The Unseen Resilience: Data Center Fire Safety, 2020–2025

A Strategic Framework for Protecting Mission-Critical Infrastructure

Company Logo

A Period of Reckoning: High-Profile Incidents Have Accelerated a Strategic Shift

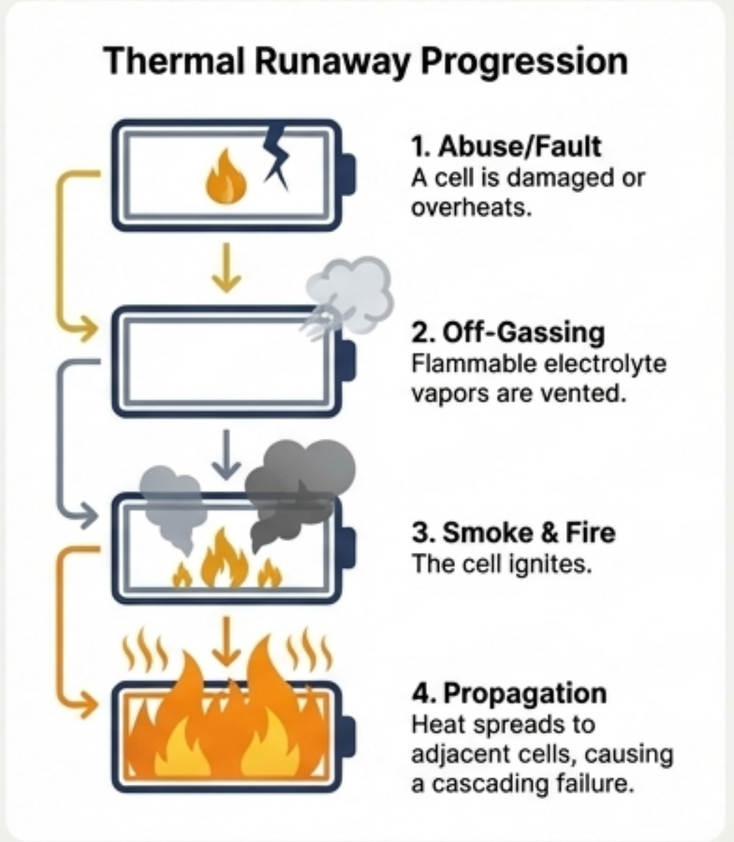
The 2020–2025 period was defined by escalating operational demands and the harsh lessons from significant fire events. Incidents at facilities like **OVHcloud (2021)** and **SK C&C/Kakao (2022)** demonstrated that conventional approaches were insufficient, leading to catastrophic data loss and multi-day outages. In response, the industry has solidified its approach around a multi-layered strategic framework: **Defense-in-Depth**.

Prevention	Detection	Suppression	Containment	Recovery
Proactively eliminate ignition sources.	Identify incipient fires in seconds.	Extinguish fires with precision.	Limit fire spread through physical barriers.	Protect personnel and ensure business continuity.

Layer 1 | Prevention: The Lithium-Ion Challenge Creates a New Fire Paradigm

While data centers have always managed electrical fire risks, the widespread adoption of **Lithium-ion batteries** for UPS systems between 2020–2025 introduced the unique hazard of **thermal runaway.** This self-accelerating chemical reaction can reignite after suppression and release explosive flammable gases, making prevention and specialized mitigation critical.

- **The Hazard:** Thermal runaway is a chain reaction, not a simple Class A fire. It is difficult to extinguish with traditional agents alone, as cooling is paramount.
- **The Industry Response:** Rapid development and adoption of **NFPA 855** (Standard for Energy Storage Systems) to codify new safety requirements.
- **The Strategy:** A shift from simple suppression to proactive risk mitigation through specialized detection, engineering controls, and robust containment.



The 2022 fire at the SK C&C data center in South Korea, which originated in a Li-ion battery room, burned for over **8 hours** and caused a massive, multi-day outage for Kakao services.

