteanu, R.A. Overview of Protocols and Standards for Wireless Sensor Networks in Critical Infrastructures. *Future Internet* **2024**, *16*, 33. https://doi.org/10.3390/fi16010033

Academic Editor: Ping Wang

Received: 26 December 2023
Revised: 13 January 2024
Accepted: 19 January 2024
Published: 21 January 2024

1. Introduction

The present era is filled with global challenges and radical changes in the daily life of the average person. From the year 2010 to 2023, significant global crises have occurred, such as economic crises, pandemics, major climate change-induced disasters, and war conflicts. However, where the economy can sustain a considerable impact is when all these adverse phenomena converge on a critical infrastructure. Disruptions to critical infrastructure can lead to severe economic consequences and substantial harm to the welfare of citizens, particularly the disadvantaged. The economic and social impacts of critical infrastructure disruption primarily result from the loss of the services they provide rather than the cost of physical damages to the assets themselves. For instance, direct damages from disasters to power generation and transport infrastructures are estimated at USD 18 billion annually in low- and middle-income countries globally. However, the estimated cost of the associated service disruptions (energy and transport) ranges from USD 391 billion to USD 647 billion, making it at least 20 times larger. The United Nations Office for Disaster Risk Reduction's report titled "Making Critical Infrastructure Resilient" [1] emphasizes the impact of disasters on critical infrastructures in Europe and Central Asia. According to the Sendai Framework for Disaster Risk Reduction, 1889 infrastructure assets in 20 countries suffered damage in 2018, resulting in economic losses exceeding USD 3 billion. Climate change intensifies these risks, affecting extreme weather events, droughts, and floods, and particularly impacting the energy, transportation, and water sectors. Predictions indicate a 60% increase in damages due to extreme weather events in the region over the next 30 years [1]. Responding to these challenges, the U.S. Department of Agriculture is investing USD 285 million in critical infrastructure [2]. Additionally, the

U.S. Department of Homeland Security, Israel National Cyber Directorate, and Binational Industrial Research and Development Foundation (BIRD Foundation) invested USD 3.85 million in critical infrastructure cybersecurity projects [3]. The European Investment Bank Group has pledged EUR 8 billion for security investments until 2027, focusing on military mobility, space, green security, and critical infrastructure [4]. Siemens announced a USD 150 million investment in a high-tech manufacturing plant to support American data centers and critical infrastructure [5]. This review seeks to delve into the realm of critical infrastructure, specifically examining the integration of wireless sensor networks within these crucial systems. The review follows a systematic approach, meticulously scrutinizing the protocols employed in wireless sensor networks for critical infrastructure. It places a keen focus on unraveling the intricacies of security standards embedded within these networks, shedding light on the protective measures implemented. Furthermore, this review navigates through the landscape of manufacturing standards, emphasizing the pivotal considerations necessary in delivering components destined for integration into such networks. This comprehensive exploration aims to unravel the nuanced layers of wireless sensor network implementation in critical infrastructure, from protocol intricacies to robust security and manufacturing precision.

This document's structure can be refined as follows: Section 2 delves into an in-depth study of critical infrastructures at a global level, categorizing them comprehensively. Section 3 analyzes the technological applications of WSNs, focusing on the essential protocols and standards required for their deployment in critical infrastructures. Section 4 presents the methodology used for the bibliographic review and illustrates the results through diagrams. Finally, Section 5 engages in a discussion, studying the results obtained from the bibliographic research.

2. Critical Infrastructures

2.1. Critical Infrastructure Definition

The term critical infrastructure refers to the physical and virtual assets, systems, and networks that are crucial for the functioning of a society. These infrastructures are considered vital due to their significant impact on national security, economic stability, and public health and safety. Their incapacitation, destruction, or disruption can have severe consequences, leading to societal vulnerabilities and adverse effects on citizens. Critical infrastructure is a fundamental component of modern society, encompassing assets, systems, and networks that are essential for the maintenance of vital societal functions. The protection and resilience of critical infrastructure is paramount to ensuring citizens' security and well-being [6,7].

2.1.1. The European Union Perspective

In the European Union, the European Program for Critical Infrastructure Protection (EPCIP) provides the overall framework for activities aimed at enhancing the protection and resilience of critical infrastructures across all EU member states. The program acknowledges that threats to critical infrastructure extend beyond terrorism and include criminal activities, natural disasters, and accidents. It adopts an all-hazards cross-sectoral approach to effectively address these threats. The EPCIP is supported by the Directive on European Critical Infrastructures, which identifies and designates European critical infrastructures (ECIs) in the energy and transport sectors. The directive mandates the preparation of operator security plans by the owners/operators of designated ECIs, promoting advanced business continuity planning. It also emphasizes the appointment of security liaison officers to facilitate coordination between the owner/operator and the responsible national authority for critical infrastructure protection [6,7].

2.1.2. The United States Perspective

In the United States, Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience outlines the national policy for strengthening and maintaining secure, functioning, and resilient critical infrastructure. The directive identifies 16 sectors that are crucial to national security, economic well-being, and public health and safety. These sectors range from energy, transportation, and communication to healthcare, government facilities, and information technology. Through the Cybersecurity and Infrastructure Security Agency (CISA), the US government leads efforts to enhance the security and resilience of critical infrastructure sectors. CISA works collaboratively with public and private sector stakeholders, providing strategic direction, developing risk management frameworks, and offering tools and resources to improve sector-specific security measures [8].

2.2. Critical Infrastructure Sectors

Critical infrastructure sectors are categorized differently in different nations. Variations between countries can be explained by differences in conceptualizations of what are critical and country-specific peculiarities and traditions. Sociopolitical factors and geographical and historical preconditions determine whether a sector is deemed to be critical. As an example, the National Infrastructure Protection Plan (NIPP) in the US divided critical infrastructure into 16 sectors in 2013 [3]. On the other hand, the European Union divided critical infrastructure into 13 sectors [4], Australia into 11 sectors, and India 12 [5]. In Table 1, the differences regarding critical infrastructure sectors as addressed in six countries are shown [4–6,8]. The connection of the content of the rows of Table 1 with the content of the columns is declared by the symbol ■

Table 1. CI sectors.

Sectors	**Countries**						
	Germany	**United Kingdom**	**Japan**	**United States**	**China**	**India**	**Australia**
Banking and Finance	■	■	■	■	■	■	■
Central Government/Government Services	■	■	■	■		■	
Chemical and Nuclear Industry		■	■	■			
Emergency/Rescue Services		■		■			
Energy	■	■	■	■	■	■	■
Food/Agriculture	■	■		■			■
Health Services	■			■			■
Information Services/Media	■		■				
Military Defense/Army/Defense Facilities		■		■	■		■
Telecommunications /Public Communications		■		■	■	■	■
Transportation	■	■	■	■	■	■	■
Water (Supply)/Sewerage	■	■	■	■	■	■	■
Space		■					■
Critical Manufacturing				■			

Information and Communication Technology	■	■	■	■	■
Dams			■		
e-Government Services				■	
Strategic and Public Enterprises					■
Higher Education and Research					■

Core Sectors

Table 1 and Figure 1 in this document highlight key sectors that are essential to the modern world and that are commonly recognized across nations. These sectors include finance, central government, telecommunication, emergency/rescue services, energy, health services, food, transportation, and water supply. They are identified as core sectors due to their critical roles in society, where any significant disruption could have disastrous consequences [9]. In studies [7,8,10–13], definitions are given to clarify the above sectors and their importance to modern society.

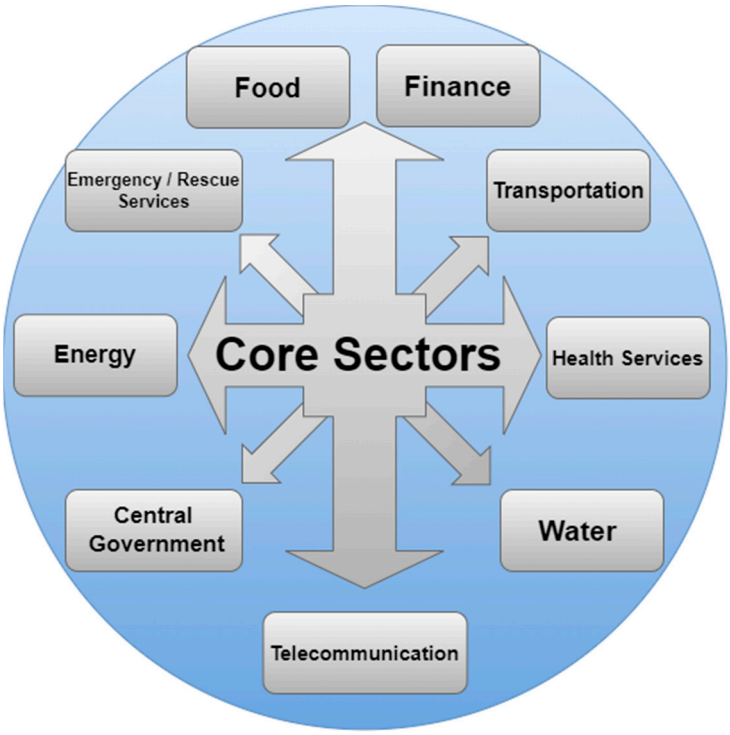

Figure 1. Core sectors of critical infrastructure.

- Finance

The financial services sector encompasses a diverse range of institutions, including depository institutions, investment product providers, insurance companies, credit, and financing organizations, as well as critical financial utilities and services that support these functions. Financial institutions vary in size and scope, ranging from massive global corporations with extensive assets and thousands of employees to community banks and credit unions serving specific localities with a smaller workforce. These financial entities offer a wide array of products that cater to customers' needs, such as individual savings accounts, financial derivatives, credit for large organizations, and investments in foreign

countries. These products enable customers to perform various financial activities, including depositing funds, making payments, providing credit and liquidity, investing for short or long terms, and transferring financial risks between parties.

- Government/Public Administration

This sector refers to the entities responsible for governing and managing essential government services and functions. These entities are vital in ensuring the smooth operation and continuity of various government processes and services that are critical to the functioning of a society and the well-being of its citizens. Public administration plays a crucial role in maintaining law and order, providing public services, managing public resources, and making policy decisions that impact the overall functioning of a country or region. In times of crisis or emergencies, the public administration sector becomes even more critical, as it coordinates disaster response efforts, ensures public safety, and implements contingency plans to minimize the impact of disruptive events on society.

- Telecommunications

Over the years, the telecommunications sector has undergone a significant transformation, evolving from traditional voice services to a multifaceted and interconnected industry. It now encompasses a broad range of services, including data transmission, internet connectivity, mobile and fixed telecommunications, satellite communication, broadcasting, and more. This diversity ensures that businesses, governments, and individuals can access and utilize critical services, contributing to economic growth and societal development. As a critical infrastructure sector, telecommunication plays a significant role in supporting other sectors' operations. It provides essential services that enable the smooth functioning of transportation systems, energy distribution networks, emergency services, healthcare facilities, financial institutions, and public administration, among others. The sector serves as a lifeline during emergencies, enabling coordination among first responders, disseminating vital information to the public, and facilitating disaster response efforts.

