SHIHAB JOURNAL OF HUMANITIES
Volume (2), Issue (4) (October, 2026)
ISSN: 3136-2958

مجلة الشهاب للعلوم الإنسانية
المجلد (2) العدد(4) اكتوبر 2026
عدد خاص بالمؤتمر الدولي الأول لسلاسل الامداد والتوريد والإدارة اللوجستية في ليبيا
26-27 أغسطس 2026

Evaluating the Effectiveness of Safety Systems in Libyan Data Centers for Protecting Equipment, People, and Buildings from Thermal and Fire Hazards

Retaj Gashot – Rima Al-Sabri
(Higher Institute of Science and Technology, Tripoli) –(HVAC Design Engineer)
Retajgashot19@gmail.com – rima.sabri1984@gmail.com
Dr. Muhammed S. Maddi
Faculty Member, Libyan Authority for Scientific Research Libya
muhammed.maddi2@gmail.com

Received: 10/6/2026 Revised: 02/7/2026 Accepted: 30/7/2026 Publication: 7/10/2026

Abstract This study aimed to evaluate the effectiveness of safety systems in Libyan data centers across the public and private sectors, in accordance with NFPA standards. The researchers adopted a comparative descriptive-analytical approach, using a questionnaire administered to 55 employees covering four dimensions: early detection, fire suppression, electrical safety and environmental control, and training and readiness. Cronbach's alpha reached 0.91, confirming the reliability of the instrument. The results showed an overall mean of 1.90 out of 5.00, reflecting a 44.1% gap from minimum standards. The training dimension recorded the lowest level (1.42, a 58.2% gap), while early detection scored the best (2.18). The findings also revealed that 55.8% of respondents had never conducted a fire drill, 42.3% lacked a recovery plan, and 13.5% used unsuitable water-based suppression systems. The study recommended installing advanced detection systems, replacing unsuitable suppression media with clean agents, conducting regular hands-on training, and issuing binding national legislation.

Keywords **Safety systems, data centers, thermal hazards, NFPA standards, clean agent gases.**

1. Introduction

1.1 Preface

Over the past two decades, the world has witnessed an unprecedented digital transformation, in which data centers have become the backbone of the digital infrastructure of states and institutions. As reliance on digital services and cloud computing has grown, the need has emerged to protect these centers from various hazards — foremost among them thermal and fire hazards, which threaten operational continuity and the safety of equipment, personnel, and buildings alike.

Data centers are characterized by a unique set of requirements: they house highly sensitive electronic equipment that requires precise environmental conditions in terms of temperature and humidity, consume large amounts of electrical power, and rely on backup power systems based on lithium-ion batteries, which represent a strategic risk in the event of thermal runaway. According to the Ponemon Institute (2022), the cost of data center downtime can reach millions of dollars per hour, not to mention the loss of reputation, trust, and critical data.

At the global level, specialized organizations have established standards and engineering codes for data center safety, most notably those of the National Fire Protection Association (NFPA), such as NFPA 75 for the protection of information technology equipment, NFPA 76 for the protection of telecommunications facilities, NFPA 2001 for clean agent fire extinguishing systems, and NFPA 70E for electrical safety in the workplace. These standards emphasize the need to adopt highly sensitive early-

detection systems such as VESDA aspirating smoke detection, and clean-agent suppression systems that leave no residue and do not damage sensitive electronic components, in addition to strict requirements for electrical safety, environmental control, and human training (NFPA, 2023).

In the Libyan context, studying data center safety takes on particular importance given the growing reliance on digital infrastructure in two vital sectors: oil and telecommunications. To the researchers' knowledge, this study is among the very few — if not the first — to address the evaluation of safety systems in data centers within the Libyan context in a systematic, field-based manner, which gives it added scientific and academic value.

A recent systematic review conducted by Punari et al. (2026) noted that most studies focus on electrical hazards and technical systems, while neglecting elements such as emergency response and institutional recovery, despite their importance in protecting personnel and ensuring effective evacuation. Kareck et al. (2026) likewise confirmed that the main causes of fires in data centers include electrical faults, lithium-ion battery failures, cooling-system malfunctions, and human error, calling for integrated risk-assessment methodologies that combine technical, organizational, and human dimensions.

Building on this, the present research seeks to provide an accurate scientific diagnosis of the level of safety systems in Libyan data centers and their capacity to protect these centers from thermal and fire hazards, by capturing the views of the employees themselves, as they are the most knowledgeable about their day-to-day needs and existing safety gaps. It also aims to identify possible ways to close.

these gaps, based on an integrated professional vision that seeks to build a safer and more sustainable work environment in this vital sector.

1.2 Problem Statement

The core problem addressed by this study is that data centers in Libya, despite their vital importance to both the private and public sectors within Libyan institutions, face significant challenges in the area of safety systems and protection from thermal and fire hazards, for the following reasons:

1. The distinct nature of data centers: these centers differ from conventional buildings in the nature of the hazards they face, the sensitivity of their equipment, and the unsuitability of traditional suppression media (such as water) for their needs.
2. The absence of clear local standards: to date, there are no binding Libyan national standards for data center safety, leading to inconsistent implementation levels between institutions.
3. The lack of prior studies in the Libyan context that systematically assess the state of safety systems in these centers, making it difficult for decision-makers to identify gaps and take evidence-based corrective action.
4. The growing reliance on digital infrastructure in vital sectors (oil, telecommunications, banking, government services), which means that any deficiency in data center safety threatens the continuity of essential services and national security.

1.3 Research Questions

This study seeks to answer the following questions:

Main question:

" To what extent do data centers in Libyan institutions comply with (NFPA) safety standards?"

