fire

MDPI

Systematic Review

Reframing Data Center Fire Safety as a Socio-Technical Reliability System: A Systematic Review

Riza Hadafi Punari [1], Kadir Arifin [1,*], Mohamad Xazaquan Mansor Ali [1,*], Kadaruddin Ayub [1], Azlan Abas [1] and Ahmad Jailani Mansor [2]

[1] Centre for Research in Development, Social and Environment (SEEDS), Faculty of Social Sciences and Humanities, Universiti Kebangsaan Malaysia (UKM), Bangi 43600, Malaysia; p165964@siswa.ukm.edu.my (R.H.P.)
[2] Department of Occupational Safety and Health Malaysia, Ministry of Human Resources, Government Administrative Centre, Putrajaya 62530, Malaysia
* Correspondence: kadir@ukm.edu.my (K.A.); xazaquan@ukm.edu.my (M.X.M.A.)

Abstract

Data centers are critical digital infrastructure supporting cloud computing, artificial intelligence, and global information services. Despite their high-reliability design, they remain vulnerable to fire incidents due to continuous operation, high electrical loads, dense power systems, and the increasing use of lithium-ion batteries. Although such events are rare, their consequences can be severe, including service disruption, equipment damage, financial loss, and risks to data integrity. This study presents a systematic literature review of fire safety risk management frameworks in data centers, following PRISMA guidelines. Peer-reviewed studies published between 2020 and 2025 were retrieved from Scopus and Web of Science, screened, and appraised using structured quality criteria. Twelve empirical studies were synthesized and benchmarked against NFPA 75 and NFPA 76 standards. The findings are organized into three domains: Strategic Management, Fire Risk, and Fire Preparedness. The results show a strong focus on technical prevention and electrical hazards, while organizational readiness, emergency response, and recovery remain underexplored. Benchmarking indicates that industry standards adopt a more comprehensive lifecycle approach than the academic literature. This study reframes data center fire safety as a socio-technical reliability system and highlights critical gaps, providing a foundation for future research and improved fire safety governance and resilience.

Keywords: data center fire safety; fire safety management; fire risk management; data center resilience; critical infrastructure protection

Academic Editors: Ruiyu Chen, Pengjie Liu, Lihua Jiang and Zonghou Huang

Received: 20 February 2026
Revised: 31 March 2026
Accepted: 3 April 2026
Published: 8 April 2026

1. Introduction

In the digital economy, data centers have become the core of organizational information systems, functioning as centralized facilities for storing, processing, and distributing digital information. They house critical information technology (IT) infrastructure, such as servers, storage systems, and networking equipment, that support essential business operations, including enterprise resource planning, e-commerce, and cloud-based services [1]. Data centers play a central role in digital transformation by enabling virtualization, remote data access, and large-scale analytics. The rapid expansion of artificial intelligence, the Internet of Things (IoT), and cloud computing has significantly increased global demand for high-performance data center infrastructure [2].

In cloud computing environments, data centers provide the computational, storage, and networking resources required to deliver scalable, reliable services [3]. These infrastructures support multiple service models, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), which represent different levels of resource provisioning in data center operations [4]. Efficient resource management strategies such as optimized virtual machine (VM) allocation are essential for reducing energy consumption while maintaining service performance [5,6]. Emerging artificial intelligence techniques, including Q-learning-based optimization, further enhance dynamic resource allocation and energy efficiency [6]. In addition, modern network architectures such as fat-tree and spine–leaf topologies improve system scalability, performance, and fault tolerance [7,8]. High system availability is typically achieved through distributed storage, redundancy mechanisms, and real-time monitoring systems that support reliable and uninterrupted data services [9]. Consequently, data centers play a critical role in maintaining business continuity and operational resilience, as unplanned downtime can result in significant financial and reputational losses, with the average cost of a single outage exceeding USD 690,000 [10].

Despite their high-reliability design, data centers remain vulnerable to fire incidents due to continuous operation, high electrical loads, dense power distribution systems, and the increasing adoption of lithium-ion battery storage systems. Fires in data centers pose serious risks to both physical infrastructure and operational continuity. A single fire incident can cause severe service disruptions, resulting in downtime, data loss, and reduced productivity, particularly in industries that rely heavily on continuous computing and storage services [11]. Recovery processes are often complex and time-consuming due to the interdependent nature of IT infrastructure and service networks. From a physical perspective, fires can damage or destroy high-value equipment such as servers, power distribution units, and battery systems, with the risk amplified by dense equipment layouts and combustible materials within facilities [12,13]. In addition to direct infrastructure damage, such incidents may also generate broader environmental impacts through increased carbon emissions and resource consumption during reconstruction and repair processes [14].

To mitigate these risks, modern data centers employ a range of fire prevention, detection, and suppression technologies. Early-warning detection systems, such as Very Early Warning Smoke Detection (VEWSD) technologies, are designed to detect incipient fires before they escalate into larger incidents [15]. Fire suppression technologies have also evolved to minimize damage to sensitive electronic equipment, including water mist systems, clean-agent suppression technologies, and alternative agents such as perfluorohexanone [16,17]. In addition, innovative suppression approaches such as liquid nitrogen injection have demonstrated promising cooling and inerting capabilities with minimal damage to electronic components [18].

Beyond technical solutions, effective fire safety management in data centers requires comprehensive regulatory compliance and systematic risk management frameworks. Data center operators must comply with stringent safety standards and integrate fire protection strategies into both architectural and operational design. This includes facility compartmentalization, smoke management systems, and safe emergency egress arrangements to protect personnel and assets [19]. Continuous monitoring of environmental parameters such as temperature, humidity, and airflow is also essential to prevent overheating and other conditions that may trigger fire incidents [13,20,21]. Regular maintenance and testing of fire protection systems further ensure system reliability and operational readiness [22]. In addition, disaster recovery and business continuity planning play an important role in minimizing operational disruption following fire incidents by enabling rapid service restoration through redundant systems and cloud-based recovery mechanisms [23]. The

adoption of modular and intelligent fire control designs can also support faster detection, localized suppression, and improved system maintainability [16].

Despite these technological and regulatory developments, existing research on fire safety in data centers remains fragmented. Many studies focus primarily on technical aspects such as thermal management, electrical faults, or suppression technologies. In contrast, fewer studies examine fire safety management from a broader organizational and risk management perspective. As data centers continue to expand in scale and complexity, a comprehensive understanding of how fire safety risk management frameworks are implemented and what factors influence their effectiveness becomes increasingly important.

Unlike conventional buildings, data centers operate under unique conditions characterized by continuous operation, high-density electrical infrastructure, and strict requirements for service continuity. The presence of uninterruptible power supply (UPS) systems, lithium-ion batteries, and advanced cooling architectures introduces distinct fire risk profiles, including electrical arc faults, thermal runaway, and heat accumulation. In addition, the need to maintain uninterrupted digital services limits the feasibility of conventional fire response strategies, requiring specialized approaches to detection, suppression, and operational control. These characteristics make fire safety management in data centers fundamentally different from that in traditional facilities. Importantly, while general fire safety principles are applicable across building types, their direct application to data centers is limited due to the unique interplay between high-density electrical systems, continuous operation, and strict service continuity requirements. Unlike conventional facilities, data centers cannot rely on standard fire response strategies such as immediate shutdown, water-based suppression, or full evacuation without risking severe operational disruption. Therefore, fire safety in data centers must be understood as a specialized, context-dependent system requiring tailored risk management, detection, suppression, and recovery strategies.

Therefore, this study conducts a systematic literature review (SLR) to examine how fire safety risk management frameworks are implemented in data centers and to identify the key components that contribute to their effectiveness. The central research question guiding this review is: *How do data centers implement fire safety risk management frameworks, and what components ensure their effectiveness in mitigating fire risks and maintaining operational resilience?*

To address this question, the study pursues three main objectives:

1. To critically examine fire safety management practices implemented in data center environments.
2. To identify key fire risk factors reported in the existing literature.
3. To assess current fire preparedness and response strategies in data center operations.

By systematically synthesizing evidence from existing studies, this review aims to clarify the critical success factors for effective fire safety risk management and to highlight areas requiring further research. The findings are intended to support researchers, practitioners, and policymakers in strengthening fire safety governance and enhancing the resilience of critical digital infrastructure in an increasingly data-dependent world.

2. Methods

The methodology employed in this research was based on the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) adopted from Moher et al. [24] to formulate the research question, develop systematic searching strategies, appraise quality, and conduct data abstraction and analysis. This review included three main aspects, namely the data center (population), fire safety (interest), and risk management (context), and aims to answer the following questions: (1) How are fire safety management strategies

implemented in data centers? (2) What risk factors in the literature are contributing to fire incidents in data centers? (3) What gaps exist in current fire preparedness and response to improve fire safety management?

2.1. Systematic Searching Strategies

The three main stages in the systematic searching strategy process are identification, screening, and eligibility based on PRISMA, as shown in Figure 1.

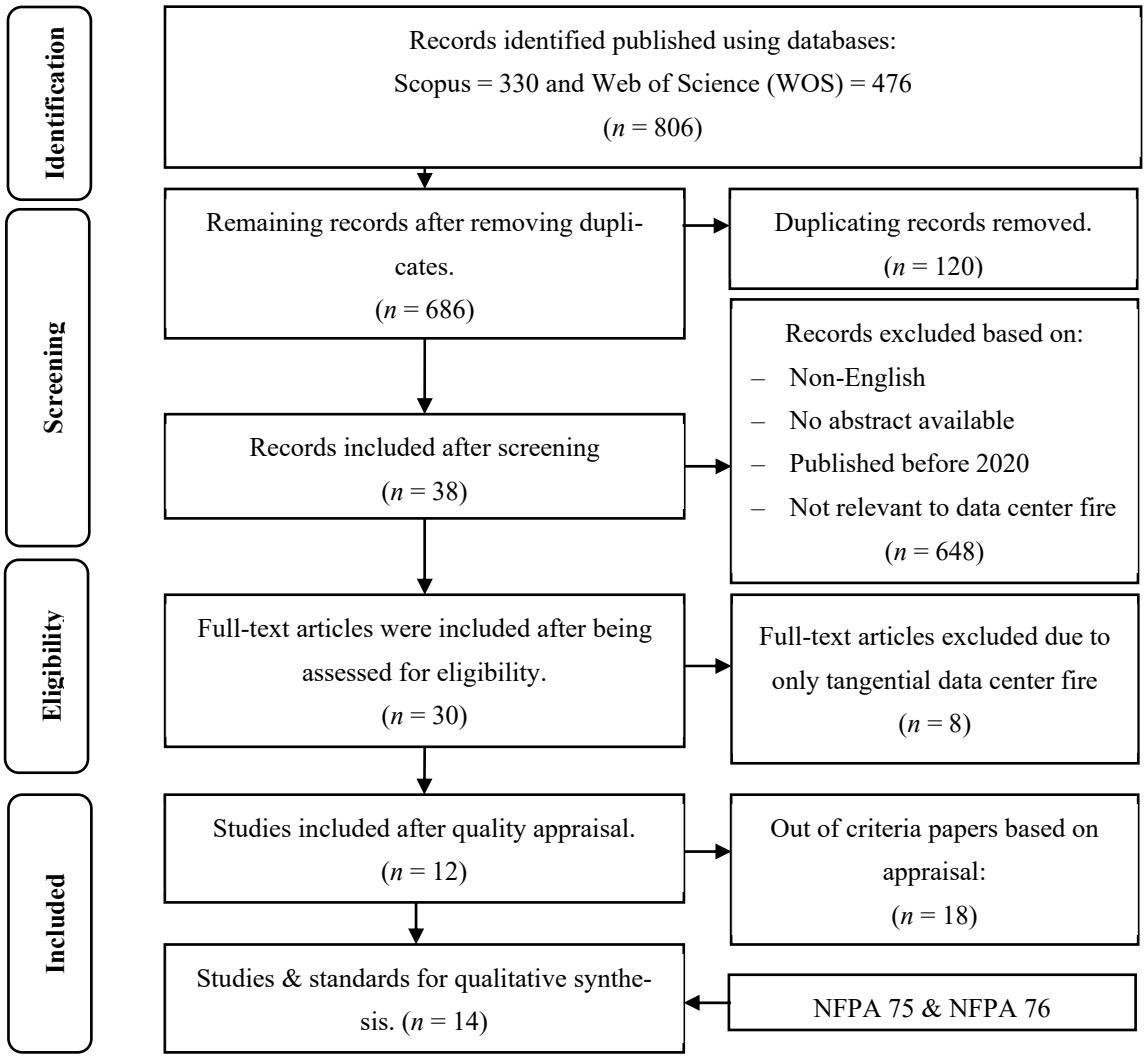

Figure 1. This outlines the core stages defined by the PRISMA framework, as adapted from Moher et al. [24].