- Emergency/Rescue Services

The emergency services sector comprises a vast network of skilled and trained personnel dedicated to offering a wide range of prevention, preparedness, response, and recovery services in various situations. This community operates during routine activities and emergencies alike. The emergency services sector encompasses numerous facilities and equipment, involving both paid professionals and volunteers, organized primarily at federal, state, local, and government levels. The Red Cross and Red Crescent Societies, civil protection authorities, police, fire, ambulance, paramedic, and emergency medicine services, as well as specialized emergency units of organizations providing electricity, transportation, communications, and other related services, all fall under the category of emergency services.

- Energy

The energy sector plays a pivotal role in critical infrastructures worldwide. Its protection is paramount to ensure a stable and continuous energy supply, essential for the functioning of various sectors and the overall well-being of nations. The sector is composed of three interconnected segments: electricity, oil, and natural gas. The electricity segment comprises a vast network of power plants, with a mix of coal, nuclear, natural gas, hydroelectric, oil, and renewable sources. Given its interconnected nature and vital role in supporting critical operations across diverse sectors, safeguarding the energy sector is crucial to maintaining economic stability, public welfare, and overall societal resilience.

- Health Services

The health sector is a critical component of a nation's infrastructure, safeguarding all sectors of the economy from various hazards, including terrorism, infectious disease outbreaks, and natural disasters. Its significance lies in providing medical and hospital care

and supplying essential medicines, vaccines, and pharmaceuticals. The sector's ability to effectively respond to and mitigate health-related threats significantly contributes to societal well-being, economic productivity, and overall national resilience in the face of diverse challenges.

- Food

The food sector holds a paramount position among critical infrastructures. Its contribution to national security, economic stability, and public health and safety is indispensable. Comprising diverse entities, including farms, manufacturers, processors, storage facilities, restaurants, and retail establishments, the food sector establishes vital linkages with various other critical infrastructure sectors, such as water, transportation, energy, chemicals, and information technology. These interdependencies underscore the sector's significance in supporting the functionality and resilience of critical infrastructures in a country.

- Transportation

The transportation systems sector is a crucial component of critical infrastructures worldwide, serving as a key economic sector that enables the movement of people, essential commodities, and vital resources like food, water, medicines, and fuel. It encompasses various modes of transportation, each presenting its unique challenges and vulnerabilities to potential threats, ranging from accidents and human errors to deliberate malevolent actions such as sabotage and terrorist attacks. Transportation critical infrastructures can be broadly classified into subsectors such as aviation, maritime, public transport, road, and rail, and, in addition, in some countries like the USA, postal and pipeline systems. Each mode operates independently, yet their interdependencies with other critical infrastructures make effective risk assessment and management a complex task. Aviation encompasses a wide range of assets, including aircraft, air traffic control systems, and numerous airports and heliports. The road subsector encompasses highways, motor carrier systems, vast networks of roadways, bridges, tunnels, and commercial vehicles, including hazardous material carriers. The maritime transportation system covers coastlines, ports, waterways, and their intermodal landside connections. Public transport and passenger rail entail various passenger services, including buses, trains, and subways, with substantial daily passenger trips. The transportation systems sector can play a pivotal role in ensuring a secure and robust critical infrastructure landscape for nations across the globe.

- Water Supply

The water sector is an integral part of critical infrastructures worldwide, encompassing various systems that provide fresh water and manage wastewater. It plays a pivotal role in contemporary human existence, as water is one of the most essential commodities for survival, second only to air. Efficient wastewater systems are crucial in separating treated drinking water from human waste, minimizing the potential for waterborne disease outbreaks, and ensuring public health. The water sector is interconnected with other critical infrastructures, such as energy, food/agriculture, and transportation systems. In the water and wastewater systems, disruptions or dysfunctions have debilitating effects on economic security and public health and safety. Due to its crucial role in sustaining human life, society's expectations, global development, and overall human health heavily rely on efficiently operating and managing water critical infrastructures.

2.3. Critical Infrastructures and Industry 4.0

Throughout history, societies have continuously evolved, and this natural progression has significantly impacted the industrial sector. The industrial sector itself has undergone four distinct and challenging periods of transformation. The initial period, from 1784 to the mid-19th century, witnessed the introduction of steam-powered machinery, revolutionizing mechanical manufacturing. The second phase, spanning from the late 19th century to the 1970s, marked the era of electric-powered mass production, characterized

by assembly lines and division of labor. The third period, from the 1970s to the present day, witnessed remarkable advancements in electronics, information technology, and automation of complex tasks. As societies progress, the industrial sector remains at the forefront of innovation, shaping the course of human development and ushering in new opportunities and challenges. Today, humanity stands at the threshold of a new era known as the fourth industrial revolution or Industry 4.0 [14,15].

Industry 4.0 (I4.0) was initially introduced in 2011 as a strategic initiative by the German government. Since then, various other nations have followed suit with their initiatives, including the United States' Advanced Manufacturing Partnership, China's Made in China, Britain's Smart Factory, and Japan's Super Smart Society. Today, the concept of the fourth industrial revolution is being embraced by all developed countries. The essence of Industry 4.0 lies in its aim to transition from centralized production to a more flexible and self-controlled approach. This evolution is a logical outcome of the progress made in computer-integrated manufacturing and flexible manufacturing systems over the past decades and the widespread adoption of digitization in recent years. It is worth noting that the development of I4.0 solutions and technologies has not only benefited the manufacturing sector but has also had a positive impact on the service sector, where applications like big data solutions in banking and marketing have emerged [16].

As expected, critical infrastructures are interconnected with this important industrial evolution. The concept of Industry 4.0 plays a vital role in critical infrastructure, as some of its technologies are already or will become integral parts of various sectors. These technologies include industrial automation, robotics, sensors, cyber–physical systems, Industrial Internet of Things (IIoT) [17], big data, block chain, edge computing, digital twin, and artificial intelligence, which are widely considered in manufacturing and service industries [18–21]. However, the adoption of Industry 4.0 solutions in critical infrastructure also introduces potential risks that need to be carefully addressed, such as cybersecurity and reliability concerns [14,22]. A pivotal aspect of Industry 4.0 is the IIoT. The Industrial Internet of Things plays a crucial role in the advancement of critical infrastructures through the utilization of intelligent sensors, fast communication protocols, and robust cybersecurity mechanisms. The establishment and effective management of sensor networks form the foundation of IIoT, making it a significant component that profoundly influences both Industry 4.0 and critical infrastructures.

3. Communication Technologies and Wireless Sensors Networks

Over the years, both the scientific community and the industry sector have been dedicated to developing protocols and standards to ensure the efficient operation of sensor networks. Given the diversity of scenarios and requirements, it became evident that a single "golden" protocol or standard would not be sufficient. As a result, the creation of numerous distinct protocols and standards to address various needs and situations has offered a plethora of different options. A sensor network comprises interconnected small devices known as sensors and nodes, working together to collect and transmit data from their surroundings. These sensor networks find application in various fields such as military, agriculture, environmental monitoring, home automation, healthcare, automotive, industrial sectors, etc. As it becomes evident, many of the above sections are also characterized as critical infrastructure. Each field has specific requirements such as network extension, compactness, mobility (which necessitates wireless sensors with autonomous power sources), cost, and performance. Sensor networks can be categorized into wired and wireless networks, each utilizing different protocols and offering different advantages.

Wired communication technologies have played a significant role in industrial monitoring and control networks and have a significant development lead regarding wireless networks. Useful data for understanding the gap between the two technologies can be obtained from the annual research published by HMS Networks [22,23]. HMS Networks

conducts an annual assessment of the industrial network market to estimate the distribution of new nodes within factories. In Figure 2, the timeline of the industrial network market shares is shown. Both technologies at the top of the timeline—Fieldbus and Industrial Ethernet—are wired technologies; wireless networks have the lowest percentage of uses for the industrial environment. To better study the long-term development of these networks, it is useful to consider the annual growth of each technology, as depicted in Figure 3. The yearly expansion of wireless networks is consistently making significant strides. According to research conducted by HMS Networks, industrial wireless networks have experienced a remarkable 22% growth in the past year, and their market share reached 8% in 2023, marking a 1% increase from 2022. This acceleration can be attributed to the increasing introduction of wireless solutions in industrial automation, with common applications including replacing cables, enabling wireless machine access, and facilitating connectivity with mobile industrial equipment.

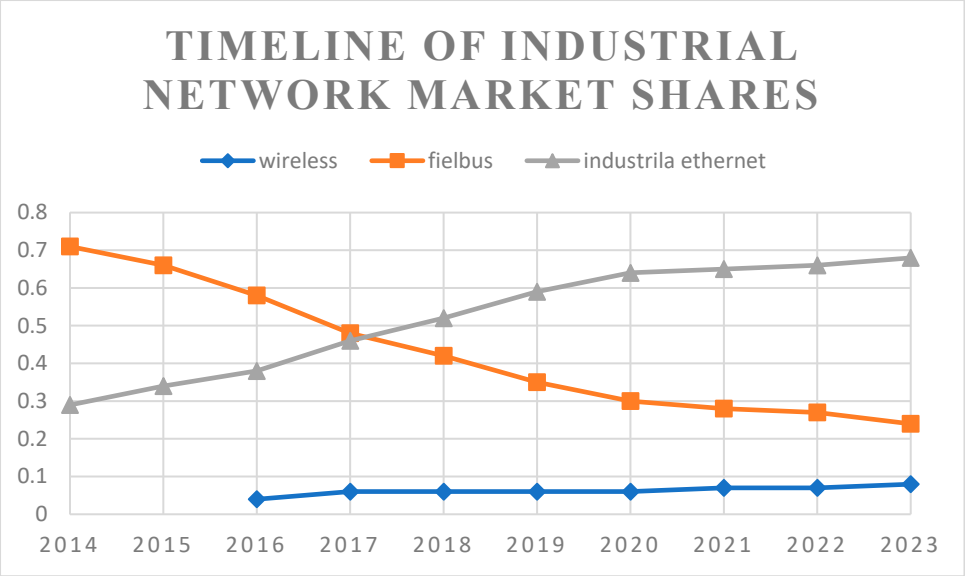

Figure 2. Timeline of industrial network market shares by HMS Networks.

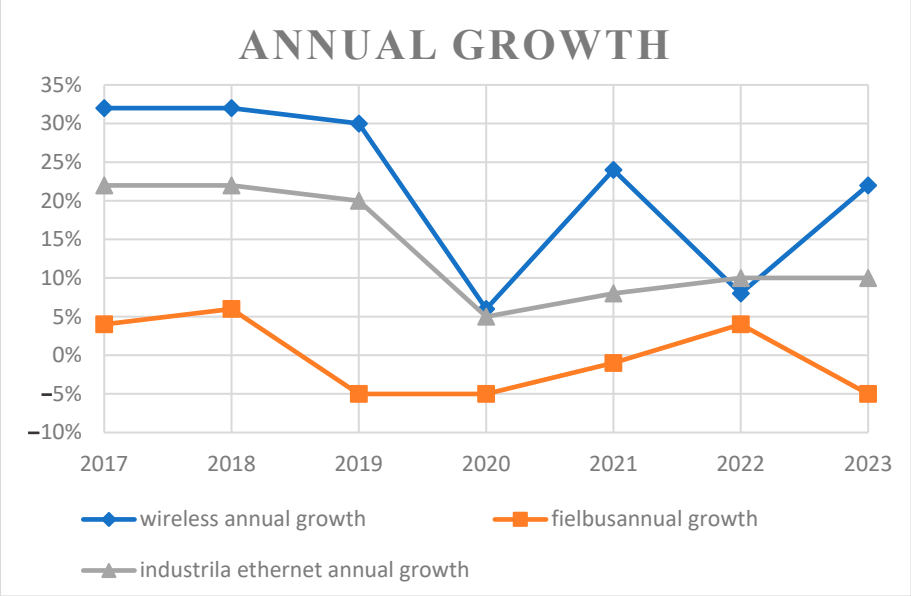

Figure 3. Timeline of annual growth of network market shares by HMS Networks.