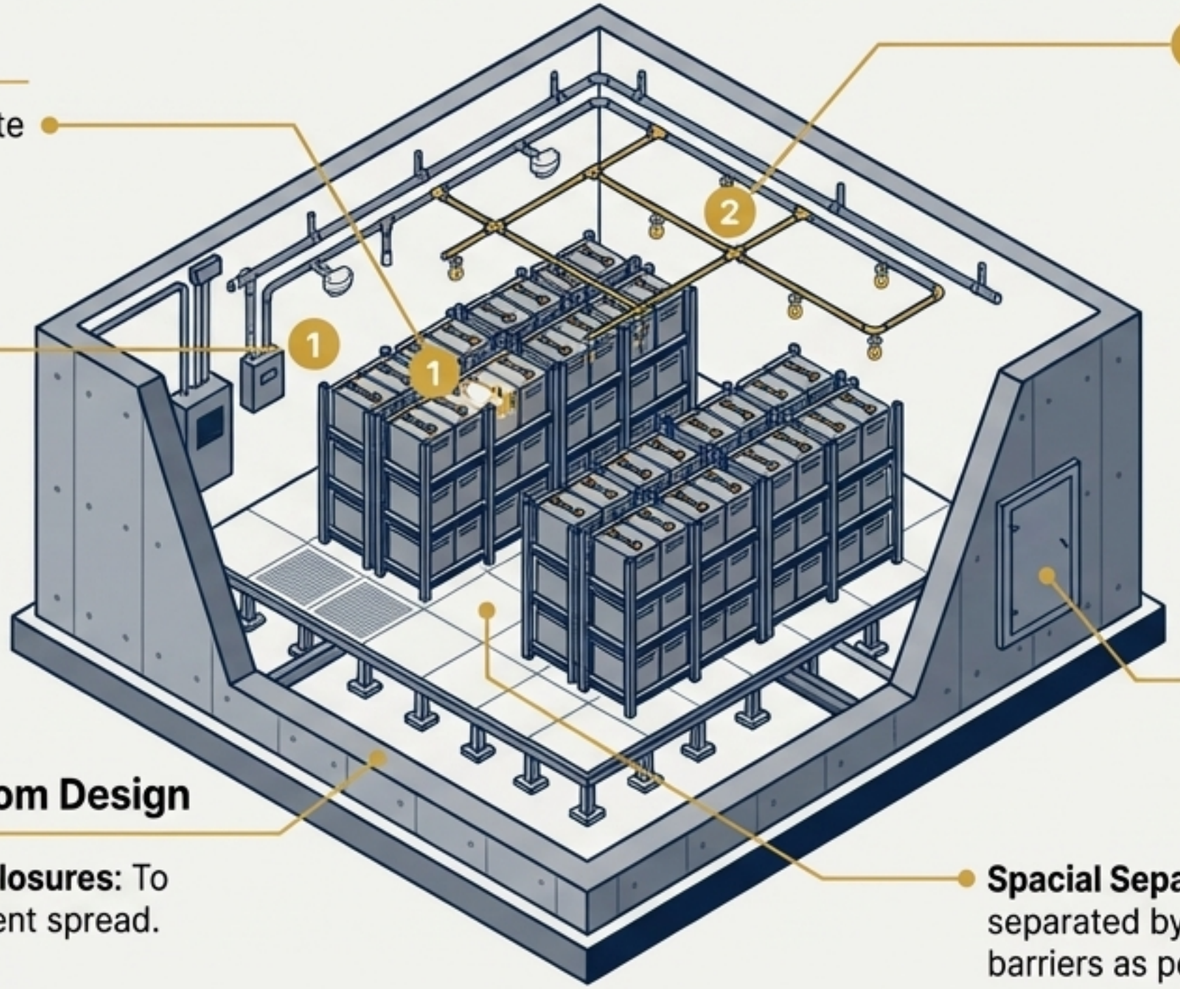
Best Practices for Lithium-Ion Battery Safety Are Now Codified

The industry converged on a multi-pronged strategy for Li-ion UPS rooms, combining very early detection with robust suppression and containment, as guided by NFPA 855 and lessons from incidents.

1 Early Warning Detection

Off-Gas Sensors: Detect electrolyte vapor *before* thermal runaway, signaling the BMS to disconnect the failing module.

Aspirating Smoke Detection (ASD): Set to very high sensitivity to detect the earliest traces of smoke.



2 Water-Based Suppression

Automatic Sprinklers or Water Mist: Industry consensus confirms water is essential for cooling to stop thermal runaway propagation. Clean agents alone are insufficient.

NFPA 855-2023 mandates a **high sprinkler density of 0.30 gpm/ft²** over **2,500 ft²**.

Explosion/Deflagration Venting: Pressure relief panels required by IFC 2024 to safely manage gas ignition risk.