2.1.1. Identification

The identification stage involved a systematic search of the literature using structured keyword combinations directly aligned with the research focus on data center fire safety and risk management. Unlike the earlier generic description, the search strategy was explicitly developed based on three core conceptual components: (i) data center environments, (ii) fire-related hazards and failure mechanisms, and (iii) fire safety management and suppression measures. To ensure comprehensive coverage, the search incorporated synonyms, related terms, and alternative expressions for each concept. For the data center domain, terms such as "data center", "data centre", "server room", "IT facility", "computer room", and "information and communication technology (ICT)" were used. Fire-related risks were captured using terms including "electrical fire", "arc fault", "overheating", "equipment

failure", "fire", and "fires". These were further combined with management-oriented terms such as "safety", "management", and "suppression" to ensure relevance to fire safety practices and risk control. The search strings were constructed using Boolean operators (AND, OR) to systematically integrate these three components, ensuring both breadth and specificity of results. The final search queries were applied to two major databases, Scopus and Web of Science (WoS), as detailed in Table 1. This structured search strategy yielded a total of 806 records (Scopus = 330; WoS = 476), forming the initial dataset for the subsequent screening process.

Table 1. The search strings.

Database	Search String
SCOPUS	TITLE-ABS-KEY(("data center" OR "data centre" OR "server room" OR "IT facility" OR "computer room" OR "information and communication technology" OR "ICT") AND ("electrical fire" OR "arc fault" OR "overheating" OR "equipment failure" OR "fire" OR "fires") AND ("safety" OR "management" OR "suppression"))
WOS	TS=(("data center" OR "data centre" OR "server room" OR "IT facility" OR "computer room" OR "information and communication technology" OR "ICT") AND ("electrical fire" OR "arc fault" OR "overheating" OR "equipment failure" OR "fire" OR "fires") AND ("safety" OR "management" OR "suppression"))

2.1.2. Screening

This study screened all 806 identified records using predefined inclusion and exclusion criteria. The initial filtering was supported by database sorting functions, followed by manual screening based on title and abstract. The authors removed 120 duplicate articles from the selected articles. During the screening phase, the authors applied several exclusion criteria to ensure that only relevant studies were retained for further assessment and included in the review, based on title and abstract. Publications written in languages other than English were excluded to avoid translation bias and ensure consistent interpretation of methodological details. Records without an accessible abstract were also removed, as the absence of an abstract prevents reliable preliminary assessment of a study's objectives, methods, and relevance. Studies published before 2020 were excluded to ensure alignment with current data center technologies and risk conditions. Data center infrastructure has undergone rapid transformation in recent years, including the widespread adoption of lithium-ion battery systems, increased power density in hyperscale facilities, advanced cooling architectures, and AI-driven operational controls. Earlier studies often reflect legacy system configurations and outdated fire risk profiles, which are not representative of contemporary data center environments. Therefore, restricting the review to studies from 2020 onwards ensures that the findings are technologically relevant and accurately capture emerging fire risks, particularly those associated with battery thermal runaway and high-density electrical systems.

Finally, articles that did not directly or indirectly address data center fires, fire suppression, fire propagation, thermal runaway risks, ignition mechanisms, or fire-related operational failures were excluded. These criteria ensured that the final dataset comprised only studies offering credible, up-to-date, and scientifically relevant evidence for understanding data center fire hazards and mitigation strategies. The inclusion and exclusion criteria outlined in Table 2 were used to select 38 articles and exclude 648 articles, thereby achieving the study's objectives.

Table 2. The inclusion and exclusion criteria.

Category	Inclusion Criteria	Exclusion Criteria
Language	Publications written in English	Non-English publications
Availability	Full abstract available for screening	No abstract available
Publication Year	Studies published 2020 and above	Studies published before 2020
Relevance to Topic	Studies directly or indirectly related to: i. Data center fire events ii. ignition mechanisms iii. fire suppression systems iv. thermal-runaway or overheating failures v. fire propagation or fire-induced disruptions	Studies unrelated to fire, focusing solely on: i. general cooling optimization ii. studies using data centers as computational tools for external applications (e.g., forest fire prediction, climate modelling, AI-based hazard forecasting) without addressing fire risk within the data center itself iii. energy efficiency without fire risk context iv. unrelated ICT performance topics
Study Type	Empirical, experimental, numerical, simulation, modelling, or case-study research relevant to fire behavior or fire safety in data centers	Opinion papers, editorials, non-scientific articles, posters, or studies lacking methodological detail
Document Type	Peer-reviewed journal articles or conference papers	Duplicate records, incomplete manuscripts, or non-academic sources

In addition, a substantial number of studies were excluded because they utilized data centers as computational platforms for external fire-related applications, such as forest fire prediction, climate modelling, or AI-based hazard forecasting. While these studies involve fire-related topics, they do not examine fire occurrence, ignition mechanisms, or fire prevention within data center environments. As such, they fall outside the scope of this review, which specifically focuses on fire risk and fire safety management within data center infrastructure. This exclusion criterion was necessary to maintain conceptual clarity and ensure that the synthesis remains directly relevant to data center fire safety rather than broader fire-related applications.

2.1.3. Eligibility

In the eligibility stage, the full texts of all potentially relevant articles were retrieved and thoroughly examined to determine whether they met the predefined inclusion criteria. This step ensured that only studies providing direct empirical, experimental, or modeling evidence related to data center fires, fire suppression, ignition mechanisms, thermal runaway behavior, or fire-related system failures were considered. In total, 30 articles met all eligibility requirements in the final synthesis. Meanwhile, 8 full-text articles were excluded because their focus on data center fire was only tangential. However, they mentioned overheating, thermal management, or data center operations; they did not address fire hazards, ignition processes, suppression technologies, or fire-related risk outcomes. The eligibility review ensured that the final dataset comprised only studies offering explicit and scientifically relevant contributions to the understanding of fire risk and fire safety strategies in data center environments.

2.1.4. Quality Appraisal

The remaining articles were subjected to a quality appraisal to ensure that only methodologically robust and thematically relevant studies were included. A standardized quality assessment checklist, adapted from Abouzahra et al. [25], was applied to enhance methodological rigor and transparency. Only studies that directly addressed fire safety management, fire risk factors, or fire preparedness and response in data center environments were evaluated. Three reviewers assessed each study against six criteria (QA1–QA6) to deter-

mine its relevance, analytical depth, and contribution to the review's research questions. The six criteria are:

QA1: Are the study objectives clearly stated and explicitly aligned with fire safety management in data centers?

QA2: Does the study clearly articulate its significance and practical or theoretical contribution to understanding fire risk, fire incidents, or fire safety performance in data center environments?

QA3: Is the research design or methodological approach clearly defined and appropriate for examining fire safety management practices, fire risk factors, or preparedness and response mechanisms?

QA4: Are the data sources, data collection procedures, and analytical methods described transparently and in sufficient detail to support reliable interpretation of fire safety strategies, risk factors, or preparedness gaps?

QA5: Is the study contextualized within the existing body of fire safety or data center research, including comparison or benchmarking against relevant standards, frameworks, or previous empirical findings?

QA6: Are the limitations, constraints, or contextual boundaries of the study explicitly acknowledged, particularly those affecting generalizability, applicability, or interpretation of fire safety management outcomes?

The reviewers evaluated all studies independently, and disagreements were resolved through discussion. The reviewers scored each criterion on a three-point scale, where 2 indicated complete and explicit fulfilment, 1 indicated partial fulfilment, and 0 indicated no meaningful coverage. This approach provided a consistent and transparent basis for selecting studies. In total, the reviewers appraised 30 studies shown in appendices (Table A1). Twelve studies met the quality threshold and were included in the synthesis, while 18 were excluded due to low methodological quality or limited relevance. The included studies scored between 67% and 100%, indicating adequate to high methodological rigor and strong alignment with the review objectives. In contrast, most excluded studies scored 17% to 33%, typically demonstrating only basic methodological reporting without substantive engagement with fire safety objectives, risk mechanisms, or preparedness and response.

Following the quality appraisal process, 12 empirical studies met the methodological threshold and were included in the synthesis. To strengthen analytical consistency, two benchmark fire protection standards, NFPA 75 [26] and NFPA 76 [27], were also incorporated as reference frameworks for data center and telecommunications fire safety. These standards provide authoritative guidance on fire prevention, detection, suppression, and emergency planning. Their inclusion enables the study to benchmark findings from the empirical literature against recognized industry requirements and to systematically identify both established practices and critical gaps in current fire safety management. In total, 14 sources were included in the final qualitative synthesis.

2.2. Data Extraction and Analysis

The included studies varied widely in design, ranging from simulation-based risk models to qualitative hazard assessments. To synthesize insights from this diverse body of literature, the authors applied thematic analysis, as outlined by Snyder [28], and supported their findings with basic quantitative tabulation. The analysis followed the structured approach proposed by Braun & Clarke [29] and the step-by-step process recommended by Kiger & Varpio [30]. This involved repeated reading, detailed note-taking, and inductive coding of key sections. From there, the researchers developed a set of overarching themes and sub-themes, which were then reviewed and refined for clarity and coherence.

Through this process, the findings were organized into three overarching themes: Strategic Management, Fire Risk, and Fire Preparedness.

3. Results

3.1. Thematic Distribution of Findings

The review followed a structured process of identification, screening, eligibility assessment, and inclusion, resulting in a final set of included articles that directly addressed fire safety management in data centers. Table 3 presents a structured synthesis of prior studies and standards, mapping them against three overarching analytical domains: Strategic Management, Fire Risk, and Fire Preparedness, along with their associated sub-themes. The table illustrates how existing empirical studies and authoritative standards contribute to various dimensions of fire safety management, highlighting both the coverage and gaps in the literature.

Table 3. The themes and sub-themes.

Article	Year	Country	Strategic Management								Fire Risk					Fire Preparedness		
			FRP	OR	TI	OC	CAE	PIA	OL	SI	FP	FF	CF	FFPS	EF	FERP	DCP	RRP
[31]	2020	South Korea	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
[32]	2021	Iran			x	x	x	x		x					x			
[33]	2021	South Korea			x	x	x	x	x	x								
[34]	2023	Italy			x	x		x		x					x		x	
[35]	2023	China			x	x	x	x		x					x			
[36]	2023	China	x		x	x		x	x	x	x		x	x	x		x	
[37]	2023	South Korea	x	x	x	x		x	x	x	x	x	x	x	x		x	
[38]	2024	USA	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
[39]	2025	Taiwan			x	x	x	x		x					x			
[40]	2025	China			x	x	x	x		x					x			
[41]	2025	China			x	x	x	x	x	x								
[42]	2025	China			x	x		x	x	x								
[26]	2020	USA	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
[27]	2024	USA	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x

Note: Fire Risk Planning = FRP; Organizational Readiness = OR; Technical Implementation = TI; Operational Control = OC; Compliance Audit and Evaluation = CAE; Performance and Incident Analysis = PIA; Organizational Learning = OL; Strategic Improvement = SI; Fire Potential = FP; Fire Frequency = FF; Causes of Fire = CF; Failure of Fire Prevention Systems = FFPS; Electrical Failures = EF; Fire Emergency Response Plan = FERP; Damage Control Plan = DCP; Recovery and Restoration Procedures = RRP.

Under the Strategic Management domain, most studies emphasize Technical Implementation (TI) and Operational Control (OC), indicating that engineering controls, system design, and operational procedures remain the dominant focus of fire safety research. Sub-themes such as Compliance Audit and Evaluation (CAE) and Performance and Incident Analysis (PIA) are also frequently addressed, reflecting the importance of regulatory compliance and post-incident assessment. However, Organizational Readiness (OR) and Fire Risk Planning (FRP) appear less consistently across empirical studies, suggesting that proactive organizational preparedness and structured planning are underrepresented compared to technical and operational elements. In contrast, comprehensive standards such as NFPA 75 and NFPA 76 demonstrate full coverage across all strategic management sub-themes, underscoring their holistic and prescriptive nature.

Within the Fire Risk domain, the literature demonstrates a selective focus on risk characteristics. Several studies examine Fire Potential (FP), Fire Frequency (FF), and Causes of Fire (CF), particularly in high-risk or technology-intensive environments. Nevertheless, fewer studies explicitly address Failure of Fire Prevention Systems (FFPS) and Electrical Failures (EF), despite these being well-documented contributors to fire incidents. This imbalance indicates that while fire occurrence is commonly analyzed, systemic and equipment-related failure mechanisms receive comparatively limited empirical focus. For

Fire Preparedness, the table reveals the most pronounced research gap. Only a small number of studies incorporate structured elements such as Fire Emergency Response Plans (FERP), Damage Control Plans (DCP), and Recovery and Restoration Procedures (RRP). The inclusion of these sub-themes is primarily confined to regulatory frameworks and standards (notably NFPA 75 and NFPA 76). In contrast, empirical studies tend to concentrate on prevention rather than response and recovery. This pattern highlights a reactive–preventive bias in the literature, with insufficient attention given to organizational resilience and post-incident continuity. This pattern reflects the distinctive operational nature of data centers, where fire safety is predominantly driven by electrical reliability, system continuity, and infrastructure protection, rather than occupant evacuation or conventional building fire scenarios. As a result, the observed emphasis on prevention and technical control is not merely a general safety trend but a domain-specific characteristic shaped by the operational constraints of data center environments.

