AUTRONICA

DATA CENTER

In the last five years, several high-profile datacenter fire incidents have disrupted services, caused data loss, and impacted millions of users. These events the indicate critical need for advanced fire safety solutions in data centers.

INTRODUCTION

In today's digital era, data and connectivity are fundamental to nearly every aspect of modern life. At the heart of this infrastructure are data centers, which store, process, and manage vast volumes of information while supporting the applications that drive our daily digital experiences. These facilities range from small private server rooms to expansive hyperscale centers housing millions of servers. Over the past decade, the global number of data centers has surged, fueled by rapid advancements in artificial intelligence and cloud computing—a trend expected to continue.

However, this growth has also introduced significant safety challenges, particularly the risk of fire. In the past five years, several major fire incidents have occurred worldwide, caused by diverse factors such as lithium-ion battery failures, electrical faults, HVAC system fires, and cable insulation issues.

These events have led to widespread service disruptions and affected thousands of users. For instance, a fire in Europe caused by an electrical fault disrupted millions of websites, while a lithium-ion battery fire in Asia interrupted national internet and mobile services. In the United States, a power distribution failure resulted in temporary service outages. These incidents highlight the urgent need for robust fire detection and suppression systems in data centers to ensure operational continuity, safeguard critical infrastructure, and maintain public trust.

As the data center industry scales rapidly, Autronica is uniquely positioned to deliver end-to-end fire and gas safety solutions—from design and engineering to commissioning and lifecycle support ensuring compliance, uptime, and peace of mind for hyperscale and edge operators alike.

DATA CENTER COMPONENTS

IT Equipment

IT Equipment forms the core of the data center's functionality, housing the computational and networking infrastructure that processes, stores, and transmits data. Key components within this group include:

- Racks
These are standardized frames or enclosures used to mount multiple pieces of IT hardware, such as servers and networking devices, in a compact and organized manner.

- Servers
These are computers that handle data processing, application hosting, and storage tasks.
- Routers and Switches
These networking devices manage data traffic within the data center and between external networks.

Currently datacenter capacity is measured in terms of power owing to the large amount of power consumed by the IT equipment.

Power Systems

Datacenters are power hungry, and availability of power is critical in planning new datacenters. Power infrastructure within datacenter is essential for maintaining uninterrupted operations and protecting sensitive equipment from power fluctuations or outages. This includes:

- Transformers
Transformers convert high-voltage electricity from the utility grid into lower voltages suitable for data center equipment.
- Generators (Gensets)
They provide backup power in case of a utility failure, ensuring that the data center remains operational during outages.
- Uninterruptible Power Supplies (UPS)
UPS systems offer short-term power and protection against surges and interruptions.

Cooling Systems

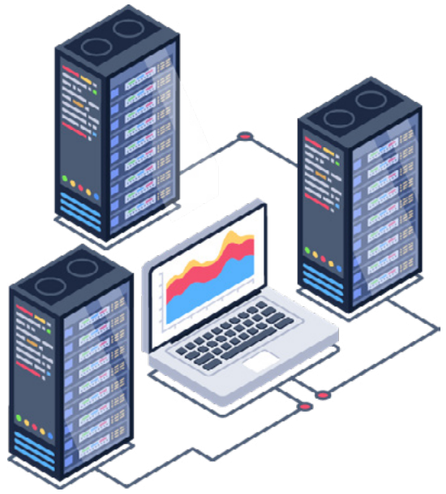
To prevent overheating and maintain optimal operating conditions for IT equipment, data centers rely on robust cooling infrastructure. There is various cooling technologies used for datacenter such as air cooling, liquid cooling are the most important besides several others. The cooling system mainly comprises:

- Chiller Plants
These systems generate chilled water or air to absorb and remove heat from the data center environment.
- Pump Systems
These circulate chilled water or coolant throughout the facility, ensuring consistent temperature control across all zones.
- Air Handling Units (AHUs) and Computer Room Air Conditioners (CRACs)
These components are used to manage airflow and temperature.