3 Containment & Room Design

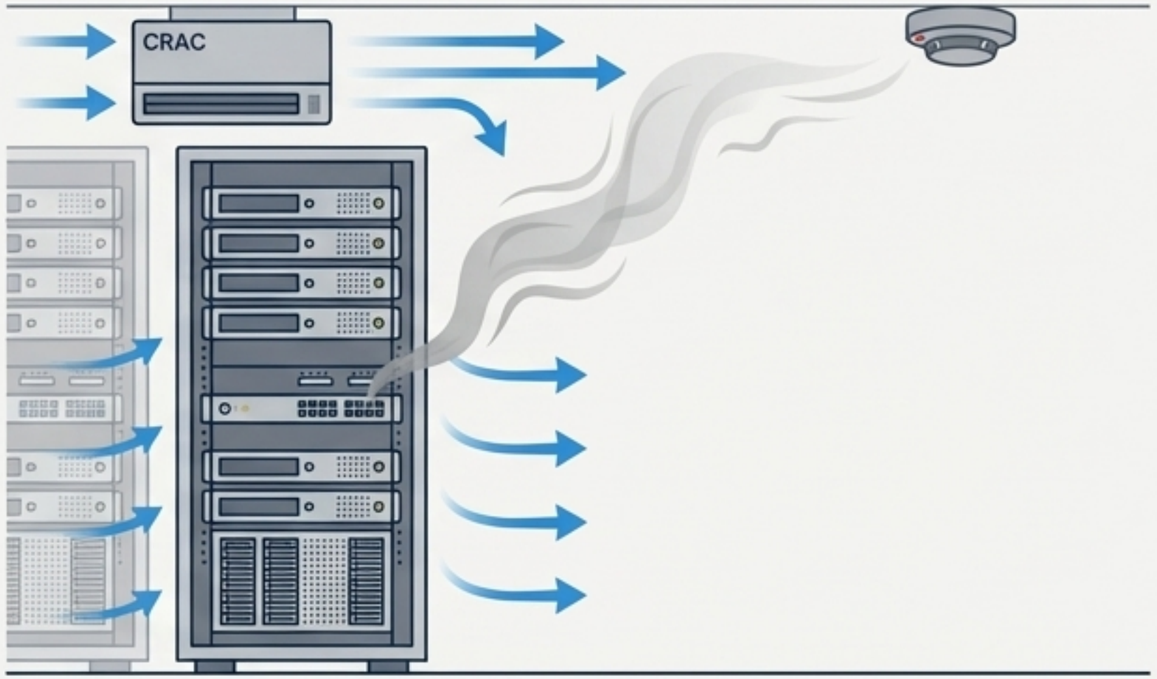
2-Hour Fire-Rated Enclosures: To contain a fire and prevent spread.

Spacial Separation: Battery arrays separated by 3 feet or fire-rated barriers as per NFPA 855.

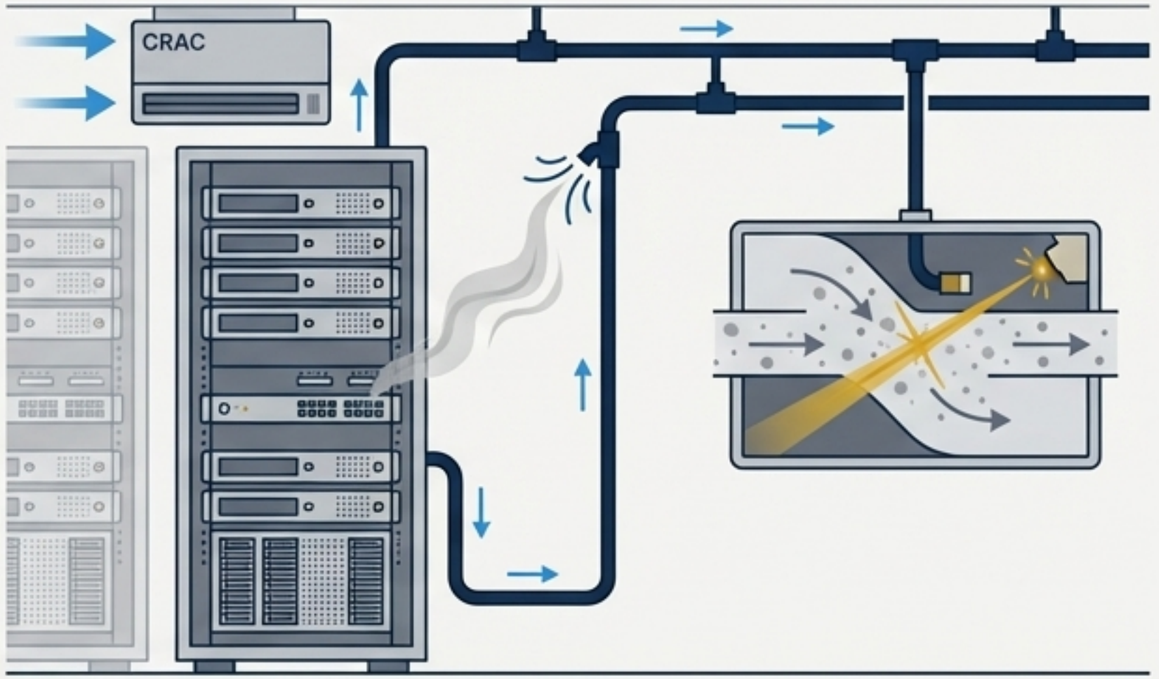
Layer 2 | Detection: High Airflow Renders Traditional Spot Detectors Obsolete

Data hall cooling systems generate powerful, high-velocity airflow (often >300 ft/min) to manage thermal loads. This same **airflow dilutes and diverts smoke**, preventing it from reaching traditional ceiling-mounted spot detectors in a timely manner. This challenge drove the widespread adoption of **Aspirating Smoke Detection (ASD)** as the best practice.