Overall, Table 3 illustrates that existing research is fragmented, with strong emphasis on technical and operational controls but limited integration of strategic planning, organizational learning, and recovery-oriented preparedness. The contrast between empirical studies and comprehensive standards further highlights the need for an integrated fire safety management framework that systematically links strategic management, fire risk characteristics, and fire preparedness across the entire fire risk management cycle.

Figure 2 illustrates the geographical distribution of the 12 peer-reviewed research articles included in this study, highlighting the countries that have contributed to the existing body of literature on fire safety management in data center environments. The two additional sources included in the review, NFPA 75 and NFPA 76, are widely recognized fire protection standards used as benchmark references in the analysis and are therefore not included in the geographical distribution presented in the figure. The findings indicate a clear regional concentration of research output in East Asia, with China emerging as the most prominent contributor with five studies, followed by South Korea with three studies. This pattern reflects sustained research interest in fire risk management and infrastructure safety within technologically advanced and highly urbanized environments. Contributions from other regions are comparatively limited. The United States, Italy, Iran, and Taiwan each contributed one study, indicating sporadic but relevant engagement with the research topic. Notably, studies are absent from regions such as Africa, South America, and much of Southeast Asia, indicating a significant geographical research gap. Overall, the distribution suggests that current scholarly evidence remains concentrated in a small number of technologically advanced countries. This uneven representation highlights the need for broader geographical research to improve the generalizability of findings and to better capture contextual differences in fire risk, regulatory frameworks, and organizational preparedness across diverse socio-economic and institutional settings.

Figure 3 illustrates the temporal distribution of the reviewed papers by year of publication, providing an overview of research activity within the selected timeframe. The figure shows variation in the number of publications over the years, with relatively low representation in the earlier period, no eligible studies identified in 2022, and increased representation in 2023 and 2025. Given the limited number of included studies, this distribution should be interpreted descriptively rather than as indicative of a definitive trend. Nevertheless, the observed pattern suggests that scholarly attention to data center fire safety has grown in recent years, particularly regarding fire risk, safety management, and organizational preparedness. These observations provide contextual support for the relevance of the present review while highlighting the need for a larger, more consistent body of empirical research in this area.

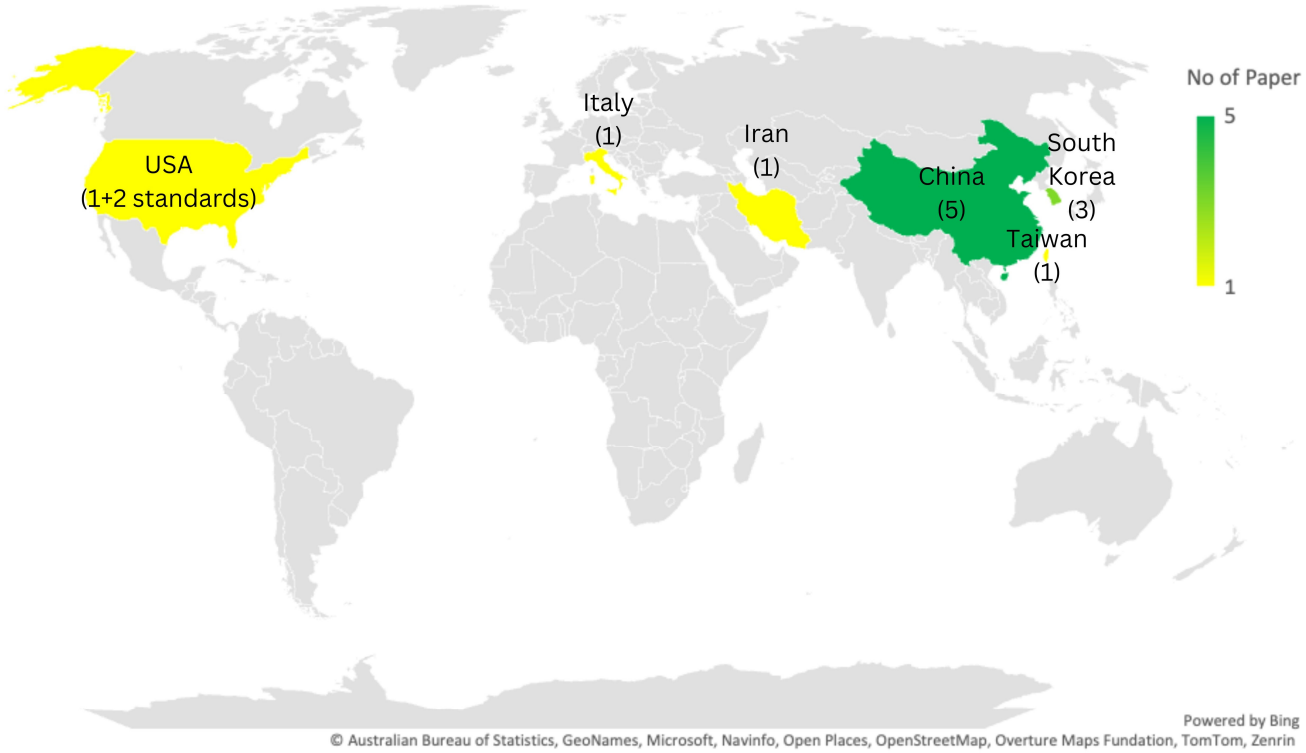

Figure 2. Number of reviewed papers and standards selected by country.

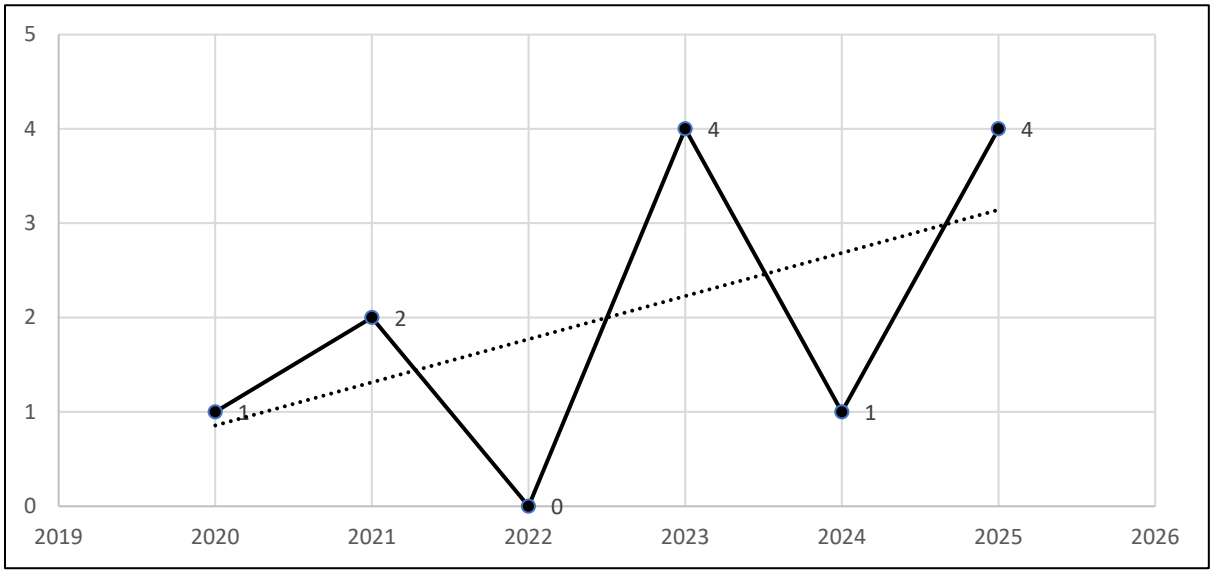

Figure 3. Number of reviewed papers selected by year published.

Table 4 summarizes the publication outlets of the studies included in this review, together with their indexing status and disciplinary focus. The distribution of papers shows that the reviewed studies are predominantly published in high-impact journals, with the majority indexed in Scopus Q1 and several also ranked Q1 in Web of Science (WOS). This indicates that the evidence base of the review is primarily drawn from well-established and reputable scholarly sources. From a disciplinary perspective, engineering-oriented journals dominate the publication landscape, including Applied Energy, Energy & Buildings, Applied Sciences, Scientia Iranica, and Thermal Science and Engineering Progress. This reflects the technical and systems-based nature of fire risk management research, which frequently focuses on infrastructure performance, energy systems, and

engineering controls. Journals within the energy and fuels domain, such as Energies, further reinforce the relevance of fire risk in energy-intensive and high-risk operational environments.

Table 4. Summary of studies by publication source.

Journal	No of Paper	SCOPUS	WOS	Field
Applied Energy	1	Q1	Q1	Engineering
Applied Sciences	1	Q1	Q3	Engineering
AUT Journal of Mechanical Engineering	1	N/A	N/A	Engineering
Energies	2	Q1	Q3	Energy & Fuels
Energy & Buildings	1	Q1	Q1	Engineering
Fire	1	Q2	Q2	Ecology
Journal of Business Continuity & Emergency Planning	1	Q4	N/A	Business Management
Journal of Cloud Computing: Advances, Systems and Applications	1	Q1	Q2	Computer Science
Journal of Electrical Engineering & Technology	1	Q2	Q3	Engineering
Scientia Iranica	1	Q2	Q2	Engineering
Thermal Science and Engineering Progress	1	Q1	Q2	Engineering

In addition to engineering and energy disciplines, the inclusion of journals such as the Journal of Cloud Computing: Advances, Systems and Applications demonstrates the growing intersection between fire safety and digital infrastructure, particularly in contexts such as data centers and information systems. The presence of the Journal of Business Continuity & Emergency Planning highlights a complementary managerial and organizational perspective, although this area remains comparatively underrepresented. Overall, Table 4 indicates that while the literature is anchored in high-quality engineering and technical journals, contributions from business management, organizational resilience, and continuity planning are limited. This imbalance suggests an opportunity for future research to integrate technical fire safety approaches with strategic management and organizational preparedness perspectives to achieve a more holistic understanding of fire risk management.

It is important to note that the relatively small number of included empirical studies reflects the limited availability of domain-specific research rather than methodological restriction, highlighting a critical gap in the existing literature.

3.2. Strategic Management

Fire incidents in data centers represent high-impact, low-frequency events with the potential to cause severe operational disruptions, financial losses, and reputational damage. The increasing complexity of data center operations, driven by high electrical loads, continuous operation, advanced cooling systems, and emerging technologies such as lithium-ion batteries, has heightened the need for a structured and strategic approach to fire safety management. Consequently, fire safety can no longer be treated solely as a technical or compliance-driven function but must be embedded within broader organizational planning and governance processes. In response to this challenge, the literature highlights a shift toward strategic fire safety planning, integrating risk assessment, organizational readiness, technical implementation, operational control, compliance assurance, performance evaluation, organizational learning, and continuous strategic improvement. This approach aligns fire safety management with principles of enterprise risk management, business continuity, and organizational resilience. Accordingly, the elements summarized in Table 5 synthesize key dimensions of strategic fire safety planning relevant to data center

environments, providing a comprehensive framework to support proactive risk mitigation, informed decision-making, and long-term operational sustainability.

Table 5. Strategic fire safety planning framework for data center operations.

Strategic Planning	Elements
Fire Risk Planning	Preventive electrical risk control measures. Recognition of elevated fire risk in data centers. Consideration of organizational failures in fire risk planning. Identification of key electrical ignition sources. Regulatory-driven fire risk planning. Adoption of risk-based fire protection programs.
Organizational Readiness	Real-time monitoring and automatic notification mechanisms. Identification of weaknesses in organizational preparedness and coordination. Management-approved emergency and response planning. Integration of fire preparedness with business continuity and disaster recovery planning.
Technical Implementation	Adoption of engineering-based fire suppression enhancements. Retrofitting and optimization of data center cooling architectures. Integration of advanced modelling, simulation, and digital tools. Implementation of thermal-aware controls at the IT and infrastructure level. Deployment of electrical fault detection technologies. Strengthening of technical fire protection systems through comprehensive standards.
Operational Control	Active regulation of cooling, airflow, and thermal parameters. Real-time monitoring and adaptive operational control systems. Continuous electrical fault monitoring with automatic power interruption. Controlled execution of fire suppression operations. Consideration of operational control failures during incidents. Implementation of procedural and operational safety controls.
Compliance Audit and Evaluation	Assessment against recognized safety standards and benchmarks. Use of threshold-based monitoring and performance indicators. Systematic review of electrical safety audit data. Post-incident audits and formal investigations. Regulatory oversight and independent compliance review mechanisms.
Performance and Incident Analysis	Systematic analysis of operational and safety performance indicators. Examination of incident, fault, and disruption data. Scenario-based and post-incident performance evaluation. Continuous performance review to support risk-informed improvement.
Organizational Learning	Leveraging operational data and experimental findings for improvement. Learning from incidents, near-misses, and failures. Identification of critical thresholds, optimal configurations, and effective technologies. Periodic review, testing, and updating of fire protection and response programs.
Strategic Improvement	Pursuit of long-term, design-oriented, and technology-enabled strategies. Integration of advanced engineering solutions and digital intelligence. Organizational and governance-level strategic transformation. Adoption of risk-based and performance-based design approaches.