From the preceding Figures 2 and 3, it is evident that wireless sensor networks have a promising future and are here to stay. Although technology is still evolving and has a considerable distance to cover before it can effectively compete with wired technologies in terms of market share, wireless sensor networks have been in use for many years. An early example dates back to the Cold War in the early 1960s, when silent Soviet submarines were detected using the sound surveillance system (SOSUS), which utilized acoustic sensors. These systems have since been adopted by the National Oceanographic and Atmospheric Administration (NOAA) for monitoring events in the oceans. The concept of WSNs can be traced back to the distributed sensor networks (DSN) program initiated in 1980 by the Defense Advanced Research Projects Agency (DARPA). Subsequent technological advancements in the following decades have provided the means for the development of WSNs capable of meeting and exceeding high-performance standards.

3.1. Wireless Sensors Networks Categorization

Wireless sensor networks offer versatile solutions for a variety of applications and can be categorized in several ways, each shedding light on their unique characteristics:

3.1.1. Categorized by Physical Environment

- Underground: WSNs deployed beneath the Earth's surface, often used in mining or geological monitoring.
- Terrestrial: these networks operate on land, making them suitable for a wide range of applications such as environmental sensing and smart agriculture.
- Underwater: submerged WSNs are essential for oceanographic research, aquatic habitat monitoring, and underwater exploration. Multimedia: these networks handle multimedia data and are valuable in applications like surveillance, video streaming, and multimedia content distribution.
- Mobile WSNs: mobile WSNs are dynamic and adaptable, making them ideal for scenarios like wildlife tracking, vehicular networks, or mobile healthcare solutions [23].

3.1.2. Categorized by Different Network Topologies

- Star: in a star topology, all sensors communicate directly with a central hub or gateway, offering simplicity in deployment.
- Mesh: sensors in a mesh network communicate through neighboring nodes, ensuring self-healing capabilities and redundancy.
- Tree: with a hierarchical structure, data flow from leaf nodes to a central sink node, enabling efficient data aggregation.
- Hybrid: combine elements of various topologies to strike a balance between reliability, efficiency, and network coverage [23–25].

3.1.3. Categorized by Applications

- Health monitoring: WSNs play a crucial role in healthcare, employing advanced medical sensors to monitor patients both in hospital and at home. These WSNs facilitate real-time monitoring of vital signs through wearable hardware. The health applications of WSNs encompass patient-wearable monitoring, home assisting systems, and hospital patient monitoring.
- Urban: WSNs offer diverse sensing capabilities that open the door to obtaining extensive information about a specified area, whether indoor or outdoor. WSNs serve as a versatile tool for measuring the spatial and temporal characteristics of various phenomena within urban settings, presenting numerous applications. In the urban context, WSNs find widespread use in areas such as smart homes, smart cities, transportation systems, and structural health monitoring.

- Flora and fauna: The essential aspects of both plant life (flora) and animal life (fauna) are crucial for any nation. The primaries are greenhouse monitoring, crop monitoring, and livestock farming. The illustration also highlights the prevalent types of sensors commonly employed in these applications.
- Environmental: The use of WSNs can enhance environmental applications requiring constant monitoring in challenging and distant locations. This includes subcategories like water monitoring, air monitoring, and emergency alerting, each involving specific types of sensors. The subsequent subsection delves into the examination of WSNs designed for these environmental applications.
- Military: The military pioneered WSNs, with early research (such as Smart Dust in the late 1990s) aiming at creating minuscule yet efficient sensor nodes for espionage. Subsequent technological advancements expanded WSN applications in the military, with a focus on battlefield surveillance, combat monitoring, and intruder detection. Various sensor types are now commonly employed in these military WSN applications.
- Industrial: Industrial wireless sensor networks (IWSNs) present numerous benefits for facilitating the intricate and dynamic processes within industrial settings. Thanks to their effortless setup, unrestricted mobility, and smart data routing capabilities, IWSNs are emerging as a promising communication option for industrial applications [23–26].

3.2. Standards and Protocols

Standards play a paramount role in security and in the electronic components manufacturing domain and, therefore, for critical infrastructure. Standards ensure a seamless and reliable integration of technology into essential systems. Standards in critical infrastructure are the linchpin for reliability, safety, security, innovation, and regulatory adherence, collectively contributing to the robustness of essential systems that underpin modern society. They define criteria for materials, tolerances, testing procedures, and security, aiming to achieve consistency and interoperability of electronic components. Adhering to these standards enhances product performance, longevity, and compatibility while facilitating industry-wide collaboration.

3.2.1. Standardization Organizations

In alignment with their philosophy, standardization organizations operate extensively across various developed nations, spanning a broad spectrum of scientific domains.

- IEEE (Institute of Electrical and Electronics Engineers): On 1 January 1963, the American Institute of Electrical Engineers (AIEE) and the Institute of Radio Engineers (IRE) joined forces to establish the Institute of Electrical and Electronics Engineers (IEEE). Initially, IEEE boasted 150,000 members, with 140,000 based in the United States. As the early 21st century unfolded, IEEE's influence spanned 39 societies, 130 journals, and over 300 annual conferences, with a focus on diverse areas like nanotechnologies, bioengineering, and robotics. From jet cockpits to medical imaging, electronics have become omnipresent. As of 2020, IEEE's membership exceeded 395,000 across 160 countries, solidifying its status as the largest global technical professional organization through a network of units, publications, and conferences [27].
- ISO (International Organization for Standardization): In 1946, a gathering of 65 representatives from 25 nations convened to deliberate on the future of international standardization. This culminated in the official establishment of ISO in 1947, comprising 67 technical committees. Since its inception, ISO has regularly disseminated information on its technical committees and published standards and organizational updates. Functioning as an independent non-governmental international entity, ISO boasts a membership of 169 national standardization bodies. Through collaborative

expertise, ISO facilitates the development of voluntary, consensus-driven, and globally pertinent international standards, fostering innovation and delivering solutions to worldwide challenges [28].

- CEN (European Committee for Standardization): CEN, the European Committee for Standardization, serves as a consortium uniting national standardization bodies from 34 European nations. This collaborative platform is dedicated to formulating European standards and technical documents across diverse products, materials, services, and processes. Recognized by the European Union and the European Free Trade Association, CEN, along with CENELEC and ETSI, is entrusted with the task of devising voluntary standards at the European level. In the interest of international and European standardization, CEN collaborates with CIE, aiming to leverage the knowledge and expertise within each organization through a formalized agreement [29].
- IEC (International Electrotechnical Commission): In 1906, the International Electrotechnical Commission (IEC) was established in London after a proposal at the 1904 International Electrical Congress. The congress recognized that the diversity in electrical systems worldwide was hindering progress. The IEC's inaugural meeting included representatives from multiple countries, with Lord Kelvin elected as the first president. Today, the IEC, a global non-profit organization, unites over 170 countries and oversees 20,000 experts worldwide. Celebrating its centenary in 2006, the IEC has adapted to 21st-century technological advancements, establishing new technical committees for areas like fuel cells, assessment methods for human exposure to electric and electromagnetic fields (including 5G), avionics, electronic displays, nanotechnology, marine energy generation, solar thermal electric plants, printed electronics, electrical energy storage systems, wearable electronic devices, personal e-transporters, and more. This reflects the IEC's commitment to staying current with evolving technologies and fostering standardization in diverse fields [30].
- IPC (Institute of Printed Circuits): Founded in the autumn of 1957, the Institute of Printed Circuits, or IPC, has remained committed to eliminating supply chain challenges, establishing industry standards, and fostering industry progress. As a worldwide trade association, IPC is devoted to enhancing the competitive excellence and financial prosperity of its electronics industry members. To achieve these goals, IPC will allocate resources to management improvement, technology enhancement programs, formulation of pertinent standards, and environmental conservation. IPC aspires to be a globally respected organization, recognized for leadership and its significant role in providing standards and quality programs for the electronics industry [31].

Other entities play a pivotal role in establishing and refining standards that govern diverse aspects of products, materials, services, and processes, such as ITU (International Telecommunication Union), BSI (British Standards Institution), ISA (International Society of Automation) MSS (Manufacturers Standardization Society), NEMA (National Electrical Manufacturers Association), JEDEC (Joint Electron Device Engineering Council), ANSI (American National Standards Institute), NIST (National Institute of Standards and Technology), and JEITA (Japan Electronics and Information Technology Industries Association). Their operations are not confined to a specific sector, reflecting a comprehensive approach to standardization that resonates with the global pursuit of quality, innovation, and harmonization. In numerous developed countries, these organizations serve as crucial pillars in fostering collaboration, ensuring adherence to best practices, and contributing to the advancement of standards across the scientific landscape.

The "Technology Certification for Critical Infrastructure Protection" report from the European Commission Joint Research Centre [32] emphasizes the significance of various IT security standards, with a focus on ISO/IEC 27001 [33], ISO 27002 [34] and ISO 15408 [35] standards. Additionally, it underscores the importance of standards such as the IEC 62351 [36] series and IEC 62443 [37] series, according to the European Union Agency for Cybersecurity (ENISA).

- ISO/IEC 27001

ISO/IEC 27001 stands as the globally recognized standard for information security management systems (ISMS), outlining essential requirements for ISMS compliance. Applicable to organizations of any size and across sectors, the standard offers comprehensive guidance for establishing, implementing, maintaining, and enhancing an effective information security management system. Compliance signifies that an organization has implemented a robust system to manage risks associated with data security, aligning with the best practices and principles outlined in this international standard. ISO/IEC 27001 promotes a comprehensive approach to information security, covering individuals, policies, and technology. An ISMS aligned with this standard serves as a tool for managing risks, enhancing cyber-resilience, and achieving operational excellence [33].

- ISO 27002

ISO/IEC 27002 is a global standard that guides organizations in establishing, implementing, and enhancing an ISMS with a focus on cybersecurity. Unlike ISO/IEC 27001, which outlines ISMS requirements, ISO/IEC 27002 provides best practices and control objectives for crucial cybersecurity areas such as access control, cryptography, human resource security, and incident response. This standard acts as a practical guide for organizations seeking to fortify their information assets against cyberthreats. Adhering to ISO/IEC 27002 recommendations enables companies to adopt a proactive approach to cybersecurity risk management, safeguarding critical information from unauthorized access and potential loss [34].