Legacy Approach



Modern Standard: ASD



NFPA 72 prohibits the use of standard smoke detectors in air velocities exceeding **1.52 m/s (300 ft/min)** unless specifically listed for those conditions—a threshold routinely surpassed in data centers.

Intelligent Detection Provides Early Warning Without Nuisance Alarms

Modern detection strategies go beyond simple smoke identification. Systems are designed for high reliability and actionable intelligence, enabling staff to investigate potential issues before they escalate into fire events and trigger suppression.

False Alarm Immunity

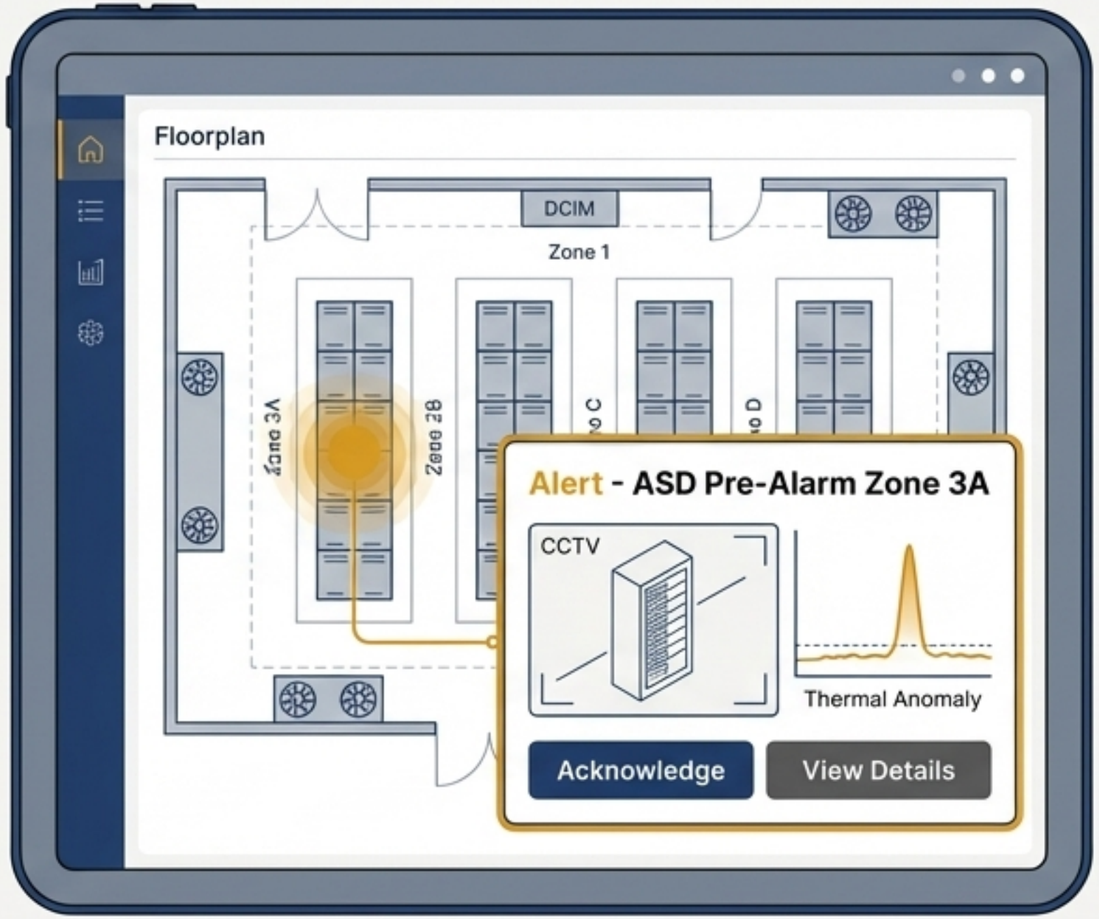
Advanced ASD units use sophisticated algorithms and laser/LED optics to **differentiate dust and airborne particulates from actual smoke,** drastically reducing false alarms.

Multi-criteria detectors (combining smoke, heat, and gas sensors) use multiple signals to confirm a fire before activating.

Multi-Stage Alarms

Systems are programmed with multiple alert thresholds (e.g., Alert, Action, Fire 1, Fire 2) to provide a staged response.

An **early "Alert" warning** allows staff to investigate a potential overheating component via DCIM or CCTV, often preventing a full fire incident.



Strategic Integration

Detection systems are **fully integrated with the BMS/DCIM,** providing real-time device status and alarm locations on facility dashboards.

Cross-zoning (requiring two separate detectors to alarm) is standard practice before triggering a costly clean agent release.