Fire risk planning in data centers increasingly emphasizes a proactive and risk-based approach to prevent high-impact fire events. The preventive deployment of network-enabled arc fault circuit interrupters (AFCIs) enables the early detection and interruption of electrical faults before fire ignition, thereby strengthening primary fire prevention controls [31]. At the same time, the continuous operation of data centers, coupled with high electrical loads and aging infrastructure, has been recognized as a significant contributor to elevated fire risk, necessitating more robust and forward-looking planning strategies [36].

Evidence from major data center incidents further highlights deficiencies in fire risk planning and disaster readiness, particularly the failure to anticipate emerging hazards such as lithium-ion battery fire scenarios, which can escalate rapidly and cause extensive service disruption [38]. Electrical phenomena, such as arcs and leakage currents, are also identified as critical ignition sources, underscoring the need for systematic monitoring and fault detection as integral components of fire risk planning [37]. Accordingly, contemporary fire safety governance frameworks mandate comprehensive, risk-based fire risk assessments and protection planning that explicitly address fire scenarios, potential impacts, and business continuity requirements to ensure organizational resilience [26,27].

Organizational readiness is a critical determinant of effective fire risk management in data center operations. The use of real-time monitoring and automatic notification systems enables the immediate recognition of electrical faults and supports a timely operational response, thereby reducing the risk of escalation [31,37]. However, evidence from major data center incidents reveals persistent weaknesses in organizational readiness, including the absence of formal fire response plans, limited emergency drills, delayed incident notification, and inadequate coordination among key stakeholders, which collectively undermine effective emergency management [38]. To address these gaps, fire safety governance frameworks emphasize the need for management-approved emergency plans, regular staff training, familiarity with fire protection systems, and the systematic sharing of information with emergency responders [26]. Furthermore, organizational readiness is strengthened when fire preparedness is integrated with business continuity and disaster recovery planning, supported by coordination with authorities having jurisdiction and alignment with local firefighting capabilities, thereby enhancing overall organizational resilience [27].

Technical implementation is a key component of fire safety management in data center operations, translating strategic objectives into practical engineering and operational measures. Studies highlight the adoption of improved fire suppression technologies, including acoustic-optimized nozzles and alternative suppression agents, to reduce secondary damage during fire suppression activities [34,36]. Data centers have also implemented retrofitting and optimization of cooling architectures such as in-row cooling, aisle containment, outdoor air cooling, and advanced heat exchanger systems to enhance thermal control and system reliability under continuous operation [32,33,39,41]. The use of advanced modeling and digital tools, including computational fluid dynamics and AI-based thermal prediction, supports proactive hotspot detection and thermal risk mitigation [40,42]. At the IT level, thermal-aware operational controls, such as CPU temperature monitoring, workload consolidation, and intelligent resource scheduling, are applied to prevent overheating and cascading failures [35]. Electrical fire prevention is strengthened through the deployment of network-enabled arc fault circuit interrupters and arc or leakage current monitoring systems, enabling the early detection of ignition precursors [37]. Evidence from major incidents further suggests that existing technical fire protection systems, including battery management systems, uninterruptible power supplies, and gaseous suppression systems, may be insufficient for emerging hazards such as lithium-ion battery fires, underscoring the need for ongoing improvement in technical design [38]. Fire safety standards therefore prescribe comprehensive technical requirements covering detection, suppression, construction, power protection, and redundancy to support systematic fire risk control in data center environments [26,27].

Operational control plays a critical role in ensuring safe and reliable data center operations by maintaining stable operating conditions and enabling a timely response to emerging risks. Active regulation of cooling and airflow parameters, including air velocity, supply air temperature, aisle containment, and refrigerant flow, is essential to prevent over-

heating and maintain thermal stability during continuous operation [32,39–41]. Real-time monitoring and control systems further support the continuous adjustment of operational conditions, such as CPU workload, airflow distribution, and environmental thresholds, allowing operators to respond promptly to abnormal conditions [33,35]. Electrical safety is enhanced through continuous monitoring of arc faults, overloads, and leakage currents, combined with automatic power interruption to facilitate immediate operational response [31,37]. During fire events, controlled suppression operations, including regulated discharge conditions and mass-limited liquid nitrogen injection, help mitigate secondary damage to critical equipment [34,36]. However, evidence from major incidents indicates that delayed power isolation and ineffective initial suppression can significantly escalate incident severity in high-risk facilities [38]. Accordingly, fire safety standards require well-defined procedural controls for power disconnection, HVAC shutdown, smoke management, suppression activation, and maintenance of fire protection systems throughout the facility lifecycle to ensure consistent operational safety [26,27].

Compliance audits and evaluations ensure that fire safety and operational controls in data centers remain effective, verifiable, and aligned with regulatory expectations. System performance is commonly assessed against ASHRAE thermal standards using standardized indices and temperature compliance thresholds to determine whether operating conditions remain within acceptable safety limits [32,33,39–41]. Threshold-based safety evaluation further integrates IT-level indicators, such as CPU temperature limits, hotspot occurrences, service-level agreement violations, and energy consumption, to support systematic performance auditing [35]. Electrical safety audits rely on the structured analysis of fault and interruption data, including arc faults, overloads, and short circuits, which is enabled by networked monitoring systems [31]. Following major incidents, post-incident compliance investigations review fire safety records, battery inspections, battery management system logs, and adherence to regulatory requirements to identify gaps and corrective actions [38]. Fire safety governance is reinforced through formal regulatory oversight, including enforcement by authorities having jurisdiction, insurance inspections, periodic audits, and third-party independent review of performance-based designs to ensure ongoing compliance and accountability [26,27].

Organizational learning supports continuous improvement in fire safety management by enabling organizations to adapt practices based on evidence and experience. Organizations increasingly leverage operational data, experimental findings, and performance evidence to refine system design, improve operational practices, and enhance awareness of fire and safety risks [31,33,36,37,41,42]. Learning from incidents and near-misses enables organizations to identify deficiencies in preparedness, redundancy, and response capabilities, which in turn drive corrective actions and strengthen governance structures [38]. In addition, evidence-based identification of critical thresholds, optimal configurations, and effective technologies supports more informed safety and operational decision-making over time [35,41,42]. Fire safety standards further institutionalize organizational learning through periodic review, testing, and updating of fire protection programs, ensuring that lessons learned are systematically embedded across the facility lifecycle [26,27].

Strategic improvement reflects a shift toward long-term, technology-enabled approaches to enhance fire safety, thermal stability, and operational reliability in high-risk and mission-critical facilities. Organizations are increasingly adopting design-oriented strategies that integrate advanced engineering solutions to address both current and emerging fire risks [32,34,39,40]. These strategic improvements emphasize the use of digital intelligence, including AI-supported prediction, adaptive control, and optimized system configurations, to enhance efficiency and proactively mitigate operational and safety risks [35,41,42]. Preventive electrical and fire protection measures are increasingly viewed

as strategic investments that support long-term risk reduction, system resilience, and management effectiveness, rather than focusing solely on short-term regulatory compliance [31,36,37]. Lessons learned from major incidents further drive organizational and governance-level changes, including enhanced redundancy, separation of critical infrastructure, strengthened emergency planning, and more robust business continuity and risk governance frameworks [38]. Fire safety standards reinforce this strategic orientation through risk-based and performance-based design approaches, periodic review, third-party assurance, and flexible protection strategies that support long-term service continuity and organizational resilience [26,27].

3.3. Fire Risk

Fire risk in data centers arises from the interaction between high electrical demand, continuous operation, and complex power and cooling infrastructures. Although fire events are relatively infrequent, their consequences can be severe, resulting in service disruption, equipment damage, and significant operational losses. Effective fire risk management, therefore, requires an understanding not only of the likelihood of fire occurrence but also of the underlying technical causes, system vulnerabilities, and failure mechanisms. Table 6 summarizes the key fire risk elements in data centers, including fire potential, fire frequency, causes of fire, failures of fire prevention systems, and electrical failures, to provide a structured overview of the main factors contributing to fire risk in these environments.

Table 6. Key fire risk factors and failure mechanisms in data centers.

Fire Risk	Elements
Fire Potential	Electrical arc faults can ignite fires rapidly. Continuous operation increases fire potential. High electrical loads raise fire risk. Lithium-ion batteries increase fire potential. DC systems pose fire and shock risks. Dense electrical installations elevate fire potential.
Fire Frequency	Electrical fires occur frequently nationwide. Arc faults are a common fire cause. Data center fires are rare but severe. Fire incidents cause major service disruption. Some unplanned outages involve fire or smoke.
Causes of Fire	Electrical faults are primary fire causes. Overloads and short circuits trigger fires. Aging infrastructure increases fire risk. Battery thermal runaway causes fires. DC arcs and leakage currents raise risk.
Failure of Fire Prevention Systems	Early electrical faults may go undetected. Conventional protection delays response. Battery management systems may fail. Gaseous suppression is ineffective for batteries. Traditional suppression has practical limits. System failure scenarios must be considered.
Electrical Failures	Arc faults are common failures. Overloads and ground faults occur frequently. UPS and battery systems fail under stress. Power cables and panels are critical points. DC line faults increase fire risk. Poor cooling leads to electrical failure.

Fire potential in data centers is strongly influenced by electrical and operational characteristics inherent to these facilities. Electrical arc faults are recognized as critical ignition sources due to extremely high arc temperatures, which can initiate fires rapidly within electrical systems [31]. The continuous operation of data centers, combined with high electrical loads, aging power infrastructure, and accumulated heat in cables and equipment, further elevates fire potential [26]. The increasing use of lithium-ion battery energy storage systems and uninterruptible power supply (UPS) equipment significantly amplifies fire potential, particularly in high-density and hyperscale environments where energy concentration is high [27,38]. In addition, arcs and leakage currents in direct current power systems introduce combined fire and electric shock risks, particularly in systems located near critical loads or end-users [37]. Fire safety standards, therefore, recognize that facilities with dense electrical installations inherently carry elevated fire potential, particularly where high service continuity is required [26,27]. Fire incidents related to electrical systems occur with notable frequency at the national level, with arc faults consistently identified as the dominant cause of electrical fires [31,37]. In contrast, fire incidents in data centers are relatively infrequent but are characterized by high impact and catastrophic potential when they occur, often resulting in major service disruptions and prolonged outages [38]. Electrical arcs and leakage currents are also frequently reported contributors to electrical accidents, reinforcing their relevance in fire risk assessment despite the lower overall frequency of data center fire events [37]. Industry surveys further indicate that unplanned outages are common in data center operations, with a proportion of these events linked to fire and smoke incidents, highlighting persistent exposure to fire-related risks even under low-frequency conditions [26].

The causes of fire in data center environments are predominantly electrical in nature. Electrical faults, including arc faults, short circuits, overloads, and deteriorated wiring, are consistently identified as primary sources of fire ignition across multiple studies and standards [26,27,31,36]. High electrical loads, aging infrastructure, and continuous operation contribute to the overheating of servers, power equipment, and battery systems, thereby increasing the likelihood of fire initiation [26,36]. Lithium-ion battery thermal runaway represents a particularly critical cause of fire, especially in high-density battery and UPS installations, where energy release can be rapid and difficult to control [38]. Furthermore, direct current systems present elevated fire and electric shock risks due to arcs and leakage currents that are difficult to detect using conventional protection devices [37].

Failures of fire prevention systems can significantly increase the severity of fire incidents in data centers. Conventional electrical protection and fire suppression systems may fail to detect early-stage faults or emerging hazards, resulting in delayed response and increased fire escalation risk [31,37]. Evidence from major incidents shows that battery management systems and gaseous fire suppression technologies can be ineffective against self-oxidizing lithium-ion battery fires, limiting their protective capability [38]. In addition, traditional fire suppression systems are subject to practical limitations, including high cost, restricted applicability, and potential equipment damage, which has prompted the exploration of alternative fire protection strategies [36]. Fire safety standards therefore recognize that fire protection systems may be impaired and require explicit consideration of system failure scenarios within risk-based and performance-based fire safety designs [26,27].