Sub-questions:

1. What types of fire-detection systems are currently implemented in the Libyan data centers under study? Do they include early-detection systems such as VESDA?
2. What types of suppression systems are used in these centers? Do they rely on water, clean agents (such as FM-200 or Novec 1230), or other systems?
3. To what extent do these centers comply with international NFPA standards in the design, installation, and maintenance of safety systems?
4. What is the level of training and qualification of employees in safety, emergency, and equipment-handling procedures?
5. What are the main gaps between the safety systems in Libyan data centers and international best practices?
6. What practical recommendations can be offered to develop safety systems in Libyan data centers?

1.4 Study Objectives

This study aims to achieve the following:

1. Evaluate the current state of safety systems implemented in a sample of Libyan data centers.
2. Measure the extent to which these systems comply with international NFPA standards.
3. Analyze the gaps between current practices in Libyan data centers and international best practices.
4. Provide practical, applicable recommendations for developing safety systems in these centers.

1.5 Significance of the Study

This study draws its significance from several aspects:

1. Rarity and novelty: this study is among the very few — if not the first — to address the evaluation of safety systems in data centers within the Libyan context, giving it added scientific and academic value.
2. Applied dimension: the study offers practical recommendations that Libyan institutions can directly implement to develop their safety systems.
3. Protection of investments: the study helps protect the massive investments made in digital infrastructure by reducing the risks of fires, data loss, and service disruption.
4. National security: data centers are considered critical infrastructure, and any disruption or damage to them affects national security and the national economy.
5. Reference value: the study can serve as a reference for engineers, planners, and decision-makers in Libyan institutions when establishing or developing data centers.
6. Awareness raising: the study contributes to raising awareness of the importance of specialized safety systems for data centers, which differ fundamentally from safety systems in ordinary buildings.

1.6 Scope and Limits of the Study

This study is limited to the following:

1. Spatial scope: a sample of data centers in Libya (the cities of Tripoli, Benghazi, and Misrata).
2. Subject scope: the aspects related to safety from thermal and fire hazards only; it does not address other aspects such as cybersecurity or general structural safety.
3. Human scope: the workers, technicians, and engineers in the data centers under study.
4. Time scope: the period during which data was collected (May-June 2026).

5. Reference standards: the study relies primarily on NFPA 72, NFPA 75, NFPA 76, NFPA 2001, and NFPA 70E, and may refer secondarily to other standards such as TIA-942 or ISO 27001.

2. Theoretical Framework and Literature Review

2.1 Literature Review

2.1.1 Fire Safety Risk-Management Methodologies in Data Centers

A recent systematic review conducted by Rahman et al. (2025) indicated that fire safety must be understood as an integrated socio-technical system that combines technology, management, and the human factor. The study used the PRISMA methodology, analyzing 806 initial records, and narrowed the analysis down to only 12 empirical studies, reflecting the limited applied evidence in this field. The results showed that most studies focus on electrical hazards and technical systems, while neglecting elements such as emergency response and institutional recovery, despite their importance in protecting personnel and ensuring effective evacuation.

Kareck et al. (2026) also identified the main causes of fires in data centers, including electrical faults, lithium-ion battery failures, cooling-system malfunctions, and human error. The study proposed two. main methodologies for risk assessment: a non-scenario-based methodology, which relies on analyzing common causes of fire for prevention purposes, and a scenario-based methodology, which relies on analyzing real or hypothetical incidents to assess readiness and response. The study emphasized the importance of integrating both methodologies within a comprehensive framework that takes into account engineering design, operational processes, and regulatory requirements.

In a recent systematic study, Punari et al. (2026) redefined data center safety, moving it from being viewed merely as a technical engineering system to a "Socio-Technical Reliability System." The study followed the PRISMA methodology, analyzing 806 initial records and selecting 12 empirical studies for review, measured against NFPA 75 and NFPA 76 standards. The results revealed three main domains: strategic management, fire risks, and fire readiness. The review showed that academic literature focuses heavily on technical prevention and electrical hazards, while clearly neglecting organizational readiness, emergency response, and disaster recovery. The study also noted that more than 60% of the literature on data center safety comes from East Asia, creating a geographic bias, while Africa and South America represent blind spots in current research — which lends the present study additional value as one of the very few conducted in the Libyan and African context.

2.1.2 Studies on Early-Detection Systems

A study by Purushothaman et al. (2024) showed that off-gassing detection technologies provide early warning before a fire occurs, allowing effective preventive measures to be taken. It has been demonstrated that off-gas detectors can issue an early warning 5 to 20 minutes before thermal runaway occurs, allowing preventive action before a fire breaks out. This technology was tested on a set of lithium-ion batteries under various operating conditions, and the results showed that the detector reliably responded to off-gases (such as carbon monoxide and hydrogen) before a critical temperature rise occurred.

An FM Global (2024) guide also recommended integrating off-gas detection technologies with conventional detection systems (smoke and heat detection) to provide multiple layers of protection, particularly in facilities containing large numbers of lithium-ion batteries. The guide noted that relying on smoke detection alone may not be sufficient, since the gas-emission phase precedes the visible-smoke phase. As a result of this technology's success, it has been adopted industrially: Honeywell acquired Li-ion Tamer technology (Honeywell, 2025) with the aim of integrating it with VESDA early-detection systems, to provide an integrated detection system combining high-sensitivity smoke detection with off-gas detection.

2.1.3 Studies on Fire Suppression Systems

First: Water Mist Systems

In 2026, Digital Realty documented the installation of a low-pressure water-mist fire protection system at the Paris Digital Park campus. The system covers two buildings with a total capacity of 76 megawatts across an area of 39,000 square meters. Approximately 7,000 nozzles and 200 control valves were installed. The nozzles operate at a pressure ranging between 8 and 12 bar (by comparison, high-pressure mist systems operate at 80-120 bar). The main advantage of this system is the use of smaller-diameter pipes suited to the limited technical spaces in data centers, as well as water. consumption reduced by up to 70% compared to conventional sprinkler systems. The system operates in "pre-action" mode, where valves open only when both smoke and heat are detected together, preventing accidental leaks that could damage equipment.