- ISO 15408

The ISO/IEC 15408 series facilitates the comparability of independent security assessments by establishing a common set of requirements for the security functionality and assurance measures applied to IT products during evaluations. These products may be implemented in hardware, firmware, or software. Evaluations provide confidence that the security features and assurance measures meet defined requirements, aiding consumers in determining whether the IT products meet their security needs. The series serves as a valuable guide for the development, evaluation, and procurement of IT products with security functionality. Its intentional flexibility allows various evaluation approaches for different security properties of diverse IT products, with users cautioned to avoid misuse that could lead to meaningless results [35].

- IEC 62351 series

IEC 62351—a set of standards focusing on the security of power system control centers and communication networks—emphasizes integrating security measures from the inception of any system. Even legacy infrastructures can adopt security-by-design principles, accounting for cyberthreats during design, development, and retrofitting. This series provides detailed guidance for safeguarding energy management systems and secure energy data exchange. Covering protocols like IEC 61850, IEC 60870-5, IEC 60870-6, IEC 61970, and IEC 61968, it addresses cyberthreats and offers countermeasures. The standard advocates a risk management approach, emphasizing continuous monitoring, testing, and implementing measures beyond traditional firewalls and encryption. IEC 62351 enhances power grid resilience, ensuring a reliable energy supply amid evolving cyberthreats [36].

- IEC 62443 series

The IEC 62443 series was created to safeguard industrial automation and control systems (IACS) across their lifespan, featuring nine standards, technical reports, and technical specifications. Initially designed for the industrial process sector, these standards (crucial for critical infrastructures like power, energy, and transport) now apply to diverse industries. Unlike IT standards, IEC 62443 is tailored to the specific performance, availability, and lifetime needs of IACS and operational technology (OT) environments. It recognizes the distinctive consequences of cyberattacks on critical infrastructure, going beyond economic impacts to potential environmental threats and risks to public health.

Grounded in industry best practices and achieved through consensus, these international standards offer a comprehensive approach. Implementing IEC 62443 addresses technology, work processes, countermeasures, and employee training, thus reinforcing security and reducing costs [37].

It is important to note that, while there is a plethora of references and suggestions for standards in the concept of cybersecurity in critical infrastructures, the hardware does not have the same popularity. Nevertheless, we must mention that IPC-A-610 and J-STD-001 by IPC, along with IEC TS 62686-1:2020, are notable and suitable in this context. J-STD-001 emphasizes the importance of process control methodology and sets acceptance criteria for soldered connections. On the other hand, IPC-A-610 provides visual acceptance standards for electrical assemblies. J-STD-001 covers material methods and acceptance criteria, whereas IPC-A-610 focuses on visual standards aligned with IPC and other relevant specifications. The IPC standards are characterized by three classes (with class number 3 as the highest level of quality) for high-reliability electronics with extended lifecycles and fail-proof quality that address applications like aerospace, military, and medical fields; both standards incorporate common requirements like coating uniformity, marking, cleaning, and conductor damage. Additionally, IEC TS 62686-1:2020 outlines minimal requirements for commercial off-the-shelf (COTS) integrated circuits and general purpose semiconductors for aerospace, defense, and high-performance (ADHP) applications [38–40].

3.2.2. Wireless Protocols

The cellular Internet of Things (IoT) refers to a category of communication technologies and protocols that enable Internet connectivity for a wide range of IoT devices using cellular networks. It allows these IoT devices to transmit and receive data over cellular infrastructures, which include technologies such as 2G, 3G, 4G, and 5G. Cellular IoT technologies encompass various standards and protocols designed for connecting IoT devices via cellular networks. Second-generation technology introduced digital voice encoding, enabling more efficient use of the radio spectrum compared with its analog predecessor. It enabled text messaging (SMS) for the first time, revolutionizing communication. In 1991, the European standard GSM (global system for mobile communications) became a global benchmark for 2G, ensuring interoperability and driving widespread adoption. This technology laid the foundation for mobile data services, paving the way for future generations of cellular networks and the evolution of modern smartphones and mobile data connectivity. The history of 3G cellular technology is a pivotal chapter in the evolution of mobile communication. Emerging in the early 2000s, 3G (or third-generation technology) marked a substantial advancement over its predecessors. It introduced high-speed data transmission, enabling not only voice calls but also video calls and mobile internet access. The rollout of 3G networks fostered the proliferation of mobile data services, leading to the birth of mobile applications, video streaming, and mobile browsing. Notable standards like UMTS (universal mobile telecommunications system) and CDMA2000 played key roles in shaping 3G. This technology laid the foundation for the mobile internet era, revolutionizing how we communicate and access information on our portable devices. Although they offer a lot for their technological development today, by the year 2025, both technologies will have been abolished as they will be considered obsolete.

- 4G Cellular (Fourth Generation)

Fourth-generation cellular technology was a watershed moment in mobile communication. Launched in the late 2000s, 4G (or fourth-generation technology) represented a remarkable leap forward from its 3G predecessor. It introduced unprecedented data speeds and low latency, ushering in the era of high-definition video streaming and faster mobile internet. The long-term evolution (LTE) standard emerged as a global benchmark for 4G, enabling seamless data connectivity. Fourth-generation technology revolutionized communications, serving as the foundation for the mobile app ecosystem, enabling high-

quality voice and video calls, and driving the widespread adoption of smartphones. Its impact extended beyond personal communication, supporting the growth of IoT and the development of smart cities and connected devices.

Fourth-generation technology has found applications in WSNs, particularly in scenarios demanding higher data rates and lower latency. In WSNs designed for applications such as real-time environmental monitoring or industrial automation, 4G provides a significant advantage. This is especially critical in situations where rapid response is essential. The paper of Yang Liu [41] discusses a novel approach in addressing the critical issue of water pipeline leakage detection. Water supply networks, as we mentioned, are one of the most common critical infrastructures for sustaining human life and the environment, yet billions of cubic meters of water are lost annually due to leaks. To combat this problem, the authors proposed an innovative system that combines machine learning and WSNs to collect data and utilizes 4G networks for remote data transmission, aiming to efficiently identify water pipeline leaks. Similarly, study [42] addressed the pressing issue of water quality monitoring at the Weija dam of the Greater Accra Region of Ghana. A set of smart water sensors and smart water ion sensor devices from Libelium were strategically placed at the Weija dam intake. The sensors continuously measured physical and chemical parameters, including pH, conductivity, calcium levels, temperature, fluoride, and dissolved oxygen. The real-time data gathered by these sensors were efficiently transmitted over a 4G network. The data acquisition system was specifically designed to send water quality data to a monitoring center using a 4G communication infrastructure. In cases where the data needed to be sent but no connection was available, the 4G communication module would enter a deep sleep mode to conserve energy. It would then periodically attempt to establish a 4G connection until it successfully transferred the data when the connection was restored.

- 5G Cellular (Fifth Generation)

As 4G networks reached their capacity limits, there was a growing need for a faster, more efficient, and more robust network. The proliferation of IoT devices, smart cities, autonomous vehicles, and augmented reality applications demanded a new solution. Fifth-generation technology is designed to deliver faster data speeds, lower latency, and massive device connectivity. It utilizes higher radio frequencies and small-cell technology to provide faster data rates, often in the gigabit range, and can simultaneously connect a vast number of devices, something that makes it ideal for the IoT.

An additional study that has been carried out for the development of 5G is that of Charles Rajesh Kumar. J et al. [43], whose article focuses on the integration of new wireless networking technologies, particularly 5G, into smart grids to address the increasing energy demands in the modern smart grid era, with a focus on the Kingdom of Saudi Arabia. The authors emphasize the need for distributed energy generation and efficient energy storage solutions to effectively meet these requirements. The integration of smart grid technologies, including advancements in WSNs and embedded systems, enables the cost-effective implementation of smart grid monitoring and automation systems. These technologies are crucial for transitioning from traditional centralized grids to modern decentralized grids that can efficiently manage energy production and consumption. The article highlights the need for a secure and efficient telecommunications network to manage various elements of the smart grid, such as control systems, electrical distribution, and transmission. Additionally, the article emphasizes the importance of ensuring that the network is cost-effective, stable, and resistant to transient power system issues and external sources of electromagnetic interference.

Lastly, the article of Daniel Corujo et al. [44] explores the practical implications of deploying 5G technology in vertical sectors, focusing on the transportation sector, particularly the railway domain The paper presents a case study involving a 5G-enabled railway deployment, which serves as an empirical analysis of 5G capabilities in a specific vertical. Two transportation use cases related to railway operations are explored. The first use case

focuses on replacing traditional cable-based train detection sensors with wireless 5G communication. This aims to eliminate the need for construction work and offers a more flexible and cost-effective solution. The second use case leverages 5G to provide live video footage of approaching level crossings to train conductors, enhancing safety conditions. The paper offers insights into the real-world applications of 5G technology in the railway sector, concluding that 5G technologies offer various system capabilities that result in performance improvements and the creation of new connectivity opportunities.

In the ever-evolving landscape of communication technologies, the journey from 2G to 5G reflects a remarkable progression that has significantly shaped the way we connect and interact. The advent of cellular IoT, spanning from 2G to 5G, has been a transformative force, enabling a myriad of IoT devices to seamlessly communicate over cellular networks. The studies cited illuminate the practical implications of these cellular advancements. From addressing water pipeline leakage using 4G-powered wireless sensor networks to deploying 5G in smart grids for efficient energy management, these technologies are at the forefront of revolutionizing critical infrastructures.

- ZigBee

ZigBee serves as a wireless network data transmission protocol, supporting mesh and cluster tree architectures. Its functionality, akin to Wi-Fi, distinguishes itself through lower energy consumption, modest bit rates (up to 200 and 50 kbps), and an operational range of about 100 m. ZigBee enables two-way communication, allowing devices to both send and receive signals, with some capable of relaying signals. Developed by the ZigBee Alliance in 2002, this technology boasts collaboration from numerous globally recognized companies, including Samsung, Philips, Siemens, Bosch, Motorola, Amazon, and Xiaomi. The initial ZigBee specification, Version 1.0, emerged in 2004, followed by the introduction of ZigBee 3.0 in 2016.

ZigBee networks adopt various topologies.

1. Star topology: primarily utilized in home networks, it features a single coordinator device, with all other end devices communicating directly with it; however, a drawback is the vulnerability of the entire network if the coordinator malfunctions.
2. Tree topology: Comprising a root and its dependent nodes where the coordinator acts as the root and end devices are placed on the last branches. While enabling the connection of more nodes and covering a larger area, this structure introduces transmission delays, and the failure of one node can impact others.
3. Mesh topology: Representing the most intricate network structure, every device can communicate directly with another, either through direct links or intermediaries. This topology is considered superior for ZigBee networks, as it facilitates data continuity by allowing another device to take over if one node fails [45].