Electrical failures play a central role in fire initiation and escalation within data center environments. Common electrical failure modes associated with fire incidents include arc faults, overloads, short circuits, ground faults, voltage surges, and transformer or panel failures [26,27,31]. Critical components such as UPS systems, power cables, battery racks, and direct current distribution lines are frequently involved in electrical fire events due to their high energy density and continuous operation [36–38]. Inadequate thermal

management further exacerbates these risks, as overheating increases the likelihood of equipment failure and subsequent electrical faults, even in cases where fire incidents are not immediately reported [32,35,39,40].

3.4. Fire Preparedness

Fire preparedness is a critical component of data center risk management, as it determines an organization's ability to detect, respond to, control, and recover from fire incidents with minimal disruption to operations. Given the high concentration of electrical equipment, power systems, and mission-critical digital infrastructure, even minor fire events can escalate rapidly if preparedness measures are inadequate. Effective fire preparedness therefore extends beyond compliance with fire codes, encompassing coordinated planning, technical readiness, and organizational capability to manage emergencies and restore services promptly. In this review, fire preparedness is conceptualized through three interrelated components: Fire Emergency Response Planning, Damage Control Planning, and Recovery and Restoration Procedures. As summarized in Table 7, these components collectively address the full emergency lifecycle, from early fault detection and coordinated response, through damage limitation, to systematic recovery and organizational learning. Together, they provide a structured framework for strengthening operational resilience, ensuring business continuity, and reducing the cascading impacts of fire incidents in data center environments.

Table 7. Key fire preparedness components for data center risk management.

Fire Preparedness	Elements
Fire Emergency Response Plan	Immediate fault and fire detection Automatic notification to safety managers Clear emergency roles and responsibilities Coordination with local fire authorities Defined power isolation decision process Staff training and emergency drills
Damage Control Plan	Automatic power shutdown to limit escalation Early isolation of affected electrical zones Rapid fire suppression to control spread Smoke and heat containment measures Protection of critical IT equipment Prevention of secondary damage
Recovery and Restoration Procedures	Identification of root cause and affected systems Phased power and system restoration Server and IT service recovery Data integrity checks and replication Service prioritization for critical operations Post-incident review and corrective actions

Effective fire emergency response in data centers relies on early detection of fire and electrical abnormalities through real-time monitoring systems, enabling timely recognition of emergency conditions and rapid decision-making by safety managers [31,37]. Automatic notification and alarm systems facilitate immediate communication among operators, emergency response teams, and relevant authorities, thereby reducing response delays [26,31,43]. Clearly defined roles, responsibilities, and command structures are essential to ensure coordinated action during fire incidents [26,27]. In addition, pre-established emergency response plans, shared with local fire departments, enhance situational awareness and improve the effectiveness of firefighting and power isolation decisions [26]. Regular training

and emergency drills further strengthen staff preparedness and ensure familiarity with fire protection systems and emergency procedures [26,38].

Damage control strategies focus on limiting fire escalation and minimizing equipment damage through automatic power shutdown and selective isolation of affected electrical circuits, which prevent the progression of electrical faults and fire spread [26,31]. Early detection and localization of arc faults and leakage currents enable corrective action before fire conditions intensify [37]. Rapid deployment of fire suppression systems, including clean-agent and alternative suppression technologies, reduces flame development and secondary damage to sensitive electronic equipment [34,36]. Furthermore, smoke management, compartmentation, and controlled ventilation are critical for limiting smoke propagation and protecting adjacent operational zones [26,27]. Effective damage control requires integration between electrical protection, fire suppression, and operational shutdown procedures to minimize equipment loss and service disruption [38].

Recovery and restoration procedures emphasize safe and systematic return to operation following fire incidents. Identification of the root cause of the incident through analysis of fault data and system logs supports informed corrective actions and prevents recurrence [27,31]. Phased restoration of power systems and IT infrastructure reduces the risk of re-ignition and secondary failures during recovery [38]. Restoration activities prioritize critical services, including data integrity checks, server recovery, and verification of system stability prior to full operational resumption [26]. The availability of redundant systems, backup infrastructure, and off-site data replication further enhances recovery speed and service continuity following major incidents [27]. Finally, post-incident reviews and documentation of lessons learned are essential for strengthening future emergency response, damage control strategies, and overall organizational resilience [26,27].

4. Discussion

This section critically interprets the findings derived from the included empirical studies and, where relevant, compares them with benchmarking insights from NFPA 75 and NFPA 76. To ensure analytical clarity, a clear distinction is maintained between evidence-based findings and normative recommendations from industry standards. Rather than restating results, the discussion synthesizes evidence to explain how current research emphasis, methodological choices, and geographical trends shape the understanding of fire safety management in data centers. The discussion is structured around six interrelated components. It begins by examining the imbalance in thematic emphasis within the literature, followed by a critical evaluation of strategic management practices, electrical fire risks, and preparedness gaps. The section then considers the theoretical and practical implications of the findings for safety science and industry stakeholders, before concluding with an assessment of key limitations and research gaps. Together, these discussions position the review's findings within the broader fire safety and risk management literature and highlight directions for more integrated, evidence-based, and resilience-oriented research in data center fire safety.

Although the conceptual structure of this study may appear applicable to other large-scale facilities, the empirical findings indicate that fire safety in data centers is shaped by distinct operational and technological conditions. In particular, the dominance of electrical fire risks, continuous operation, high power density, and the presence of lithium-ion battery systems create unique fire risk mechanisms and management constraints that are not typically observed in conventional facilities. These characteristics not only influence fire occurrence and propagation but also limit the applicability of standard fire response strategies, thereby requiring more specialized and system-oriented approaches to fire safety management.

4.1. Imbalance in Thematic Emphasis Within Data Center Fire Safety Research

The systematic review indicates that China emerges as the leading contributor in the reviewed literature, reflecting the rapid expansion of its data center infrastructure and strong national focus on fire safety and critical infrastructure risk. China plays a major role in the global data center sector due to its large digital economy and strong focus on artificial intelligence supported by extensive infrastructure investment and centralized planning aimed at meeting rapidly growing demand while managing energy use and resource constraints [44]. The analysis shows an increasing publication trend from 2023 onwards, with Chinese studies driving much of this growth, particularly in areas related to electrical fire risk, thermal management, battery safety, and system optimization. Most of these studies are published in high-impact, Scopus- and Web of Science-indexed engineering and energy journals, many ranked Q1 or Q2, which underscores their technical rigor and international visibility. However, the dominance of Chinese contributions also shapes the literature toward prevention and technical control, while organizational preparedness and post-incident recovery remain comparatively underexplored, indicating a clear direction for future research to balance technical advances with resilience and preparedness perspectives. Importantly, this interpretation is based on the distribution of the included empirical studies, rather than on normative expectations from industry standards.

The systematic review identified three emergent themes, namely Strategic Management, Fire Risk, and Fire Preparedness, which together provide a coherent framework for organizing the literature on data center fire safety. These themes encompass a broad spectrum of concerns, ranging from proactive organizational and technical measures to the nature of fire hazards and the capacity to respond to and recover from fire events. However, the distribution of studies across these themes is notably uneven. Most existing studies concentrate on Strategic Management, with emphasis on engineering controls, operational procedures, and regulatory compliance, as well as on Fire Risk, particularly the causes and likelihood of fire incidents. In contrast, relatively few studies focus on Fire Preparedness, including emergency response and recovery planning.

This pattern indicates that, although the literature can be systematically classified using the three themes, it is characterized by a strong preventive orientation that prioritizes fire prevention and risk mitigation over response readiness and continuity planning. The conceptual logic underpinning the themes is robust, as they collectively reflect the full fire safety management cycle, including pre-incident planning, hazard and risk characterization, and preparedness for post-incident response and recovery. Nevertheless, the extent of research attention within each theme is uneven. For instance, the majority of empirical studies address technical safeguards and operational controls, whereas only a limited number examine structured emergency response plans or formal recovery protocols. Focus should be on fire safety management, which is crucial for data centers to prevent catastrophic data loss, ensure business continuity, protect expensive equipment, safeguard personnel, and maintain operations [19,45].

Accordingly, while the thematic framework captures all essential dimensions of fire safety management, the depth of coverage within each theme remains partial. This imbalance highlights clear research gaps, particularly in the area of preparedness, which are examined further in the subsequent discussion. Overall, the thematic structure provides an effective synthesis of a fragmented body of literature, demonstrating that current research strongly advances knowledge on prevention and risk assessment but offers comparatively limited insight into organizational resilience and post-fire recovery. This distribution underscores the need for more integrative research that explicitly links strategic management, fire risk analysis, and preparedness measures, treating them not as isolated components but as interdependent elements of a comprehensive fire safety management approach.

The limited number of empirical studies included in this review should not be interpreted as a methodological limitation, but rather as an indication of the underdeveloped state of research in this domain. Despite a large initial dataset, most studies were excluded due to lack of direct relevance to data center fire safety, reinforcing the observation that current research is fragmented and predominantly focused on adjacent or technical domains. This further justifies the need for a more integrated and empirically grounded research agenda.

4.2. Strategic Management Practices and Gaps in Data Center Fire Safety

Strategic management in data center fire safety encompasses the planning, implementation, control, auditing, and improvement processes required to maintain safe and reliable operations. The literature shows that data centers place strong emphasis on fire risk planning and technical implementation, although the depth of coverage varies and several gaps remain. From a planning perspective, many studies and industry frameworks highlight the importance of systematic risk assessment and structured fire safety plans, including the application of general risk management frameworks such as ISO 31000 to identify fire hazards and mitigation measures [46,47]. However, proactive planning for emerging risks remains limited, as only a small number of studies explicitly address scenarios such as lithium-ion battery fires or cascading system failures, despite their growing relevance. This suggests that while fire risk planning is widely acknowledged, its scope does not yet fully reflect the evolving risk profile of modern data centers.

In contrast, technical implementation is a well-developed area within the literature. Numerous studies document the engineering controls used to prevent and manage fires, including high-sensitivity detection systems such as very early warning smoke detection and aspirating sensors, as well as advanced suppression technologies such as clean agents, inert gases, and water mist systems [19,48]. Research has also explored innovative approaches, including acoustic nozzle discharge systems and liquid nitrogen injection, aimed at suppressing fires while minimizing damage to sensitive equipment. This strong technical focus aligns closely with standards such as NFPA 75, which provide detailed requirements for detection and suppression in information technology environments. Nevertheless, much of this work is descriptive or design-oriented, with relatively few studies assessing system performance during real incidents or evaluating long-term reliability. Evidence from major fire events further indicates that technical systems alone may be insufficient if they are poorly maintained or inadequately integrated into operational procedures, highlighting an emerging recognition in the literature that technology must be supported by robust management practices [49]. While the reviewed empirical studies predominantly emphasize technical controls and engineering solutions, NFPA 75 and NFPA 76 adopt a broader, lifecycle-based approach, explicitly incorporating emergency planning, organizational readiness, and recovery processes. This contrast highlights a clear misalignment between the empirical research focus and industry expectations, indicating that current academic work remains largely prevention-centric.

Operational control and compliance auditing are also recognized as important components of strategic fire safety management. Operational control includes routine monitoring, maintenance, and adherence to safety procedures that reduce the likelihood of ignition and escalation. Studies consistently emphasize the role of environmental monitoring, particularly temperature, electrical load, and airflow, in preventing overheating and electrical failures. Some researchers propose real-time monitoring dashboards to support continuous oversight of critical fire protection systems, reinforcing the value of operational vigilance [50–52]. While operational parameters are commonly discussed, integrated operational protocols such as coordinated emergency shutdown procedures receive less attention

outside of formal standards. Compliance audit and evaluation are addressed primarily through reference to codes and best practice guidelines rather than detailed empirical investigation. Available evidence suggests that regular inspection, testing, and maintenance, often required by fire safety standards, are associated with improved fire containment and reduced downtime [53]. However, academic studies rarely provide detailed insight into internal audit processes or safety culture assessments within data centers, limiting understanding of how rigorously these requirements are applied in practice.

Continuous improvement, encompassing organizational learning and performance review, is the least developed aspect of strategic management in the literature. Performance reviews are essential for aligning individual efforts with organizational goals and fostering continuous improvement [54]. A limited number of sources acknowledge the importance of learning from incidents and near misses, where post-incident investigations can identify weaknesses in equipment, procedures, or training and inform corrective actions. Despite this conceptual recognition, empirical documentation of learning processes in data center fire safety is scarce, likely due to the infrequency of major incidents and the sensitivity surrounding operational failures. Although standards require periodic reviews, drills, and updates to fire safety plans, research evidence describing how these activities contribute to sustained improvement remains limited. Overall, the strategic management literature provides strong coverage of technical and operational dimensions of fire safety, but offers less insight into organizational preparedness, safety culture, and continuous learning. This imbalance suggests a need for future research to integrate perspectives from broader safety management and organizational resilience scholarship to complement the existing emphasis on engineering solutions.