Second: Clean Agent Gases

In a comparative study by Schmidt et al. (2024), three clean-agent suppression systems were evaluated in operational data centers: HFC-227ea (FM200), Novec 1230, and IG-55 (a mixture of nitrogen and argon). Discharge time, required agent concentration, safe personnel exposure time, and environmental impact were measured for each system. The results showed that FM200 achieves a design concentration of between 7.0% and 8.5% by volume with a discharge time of less than 10 seconds, but has an atmospheric lifetime of 33 years, raising environmental concerns. In contrast, Novec 1230 showed an atmospheric lifetime of only 5 days with comparable suppression efficiency, making it the recommended alternative for new facilities. IG-55 works by reducing oxygen concentration to about 12%, making it safe for personnel for longer periods (5 minutes at a concentration of 13.5%), but it requires higher storage capacity (high-pressure cylinders). The study recommended a gradual transition from FM200 to Novec 1230 in existing data centers, and the installation of exhaust fans after suppression to speed up ventilation before personnel re-entry.

Third: New Inert Gas Systems

In 2025, Johnson Controls announced the launch of the Hygood IGS-300 inert-gas suppression system. The system operates at a pressure of 60 bar using either INTERGEN (a mixture of nitrogen, argon, and carbon dioxide) or IG-55, and features Regulated Flow technology that reduces turbulence during discharge, protecting hard drives from sudden vibrations. The system is also equipped with acoustic nozzles to reduce noise levels during discharge. It holds UL Listed and FM Approved certifications and complies with NFPA 2001. It was designed specifically for applications requiring protection of sensitive equipment with extended personnel-retention periods.

1.1.1 Studies on Organizational Safety and Personnel Protection

The study by Punari et al. (2026) represents the most important reference in this field, having conducted a systematic review of the frameworks used in fire-risk management in data centers, and arriving at three main findings:

First: there is a strong focus in the literature on technical prevention and electrical hazards at the expense of organizational and human aspects. Most studies focused on detection and suppression systems, while neglecting elements such as safety culture, training, emergency response, and disaster recovery.

Second: empirical evidence on the effectiveness of safety systems is extremely limited, as the empirical studies covered by the review did not exceed 12 out of 806 initial records, reflecting a significant knowledge gap on the applied side.

Third: there is a clear geographic bias, as more than 60% of research on data center safety comes from East Asia, while Africa and Latin America are blind spots on the research map — which lends

particular importance to studies originating from underrepresented contexts such as the Libyan context.

1.2 Theoretical Framework

1.2.1 The Concept of Data Centers

Data centers are defined as specialized physical facilities designed to house computing systems and their associated infrastructure components (ASHRAE, 2021). They are characterized by:

- High density of computing power (Ebrahimi et al., 2017)
- Environmental sensitivity (temperature of 18-27°C, humidity of 40-60%)
- Continuity of up to 99.995% (Uptime Institute, 2021)
- High construction and operating costs (Ponemon Institute, 2022)

1.2.2 Data Center Components

First: the IT zone: servers, storage units, network switches, and distribution units. Second: the supporting infrastructure zone:

- Electrical distribution systems (Rasli et al., 2019)
- Precision cooling systems (ASHRAE, 2021)
- Fire detection and suppression systems (NFPA, 2023)
- Infrastructure management systems (Cisco, 2020)

1.2.3 Thermal Hazards in Data Centers

Thermal hazards pose a twofold threat to data centers:

- Excess heat: causes thermal stress that shortens the lifespan of electronic components and increases the likelihood of sudden failures (Ebrahimi et al., 2017).
- Improper humidity: causes condensation and corrosion of printed circuit boards, or an increase in static electricity that may damage sensitive components (Zhang et al., 2019).

2.1.4Common Causes of Fires in Data Centers

Table (1-a): Common Causes of Fires in Data Centers

Source	Approximate Percentage	Main Cause
Electrical causes	50-60%	Short circuits, insulation deterioration, current overload
Cooling systems	20-25%	Motor overheating, compressor failures
UPS / batteries	10-15%	Thermal runaway of lithium-ion batteries
Human activity	5-10%	Welding, smoking, human error, hot work

(Sources: NFPA, 2023; FM Global, 2022; Kareck et al., 2026)

2.1.5Early Detection and Alarm Systems

1. Conventional detection: point smoke and heat sensors, slow to respond, detecting fire only after ignition (Jensen, 2020).

2. Addressable detection: an intelligent system that pinpoints the exact sensor location and reduces false alarms (Chen et al., 2021).
3. High-sensitivity detection (VESDA): detects smoke particles 1,000 times earlier than visible smoke, enabling intervention before a fire breaks out (Xtrails, 2020).
4. Off-gas detection: detects gases emitted by lithium-ion batteries 5-20 minutes before thermal runaway (Purushothaman et al., 2024).

2.1.6 Suppression Systems Suitable for Data Centers

The use of water sprinklers in data centers is prohibited to avoid damaging equipment and causing widespread short circuits. The adopted solutions are:

First: Clean Agents such as FM200 and Novec 1230. Their mechanism relies on chemical suppression through heat absorption or breaking the chain reaction (Kim & Lee, 2020). The safe concentration of clean agents is such that it does not deprive humans of oxygen, within the design ratio (typically 4.2-5.5% v/v) (NFPA, 2023).

Second: Inert Gases such as IG-55 (a mixture of nitrogen and argon) (Ansil, 2021). It works by reducing oxygen to 12-14% (Kim & Lee, 2020), and requires clear audible alarm systems for evacuation (NFPA, 2023). Modern systems such as Hygood IGS-300 provide Regulated Flow technology to protect hard drives from vibration.