The power grid is the heartbeat of modern society, ensuring a continuous and reliable supply of electricity. It powers homes, businesses, hospitals, and essential services. A resilient power grid is vital for economic stability, technological advancement, and the overall well-being of communities, underpinning every facet of our interconnected lives. Saqib Ali et al. [46] proposed a prototype design suggested for remote monitoring of power grid components using ZigBee communication. The prototype, tested for various scenarios in a power plant, demonstrated effective data transmission between the remote terminal unit and the monitoring unit through ZigBee wireless technology. Results from three experiments confirmed the prototype's capability to capture dynamic changes in the power grid system over extended periods, even amid frequent minor changes.

Another interesting use of ZigBee in critical infrastructures is given in the article of Rajesh Singh's [47] research. His article is about a novel application of ZigBee technology for monitoring oil pipelines in critical infrastructures. The proposed hybrid architecture combines ZigBee and LoRa communication at 2.4 GHz, addressing the safety challenges associated with petroleum product transportation. The system involves distinct nodes for monitoring inside and outside the pipeline, using ZigBee for detecting corrosion, fire,

leakage, and location. The LoRa protocol facilitates long-range communication of critical parameters to a LoRa-based gateway, which, integrated with Wi-Fi, sends data to a cloud server for remote visualization and analysis, aiding authorities in making informed decisions during emergencies.

- NB-IoT

The Narrowband Internet of Things (NB-IoT) is an emerging IoT technology created by the Third-Generation Partnership Project (3GPP). Operating alongside LTE in licensed cellular spectrums, NB-IoT aims to establish a low-power wide-area network (LPWAN). Devices utilizing NB-IoT are designed for extended battery life, with an expectancy of up to 10 years on a single battery charge, covering approximately 10 km in range. The modules are cost-effective and offer reliable connectivity through commercial LTE operators. These modules can incorporate sensors for measuring and transmitting data (uplink) or receiving data (downlink). In 3GPP's release 13, the maximum data rates are set at 20 kbps for uplink and 100 kbps for downlink, with later releases significantly improving the uplink rate to 142.5 kbps [48].

Project [49] aims to develop a solution for the modernization and security enhancement of crucial water supply and purification systems within the scope of Industry 4.0 applications for smart cities. The focus is on assessing the renewal needs (and applicable use cases) and proposing an IoT-based solution for urban critical infrastructure. The paper outlines the IoT network architecture and specific hardware for securing water supply and wastewater treatment processes. Details include the water level control mechanism and a system ensuring optimal chemical levels for wastewater treatment. The selected technologies for revitalizing critical infrastructure via IoT networks are the NB-IoT protocol and the 4G mobile networks. NB-IoT effectively incorporates communication security protocols inherent in mobile networks, benefiting from the extensive deployment of 4G coverage, and the chosen deployment location is anticipated to have 4G coverage. Presently, the characteristics and requirements of IoT networks are adequately addressed using NB-IoT or LTE-M. However, the author notes that, as 5G protocols become standardized, the natural progression for IoT networks is to leverage the advantages provided by 5G.

Stephen Ugwuanyi's study [50] begins by clarifying that wireless sensor networks are described as the observation and management of physical phenomena along with mission-critical infrastructures, and subsequently presents research on deploying NB-IoT technology for industrial applications. It explores the practical aspects of setting up an NB-IoT test network, including different deployment testing using NB-IoT devices and an LTE/NB-IoT base station. The study focuses on the security requirements, power and latency performance, and global spectrum deployment options for a potential private licensed NB-IoT network. It highlights NB-IoT's advantages such as massive connectivity, good power utilization, long-distance transmission, and higher data throughput, particularly in 4G and 5G applications.

- LoRaWAN

LoRaWAN—a prominent LPWAN technology—has garnered substantial attention from the research community. Developed by Semtech Corporation, it facilitates long-range data transmission with low data rates. Using a chirp spread spectrum (CSS) modulation, where the chirp signal frequency varies, LoRaWAN ensures robust coverage. The modulation employs spreading factors (SFs) ranging from 7 to 12, with higher SFs providing better coverage but at the expense of data rate and power efficiency [51,52].

Study [53] focuses on establishing a range of data transmission in diverse and challenging environments, along with identifying the key radio parameters influencing this transmission. The findings guide the application of LoRaWAN in critical infrastructures by specifying the circumstances and methods suitable for implementation. The study conducted a comparative analysis of LoRaWAN communication in an urban prefabricated environment, emphasizing its applicability in critical infrastructures like residential areas,

industrial plants, sewage treatment plants, and hospitals. The results affirmed the high reliability of LoRaWAN in such setups, demonstrating sufficient coverage in Budapest for critical infrastructure protection (CIP) applications. Mobile measurements revealed that LoRaWAN could function seamlessly, even on public transport. Jammer interference measurements indicated minimal disruption, emphasizing the stability of LoRa communication. Safe box measurements exhibited positive outcomes, displaying LoRa's suitability for secure structures like containers or safety deposit boxes. Water measurements demonstrated successful data transmission at a depth of 0.6 m, suggesting potential applications in reservoir monitoring.

Another interesting study [54] delves into enhancing the security of LoRaWAN. Though LoRaWAN integrates AES-128 cryptographic protection, certain tasks, particularly those within critical infrastructure systems, require supplementary cryptographic measures, such as adherence to the GOST 34.12-2018 specification. The research proposes a software module for LoRaWAN devices, implementing encryption with a 128-bit block length ("Kuznyechik"), complying with Russian standards. The module is implemented in the IMST GmbH iM880B module, highlighting its feasibility. This software addition ensures information security beyond the LoRaWAN standard, preventing unauthorized access and specific attacks. The software implementation offers advantages in terms of flexibility, lower power consumption, and cost-effectiveness compared with hardware approaches. Tests confirmed the feasibility of additional encryption without causing errors in LoRaWAN standard operation and providing enhanced confidentiality. The flexibility of software implementation indicates easy integration into existing devices. Overall, this research presents a promising approach for industrial implementation, contributing to the evolution of secure communication in critical infrastructure systems. Lastly, a study [55] from the US Department of Defense supports the effectiveness of integrating LoRaWAN and Helium Network technologies, illustrating practical instances of a robust global network. It recommends that the Department of Defense (DoD) adopt and adapt this technology to improve environmental sensing, establish immediate tactical networks, and oversee critical infrastructure and logistics. The suggested amalgamation has the potential to furnish the DoD with a dependable, secure, and anonymous communication network utilizing LoRaWAN nodes and routers, ensuring end-to-end encryption up to AES-128 (aligning with DoD SECRET-classification standards). Application of LoRaWAN IoT devices in real-time environmental data collection, encompassing tasks like urban flood monitoring and earthquake detection, is proposed. This would aid in efficiently coordinating evacuations during natural disasters, thereby enhancing mission success and operational safety. Additionally, deploying LoRaWAN devices on personnel, vehicles, and structures for real-time information transmission in various scenarios is suggested, offering both defensive and offensive capabilities. This includes monitoring human factors, stress, vitals, and adversarial infrastructures. The study emphasizes the optimization of monitoring critical infrastructures like electricity, natural gas, water, and sewage by leveraging LoRaWAN's wireless signal range. The proposed method suggests minimal alterations to existing IoT infrastructure, ensuring low adoption costs and swift implementation. The envisioned fusion of LoRaWAN and Helium Network technologies emerges as a compelling resolution to address IoT challenges faced by the DoD. By establishing an IoT ecosystem supported by the Helium blockchain, there is the potential to significantly bolster the DoD's lethality and dominance in information warfare. The proposed technological fusion offers practical solutions for emergency management, real-time battlefield information, and safeguarding critical infrastructure.

- Bluetooth Low Energy

Bluetooth technology owes much of its success to the remarkable flexibility it affords developers. With two radio options, Bluetooth caters to a diverse range of wireless connectivity needs, making it a preferred choice for various applications. Whether facilitating

high-quality audio streaming, data transfer between devices, or communication in building automation, Bluetooth Low Energy (LE) and Bluetooth Classic radios offer tailored solutions to developers worldwide. The Bluetooth LE radio, designed for ultra-low power operation, operates across 40 channels in the 2.4 GHz unlicensed ISM frequency band. This design grants developers significant flexibility in crafting products that align with the specific connectivity demands of their target markets. Bluetooth LE supports various communication topologies, extending from point-to-point to broadcast and, more recently, mesh, enabling the creation of dependable large-scale device networks. Initially renowned for device communication, Bluetooth LE has evolved into a prominent device positioning technology, meeting the rising demand for highly accurate indoor location services [56].

The study from the Air Force Institute of Technology [57] delves into the security considerations of Bluetooth Low Energy (BLE) within CI applications, with a specific focus on WSNs, a technology routinely employed by the DoD for vital surveillance and reconnaissance missions. The investigation foresees BLE as playing a pivotal role in the upcoming wave of wireless sensor networks, heightening its significance for military operations. Highlighting the centrality of BLE in CI, particularly in WSNs, the research illustrates its diverse applications, ranging from fortifying building security and enabling automation to contributing to environmental monitoring. It underlines the increasing relevance of BLE security as the DoD undergoes infrastructural modernization. The study underscores the potential repercussions of vulnerabilities within CI systems, emphasizing their ripple effect on air force networks and mission-critical systems. The research culminates by asserting the efficacy of BLE sniffers, specifically the BLE multi-variant, in fortifying CI application security by unveiling patterns of attack traffic. While proposing the integration of automated defensive solutions in the future, the study pragmatically advises current users to cautiously adopt BLE within CI, employing robust risk management strategies to navigate potential associated risks.

As health/medical infrastructures are one of the critical infrastructures, paper [58] delves into increasing security concerns within smart health systems, specifically focusing on Internet of Medical Things (IoMT)'s devices employing Bluetooth technology. With the proliferation of IoMT devices in smart cities, there is a heightened vulnerability to cyberthreats, necessitating a robust cybersecurity strategy. The emphasis is on utilizing artificial intelligence (AI) and deep learning (DL) for a decentralized proactive intrusion detection system designed to counter cyberattacks on IoMT networks. The proposed system seeks to independently identify and block malicious traffic, ensuring comprehensive defence. A notable contribution is the introduction of the BlueTack dataset, the inaugural intrusion detection dataset for both Bluetooth Classic and BLE. This dataset facilitates the creation of a multilayer intrusion detection approach, employing advanced deep learning techniques, and demonstrating impressive performance, with F1 scores ranging between 97% and 99.5%. The recommended decentralized architecture situates this intrusion detection system on the edge nodes of smart healthcare systems, offering a pragmatic solution for deployment in smart cities.

- WirelessHART

WirelessHART—initiated in 2004 by 37 HART Communication Foundation companies—is a wireless sensor networking technology developed for process field device networks. Approved by the IEC in 2009, it is an open standard supported by various industry leaders. The latest version—IEC/PAS 62591:2016—was released in 2016. WirelessHART is an extension of the wired HART protocol, operating in the 2.4 GHz ISM band, using the IEEE 802.15.4 standard [59]. Kevin B. Hall [60] notes that, in rural American communities, electric companies managing supervisory control and data acquisition (SCADA) systems are increasingly adopting wireless administration. Given the absence of wired high-speed internet access in these rural areas, electric companies (vital components of CI) are turning

to wireless sensor and mesh networks (WSMN) for communication over extensive distances. Nodes within the rural electric grids utilize WirelessHART to transmit information back to the central SCADA controller. Lastly, study [61] highlights WirelessHART signalling as the predominant digital communication technology in process control industries, boasting over 40 million deployed devices. It emphasizes the growing challenges, particularly in anticipation of the exponential WirelessHART expansion projected until 2028, especially within sectors like oil, gas, chemical, and power generation.