4.3. Electrical Hazards and High-Consequence Fire Risks in Data Centers

The fire risk theme addresses the hazards, failure mechanisms, and event characteristics associated with fires in data centers. The literature consistently identifies electrical faults as the dominant cause of fires, reflecting the high electrical loads and continuous operation of these facilities. Common ignition sources include wiring defects, overloaded circuits, uninterruptible power supply failures, and arc faults, with the latter posing particular danger due to their extremely high temperatures. Aging infrastructure and thermal runaway in lithium-ion batteries further increase fire risk, especially in facilities with large battery banks. These findings align with fire safety standards such as NFPA 75 and NFPA 76, which emphasize electrical and battery-related hazards in risk assessments. However, it is important to note that this alignment reflects conceptual consistency rather than direct empirical validation, as most included studies do not explicitly evaluate these standards in practice. Although there is strong agreement on fire causation, much of the evidence is based on case reports rather than large-scale statistical analysis because data center fires are relatively rare.

In terms of occurrence, data center fires are widely described as low-probability but high-consequence events [19,36]. While confirmed incidents are infrequent, their impacts can be severe, including prolonged downtime and significant infrastructure loss [49,55]. This risk profile justifies strong preventive measures despite the low likelihood of occurrence. However, limited data sharing and underreporting of minor incidents and near misses constrain accurate assessment of fire frequency and recurrence. The literature also highlights gaps in early detection, as some electrical faults may not produce immediate smoke and can escape standard detection systems. Advanced electrical monitoring technologies are recommended but remain underexplored in research. Finally, fire risk modelling studies, including simulations and probabilistic approaches, provide valuable insights into technical vulnerabilities but are limited by data scarcity and often exclude

organizational and human factors. As a result, current models identify key technical risks effectively but do not fully capture the complexity of real-world fire events in data center environments.

4.4. Fire Preparedness Gaps in Data Centers

Fire preparedness refers to a data center's ability to respond effectively to a fire, limit damage during the incident, and recover operations afterwards. The review shows that this theme is the least developed in the literature, with very limited empirical evidence despite its clear importance. Industry standards such as NFPA 75 provide detailed guidance on emergency response planning, damage control, and recovery procedures, yet few academic studies examine how these requirements are implemented or tested in practice. Research rarely evaluates the existence or effectiveness of fire emergency response plans, emergency drills, or coordination with local fire authorities, even though post-incident analyses often reveal weaknesses in organizational readiness. It is essential to protect personnel through early warning and evacuation, ensure continuity of critical operations, safeguard high-value equipment and data from fire damage, and maintain compliance with mandatory fire safety regulations and standards [19]. Similarly, while technical damage control measures such as power isolation, fire suppression, and smoke management are discussed, they are usually treated in isolation rather than as part of an integrated response strategy that includes human decision-making under pressure. Recovery and restoration after a fire are even less explored, with most studies focusing on IT service continuity rather than physical facility recovery, post-fire investigation, or organizational learning.

Overall, fire preparedness remains largely guided by standards and practitioner experience rather than systematic research, highlighting a major gap in understanding how data centers actually respond to fires, restore operations, and translate lessons learned into improved resilience. The imbalance is not merely descriptive but represents a critical gap in the current body of knowledge. While the literature provides substantial insight into technical prevention and fire risk mechanisms, it offers limited empirical evidence on how data centers prepare for, respond to, and recover from fire incidents in real operational contexts. This gap is particularly significant given that data centers operate as high-reliability, low-tolerance systems, where resilience depends not only on prevention but also on organizational readiness, coordinated emergency response, and recovery governance. Therefore, future research should move beyond prevention-centric approaches and adopt a lifecycle-based and socio-technical perspective that integrates technical systems with human, organizational, and resilience-oriented dimensions.

This observation is not conceptual but empirically derived, as only a limited number of the included studies explicitly address structured preparedness components such as emergency response planning, damage control, and recovery procedures (see Table 3). This limitation is particularly critical in data center environments, where preparedness is not solely concerned with life safety but also with maintaining service continuity and minimizing system disruption. This dual requirement differentiates data center fire preparedness from conventional facilities and further highlights the need for domain-specific research.

4.5. Systematic Literature Contributions

Overall, the discussion reveals that the current evidence base is largely descriptive and technically oriented, whereas industry standards reflect a more integrated and resilience-focused framework, reinforcing the need for stronger empirical research on organizational and preparedness dimensions.

This study makes four original and field-critical contributions to the literature on data center fire safety risk management. First, this systematic literature review shifts the per-

spective on data center fire safety from engineering control to a socio-technical risk system. Most existing studies conceptualize data center fire safety primarily as an engineering or thermal management problem, with emphasis on detection, cooling, and suppression technologies. In contrast, this systematic review integrates Strategic Management, Fire Risk, and Fire Preparedness into a single analytical framework that captures the full fire-risk life cycle, from prevention and fault development to emergency response and recovery. By mapping empirical studies against organizational readiness, compliance, operational control, learning, and restoration functions, the review demonstrates that fire safety in data centers operates as a socio-technical reliability system rather than a purely technical one. This positioning aligns data center fire safety with High-Reliability Organization principles and enterprise risk management theory, where system safety emerges from the interaction of technology, human decision-making, and organizational governance. This reframing is critical for modern hyperscale and cloud-based facilities, where business continuity, reputational exposure, and digital service resilience are as strategically important as physical fire suppression performance.

Second, a key theoretical contribution of this study is the first systematic benchmarking of peer-reviewed data center fire safety research against NFPA 75 and NFPA 76. The analysis shows that these standards comprehensively address all three domains of fire safety management, namely strategic management, fire risk, and fire preparedness, whereas the academic literature remains heavily concentrated on technical prevention and system design. Critical elements such as organizational readiness, emergency response, recovery planning, and post-incident learning are largely absent from empirical studies despite being explicitly required by the standards. This reveals a structural gap in the knowledge base: industry fire governance has evolved into a mature, lifecycle-based risk system, while academic research remains fragmented and prevention-centric. By exposing this misalignment between how data centers are regulated and how they are studied, the review helps explain why many organizational and resilience-related fire risks remain weakly theorized and poorly evidenced in the scientific literature.

Third, this review makes a critical empirical contribution by clarifying why robust and comprehensive fire-incident datasets do not exist for data centers. Evidence from both the literature and regulatory standards reveals three structural barriers. First, commercial confidentiality discourages disclosure because fire incidents imply service disruption, data exposure, insurance liability, and reputational risk, particularly when events are internally contained. Second, regulatory reporting gaps arise because many incidents are suppressed by in-house systems without fire brigade involvement and are therefore logged as electrical faults, smoke events, or equipment failures rather than as fires in national statistics. Third, security-driven opacity classifies fire logs, battery events, UPS failures, and near-misses as critical infrastructure information, restricting public access even when incidents occur. Consequently, most scientific studies rely on simulations, experiments, and forensic case analyses rather than population-level fire records. This study is therefore not constrained by weak data availability; instead, it exposes the systemic under-reporting bias embedded in the data center industry itself, which represents a substantive and previously unarticulated contribution to fire-risk science.

Lastly, although the existing literature provides detailed insight into how fires originate in data centers, it offers limited evidence on how organizations actually respond when fire events occur and how operations are restored afterwards. This review shows that emergency response planning, damage control strategies, and recovery and restoration procedures are defined primarily by industry standards rather than by empirical research. This gap is particularly problematic because data centers operate as high-reliability, low-tolerance systems, where survival during a fire depends less on ignition mechanisms

than on response speed, power isolation, coordination, and recovery governance. By systematically documenting this imbalance, the study establishes a new research frontier focused on operational resilience, emergency governance, and post-fire recovery in critical digital infrastructure, shifting the field beyond prevention-centric fire engineering toward true system reliability.

The study found that fire incidents in data centers are systematically under-represented in public datasets. This is not because fires do not occur, but because the industry is governed by confidentiality, commercial sensitivity, and security regulations. Many incidents are recorded as electrical faults, smoke events, or battery failures rather than fires, particularly when suppression systems contain the event internally. As a result, academic research relies heavily on engineering experiments, simulations, and forensic case analyses rather than population-level statistics. This study therefore does not interpret the absence of large fire databases as a weakness of the field, but as an inherent characteristic of critical digital infrastructure industries.

4.5.1. Implications for Safety Science Theory and Practical

The findings of this review have important implications for safety science theory, particularly in relation to High-Reliability Organization theory, accident causation models, and risk perception frameworks. From an HRO perspective, data centers strongly reflect principles of technical redundancy and engineered reliability through multiple layers of backup power, detection, and suppression systems, supporting the idea that robust design can reduce the likelihood of catastrophic failure. However, the review also reveals a gap in organizational and human dimensions, as preparedness activities such as regular drills, training, and organizational learning are weakly represented in both research and reported practice. This challenges the assumption that data centers fully embody HRO characteristics, suggesting a reliance on technical solutions rather than a balanced safety culture. In terms of accident causation, the findings align well with Reason's Swiss Cheese Model, as major fire incidents typically result from the alignment of multiple failures across technical, organizational, and procedural layers [56,57]. At the same time, much of the existing literature examines these layers in isolation, limiting theoretical integration of how latent organizational weaknesses interact with active technical failures. The review also highlights the relevance of risk perception theory, as fire is often treated as a low-priority risk due to its low frequency despite its potentially severe consequences. This reflects common cognitive biases associated with low-probability and high-consequence events and helps explain the limited emphasis on preparedness and recovery [12,58]. Overall, the review reinforces core safety theories while exposing a gap between theoretical expectations and practical emphasis in data center fire safety, underscoring the need for future research that integrates technical, organizational, and behavioral perspectives more explicitly.

The findings of this review provide clear practical guidance for key stakeholders involved in data center fire safety. For designers and engineers, the results emphasize the need to integrate fire safety from the earliest design stages through compartmentalization, segregation of high-risk equipment such as batteries and electrical panels, reliable cooling design, and the use of advanced detection and suppression technologies aligned with NFPA 75 and NFPA 76. For operators and safety engineers, the review highlights the importance of strict compliance with standards, regular inspection and maintenance of fire protection systems, enhanced operational monitoring for early warning signs, and the development and regular rehearsal of clear emergency response procedures. The findings also stress the value of continuous improvement through post-incident reviews, even for minor events, to strengthen organizational learning and preparedness. For policymakers and regulators, the review supports wider adoption and enforcement of recognized standards, updating

regulations to address emerging risks such as lithium-ion batteries, and encouraging transparent incident reporting and independent fire safety audits to improve industry-wide learning. Finally, for fire service responders, the results underline the importance of pre-incident planning, joint training, and close coordination with data center operators to address the unique hazards of these facilities. Collectively, these practical implications show that effective fire safety in data centers depends not only on advanced technology, but also on strong management systems, preparedness, coordination, and learning to ensure operational resilience and continuity.

4.5.2. Limitations and Research Gaps in Data Center Fire Safety Studies

Despite consolidating important insights, this review is subject to several limitations that reveal clear gaps in current knowledge on data center fire safety. Most existing studies rely on conceptual analysis, simulations, or small-scale case studies, with limited empirical validation from real operational environments. Because data center fires are rare and incident data are often confidential, research frequently depends on proxy data or laboratory assumptions, which raises concerns about external validity and generalizability. There is also a strong geographical bias toward regions with mature data center industries, while evidence from developing or high-growth regions remains scarce. In addition, the literature is fragmented, with many studies focusing on isolated elements such as detection, suppression, or risk modelling, rather than examining fire safety across the full lifecycle from prevention to response and recovery. Key gaps include a lack of empirical research on recovery and restoration after fires; limited understanding of human factors such as training effectiveness, decision-making, and human–machine interaction during emergencies; and minimal analysis of coordination with external stakeholders such as fire services and utilities. Theoretical engagement with integrated safety science frameworks is also limited, as few studies adopt a socio-technical perspective that combines technical, organizational, and human dimensions. Finally, the persistent lack of transparent incident data constrains both theory-building and practical learning. Addressing these gaps will require more empirical, cross-disciplinary, and data-driven research to strengthen both the scientific foundation and real-world effectiveness of fire safety management in data centers.