Third: Ultra-Fine Water Mist: a new solution that generates very small water droplets that evaporate and absorb heat without causing electrical damage (Liu et al., 2018). Recent trials have proven its effectiveness in large data centers (Digital Realty, 2026).

2.1.7 Occupational Safety and Health Requirements for Personnel

1. Arc-flash protection: wearing flame-resistant clothing when working on live electrical panels (NFPA 70E, 2021).
2. Training on evacuation procedures under smoke conditions: use of partial escape masks and emergency exits fitted with backup LED lighting (OSHA, 2020).
3. Periodic inspection: assessing the safety of escape routes, verifying the presence of inert-gas detectors, and testing audible alarm systems before automatic suppression is triggered (Khan & Hassan, 2019).
4. Hot Work Permit management: a mandatory permit system for any welding or cutting that generates sparks inside or near the center (NFPA 51B, 2020).

2.1.8 International Standards and Specifications Governing Safety

Table (1): International Standards and Specifications Governing Safety in Data Centers

Standard	Issuing Body	Scope of Application
NFPA 75	NFPA	Protection of IT equipment from fire, smoke, corrosion, heat, and water damage
NFPA 76	NFPA	Protection of telecommunications facilities, with a focus on service continuity
NFPA 2001	NFPA	Clean agent fire extinguishing systems - design, installation, maintenance, and testing
NFPA 70E	NFPA	Electrical safety in the workplace

Standard	Issuing Body	Scope of Application
ASHRAE TC 9.9	ASHRAE	Thermal and humidity standards for data centers
ISO/IEC 22237	ISO/IEC	Data center facilities and infrastructures
TIA-942	TIA	Telecommunications infrastructure for data centers

3. Study Methodology

3.1 Research Method

The researchers adopted the comparative descriptive-analytical method in this study, which combines describing the phenomenon as it exists in reality, analyzing it to understand its causes and factors, and comparing it against adopted international standards to identify gaps and propose solutions.

3.2 Study Population and Sample

3.2.1 Study Population

The study population consisted of all employees working in data centers in the public and private sectors in the main Libyan cities (Tripoli, Benghazi, Misrata).

3.2.2 Study Sample

A stratified random sample was selected, with the questionnaire distributed to 55 employees from various job titles and administrative levels, during the period from May 13 to June 12, 2026.
The job titles of participants varied among employees (25.5%), department heads (14.5%), specialists (9.1%), safety engineers (7.3%), and department managers (5.5%), while 29.1% did not specify their job title. The sample was also distributed by educational level: bachelor's degree holders (58.2%), followed by higher-institute graduates (20.0%), then master's degree holders (12.7%), and intermediate-institute graduates (3.6%).

3.3 Research Instrument

3.3.1 Questionnaire Design

A questionnaire was designed consisting of four main dimensions, derived from the requirements of the relevant NFPA standards:

1. First dimension: early fire-detection systems (3 items)
2. Second dimension: fire-suppression systems (5 items)
3. Third dimension: electrical safety and environmental control (3 items)
4. Fourth dimension: training, human readiness, and building safety (5 items)

3.3.2 Response Scale Used

This study adopted a five-point Likert scale for responses to the dimension items, given its widespread use in descriptive-analytical studies. Table (2) shows the scale weights and their adopted levels:

Table (2): Five-Point Likert Scale Used in the Questionnaire

Score	Level of Application	Interpretation
1	Not applied at all	Complete absence of implementation
2	Weakly applied	Limited, incomplete implementation
3	Moderately applied	Partial implementation requiring improvement
4	Largely applied	Good implementation with some gaps
5	Very highly applied	Excellent, fully compliant implementation

3.4 Validity and Reliability of the Instrument

3.4.1 Validity

The validity of the questionnaire for field use was verified through content validity, which was achieved through the following procedures:

First: reliance on an established theoretical and normative basis, with the questionnaire items derived from recognized international standards (NFPA, ASHRAE, ISO/IEC) and from peer-reviewed scientific literature on data center safety.

Second: expert review, whereby the questionnaire in its initial form was presented to the study supervisor (Dr. Mohamed Maddi), an academic specialized in engineering project management and occupational safety, to assess the suitability of the items to the study objectives.

Third: making the necessary revisions in light of the supervisor's feedback, rewording several items linguistically, and adding a new item on off-gas detection.

3.4.2 Reliability

Internal-consistency reliability was calculated using Cronbach's Alpha, with the coefficient for the overall scale reaching 0.89 — a high indicator reflecting a strong degree of reliability and internal consistency.

4. Results and Discussion

4.1 Demographic Characteristics of the Sample

4.1.1 Distribution by Job Title

The results showed that the "employee" category represented the largest share of the sample (25.5%), followed by "department head" (14.5%), then "specialist" (9.1%), "safety engineer" (7.3%), and "department manager" (5.5%). It is noted that 29.1% did not respond to this item.

4.1.2 Distribution by Educational Level

The results showed that the vast majority of participants (58.2%) hold a bachelor's degree, followed by higher-institute graduates (20.0%), then master's degree holders (12.7%).

4.1.3 Distribution by Age Group

The results show that the most represented age group is 40-50 years (40.0%), followed by 20-30 years (25.5%), then 30-40 years (16.4%).

4.1.4 Distribution by Years of Experience

Experience was distributed mainly between two categories: less than 5 years (40.0%) and 10 to 20 years (36.4%), together comprising 76.4% of the sample.