- 6LowPAN

Smita Sanjay Ambarkar [62] explains the range of 6LowPAN from smart home to critical infrastructure and studies the enhancement of IoT network security against routing protocol for low-power and lossy networks (RPL) attacks. It highlights the vulnerability of IoT networks to various RPL attacks, like HELLO flood, version number, and rank attacks. The paper proposes a mutual authentication scheme to protect the network from these threats. The proposed method is evaluated for its effectiveness in mitigating these attacks, focusing on power consumption and network performance. The results demonstrate that the scheme effectively blocks unauthenticated nodes and improves network performance.

On the whole, wireless communication technologies play significant roles (as addressed in the referenced literature), showing various advantages and disadvantages in their use. In his study [63], Jafaru Ibrahim highlights several benefits of wireless networks compared with traditional ones, including ease and speed of installation, superior mobility, efficiency, and the elimination of the need for hubs and switches. Payal Soni, in his research [64], gives additional advantages such as low cost-effectiveness and the potential for extensive network coverage expansion. Adam B. Noe, in his work [65], states that wireless networks are distinguished by their quick deployment time and the ability to incorporate a larger number of sensors compared with wired networks. These insights collectively underscore the growing relevance and utility of wireless technologies in various applications.

In Figure 4, a comparative presentation of the referenced wireless communication protocols' features is displayed.

Figure 4 illustrates the distinct characteristics of each wireless communication protocol, making it clear why a specific WSN must be developed to meet the unique needs of different infrastructures. No single protocol effectively covers all scenarios. For instance, 5G offers high data rates but incurs higher costs due to frequency band commitments. LoRa, while cost-effective and capable of long-range coverage, is limited by its use only in industrial, scientific, and medical bands (ISM bands), with a lower data rate of 50 kbps impacting its versatility. Similarly, ZigBee boasts a higher data rate but cannot cover extensive distances and has a higher power consumption. This interplay of advantages and disadvantages across all protocols underscores the importance of precise study and design for the optimal configuration of a WSN.

Figure 4. Comparison of protocols.

4. Bibliographic Research

Our bibliographic research was conducted using the Scopus and Google Scholar platforms, focusing on results related to wireless sensor networks in critical infrastructures. Initially, we retrieved several thousand results. However, to refine our search, we applied filters based on publication dates (2019–2023) and on keywords such as "Critical Infrastructure WSN", "critical WSN", and "CI sensor networks", significantly reducing the number of results. Throughout our bibliographic research, we frequently encountered the term "critical" used in various contexts, such as "critical applications", "critical timing", "critical areas", and "critical demands". However, these instances often did not directly pertain to the specific and highly relevant concept of "critical infrastructure". As our study delved deeper into critical infrastructures, it became increasingly apparent that, for a more focused and relevant analysis, it was crucial to selectively examine publications that explicitly referred to "critical infrastructure" as a distinct term. To accomplish this, detailed and precise examination of the term "Critical Infrastructures", and specifically studying "Wireless Sensor Networks", we undertook additional steps to enhance the quality of our research. These steps included omitting duplicate papers, excluding those with identical titles, and eliminating those with insufficient or less-relevant content. Throughout our research, we remained focused on individual papers that addressed our primary criteria and aligned with the objectives outlined in the introduction. Consequently, we narrowed down our references to a total of 22 papers (Table 2).

Table 2. Bibliographic research.

Citation	Reference Number	CI Sector	Wireless Communication Technologies/Protocols	Standards	Type of Paper	Year
63	[41]	Water	ZigBee and 4G wireless	-	Journal Article	2019
26	[42]	Water	ZigBee and 4G	-	Journal Article	2020
26	[43]	Energy	5G	-	Journal Article	2021
1	[44]	Transportation Sector	5G	-	Journal Article	2023
1	[46]	Energy	ZigBee	IEEE 802.15.4	Conference Paper	2020
10	[47]	Energy	ZigBee/LoRaWAN	-	Journal Article	2021
22	[49]	Water	NB-IoT	ISO 37120, ISO 37122 ISO 37120, ISO 37123 ISO/IEC 27001: 2017 n RDL 8/2011, ISO 27002	Journal Article	2023
2	[50]	Industrial/Manufacturing	NB-IoT	3GPP standardization	Conference Paper	2020
	[53]	Health Industrial Transportation	LoRaWAN	-	Journal Article	2022
-	[54]	Industrial/Manufacturing	LoRaWAN	-	Conference Paper	2021
-	[55]	Military, Emergency/Rescue Services	LoRaWAN, Helium	AES-128	Conference Paper	2023
6	[58]	Health	Bluetooth Low Power	-	Journal Article	2022
-	[60]	Energy	ZigBee PRO, WirelessHART, and ISA 100.11a.	-	Journal Article	
20	[66]	General Reference to Smart Grids, Intelligent Transport Systems, Healthcare and Medical, Industrial/Manufacturing	General Reference to 5G, LoRaWAN,	-	Journal Article	2021
18	[67]	General Reference to healthcare	-	-	Conference Paper	2020
9	[68]	General Reference to Critical Public Infrastructure Energy Transport Health	General Reference to 6LowPAN	-	Journal Article	2020

2	[62]	General Reference to Critical Infrastructure	6LowPAN	RPL (Routing Protocol for Low-Power and Lossy Networks)	Journal Article	2021
	[69]	General Reference to Medical Bridges	-	-	Journal Article	2021
4	[70]	Transportation Sector	-	-	Conference Paper	2019
6	[71]	General Reference to Pipeline (Oil, Gas, And Water) Monitoring	-	-	Journal Article	2019
-	[72]	Railroad/Subway and Bridge Monitoring Railway Infrastructure Transportation Sector	Multi-Parent Hierarchical (MPH), Ad-Hoc On-Demand Distance Vector (AODV)	-	Conference Paper	2019
1	[73]	General Reference to Military, Manufacturing, Health Care, Railways, Highways, Rivers, Oil or Gas Pipelines, and Energy	Linear Wireless Sensor Networks (LWSNs)	-	Journal Article	2023

The term "general reference" is used to describe studies that provide a brief and general mention of a CI sector without delving into detailed analysis or exploring specific scenarios and characteristics of that sector. This approach often lacks depth and a comprehensive understanding of the unique aspects and challenges within each CI sector.

5. Discussion

The literature review yielded significant insights. Initially, an extended search of the literature and bibliography referring to the quite noteworthy and significant "CI" term was conducted in Google Scholar and Scopus. Using strict keyword criteria included in article titles and focusing on publications extending from 2019 to 2023, we obtained 1667 results from Scopus and 2,610 from Google Scholar. However, when the definition "WSN" was added, the number of appropriate articles was drastically reduced. Scopus yielded only 144 and Google Scholar a mere 82. Further refining of the inquiry while including both "CI" and "WSN" terms via an AND function, either by being located in the title or included as official keywords in the paper's abstract sections, Scopus results diminished to 15, while Google Scholar provided a solitary result. In total, 22 referenced papers, including 17 journal articles and 7 conference papers, substantially support the idea of WSN implemented in CI sectors, contrary to the remaining published review papers that suffice to merely describe the topic and record the achievements of the scientific community referring to it. Such an outcome of the addressed literature indicated two research outcomes.

First, many publications we studied require a thorough examination to ascertain their relevance to WSNs in CIs. On the other hand, it suggests that this research area, whilst blending WSNs with CIs, offers substantial scope for future exploration in a variety of directions. The literature search referring to the core sectors where CIs play a significant role is highlighted in Figure 5 and Table 2.

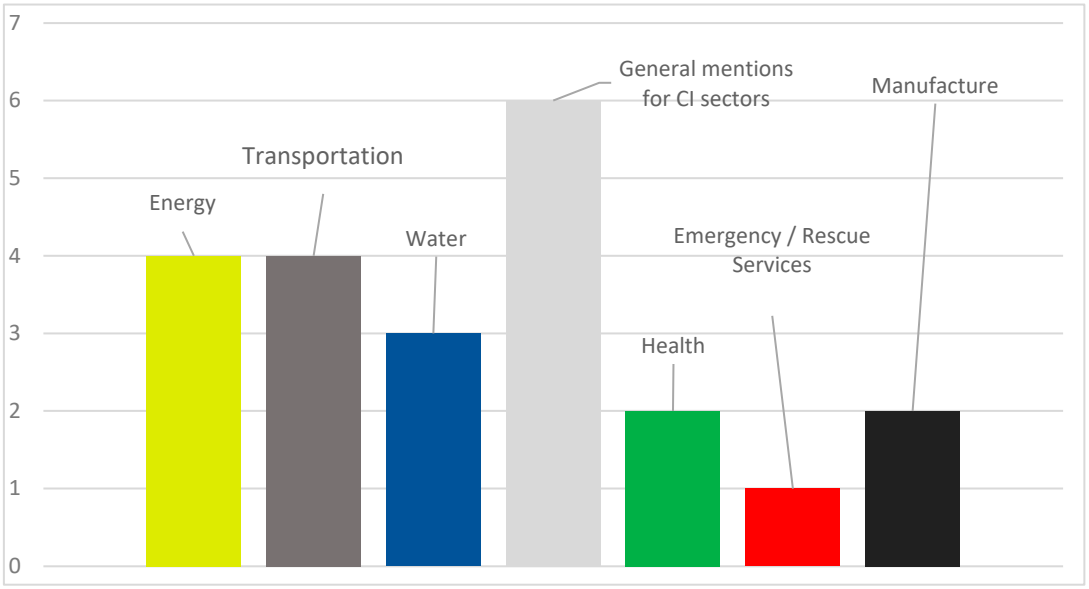

Figure 5. Bibliography results of CI sectors.

It reveals that the most prevalent approach in the studied literature seems to be addressed generally and not specifically, which refers broadly to various sectors without an in-depth analysis of any specific area. The energy and transportation sectors emerge as the secondary focal points, while the more humanitarian sectors such as health and emergency/rescue services are low in preference. Regarding the range of use of wireless communication protocols and technologies implemented in CIs, as addressed in the referenced literature, their range of use is presented in Figure 6, where it is evident that cellular communication and ZigBee emerge as the most popular protocols, followed closely by LoRaWAN.