Layer 3 | Suppression: The Clean Agent Landscape Is Reshaped by Environmental Regulation

While gaseous suppression remains a cornerstone for protecting IT assets without water damage, the market has undergone a fundamental transition. The phase-down of high-GWP HFC agents has forced a move toward more sustainable alternatives.

The Regulatory Driver: The 2020 **American Innovation & Manufacturing (AIM) Act** mandates an 85% reduction in HFC production by 2036. This led manufacturers to cease FM-200 production by 2022-2023, making refills scarce and expensive (from ~$12/lb to **$70+/lb** by 2024).

Agent	Type	GWP	Atmospheric Lifetime	Status
FM-200 (HFC-227ea)	Halocarbon	~3,500	~33 years	**Being Phased Out**
Novec™ 1230 (FK-5-1-12)	Halocarbon	~1	~5 days	**Preferred HFC Replacement***
Inert Gases (Inergen, etc.)	Nitrogen/Argon Mix	0	0	**Environmentally Ideal**

**While environmentally safe, 3M's 2022 announcement to exit PFAS manufacturing by 2025 has created long-term supply uncertainty for Novec™ 1230, prompting some to favor inert gases as a "future-proof" solution.*

Water-Based Suppression: Engineered for Reliability, Not Risk

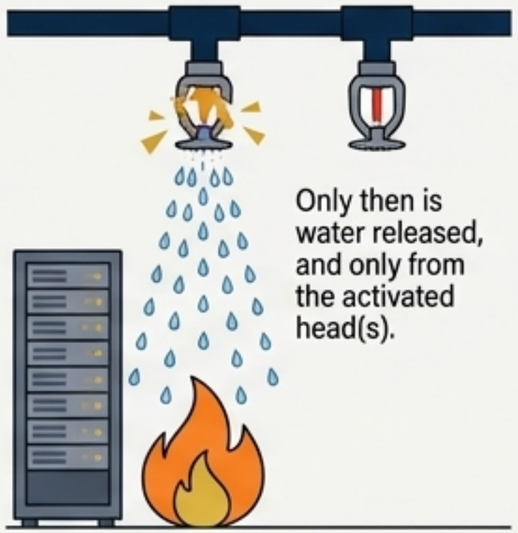
Automatic sprinklers are a non-negotiable life safety and building protection requirement under the IBC for virtually all data centers. The industry's focus is on mitigating water damage risk through advanced system design.

Double-Interlock Pre-Action System

Normal State

Trigger 1 (Detection)

Trigger 2 (Activation)



This two-trigger design virtually eliminates accidental discharge from false alarms or physical damage.

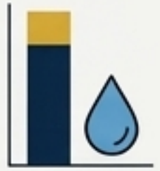
The Rise of Water Mist

Concept

High-pressure systems create a fine mist (<200 µm) that suppresses fire through rapid cooling and oxygen displacement.

Key Advantage

Uses **50-80% less water** than traditional sprinklers, dramatically reducing potential collateral damage.



Industry Acceptance

By 2025, FM Global has approved specific water mist systems as equivalent protection for data halls (HC-2/HC-3), validating the technology for mission-critical use.

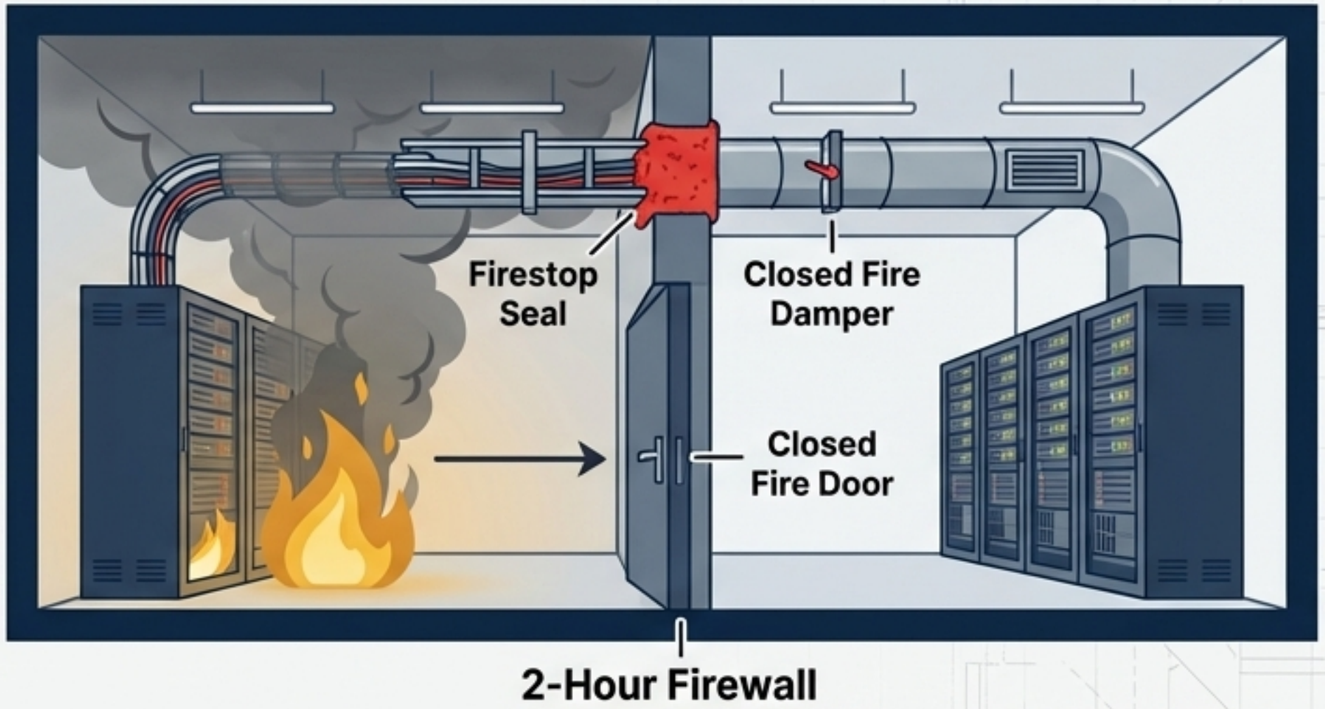
Layer 4 | Containment: Passive Protection Is the Ultimate Failsafe