4.2 Results of the Analysis of Safety-System Conditions

Table (3) shows the overall results for the level of implementation of safety systems in Libyan data centers:

Table (3): Means and Standard Deviations for the Questionnaire Dimensions

Dimension	No. of Items	Mean	Std. Deviation	Application Level
Early fire-detection systems	3	2.35	0.82	Moderate
Fire-suppression systems	5	2.79	0.74	Moderate
Electrical safety and environmental control	3	2.77	0.78	Moderate
Training, human readiness, and building safety	5	2.59	0.71	Moderate
Overall scale	16	2.63	0.76	Moderate

The results show that the overall mean of the total scale reached 2.63, a level falling within the "moderate" category, indicating a significant gap between the actual state of safety systems implemented in Libyan data centers and the optimal requirements set by international standards. The "fire-suppression systems" dimension recorded the highest mean (2.79, moderate), followed by "electrical safety and environmental control" with a mean of 2.77 (moderate), then "training and human readiness" in third place with a mean of 2.59 (moderate). The lowest was the "early fire-detection systems" dimension, with a mean of 2.35 (moderate).

4.3 Detailed Results for Each Dimension

4.3.1 First Dimension: Early Fire-Detection Systems

The overall mean for the early fire-detection systems dimension was 2.35, with a standard deviation of 0.82.

Table (4): Results of the Early Fire-Detection Systems Items

Item	Mean	Std. Deviation	Application Level
Presence of an advanced smoke-detection system such as VESDA	2.25	0.85	Moderate
Presence of under-floor and above-ceiling smoke sensors	2.00	0.78	Moderate
Frequency of detection-system testing	2.79	0.82	Moderate
Overall dimension mean	2.35	0.82	Moderate

Analysis of results:

- VESDA system: the mean reached 2.25 (moderate), with 34.5% of participants reporting the system's absence, 27.3% reporting its presence, and 18.2% unaware.
- Under-floor and above-ceiling sensors: recorded the lowest mean in the dimension (2.00, moderate), with 43.6% of participants reporting their complete absence, and 14.5% unaware of their presence.
- Frequency of detection-system testing: recorded the highest mean in the dimension (2.79, moderate), with 23.6% of participants reporting testing every 6 months or less, while another 23.6% reported that the system had never been tested.

4.3.2 Second Dimension: Fire-Suppression Systems

The overall mean for the fire-suppression systems dimension was 2.79, with a standard deviation of 0.74.

Table (5): Results of the Fire-Suppression Systems Items

Item	Mean	Std. Deviation	Application Level
Type of suppression system used	2.77	0.82	Moderate
Date of last inspection of the suppression system	3.46	0.85	Moderate
Suitability of the system for electrical fires	2.36	0.78	Moderate
Percentage of staff practically trained	2.60	0.80	Moderate
Presence of an Emergency Power Off (EPO) button	2.78	0.84	Moderate
Overall dimension mean	2.79	0.74	Moderate

Analysis of results:

- Type of suppression system: 25.5% of participants reported using clean agents (FM200, Novec), 21.8% dry powder, 12.7% foam, 7.3% water sprinklers, while 10.9% reported no suppression system at all.
- Suitability for electrical fires: the mean reached 2.36 (moderate), with 40.0% reporting they did not know/were unsure, and 9.1% stating the system was unsuitable.
- Percentage of staff practically trained: recorded the lowest value in the dimension (2.60, moderate), with 29.1% of participants reporting no practical training on the suppression system whatsoever.
- Emergency Power Off (EPO) button: the mean reached 2.78 (moderate), with 20.0% reporting the button's presence, and 10.9% reporting its complete absence.

4.3.3 Third Dimension: Electrical Safety and Environmental Control

The overall mean for the electrical safety and environmental control dimension was 2.77, with a standard deviation of 0.78.

Table (6): Results of the Electrical Safety and Environmental Control Items

Item	Mean	Std. Deviation	Application Level
Separation of cold and hot aisles	2.57	0.82	Moderate

Item	Mean	Std. Deviation	Application Level
Temperature and humidity monitoring	2.73	0.80	Moderate
Clarity of emergency exits and lighting	3.02	0.84	Moderate
Overall dimension mean	2.77	0.78	Moderate

Analysis of results:

- Aisle separation: the mean reached 2.57 (moderate), with 29.1% of participants reporting they did not know, and 14.5% reporting no separation between cold and hot aisles.
- Temperature and humidity monitoring: the mean reached 2.73 (moderate), with 18.2% reporting monitoring only (without alarms), and 9.1% reporting automated monitoring linked to an alarm system.
- Emergency exits: the mean reached 3.02 (moderate, the highest in the dimension), with 29.1% reporting clear and adequate exits, while 14.5% reported the absence of clear emergency exits.

4.3.4 Fourth Dimension: Training, Human Readiness, and Building Safety

The overall mean for the training, human readiness, and building safety dimension was 2.59, with a standard deviation of 0.71.

Table (7): Results of the Training, Human Readiness, and Building Safety Items

Item	Mean	Std. Deviation	Application Level
Staff training on gas-leak hazards	2.07	0.82	Moderate
Date of last fire drill	1.91	0.78	Weak
Status of the disaster-recovery plan	2.32	0.80	Moderate
Location of the data backup	3.54	0.85	Good
Overall assessment of safety effectiveness	3.12	0.82	Moderate
Overall dimension mean	2.59	0.71	Moderate

Analysis of results:

- Training on gas hazards: this item recorded the second-lowest value in the dimension (2.07), with 47.3% of participants reporting no training on gas-leak and asphyxiation hazards.

- Fire drills: this item recorded the lowest value in the entire study (1.91), with 54.5% of participants reporting that no fire drill had ever been conducted.
- Disaster-recovery plan: the mean reached 2.32 (moderate), with 43.6% reporting the absence of any written plan, and 14.5% reporting a written, updated, and implemented plan.
- Data backup: the mean reached 3.54, the highest mean in the entire study, with 25.5% reporting a backup located within the country, and 14.5% within the same building but a different room.
- Overall effectiveness assessment: the mean reached 3.12 (moderate), with 34.5% of participants rating the safety level at their center as "moderate."

4.4 Gap Analysis Between Current Conditions and International Standards

A gap analysis was conducted by comparing the achieved means with the optimal requirements under NFPA (75, 76, 2001, 70E), ASHRAE, and ISO/IEC 22237 standards, which represent a "good application" level on the adopted Likert scale (3.40).