5. Conclusions

This systematic review synthesizes current research on fire safety risk management in data centers and shows that the literature is strongly dominated by technical and engineering perspectives, particularly on electrical hazards, thermal management, and fire suppression systems. While this focus reflects the high-impact nature of data center fires, it also indicates a narrow emphasis on prevention, with less attention given to response capability and organizational resilience. Three interrelated themes were identified: Strategic Management, Fire Risk, and Fire Preparedness. Together, these themes represent the full fire safety management cycle, yet research coverage is uneven. Strategic management practices and fire risk mechanisms are well documented, whereas fire preparedness, including emergency response, damage control, and post-fire recovery, remains underexplored. This imbalance suggests that fire safety in data centers is often treated as a technical problem rather than a socio-technical system involving technology, people, and organizational processes.

The literature is geographically concentrated in technologically advanced regions, particularly China, where studies are commonly published in high-impact engineering journals. Although these contributions strengthen the technical evidence base, they also reinforce a prevention-oriented narrative and limit insights into organizational practices and recovery strategies across diverse contexts. Overall, the review confirms the relevance

of established safety science theories while highlighting a gap between theoretical expectations and research emphasis in practice. Effective fire safety in data centers requires not only advanced technologies but also integrated management, preparedness, and learning mechanisms. This study identifies a critical research gap in fire preparedness, particularly in emergency response, damage control, and recovery processes, and calls for more empirical and resilience-oriented research in these areas. Future research should therefore adopt more empirical and cross-disciplinary approaches that address human, organizational, and recovery dimensions to support resilient and sustainable data center operations.

Author Contributions: M.X.M.A., K.A. (Kadir Arifin) and R.H.P.; methodology, M.X.M.A. and R.H.P.; software, R.H.P.; validation, M.X.M.A., K.A. (Kadir Arifin) and A.J.M.; formal analysis, R.H.P. and M.X.M.A.; investigation, R.H.P.; resources, K.A. (Kadir Arifin) and M.X.M.A.; data curation, R.H.P.; writing—original draft preparation, R.H.P. and M.X.M.A.; writing—review and editing, K.A. (Kadir Arifin), K.A. (Kadaruddin Ayub), A.A. and A.J.M.; visualization, R.H.P.; supervision, K.A. (Kadir Arifin) and M.X.M.A.; project administration, M.X.M.A.; funding acquisition, R.H.P. All authors have read and agreed to the published version of the manuscript.

Funding: The authors gratefully acknowledge the support of Universiti Kebangsaan Malaysia (UKM) and Etika Info Sdn. Bhd. This research was funded under Grant SK-2025-031.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or generated in this study. All data supporting the findings are derived from published literature and publicly available standards cited in the manuscript.

Acknowledgments: The authors gratefully acknowledge the administrative and technical support provided by the Centre for Research in Development, Social and Environment (SEEDS), Faculty of Social Sciences and Humanities, Universiti Kebangsaan Malaysia (UKM) and Department of Occupational Safety and Health Malaysia (DOSH). The authors also thank colleagues and industry practitioners who provided informal insights regarding fire safety governance and data center operational practices during the conceptual development of this study. Their perspectives contributed to refining the analytical framing of the review. During the preparation of this manuscript, the authors used ChatGPT (OpenAI, GPT-5) for language refinement, structural editing, and clarity enhancement of selected manuscript sections. The authors have reviewed and edited the output and take full responsibility for the content of this publication.

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

Appendix A

Table A1. Quality appraisal result based on established criteria.

No	Paper	QA1	QA2	QA3	QA4	QA5	QA6	Criteria Fulfilled (%)	Decision
1	Cai et al. [59]	0	0	0	2	0	1	25%	Exclude
2	Zhang et al. [60]	0	0	0	2	0	1	25%	Exclude
3	Li et al. [61]	1	2	0	0	0	1	33%	Exclude
4	Tricomi et al. [62]	0	1	0	2	0	1	33%	Exclude
5	Lei et al. [63]	0	1	0	2	0	1	33%	Exclude
6	Tang et al. [64]	0	0	0	2	0	1	25%	Exclude
7	Strianese et al. [34]	2	2	2	2	2	1	92%	Include
8	Hong et al. [65]	0	0	0	2	0	1	25%	Exclude
9	Olabisi & Mayowa [66]	0	0	0	2	0	1	25%	Exclude
10	Singh et al. [39]	2	2	2	2	2	2	100%	Include
11	Wang et al. [40]	2	2	2	2	2	2	100%	Include
12	Wang et al. [67]	0	0	0	2	0	1	25%	Exclude
13	Narimani & Abbassi [32]	2	2	2	2	2	2	100%	Include

Table A1. *Cont.*

No	Paper	QA1	QA2	QA3	QA4	QA5	QA6	Criteria Fulfilled (%)	Decision
14	Song & Chen [68]	0	0	0	2	0	1	25%	Exclude
15	Zhong et al. [69]	0	0	0	2	0	1	25%	Exclude
16	Mao et al. [35]	2	2	2	2	1	1	83%	Include
17	Cicek & Sarı [70]	0	0	0	2	0	2	33%	Exclude
18	Kong & Ra [31]	2	2	2	2	2	1	92%	Include
19	Meng et al. [36]	2	2	2	2	2	1	92%	Include
20	Hwang & Lee [33]	1	1	2	2	1	1	67%	Include
21	Hsu et al. [71]	0	0	0	2	0	0	17%	Exclude
22	Hefley et al. [38]	2	2	2	2	1	1	83%	Include
23	Cheng et al. [41]	1	1	2	2	1	1	67%	Include
24	Han & Yoon [37]	1	2	2	2	2	1	83%	Include
25	Guo et al. [42]	1	2	2	2	1	2	83%	Include
26	Atkinson et al. [72]	0	0	0	2	0	0	17%	Exclude
27	Su & Chen [73]	0	0	0	2	0	0	17%	Exclude
28	Bognár et al. [74]	0	0	0	2	0	0	17%	Exclude
29	Akbar et al. [75]	0	0	0	2	0	0	17%	Exclude
30	Aghasi et al. [76]	0	0	0	2	0	0	17%	Exclude

References

1. Finch, P.; Eng, C. Indirect evaporative cooling drives data center efficiency. *ASHRAE J.* **2020**, *62*, 40–47. Available online: https://kaodata.com/uploads/resources/ASHRAE-Kao-Data-Indirect-Evaporative-Cooling-Drives-Data-Center-Efficiency-2020.pdf (accessed on 2 April 2026).
2. Chen, T.; Gao, X.; Chen, G. The Features, Hardware, and Architectures of Data Center Networks: A Survey. *J. Parallel Distrib. Comput.* **2016**, *96*, 45–74. [CrossRef]
3. Rage, A.N. The Cloud Computing: A Review Paper. *Str. Art Urban Creat.* **2025**, *6*, 980–989. [CrossRef]
4. Goyal, S.; Bhushan, S. An Optimized Model for Energy Efficiency on Cloud System Using PSO & CUCKOO Search Algorithm. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 138–144. [CrossRef]
5. Manjunatha, S.; Suresh, L. Minimization of Energy Using Heuristic Resource Allocation and Migration for Cloud Computing. *Int. J. Knowl. Syst. Sci.* **2021**, *12*, 74–83. [CrossRef]
6. Mohammadi, P. Achieving Cost Efficiency in Cloud Data Centers through Model-Free Q-Learning. In *Proceedings of the International Conference on Electrical and Electronics Engineering*; Springer Nature: Singapore, 2024; pp. 457–468.
7. Chkirbene, Z.; Hamila, R.; Foufou, S. A Survey on Data Center Network Topologies. In *Ubiquitous Networking*; Boudriga, N., Alouini, M.S., Rekhis, S., Sabir, E., Pollin, S., Eds.; Springer: Cham, Switzerland, 2018.
8. Wang, B.; Qi, Z.; Ma, R.; Guan, H.; Vasilakos, A.V. A Survey on Data Center Networking for Cloud Computing. *Comput. Netw.* **2015**, *91*, 528–547. [CrossRef]
9. Qiu, Y.; Jiang, C.; Fan, T.; Wan, J. An Edge Computing Platform for Intelligent Internet Data Center Operational Monitoring. In *Proceedings of the Communications in Computer and Information Science*; Springer: Berlin/Heidelberg, Germany, 2019; Volume 913, pp. 16–28.
10. UL LLC. *NFPA 75 and Fire Protection and Suppression in Data Centers*; UL LLC: Northbrook, IL, USA, 2015.
11. Wu, Y.; Wang, J.; An, Q.; Ding, Z.; Dai, J. Computility-Power Coupled Scheduling of Data Centers Toward Grid Resilience Enhancement. In *Proceedings of the 2024 IEEE 2nd International Conference on Power Science and Technology, ICPST 2024*; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2024; pp. 1105–1110.
12. Arifin, K.; Ali, M.X.M.; Abas, A.; Juhari, M.L.; Khalid, M.S.; Zulkifly, S.S. Linking Management Leadership and Safety Outcomes: A Multidimensional View of Safety Performance Constructs. *Int. J. Occup. Saf. Ergon.* **2025**, 1–13. [CrossRef]
13. Grabis, J.; Kampars, J.; Pinka, K.; Mosāns, G.; Matisons, R.; Vindbergs, A. Solutions for Monitoring and Anomaly Detection in Dynamic IT Infrastructure: Literature Review. In *Proceedings of the International Conference on Cloud Computing and Services Science, CLOSER—Proceedings*; Science and Technology Publications, Lda: Setúbal, Portugal, 2021; Volume 2021-April, pp. 224–231.
14. Görkem Üçtuğ, F.; Can Ünver, T. Life Cycle Assessment-Based Environmental Impact Analysis of a Tier 4 Data Center: A Case Study in Turkey. *Sustain. Energy Technol. Assess.* **2023**, *56*, 103076. [CrossRef]
15. Salwan, S. Data Center Fire Suppression. *Consult. Specif. Eng.* **2008**, *43*, 16–18.
16. Li, Z.; Liu, J. Design of Integrated Fire Prevention and Control System for Modular Data Center. In *Proceedings of the 2021 IEEE International Conference on Artificial Intelligence and Industrial Design, AIID 2021*; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2021; pp. 705–708.
17. Arifin, K.; Ali, M.X.M.; Wan Isa, W.M.Z.; Juhari, M.L.; Abas, A. Assessing Risk Management Practices on Workplace Safety Factors Among Malaysian Firefighters. *Sage Open* **2025**, *15*, 1–21. [CrossRef]