If a fire cannot be immediately suppressed, the building itself becomes the final line of defense. **Compartmentalization**—dividing the facility into distinct, fire-rated zones—is essential for limiting the scope of an incident and protecting the rest of the facility.

- **Fire-Rated Construction:** Using **1- to 2-hour fire-rated** walls and enclosures (slab-to-slab) around data halls, electrical rooms, and battery rooms.

- **Firestopping Penetrations:** Meticulously sealing every opening for cables, conduits, and pipes with UL-listed firestop materials to maintain the wall's integrity.

- **Fire-Rated Doors & Dampers:** Installing self-closing doors and automatic dampers that seal off compartments upon a fire alarm.



Lesson from OVHcloud (2021)

The fire completely destroyed the unsprinklered SBG2 building. However, a **2-hour firewall** partially protected the adjacent SBG1 hall, demonstrating the life-saving value of robust passive barriers even in a catastrophic event.

Layer 5 | Recovery: Protecting Personnel and Ensuring Business Continuity

A holistic fire safety strategy extends beyond suppression to ensure personnel can evacuate safely and the business can recover swiftly. This involves integrated life safety systems and a well-rehearsed incident response plan.

Protecting Personnel (Life Safety)

- **Clear Egress:** Illuminated exit paths and signage with UPS/generator backup.

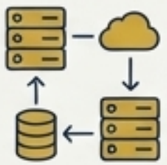
- **Intelligent Alarms:** Emergency Voice/Alarm Communication Systems (EVACS) that overcome high ambient noise in data halls.

- **Fail-Safe Access Control:** All security doors on egress paths **automatically unlock** upon a fire alarm, prioritizing life safety over security.

Ensuring Recovery (Incident Response)

- **Pre-Incident Planning:** Regular coordination with local fire departments, including site tours and sharing information on special hazards (e.g., clean agents, Li-ion batteries).