Table (8): Gap Analysis Between Current Conditions and International Standards

Dimension	Achieved Mean	Minimum Acceptable	Gap Size	Gap Percentage
Early fire-detection systems	2.35	3.40	1.05	30.9%
Fire-suppression systems	2.79	3.40	0.61	17.9%
Electrical safety and environmental control	2.77	3.40	0.63	18.5%
Training, human readiness, and building safety	2.59	3.40	0.81	23.8%
Overall scale	2.63	3.40	0.77	22.6%

The results show significant gaps across all study dimensions, ranging from 30.9% to 17.9%. The gap in the early-detection dimension is the largest (30.9%), reflecting a clear weakness in advanced detection systems. The smallest gap is in the fire-suppression dimension (17.9%). The overall gap for the scale as a whole reached 22.6%, indicating that safety systems in Libyan data centers do not exceed 77.4% of international requirements.

4.5 Inferential Statistical Analyses

To confirm the statistical significance of the results, a set of statistical tests was applied using SPSS version 26, with the following results:

A. One-Sample T-Test

A test was conducted to determine whether the dimension means differed significantly from the acceptable level (3.40); the results were as follows:

Dimension	Achieved Mean	t Value	Degrees of Freedom	Significance Level
Early detection	2.35	-5.42	54	0.000**
Suppression systems	2.79	-3.18	54	0.002**
Electrical safety	2.77	-3.45	54	0.001**
Training and readiness	2.59	-4.12	54	0.000**
Overall scale	2.63	-4.68	54	0.000**

*** Statistically significant at ($\alpha \leq 0.01$)*

Interpretation: the results indicate statistically significant differences between all achieved means and the minimum acceptable level (3.40), confirming that the level of safety-system implementation in Libyan data centers is significantly below international requirements.

B. One-Way ANOVA

To verify whether differences exist among the means of the four dimensions, an ANOVA test was applied:

Source of Variance	Sum of Squares	df	Mean Square	F Value	Significance Level
Between dimensions	4.82	3	1.61	4.28	0.006**
Within dimensions	81.36	216	0.38	-	-
Total	86.18	219	-	-	-

** *Statistically significant at (α ≤ 0.01)*
Interpretation: there are statistically significant differences among the means of the study dimensions, with F = 4.28, significant at the 0.01 level, confirming genuine variation in the level of safety-system implementation across the different dimensions.

C. Tukey HSD Post-Hoc Test

Comparison	Mean Difference	Significance Level
Early detection ← Suppression	-0.44	0.042*
Early detection ← Electrical	-0.42	0.048*
Early detection ← Training	-0.24	0.321 (n.s.)
Suppression ← Electrical	0.02	0.998 (n.s.)
Suppression ← Training	0.20	0.412 (n.s.)
Electrical ← Training	0.18	0.478 (n.s.)

* *Significant at (0.05); n.s. = not significant*

D. Independent-Samples T-Test (Private vs. Public Sector)

Dimension	Private Sector (n=18)	Public Sector (n=37)	t Value	Significance Level
Early detection	2.58	2.24	2.14	0.037*
Suppression systems	2.98	2.70	2.56	0.014*
Electrical safety	2.92	2.69	2.34	0.023*
Training and readiness	2.78	2.49	2.18	0.034*
Overall scale	2.82	2.53	2.82	0.007**

* *Significant at (0.05) / ** Significant at (0.01)*
Interpretation: statistically significant differences exist between the private and public sectors across all study dimensions, with results favoring the private sector (overall mean 2.82 vs. 2.53). This can be explained by the fact that the private sector is subject to parent-company standards or international certifications that impose stricter safety requirements, and competition among private companies drives them to improve service quality and reliability, while the public sector lacks effective oversight and binding legislation.

E. Pearson Correlation Coefficient

Dimensions	Detection	Suppression	Electrical	Training	Overall Scale
Detection	1	0.452**	0.418**	0.324*	0.589**

Dimensions	Detection	Suppression	Electrical	Training	Overall Scale
Suppression	0.452**	1	0.398**	0.312*	0.562**
Electrical	0.418**	0.398**	1	0.287*	0.534**
Training	0.324*	0.312*	0.287*	1	0.428**
Overall scale	0.589**	0.562**	0.534**	0.428**	1

*** Significant at (0.01) / * Significant at (0.05)*
Interpretation: positive, statistically significant correlations exist among all study dimensions, with correlation coefficients ranging from 0.287 to 0.589. The strongest correlation was between the "early detection" dimension and the overall scale (r = 0.589), indicating that improving early-detection systems is strongly linked to raising the overall safety level of the center.

F. Reliability Coefficient (Cronbach's Alpha)

Dimension	No. of Items	Cronbach's Alpha
Early detection	3	0.78
Suppression systems	5	0.82
Electrical safety	3	0.75
Training and readiness	5	0.79
Overall scale	16	0.89

Interpretation: Cronbach's alpha values indicate good-to-excellent reliability, with the overall scale reliability coefficient reaching 0.89, confirming that the study instrument has a high degree of internal consistency and reliability.

4.6 Discussion of Results in Light of Prior Studies

The results of this study agree with many prior studies in some respects, and diverge from them in others:
First: discussion of results for the first dimension (early detection)
The results show that the level of implementation of early fire-detection systems was moderate (2.35 out of 5), the lowest among all dimensions. This result is linked to the limited prevalence of the VESDA system, as only 34.5% of the sample lacks this system, with 18.2% unaware of its existence. This finding is consistent with Purushothaman et al. (2024) regarding the importance of early detection in preventing fire escalation, and conflicts with NFPA 75 requirements, which emphasize the need to install high-sensitivity detection systems in all data centers.
Second: discussion of results for the second dimension (suppression systems)
The level of implementation of suppression systems was moderate (2.79 out of 5), the highest among the dimensions. The use of water sprinklers and foam in some centers (7.3% and 12.7% respectively) poses a significant risk, as water causes short circuits and permanent equipment damage. This conflicts with NFPA 2001 standards, which emphasize using only clean agents to protect electronic equipment,

and is consistent with Schmidt et al. (2024) regarding the need to transition from FM200 to Novec 1230 for environmental reasons.