18. Wang, Y.; Su, H.; Wang, G.; Gao, L.; Du, Y. Effects of Liquid Nitrogen for Fire Prevention in Data Centers on Typical Integrated Circuit Chips. *Fire Mater.* **2025**, *49*, 1073–1087. [CrossRef]
19. Donohue, S.S.; Suski, M.; Chen, C. Fire Protection and Life Safety Design in Data Centers. In *Data Center Handbook: Plan, Design, Build, and Operations of a Smart Data Center*; Wiley: Hoboken, NJ, USA, 2021; pp. 533–550.
20. Arifin, K.; Ahmad, M.A.; Abas, A.; Mansor Ali, M.X. Systematic Literature Review: Characteristics of Confined Space Hazards in the Construction Sector. *Results Eng.* **2023**, *18*, 101188. [CrossRef]
21. Arifin, K.; Ahmad, M.A.; Abas, A.; Juhari, M.L.; Ali, M.X.M.; Mohd Fadzil, L. Identification of Root Cause of Fatal Confined Space Incidents in Malaysia and Strategies for Prevention. *Discov. Sustain.* **2024**, *5*, 36. [CrossRef]
22. Abia, D.; Aina, I.; Enigbokan, A.; Ajayi, S.; Aikhoje, E. Fire Critical Equipment Integrity Dashboard: An Effective Tool for Fire Risk Reduction. In *Proceedings of the Society of Petroleum Engineers—SPE Nigeria Annual International Conference and Exhibition, NAIC 2023*; Society of Petroleum Engineers: Richardson, TX, USA, 2023.
23. Malik, A.K.; Mann, M. Optimizing Disaster Recovery: A Comprehensive Study on Global Server Load Balancing in Network Solutions. In *Proceedings of the Lecture Notes in Electrical Engineering*; Springer Science and Business Media Deutschland GmbH: Singapore, 2025; Volume 1278, pp. 51–60.
24. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *BMJ* **2009**, *339*, 332–336. [CrossRef] [PubMed]
25. Abouzahra, A.; Sabraoui, A.; Afdel, K. Model Composition in Model Driven Engineering: A Systematic Literature Review. *Inf. Softw. Technol.* **2020**, *125*, 106316. [CrossRef]
26. *NFPA 75*; Standard for the Fire Protection of Information Technology Equipment. NFPA: Quincy, MA, USA, 2020.
27. *NFPA 76*; Standard for the Fire Protection of Telecommunications Facilities. NFPA: Quincy, MA, USA, 2024.
28. Snyder, H. Literature Review as a Research Methodology: An Overview and Guidelines. *J. Bus. Res.* **2019**, *104*, 333–339. [CrossRef]
29. Braun, V.; Clarke, V. Reflecting on Reflexive Thematic Analysis. *Qual. Res. Sport Exerc. Health* **2019**, *11*, 589–597. [CrossRef]
30. Kiger, M.E.; Varpio, L. Thematic Analysis of Qualitative Data: AMEE Guide No. 131. *Med. Teach.* **2020**, *42*, 846–854. [CrossRef]
31. Kong, H.S.; Ra, W.J. Usability of Arc Fault Circuit Interrupters with Network Function. *Sci. Iran.* **2020**, *27*, 607–613. [CrossRef]
32. Narimani, M.; Abbassi, A. Evaluation of Cooling Air Distribution System at Amirkabir University's High-Speed Data Processing Center. *AUT J. Mech. Eng.* **2021**, *5*, 153–172. [CrossRef]
33. Hwang, J.; Lee, T. Study on the Design and Operation of an Outdoor Air-Cooling System for a Computer Room. *Energies* **2021**, *14*, 1670. [CrossRef]
34. Strianese, M.; Torricelli, N.; Tarozzi, L.; Santangelo, P.E. Experimental Assessment of the Acoustic Performance of Nozzles Designed for Clean Agent Fire Suppression. *Appl. Sci.* **2023**, *13*, 186. [CrossRef]
35. Mao, L.; Chen, R.; Cheng, H.; Lin, W.; Liu, B.; Wang, J.Z. A Resource Scheduling Method for Cloud Data Centers Based on Thermal Management. *J. Cloud Comput.* **2023**, *12*, 84. [CrossRef]
36. Meng, J.; Wang, T.; Li, G.; Kang, J. Simulation Test on Cooling and Fire Suppression with Liquid Nitrogen in Computer Room of Data Center. *Fire* **2023**, *6*, 116. [CrossRef]
37. Han, S.Y.; Yoon, Y.H. Fault Analysis Method in Case of Arc and Leakage Current in Smart Grid Systems. *J. Electr. Eng. Technol.* **2023**, *18*, 4455–4461. [CrossRef]
38. Hefley, B.; Haynes, S.; Green, T. Did My App Just Crash? A Case Study of the Kakao Superapp Disruption Event. *J. Bus. Contin. Emer. Plan.* **2024**, *17*, 261–283. [CrossRef]
39. Singh, N.; Permana, I.; Agharid, A.P.; Wang, F.J. Innovative Retrofits for Enhanced Thermal Performance in Data Centers Using Independent Row-Based Cooling Systems. *Therm. Sci. Eng. Prog.* **2025**, *57*, 103101. [CrossRef]
40. Wang, N.; Guo, Y.; Huang, C.; Tian, B.; Shao, S. Multi-Scale Collaborative Modeling and Deep Learning-Based Thermal Prediction for Air-Cooled Data Centers: An Innovative Insight for Thermal Management. *Appl. Energy* **2025**, *377*, 124568. [CrossRef]
41. Cheng, H.; Yang, T.; Cheng, Q.; Zhao, Y.; Wang, L.; Yuan, W. Influence of Non-Uniform Airflow on Two-Phase Parallel-Flow Heat Exchanger in Data Cabinet Cooling System. *Energies* **2025**, *18*, 923. [CrossRef]
42. Guo, H.; Yu, H.; Zhao, S.; Chen, H.; Li, C. Improving the Local Thermal Environment in Data Centers via Supply–Demand Matching. *Energy Build.* **2025**, *347*, 116350. [CrossRef]
43. Arifin, K.; Ali, M.X.M.; Abas, A.; Juhari, M.L. Communication and Coordination as Drivers of Safety Behaviours and Outcomes in Coal-Fired Power Plants. *PLoS ONE* **2026**, *21*, e0341341. [CrossRef]
44. Zhang, N.; Duan, H.; Guan, Y.; Mao, R.; Song, G.; Yang, J.; Shan, Y. The "Eastern Data and Western Computing" Initiative in China Contributes to Its Net-Zero Target. *Engineering* **2025**, *52*, 256–261. [CrossRef]
45. Xiahou, X.; Chen, J.; Zhao, B.; Yan, Z.; Cui, P.; Li, Q.; Yu, Z. Research on Safety Resilience Evaluation Model of Data Center Physical Infrastructure: An ANP-Based Approach. *Buildings* **2022**, *12*, 1911. [CrossRef]
46. Purwanti, L.; Triyuwono, I.; Maski, G.; Pusposari, D.; Prakoso, A.; Ibrahim, M. The Impact of ISO 31000 Adoption on the Performance of Banking Companies in Indonesia. *Cogent Bus. Manag.* **2025**, *12*, 2507222. [CrossRef]

47. Widianti, T.; Firdaus, H.; Rakhmawati, T. Mapping the Landscape: A Bibliometric Analysis of ISO 31000. *Int. J. Qual. Reliab. Manag.* **2024**, *41*, 1783–1810. [CrossRef]
48. Liu, F.; Zhao, Z.; Yao, H.W.; Liang, D. Application of Aspirating Smoke Detectors at the Fire Earliest Stage. In *Proceedings of the Procedia Engineering*; Elsevier Ltd.: Amsterdam, The Netherlands, 2013; Volume 52, pp. 671–675.
49. Ansari, A.; Memon, Z.A. The Datacenter Management System Using IoT Sensors. In *Proceedings of the 2022 International Conference on Emerging Trends in Smart Technologies, ICETST 2022*; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2022.
50. Ryder, N.L.; Geiman, J.A.; Weckman, E.J. Hierarchical Temporal Memory Continuous Learning Algorithms for Fire State Determination. *Fire Technol.* **2021**, *57*, 2905–2928. [CrossRef]
51. Mendis, R.; Pathinayake, J.; Sandeepa, K.; Nalanda, C.; Pandithage, D.; Gamage, N. "AFMERS"—Advance Fire Monitoring and Emergency Response System. In *Proceedings of the 2024 International Conference on Computer and Applications, ICCA 2024*; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2024.
52. Pan, G.; Xie, Y.; Yang, Q. IoT-Based Cloud Monitoring System for Building Fires. *Int. J. Metrol. Qual. Eng.* **2025**, *16*, 1. [CrossRef]
53. Mia, M.M. A Systematic Review on the Impact of NFPA-Compliant Fire Protection Systems on U.S. Infrastructure Resilience. *Int. J. Bus. Econ. Insights* **2025**, *5*, 324–352. [CrossRef]
54. Norman, K.; Pearson, L.; Knight, K. How to Undertake Annual Appraisals and Ongoing Performance Reviews. *Nurs. Manag.* **2023**, *30*, 28–33. [CrossRef]
55. Ali, M.X.M.; Arifin, K.; Abas, A.; Ahmad, M.A.; Khairil, M.; Cyio, M.B.; Samad, M.A.; Lampe, I.; Mahfudz, M.; Ali, M.N. Systematic Literature Review on Indicators Use in Safety Management Practices among Utility Industries. *Int. J. Environ. Res. Public Health* **2022**, *19*, 6198. [CrossRef]
56. Ali, M.X.M.; Juhari, M.L.; Arifin, K.; Abas, A.; Don Ramli, D.R.; Zulkifli, S.S. Ammonia Leakage and Safety Research: A Century of Progress, Present Risks, and Future Directions through a Bibliometric Lens. *Paper Asia* **2025**, *41*, 355–373. [CrossRef]
57. Shabani, T.; Jerie, S.; Shabani, T. A Comprehensive Review of the Swiss Cheese Model in Risk Management. *Saf. Extrem. Environ.* **2024**, *6*, 43–57. [CrossRef]
58. Rigit, S.H.; Arifin, K.; Lui Juhari, M.; Ali, M.X.M.; Zulkifly, S.S. Contributing Factors to Occupational Accidents in Manufacturing Industry: Insights from a Systematic Literature Review. *Multidiscip. Rev.* **2025**, *9*, e2026075. [CrossRef]
59. Cai, Z.; Wang, C.; Luo, Q.; Chen, W. Enhancing Heat Transfer Characteristics and Optimization of a Multi-Jet Cooling System. *Appl. Therm. Eng.* **2024**, *248*, 123288. [CrossRef]
60. Zhang, Z.; Niu, B.; Zhang, Z.; Shi, M. Optimization on Jet-Induced Ventilation to Enhance the Uniformity of Airflow Distribution in Data Center. *Energy Sci. Eng.* **2021**, *9*, 1973–1996. [CrossRef]
61. Li, Y.; Zhu, C.; Gao, R.; Yang, B. Influence Mechanism of the Nano-Structure on Phase Change Liquid Cooling Features for Data Centers. *Energy Eng. J. Assoc. Energy Eng.* **2025**, *122*, 4523–4539. [CrossRef]
62. Tricomi, G.; Scaffidi, C.; Merlino, G.; Longo, F.; Puliafito, A.; Distefano, S. A Resilient Fire Protection System for Software-Defined Factories. *IEEE Internet Things J.* **2023**, *10*, 3151–3164. [CrossRef]
63. Lei, T.; Lv, F.; Liu, J.; Feng, J. Research on Electrical Equipment Monitoring and Early Warning System Based on Internet of Things Technology. *Math. Probl. Eng.* **2022**, *2022*, 6255277. [CrossRef]
64. Tang, Y.; Bai, X.; Jin, C.; Fu, Y.; Mao, W.; Xu, X. Experimental and Numerical Study on the Thermal Environment of a Data Center. *Build. Environ.* **2022**, *212*, 108741. [CrossRef]
65. Hong, S.; Dang, C.; Hihara, E.; Sakamoto, H.; Wada, M. Improved Two-Phase Flow Boiling in a Minichannel Heat Sink for Thermal Management of Information and Communication Technology (ICT) Equipment. *Appl. Therm. Eng.* **2020**, *181*, 115957. [CrossRef]
66. Olabisi, P.O.; Mayowa, A.A. Development of a Predictive Real-Time Temperature Management Framework for Data Centers Using a Hybrid Deep Learning Model. *IIUM Eng. J.* **2025**, *26*, 200–219. [CrossRef]
67. Wang, N.; Guo, Y.; Yu, H.; Shao, S. Investigation on Performance Enhancement of Micro-Channel Separated Heat Pipe in Data Center: A Coupled Heat-Mass-Flow Characterization Approach. *Appl. Therm. Eng.* **2024**, *248*, 123327. [CrossRef]
68. Song, M.X.; Chen, K. Numerical Study on the Optimal Power Distribution of Server Racks in a Data Center. *Build. Simul.* **2023**, *16*, 983–995. [CrossRef]
69. Zhong, L.; Shi, J.; Li, Y.; Wang, Z. Thermo-Hydrodynamic Features of Grooved Heat Sink with Droplet-Shaped Fins Based on Taguchi Optimization and Field Synergy Analysis. *Energies* **2025**, *18*, 3396. [CrossRef]
70. Cicek, K.; Sarı, A. A Novel Risk Assessment Approach for Data Center Structures. *Earthq. Struct.* **2020**, *19*, 471–484. [CrossRef]
71. Hsu, W.T.; Lee, N.; Yun, M.; Lee, D.; Cho, H.H. Unidirectional Wicking-Driven Flow Boiling on Tilted Pillar Structures for High-Power Applications. *Int. J. Heat Mass Transf.* **2022**, *189*, 122673. [CrossRef]
72. Atkinson, E.; Spillane, J.; Bradley, J.; Brooks, T. Challenges in the Adoption of Mobile Information Communication Technology (M-ICT) in the Construction Phase of Infrastructure Projects in the UK. *Int. J. Build. Pathol. Adapt.* **2022**, *40*, 327–344. [CrossRef]

73. Su, C.; Chen, W. Design of Remote Real-Time Monitoring and Control Management System for Smart Home Equipment Based on Wireless Multihop Sensor Network. *J. Sens.* **2022**, *2022*, 6228440. [CrossRef]
74. Bognár, G.; Szabó, P.G.; Takács, G. Thermal Characterization Methodologies for Experimental Minichannel Heat Sink Designs in Printed Circuit Board Assemblies. *Case Stud. Therm. Eng.* **2024**, *64*, 105468. [CrossRef]
75. Akbar, S.; Ur, S.; Malik, R.; Choo, K.-K.R.; Khan, S.U.; Ahmad, N.; Anjum, A. A Game-Based Thermal-Aware Resource Allocation Strategy for Data Centers. *IEEE Trans. Cloud Comput.* **2019**, *9*, 845–853. [CrossRef]
76. Aghasi, A.; Jamshidi, K.; Bohlooli, A.; Javadi, B. A Decentralized Adaptation of Model-Free Q-Learning for Thermal-Aware Energy-Efficient Virtual Machine Placement in Cloud Data Centers. *Comput. Netw.* **2023**, *224*, 109624. [CrossRef]