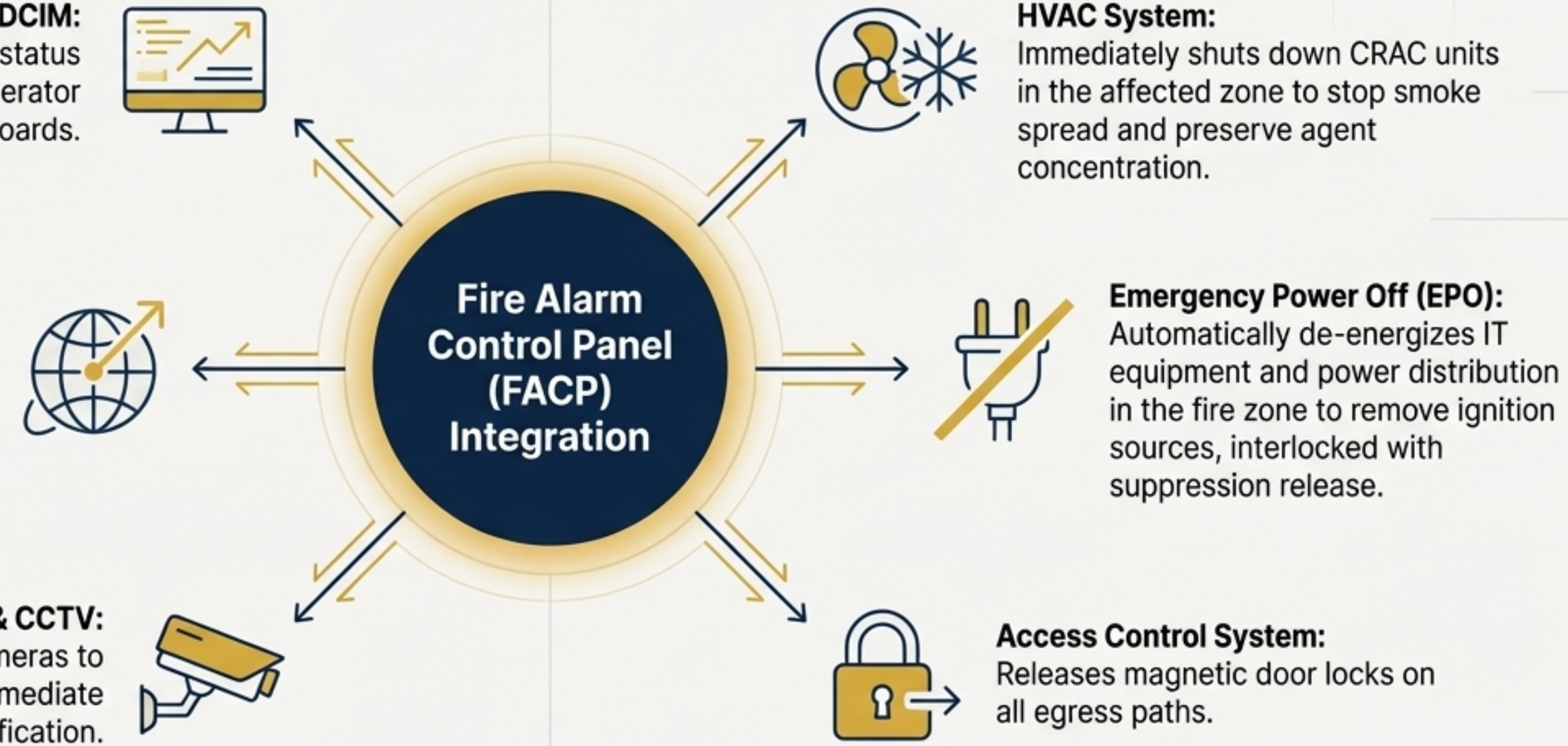
- **Post-Discharge Cleanup:** Pre-vetted specialist teams for water removal and soot/residue cleaning to restore the environment quickly.



- **IT Service Failover:** Business continuity plans that leverage redundancy to shift workloads away from affected equipment to secondary systems or sites.

The Integrated System: A Coordinated, Automated Defense

The effectiveness of a data center's fire response hinges on the seamless integration of its safety and building control systems. A single verified alarm event triggers a pre-programmed cascade of automated actions to contain the threat and mitigate damage.



BMS / DCIM:
Provides real-time alarm status and location on operator dashboards.

HVAC System:
Immediately shuts down CRAC units in the affected zone to stop smoke spread and preserve agent concentration.

Remote Monitoring:
Sends automated alerts to the Network Operations Center and/or a UL-listed central station.

Emergency Power Off (EPO):
Automatically de-energizes IT equipment and power distribution in the fire zone to remove ignition sources, interlocked with suppression release.

Security & CCTV:
Automatically directs cameras to the alarm zone for immediate visual verification.

Access Control System:
Releases magnetic door locks on all egress paths.

The Horizon: Next-Generation Technologies Are Moving from Pilot to Practice

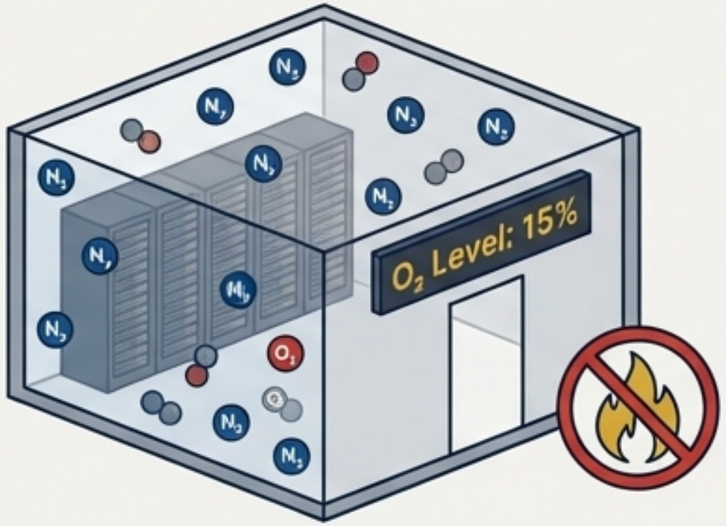
While the 2020–2025 framework is robust, new technologies are emerging to provide even earlier detection and proactive prevention, further reducing the probability of a fire event.