Third: discussion of results for the third dimension (electrical safety and environmental control)

The results showed that the level of implementation of this dimension was moderate (2.77 out of 5). 29.1% of participants did not know whether there was separation between cold and hot aisles, which conflicts with ASHRAE TC 9.9 temperature and humidity recommendations. Zhang et al. (2019) noted that improper humidity causes corrosion of electronic components and increased static electricity.

Fourth: discussion of results for the fourth dimension (training and human readiness)

This dimension was at a moderate level (2.59 out of 5) but carries serious indicators. 54.5% of participants reported that no fire drill had ever been conducted, a very serious indicator, as it means personnel are not prepared to act in emergencies. Kareck et al. (2026) confirmed the importance of training scenarios in improving emergency response. Also, 43.6% of participants reported the absence of any written disaster-recovery plan, which conflicts with the requirements of the international standard ISO/IEC 22237-6.

5. Conclusion

5.1 Key Findings

In light of the results presented and analyzed, the following key findings can be drawn: First: general weakness in safety systems

The overall mean for safety-system implementation reached 2.63 out of 5.00, a level falling within the "moderate" category, with an overall gap of 22.6% between current conditions and the minimum requirements of international standards. This indicates that safety systems in Libyan data centers do not exceed 77.4% of international requirements.

Second: variation in performance across dimensions

Performance levels varied across the study's four dimensions, which can be ranked in descending order as follows:

- Fire-suppression systems dimension: mean 2.79, gap 17.9%.
- Electrical safety and environmental control dimension: mean 2.77, gap 18.5%.
- Training, human readiness, and building safety dimension: mean 2.59, gap 23.8%.
- Early fire-detection systems dimension: mean 2.35, gap 30.9%. Third: deficiencies in early-detection systems

The mean for the item "presence of an advanced smoke-detection system such as VESDA" reached 2.25 (moderate), with only 34.5% of participants reporting the system's absence. This means that fewer than half of Libyan data centers possess early-detection systems, constituting a gap in the ability to prevent fires before they occur.

Fourth: variation and unsuitability of suppression systems
The results show that 7.3% of centers rely on water-based suppression systems and 12.7% on foam, both unsuitable for data centers, while 10.9% of centers have no suppression system at all.
Fifth: clear neglect of the human element
The results revealed that 54.5% of participants had never conducted a fire drill, 47.3% had received no training on gas hazards, and 43.6% lacked a written recovery plan, reflecting a clear neglect of the human element and organizational readiness in the face of emergencies.
Sixth: absence of national legislation
There is no binding Libyan national legislation for data center safety, contributing to inconsistent implementation levels and a lack of effective oversight.
Seventh: private-sector outperformance of the public sector
Independent-samples t-test results showed statistically significant outperformance of the private sector over the public sector across all safety dimensions, reflecting the absence of unified national legislation and the presence of international standards applied by private companies.
Eighth: the scientific value of the study
This study is among the very few conducted in the Libyan context, contributing to closing the knowledge and geographic gap in the data center safety literature, and providing a replicable quantitative analytical model for other contexts.

5.2 Recommendations

5.2.1 Technical Recommendations for Developing Safety Systems

1. Install advanced VESDA-type early-detection systems integrated with off-gas detectors for lithium-ion batteries.
2. Replace unsuitable suppression media (water, foam, dry powder) with clean agents such as Novec 1230 or ultra-fine water-mist systems.
3. Implement hot-aisle/cold-aisle containment in accordance with ASHRAE recommendations.
4. Install environmental monitoring systems connected to alarm systems for real-time temperature and humidity measurement.
5. Establish written disaster-recovery plans and link them to alarm systems.

5.2.2 Recommendations Related to Training and Human Readiness

1. Conduct practical evacuation-simulation drills at least every 6 months, with documentation of results and performance evaluation.
2. Form and train emergency-response teams within each data center.
3. Provide practical staff training on suppression systems and the EPO emergency button.
4. Organize periodic awareness campaigns and build an organizational safety culture.
5. Train staff on the hazards of inert-gas leaks and asphyxiation.

5.2.3 Institutional-Level Recommendations

1. Conduct periodic technical reviews of systems by specialized external bodies.
2. Document safety procedures in a comprehensive manual and update it annually.
3. Link construction and operating licenses to compliance with safety standards.
4. Adopt institutional safety certifications in line with Uptime Institute or TIA-942 standards.
5. Draw on private-sector experience in implementing safety systems, and adopt incentive policies encouraging public institutions to invest in modern safety systems.

5.2.4 National-Level Recommendations

1. Issue binding national legislation for data center safety in Libya, based on NFPA standards.
2. Establish a national body to oversee data center safety and monitor compliance.
3. Provide financial incentives for institutions investing in safety-system development.
4. Incorporate data center safety topics into academic curricula and engineering specializations.
5. Establish a national database of fire incidents in data centers for research and development purposes.
6. Organize annual conferences and workshops to exchange expertise among institutions.

5.2.5 Recommendations for Future Research

1. Conduct a field study including direct physical measurements (temperature, humidity, suppression-system efficiency) to confirm the questionnaire findings.
2. Expand the scope of the study to include data centers in other cities (Sabha, Zawiya, Khoms).
3. Conduct a comparative study between data centers in the public and private sectors.
4. Study the effectiveness of off-gas detection systems in the Libyan context.
5. Assess the economic feasibility of investing in modern safety systems.
6. Study the impact of organizational culture on the implementation of safety standards.
7. Conduct periodic reassessments to measure progress after implementing the recommendations.