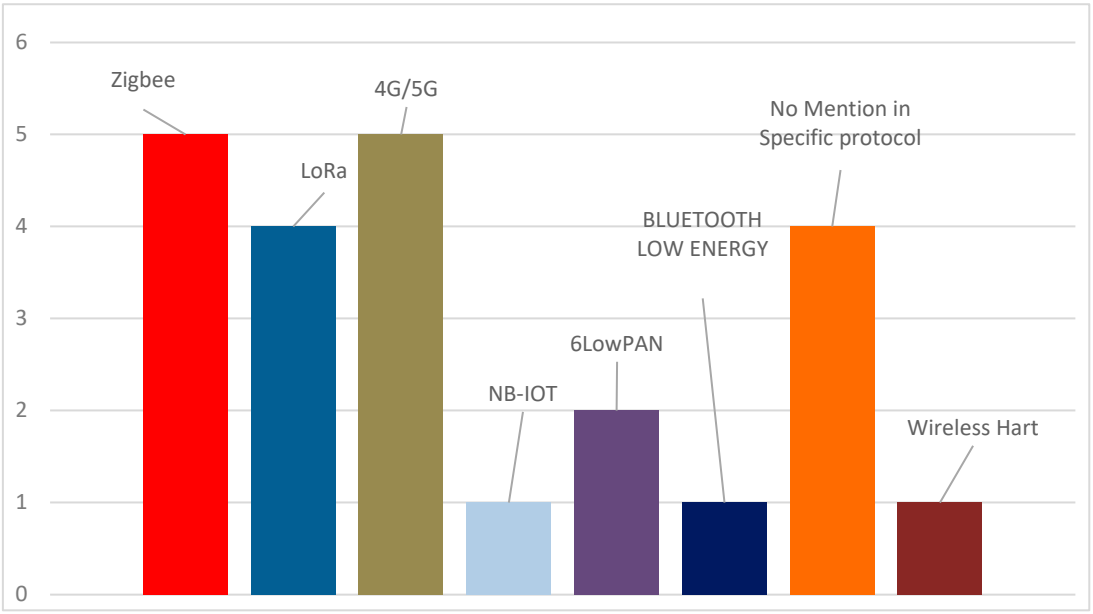

Figure 6. Bibliography results of CI communication protocols.

As stated in [41,42], which address the water key sector, 4G communication technology is used, while 5G is implemented in the energy sector, as stated in [43], and in the transportation sector, as stated in [44]. In [66], 5G is generally addressed as a useful implementation in smart grids and intelligent transport systems and healthcare, medical, industrial, and manufacturing sectors on the whole. ZigBee, on the other hand, poses another application filed concerning the water sector, as outlined in [41,42], and also the energy sector, as stated in [46,47,60]. LoRaWAN has a stake in the field of CI sectors such as the energy sector [47], health industrial transportation, industrial/manufacturing sectors [53], military, and emergency/rescue services. LoRaWAN where Helium comes in place, as commented in [54,55] and according to [66], is generally implemented in smart grids and intelligent transport systems and healthcare, medical, industrial, and manufacturing sectors.

It is worth noting that communication standards are rarely mentioned in the referenced literature, merely in three conference papers, e.g., in [46] (where the IEEE 802.15.4 standard is addressed), in [50] (where 3GPP is mentioned), and in [55] (where AES-128 is also mentioned). Two journal papers refer to communication standards, e.g., in [62] (where the routing protocol for low-power and lossy networks (RPL) is mentioned) and in [49] (where the ISO 37120, ISO 37122, ISO 37120, ISO 37123, ISO/IEC 27001:2017, n RDL 8/2011, and ISO 27002 protocols are mentioned).

Each of these three protocols exhibit unique advantages and disadvantages, reflecting the varied requirements of different sectors and environments within critical infrastructures. Additionally, it is noteworthy that a general approach (not to mention a specific protocol) is often adopted in publications that investigate security or topology in wireless sensor networks. Another significant finding is the infrequent mention of standards, particularly those pertaining to the quality of equipment and components suitable for use in sensors, nodes, gateways, and other WSN equipment in a critical infrastructure. References to such quality standards are exceedingly rare, in fact almost non-existent. This gap highlights a potential area of concern in ensuring the reliability and effectiveness of WSNs within critical infrastructural systems. This notable absence of information gives the opportunity for future work and study in the field of critical infrastructures. Finally, CI encompasses a broad spectrum of sectors, each with diverse and specific infrastructures. This diversity poses challenges in conducting studies that precisely match a type of WSN with a specific CI sector. Future research focusing on the development of WSNs with stringent standards and specifications tailored to particular CI sectors and subcategories holds significant potential and interest. This approach could lead to more targeted and effective integration of WSNs in critical infrastructure management.

Author Contributions: Conceptualization, S.D., N.P., P.P., and D.D.P.; methodology, S.D., N.P., P.P., and D.D.P.; validation, S.D., N.P., V.C., P.P., D.D.P. and R.A.M.; formal analysis, S.D., N.P., P.P., D.D.P. and R.A.M.; investigation, S.D., N.P., V.C., P.P., D.D.P. and R.A.M.; resources, S.D., N.P., V.C., P.P. and D.D.P.; data curation, S.D., N.P., V.C., P.P., D.D.P. and R.A.M.; writing—original draft preparation, S.D., N.P., and V.C.; writing—review and editing, S.D., N.P., V.C., P.P., D.D.P. and R.A.M.; visualization, S.D., N.P., V.C., P.P. and D.D.P.; supervision, P.P. and D.D.P.; project administration, S.D., N.P., P.P., D.D.P. and R.A.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Any data presented in this study are available within the article.

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

References

1. United Nations Office for Disaster Risk Reduction—Regional Office for Europe & Central Asia. *Making Critical Infrastructure Resilient*; United Nations Office for Disaster Risk Reduction—Regional Office for Europe & Central Asia: Brussels, Belgium, 2020.
2. United States Department of Agriculture (USDA). *USDA Rural Development FY 2022 Awards Rural Energy for America Program*; United States Department of Agriculture: Washington, DC, USA, 2022; Volume 2023.
3. Vogelman, S.J. The Fortnightlya Review of Middle East Regional Economic & Cultural News & Developments. Available online: https://atid-edi.com/category/fortnightly/ (accessed on 7 November 2023).
4. Willis, R. European Investment Bank Pledges Record Funding for Europe's Security Infrastructure, Vows More Support for Ukraine. Available online: https://www.eib.org/en/press/all/2023-227-eib-pledges-record-funding-for-europe-s-security-infrastructure-vows-more-support-for-ukraine (accessed on 1 December 2023).
5. Florian Martens, S.K. Siemens to Invest More than US$500 million in U.S. Manufacturing for Critical Infrastructure in 2023. Available online: https://press.siemens.com/global/en/pressrelease/siemens-invest-more-us500-million-us-manufacturing-critical-infrastructure-2023 (accessed on 5 December 2023).
6. Commission of the European Communities. *Communication from the Commission on a European Programme for Critical Infrastructure Protection*; Commission of the European Communities: Brussels, Belgium, 2006.
7. European Parliament. Resilience of Critical Entities and Repealing Council Directive 2008/114/EC. Available online : https://eur-lex.europa.eu/eli/dir/2022/2557/oj (accessed on 14 September 2023.
8. Moteff J.; Parfomak P. Critical Infrastructure Identification, Prioritization, and Protection, 2004. Available online : https://apps.dtic.mil/sti/citations/ADA454016 (accessed on 20 July 2023).
9. Brunner, E.M.; Suter, M. *International CIIP Handbook 2008/2009*; Center for Security Studies (CSS), ETH Zürich: Zürich, Switzerland, 2008.
10. A Proclamation on Critical Infrastructure Security and Resilience. Available online: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/31/a-proclamation-on-critical-infrastructure-security-and-resilience-month-2023/ (accessed on October 2023.
11. Commission of the European Communities. Green Paper on a European Programme for Critical Infrastructure Protection; Commission of the European Communities: Brussels, Belgium, 2005.
12. Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. Available online: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32008L0114 (accessed on 26 November 2023).
13. Theoharidou, M.; Kandias, M.; Gritzalis, D. Securing Transportation-Critical Infrastructures: Trends and Perspectives. In *Global Security, Safety and Sustainability & e-Democracy. e-Democracy ICGS3 2011 2011. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*; Georgiadis, C.K., Jahankhani, H., Pimenidis, E., Bashroush, R., Al-Nemrat, A., eds; Springer: Berlin/Heidelberg, Germany, 2012; Volume 99.
14. Wisniewski, M.; Gladysz, B.; Ejsmont, K.; Wodecki, A.; Van Erp, T. Industry 4.0 Solutions Impacts on Critical Infrastructure Safety and Protection–A Systematic Literature Review. *IEEE Access* **2022**, *10*, 82716–82735.
15. Davies, R.; *Industry 4.0, Digitalisation for Productivity and Growth*; European Parliamentary Research Service: Brussels Belgium, 2015.
16. Majstorovic, V.D.; Mitrovic, R. Industry 4.0 Programs Worldwide. In Proceedings of the 4th International Conference on the Industry 4.0 Model for Advanced Manufacturing, Belgrade, Serbia, 3–6 June 2019.
17. Sisinni, E.; Mahmood, A. Wireless Communications for Industrial Internet of Things: The LPWAN Solutions. In *Wireless Networks and Industrial IoT*; Mahmood, N.H., Marchenko, N., Gidlund, M., Popovski, P., eds.; Springer: Cham, Switzerland, 2021.
18. Amit Shukla, H.K. Application of robotics in offshore oil and gas industry—A review part II. *Robot. Auton. Syst.* **2015**, *75*, 508–524**.**
19. Brucherseifer, E.; Winter, H.; Mentges, A.; Mühlhäuser, M.; Hellmann, M. Digital Twin conceptual framework for improving critical infrastructure resilience. *at-Automatisierungstechnik* **2021**, *69*, 1062–1080.
20. Laplante, P.; Amaba, B. Artificial Intelligence in Critical Infrastructure Systems. *Computer* **2021**, *54*, 14–24.
21. Wu, Y.; Dai, H.N.; Wang, H. Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0. *IEEE Internet Things J.* **2020**, *8*, 2300–2317.
22. Alqudhaibi, A.; Albarrak, M.; Aloseel, A.; Jagtap, S.; Salonitis, K. Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations. *Sensors* **2023**, *23*, 4539.
23. Singh, M.K.; Amin, S.I.; Imam, S.A.; Sachan, V.K.; Choudhary, A. A Survey of Wireless Sensor Network and its types. In Proceedings of the 2018 international conference on advances in computing, communication control and networking (ICACCCN), Greater Noida, India, 12–13 October 2018.
24. Kandris, D.; Nakas, C.; Vomvas, D.; Koulouras, G. Applications of Wireless Sensor Networks: An Up-to-Date Survey. *Appl. Syst. Innov.* **2020**, *3*, 14.
25. Sharma, S.; Kumar, D.; Kishore, K. Wireless Sensor Networks—A Review on Topologies and Node Architecture. *Int. J. Comput. Sci. Eng*. **2013**, *1*, 19–25.
26. Yoo, S.E.; Kim, T. Industrial wireless sensor networks: Protocols and applications. *Sensors* **2020**, *20*, 5809. https://doi.org/10.3390/s20205809.