AI & Video Analytics

Machine learning algorithms analyze CCTV feeds to detect smoke or flame signatures visually, often faster than traditional detectors in large, open spaces. AI also analyzes sensor data to predict failures before they occur.

Status: Piloted in hyperscale facilities; being integrated as a supplementary detection layer.

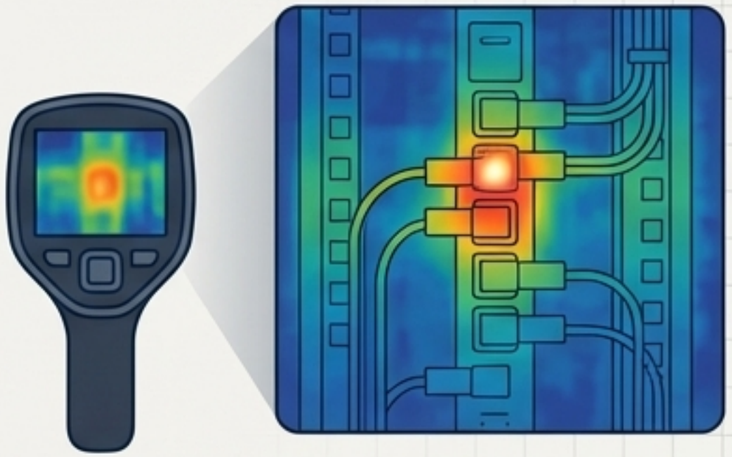
Oxygen Reduction Systems (ORS)



Continuously injects nitrogen into a sealed room to maintain oxygen at ~15%, a level breathable for short periods but insufficient to support combustion. The fire is prevented from ever starting.

Status: Gaining traction in Europe and for unmanned edge sites; received FM Approval in 2022, increasing credibility.

Advanced Thermal Monitoring



Fixed thermal imaging cameras continuously scan for hotspots on battery terminals, PDUs, and cable trays, providing warnings of overheating long before smoke is produced.

Status: Becoming more cost-effective and integrated into standard security and BMS platforms.

The Regulatory Landscape: A Guide to Key Codes and Standards

Standard	Governing Body	Primary Domain & Key Mandates (2020-2025)
NFPA 75	NFPA	**IT Equipment Protection**:: Specifies detection above/below raised floors; allows sprinkler omission only under strict conditions (1-hr rated room + VEWFD + clean agent); basis for EPO.
NFPA 72	NFPA	**Fire Alarms & Detection:** Governs ASD installation, multi-stage alarms, and cross-zoning for suppression release. Sets airflow limits for standard detectors.
NFPA 2001	NFPA	**Clean Agent Systems:** Defines agent design concentrations, discharge times (10s for halocarbons), and 10-minute hold time. Acknowledges HFC phasedown.
NFPA 855	NFPA	**Energy Storage Systems:** The definitive standard for Li-ion safety. Mandates sprinklers, gas detection, and separation/containment for battery installations.
IBC / IFC	ICC	**Building & Fire Codes:** The legally adopted code in most jurisdictions. Mandates sprinklers in almost all data centers and sets requirements for fire-rated construction and egress.
FM Data Sheet 5-32	FM Global	**Insurance Standards:** Often exceeds minimum code. Recommends dual detection, robust passive protection, and provides guidance for using new tech like water mist.

Key Trends & Data Points, 2020-2025

HFC PHASE-OUT

Production of FM-200 (GWP ~3500) ceased by 2023 under the AIM Act, with refill costs spiking over 500%. The industry has shifted to low-GWP Novec 1230 (GWP ~1) and zero-GWP Inert Gases.

LI-ION IS A WATER FIGHT

Consensus and codes (NFPA 855) now mandate water-based suppression (sprinklers/mist) for Li-ion batteries to provide essential cooling that clean agents cannot.

PRE-ACTION IS STANDARD

Double-interlock pre-action sprinklers are now the default in server rooms, virtually eliminating the risk of accidental water discharge from a single point of failure.

DETECTION BEATS HIGH AIRFLOW

With air velocity often exceeding 300 ft/min, Aspirating Smoke Detection (ASD) has become the standard to provide the necessary very early warning.

COMPARTMENTALIZATION IS KEY

Lessons from major fires have reinforced that 1- to 2-hour fire-rated enclosures are a critical, non-negotiable layer to contain events and prevent total facility loss.

ACOUSTIC NOZZLES ARE MANDATORY

To prevent loud (~130 dB) clean agent discharges from damaging spinning hard disk drives, acoustic nozzles that reduce noise below ~110 dB are now a de facto requirement.

The Modern Resilience Framework: Defense-in-Depth in Practice

Data center resilience is not achieved by any single technology, but through an integrated, multi-layered strategy. Each layer serves a unique purpose, creating a system that is robust, intelligent, and capable of protecting mission-critical operations against evolving threats.