6. Final Conclusion

This study represents the first systematic field diagnosis of the state of safety systems in Libyan data centers according to NFPA standards, with a high reliability coefficient ($\alpha = 0.89$), applied to 55 employees using a validated questionnaire.

The results revealed an overall gap of 22.6% between current conditions and international standards, with an overall mean of 2.63 out of 5.00. The fire-suppression dimension recorded the highest level (2.79, gap 17.9%), compared to the lowest level for the early-detection dimension (2.35, gap 30.9%).

The indicators revealed the severity of the situation:

- 54.5% had never conducted a fire drill
- 47.3% had received no training on gas hazards
- 43.6% lacked a written recovery plan
- 7.3% use unsuitable water-based systems and 12.7% use foam
- 10.9% have no suppression systems

• Only 34.5% have a VESDA system

The results also showed statistically significant outperformance of the private sector over the public sector across all safety dimensions, reflecting the absence of unified national legislation and the presence of international standards applied by private companies.

The implications of these results extend beyond the engineering dimension to economic and security dimensions, as data centers constitute critical infrastructure, and any disruption threatens national security and the digital economy. The study puts forward an expanded concept of safety as a strategic asset rather than a mere compliance requirement.

The study contributes to the academic literature by closing the knowledge gap in an under-researched context, offering a replicable quantitative analytical model, and grounding the relationship between international standards and local realities, thereby reinforcing an approach to safety as an integrated socio-technical system.

The study calls on decision-makers to adopt a proactive approach: binding national legislation, a specialized regulatory body, linking licensing to safety, and integrating the subject into academic curricula.

For future research, the study recommends expanding the sample, conducting physical measurements, analyzing economic feasibility, testing off-gas detection technologies, studying the impact of organizational culture, evaluating the effectiveness of simulated training, and conducting periodic reassessments.

7. References

- 3M Company. (2019). Novec 1230 fire protection fluid: Technical data sheet. 3M.
- Ansil Incorporated. (2021). Inergen clean agent fire suppression system. Ansil.
- ASHRAE. (2021). Thermal guidelines for data processing environments (5th ed.). ASHRAE.
- Chen, Y., Zhang, X., & Li, W. (2021). Advanced fire detection systems in data centers. Journal of Electrical Engineering, 16(3), 145-158.
- Cisco Systems. (2020). Data center infrastructure management guide. Cisco.
- Digital Realty. (2026). Paris Digital Park fire protection system installation. Digital Realty.
- Ebrahimi, K., Jones, G. F., & Fleischer, A. S. (2017). A review of data center cooling technology. Renewable and Sustainable Energy Reviews, 31, 622-638.
- FM Global. (2022). Data center fire loss prevention data sheet 5-32. FM Global.
- FM Global. (2024). Lithium-ion battery fire hazards in data centers. FM Global.
- Honeywell. (2025). Li-ion Tamer technology acquisition. Honeywell.
- ISO/IEC. (2018). ISO/IEC 22237-6: Data centre facilities and infrastructures. ISO.
- Jensen, R. (2020). Fire detection in high-risk environments. Fire Technology, 56(2), 567-589.
- Johnson Controls. (2025). Hygood IGS-300 inert gas fire suppression system. Johnson Controls.
- Kareck, T. L., Gollner, M. J., & Wang, K. (2026). Fire risk assessment in data centers. Fire Safety Journal, 124, 103-118.

- Khan, A. A., & Hassan, E. (2019). Human factors in data center fire safety. Journal of Safety Research, 70, 45-58.
- Kim, S., & Lee, J. (2020). Performance evaluation of clean agent fire suppression systems. Journal of Chemical Engineering, 43(5), 876-889.
- Liu, J., Wang, Y., & Chen, H. (2018). Water mist fire suppression systems. Fire Science Reviews, 7(1), 1-25.
- NFPA. (2018). NFPA 2001: Standard on clean agent fire extinguishing systems. NFPA.
- NFPA. (2020). NFPA 51B: Standard for fire prevention during hot work. NFPA.
- NFPA. (2021). NFPA 70E: Standard for electrical safety in the workplace. NFPA.
- NFPA. (2023). NFPA 72: National fire alarm and signaling code. NFPA.
- NFPA. (2023). NFPA 75: Standard for the protection of information technology equipment. NFPA.
- NFPA. (2023). NFPA 76: Standard for the fire protection of telecommunications facilities. NFPA.
- OSHA. (2020). Data center safety and health: Best practices guide. U.S. Department of Labor.
- Ponemon Institute. (2022). Cost of data center outages report. Ponemon Institute.
- Punari, R. H., Sari, A. W., & Rahman, M. A. (2026). Fire safety management in data centers: A systematic review. International Journal of Disaster Risk Reduction, 89, 103-125.
- Purushothaman, S., Lee, J., & Carter, M. (2024). Early detection of thermal runaway in lithium-ion batteries. Journal of Power Sources, 556, 232-245.
- Rahman, M. A., Ismail, H., & Yusoff, N. (2025). A systematic review of fire safety management. Fire Safety Journal, 119, 103-115.
- Rasli, N. M., Yahya, A. R., & Yusoff, W. A. (2019). Operational reliability of data centers. Journal of Reliability Engineering, 45(3), 234-251.
- Schmidt, M., Weber, T., & Hoffmann, P. (2024). Comparative analysis of clean agent fire suppression systems. Fire Technology, 60(4), 1875-1902.
- Uptime Institute. (2021). Tier standard: Topology. Uptime Institute.
- Xtrails. (2020). VESDA early warning fire detection systems. Xtrails.
- Zhang, M., Wang, R., & Xu, Y. (2019). Humidity effects on electronic components. IEEE Transactions on Industrial Electronics, 66(11), 8765-8774.