27. History of IEEE. Availabe online: https://www.ieee.org/about/ieee-history.html?utm_source=linkslist_text&utm_medium=lp-about&utm_campaign=history (accessed on 12 November 23).
28. About of ISO. Availabe online: https://www.iso.org/about-us.html (accessed on 5 December 23).
29. About of CEN. Availabe online: https://www.cencenelec.eu/about-cen/ (accessed on 7 December 23).
30. About of IEC. Availabe online: https://www.iec.ch/history/how-why-iec-was-started (accessed on 5 December 23).
31. About of IPC. Availabe online: https://www.ipc.org/about-ipc (accessed on 9 December 23).
32. Lewis, A.M. *Technology Certification for Critical Infrastructure Protection*; EUR 26808; European Commission Joint Research Centre Institute for the Protection and Security of the Citizen: Brussels, Belgium, 2014.
33. *ISO/IEC 27001*. 2022. Available online: https://www.iso.org/standard/27001 (accessed on 15 October 2023).
34. *ISO/IEC 27002:2022*. 2022. Available online: https://www.iso.org/standard/75652.html (accessed on 15 October 2023).
35. *ISO/IEC 15408-1:2022*. 2022. Available online: https://www.iso.org/standard/72891.html (accessed on 15 October 2023).
36. *IEC 62351*. 2023. Available online: https://www.iec.ch/blog/cyber-security-understanding-iec-62351 (accessed on 15 October 2023).
37. *IEC 62443*. 2021. Available online: https://www.iec.ch/blog/understanding-iec-62443 (accessed on 15 October 2023).
38. Prepared Statement of Dave Whitehead, Vice President of R&D Schweitzer Engineering Laboratories. Available online: https://www.ferc.gov/sites/default/files/2020-08/Whitehead-SchweitzerEngineeringl.pdf (accessed on 15 October 2023).
39. *IEC TS 62686-1*. International Electrotechnical Commission. 2020. Available online: https://webstore.iec.ch/preview/info_iects62686-1%7Bed3.0%7Den.pdf (accessed on 27 June 2023).
40. IPC J-STD-001 and IPC-A-610. 2020. Available online: https://www.ipc.org/news-release/ipc-releases-new-h-revision-two-leading-standards-electronics-assembly-ipc-j-std-001 (accessed on 8 August 2023).
41. Liu, Y.; Ma, X.; Li, Y.; Tie, Y.; Zhang, Y.; Gao, J. Water Pipeline Leakage Detection Based on Machine Learning and Wireless Sensor Networks. *Sensors* **2019**, *19*, 5086.
42. Adu-Manu, K.S.; Katsriku, F.A.; Abdulai, J.-D.; Engmann, F. Smart River Monitoring Using Wireless Sensor Networks. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8897126. https://doi.org/10.1155/2020/8897126.
43. Kumar, J.C.R.; Almasarani, A.; Majid, M.A. 5G-Wireless Sensor Networks for Smart Grid-Accelerating technology's progress and innovation in the Kingdom of Saudi Arabia. *Procedia Comput. Sci.* **2021**, *182*, 46–55. https://doi.org/10.1016/j.procs.2021.02.007.
44. Corujo, D.; Quevedo, J.; Cunha, V.; Perdigão, A.; Silva, R.; Santos, D.; Aguiar, R.L.; Paixão, P.; Silva, P.E.; Antunes, R.; et al. An Empirical Assessment of the Contribution of 5G in Vertical Industries: A Case for the Transportation Sector. *IEEE Access* **2023**, *11*, 15348–15363. https://doi.org/10.1109/ACCESS.2023.3243732.
45. Czeczot, G.; Rojek, I.; Mikołajewski, D. Analysis of Cyber Security Aspects of Data Transmission in Large-Scale Networks Based on the LoRaWAN Protocol Intended for Monitoring Critical Infrastructure Sensors. *Electronics* **2023**, *12*, 2503.
46. Ali, S.; Rehman, O.; Cha, K.; Balushi, T.A.; Nadir, Z. Performance Analysis of ZigBee-based IoT Prototype for Remote Monitoring in Power Grid Systems. In Proceedings of the 9th International Conference on Smart Media and Applications, Jeju, Republic of Korea, 17–19 September 2020; pp. 384–389.
47. Singh, R.; Baz, M.; Narayana, C.; Rashid, M.; Gehlot, A.; Shaik, V.A.; Alshamrani, S.; Prashar, D.; Saeed, A. Zigbee and Long-Range Architecture Based Monitoring System for Oil Pipeline Monitoring with the Internet of Things. *Sustainability* **2021**, *13*, 10226. https://doi.org/10.3390/su131810226.
48. Trigkas, A.; Sarigiannis, G.; Daousis, S.; Papageorgas, P.; Agavanakis, K.; Panagiotopoulos, K. NB-IoT for environmental monitoring and a fire early warning detection system in Mount Pentelicus. *AIP Conf. Proc.* **2022**, *2437*, 020069. https://doi.org/10.1063/5.0092309.
49. Villar Miguelez, C.; Monzon Baeza, V.; Parada, R.; Monzo, C. Guidelines for Renewal and Securitization of a Critical Infrastructure Based on IoT Networks. *Smart Cities* **2023**, *6*, 728–743.
50. Ugwuanyi, S.; Hansawangkit, J.; Irvine, J. NB-IoT Testbed for Industrial Internet of Things. In Proceedings of the 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 20–22 October 2020; pp. 1–6.
51. Haxhibeqiri, J.; De Poorter, E.; Moerman, I.; Hoebeke, J. A Survey of LoRaWAN for IoT: From Technology to Application. *Sensors* **2018**, *18*, 3995.
52. Daousis, S.; Sarigiannis, G.; Trigkas, A.; Agavanakis, K.; Papageorgas, P. The Blue Bee project: A proposal for the development of an internet of ships sensing network for environmental data collection and sharing. *AIP Conf. Proc.* **2022**, *2437*, 020068. https://doi.org/10.1063/5.0092306.
53. Borsos, D.; Kohanecz, Á.; Kozma, D. LoRa and LoRaWAN in the Aspect of Critical Infrastructures. *Tech. Univ. Ostrav. Saf. Eng. Ser.* **2022**, *17*, 1–11. DOI: 10.35182/tses-2022-0001
54. Mikhailovich, P.P.; Victorovich, C.A.; Nikolayevich, Y.N.; Yuryevich, Z.M. Implementation of GOST 34.12-2018 Encryption for LoRaWAN End-devices. In Proceedings of the 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russia, 13–14 May 2021.
55. Reyneke, M.A.; Mullins, B.E.; Reith, M.G. LoRaWAN & The Helium Blockchain: A Study on Military IoT Deployment. *Int. Conf. Cyber Warf. Secur.* **2023**, *18*, 327–337.
56. Woolley, M. The Bluetooth Low Energy Primer. *Bluetooth Blog* **2022**, *15*, 2022.

57. Gutierrez del Arroyo, J.A.; Air Force Institute of Technology Wright-Patterson AFB OH Wright-Patterson AFB United States. *Enhancing Critical Infrastructure Security Using Bluetooth Low Energy Traffic Sniffers*; Air Force Air University: Maxwell AFB, AL, USA, 2017.
58. Zubair, M.; Ghubaish, A.; Unal, D.; Al-Ali, A.; Reimann, T.; Alinier, G.; Hammoudeh, M.; Qadir, J. Secure Bluetooth Communication in Smart Healthcare Systems: A Novel Community Dataset and Intrusion Detection System. *Sensors* **2022**, *22*, 8280.
59. Joseph W.; *A Basic Guide to the HART Protocol*; Texas Instruments: Dallas, TX, USA, 2023.
60. Hall, K.B.; Ngalamou, L. Securing Wireless Scada Systems in Rural American Power Grids. In Proceedings of the IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 10–12 October 2019.
61. Rondeau, C.; Temple, M. DNA Feature Selection for Discriminating WirelessHART IIoT Devices. In proceedings of the 53rd Hawaii International Conference on System Sciences, Mānoa, HI, USA, 7–10 January 2020; https://doi.org/10.24251/HICSS.2020.782.
62. Ambarkar, S.S.; Shekokar, N. An efficient authentication technique to protect iot networks from impact of rpl attacks. *Int. J. Eng. Trends Technol.* **2021**, *69*, 137–145. https://doi.org/10.14445/22315381/IJETT-V69I10P217.
63. Ibrahim, J.; Tonga, D.A.; Danladi; Aderinola, M. Comparative Analysis Between Wired and Wireless Technologies in Communications: A Review. *Int. J. Electr. Electron. Data Commun.* **2017**, *5*, 24–27.
64. Soni, P.; Subhashini, J. Future smart grid communication-deployment of IoT: Opportunities and challenges. *Indones. J. Electr. Eng. Comput. Sci.* **2021**, *23*, 14. https://doi.org/10.11591/ijeecs.v23.i1.pp14-22.
65. Noel, A.B.; Abdaoui, A.; Elfouly, T.; Ahmed, M.H.; Badawy, A.; Shehata, M.S. Structural Health Monitoring Using Wireless Sensor Networks: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1403–1423. https://doi.org/10.1109/COMST.2017.2691551.
66. Husnoo, M.A.; Anwar, A.; Chakrabortty, R.K.; Doss, R.; Ryan, M.J. Differential Privacy for IoT-Enabled Critical Infrastructure: A Comprehensive Survey. *IEEE Access* **2021**, *9*, 153276–153304. https://doi.org/10.1109/access.2021.3124309.
67. Hafsa Benaddi; Khalil Ibrahimi; Abderrahim Benslimane, J.Q. A Deep Reinforcement Learning Based Intrusion Detection System (DRL-IDS) for Securing Wireless Sensor Networks and Internet of Thing. In Proceedings of the Wireless Internet: 12th EAI International Conference, WiCON 2019, TaiChung, Taiwan, 26–27 November 2019. https://doi.org/10.1007/978-3-030-52988-8_7.
68. Lazrag, H.; Chehri, A.; Saadane, R.; Rahmani, M.D. Efficient and secure routing protocol based on Blockchain approach for wireless sensor networks. *Concurr. Comput. Pract. Exp.* **2020**, *33*, e6144. https://doi.org/10.1002/cpe.6144.
69. Otoum, S.; Kantarci, B.; Mouftah, H. A Comparative Study of AI-Based Intrusion Detection Techniques in Critical Infrastructures. *ACM Trans. Internet Technol.* **2021**, *21*, 1–22. https://doi.org/10.1145/3406093.
70. Basu, K.; Dey, S.; Nandy, S.; Sen, A. Sensor Networks for Structural Health Monitoring of Critical Infrastructures Using Identifying Codes. In Proceedings of the 2019 15th International Conference on the Design of Reliable Communication Networks (DRCN), Coimbra, Portugal, 19–21 March 2019; pp. 43–50.
71. Subhan, F.; Noreen, M.; Imran, M.; Tariq, M.; Khan, A.; Shoaib, M. Impact of Node Deployment and Routing for Protection of Critical Infrastructures. *IEEE Access* **2019**, *7*, 11502–11514. https://doi.org/10.1109/ACCESS.2019.2891667.
72. Valdivia, L.J.; Del-Valle-Soto, C.; Rosas-Caro, J.C. Wireless communication for railway applications: Reactive and proactive protocols. In Proceedings of the 2019 International Conference on Electronics, Communications and Computers (CONIELECOMP), Cholula, Mexico, 27 February 2018–1 March 2019; pp. 21–26.
73. Yang, H. A practical method for connectivity and coverage reliability analysis for linear wireless sensor networks. *Ad Hoc Netw.* **2023**, *146*, 103183. https://doi.org/10.1016/j.adhoc.2023.103183.