DATA CENTER TYPES

Enterprise Data Centers

An enterprise data center is owned and operated by a single organization with full control over its infrastructure. These data centers are typically located on-premises, such as within a company's headquarters or campus, or in a dedicated off-site facility that is exclusively used by the organization. For example, a financial institution might design its private data center to meet strict regulatory requirements and ensure ultra-low latency for trading applications. One of the key advantages of a private data center is the high level of control it offers over infrastructure and security.



Managed Services Data Centers

A managed data center is a facility that is operated by a third-party provider, which takes full responsibility for managing the hardware, software, and overall infrastructure. This model is especially beneficial for organizations that prefer to outsource their IT operations to focus on core business activities.
In a managed data center, the provider handles everything from server maintenance and software updates to network management and security. For example, a retail company might use a managed data center to host its e-commerce .platform, relying on the provider to ensure uptime, scalability, and data protection without needing in-house IT staff. Another example is a small law firm choosing a managed data center to securely store client data and run legal software.

Colocation Data Center

A colocation data center is a facility where businesses rent space from a third-party provider to house their IT infrastructure. These facilities offer essential services such as power, cooling, bandwidth, and physical security, allowing companies to focus on managing their own hardware without worrying about the underlying infrastructure.
In this model, clients bring their own servers and storage equipment, which they install in racks or cages provided by the colocation provider. For example, a growing tech startup using this service. Another example is a media company that needs to stream large volumes of content globally, it can collocate its servers to reduce latency and improve performance.

Edge Data Centers

Edge data centers are located closer to end-users or devices, often at the network's edge, to reduce latency and improve performance, especially for real-time applications. By processing data locally rather than sending it to a centralized facility, edge data centers enable faster response times. For example, edge data centers can process traffic data in real time to optimize signal timings. Similarly, autonomous vehicles rely on edge computing to make split-second decisions based on sensor data. platform, relying on the provider to ensure uptime, scalability, and data protection without needing in-house IT staff. Another example is a small law firm choosing a managed data center to securely store client data and run legal software.

Cloud Data Centers

A cloud data center is hosted by cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP). These providers deliver virtualized infrastructure and services over the internet. Cloud data centers are known for being highly scalable, flexible, and cost-efficient. Organizations can quickly scale resources up or down based on their needs, paying only for what they use.
Cloud data storage is driven by change in consumer behavior and availability of online services. Data and applications reside in the cloud as opposed to previously located on consumer devices.

Hyperscale Data Centers

Hyperscale data centers are massive facilities operated by major tech companies like Amazon, Google, and Microsoft.
These centers support millions of servers and are designed to handle enormous volumes of data with a focus on scalability, efficiency, and automation. For instance, a hyperscale data center might power global services like Google Search, Microsoft Azure cloud computing, or Amazon's e-commerce platform. Their scale allows them to deliver services to billions of users while maintaining high availability and performance.

Micro Data Centers

A micro data center is a compact, self-contained computing facility designed to deliver data processing and storage capabilities close to the source of data generation. Micro data centers are small, often fitting into a single rack or enclosure, and are ideal for edge computing environments.
These centers typically include servers, storage, networking equipment, power, and cooling systems, all integrated into a secure, modular unit. Because of their size and portability, micro data centers can be deployed in remote locations, retail stores, factories, or even outdoor environments where space and connectivity are limited.

FIRE RISK

Data centers present a unique fire risk profile that necessitates fire detection systems tailored to these specialized environments. Standards like NFPA 72 provide generalized requirements but they are not sufficient to ensure early fire detection in data centers. The data centers safety system design needs detailed fire risk assessments covering ignition sources, fuel loads, and potential fire dynamics.

The fire in datacenter could emanate from electrical faults or stored fuel or similar for which detection and suppression method are well established. Another more recent fire risk comes from Lithium-ion batteries with less known fire suppression methods. Based on this fire risk in data centers can be broadly categorized as follows:

LITHIUM ION BATTERY

Lithium-ion batteries (LIBs) are commonly integrated with Uninterruptible Power Supply (UPS) to provide backup power during main line outages. Compared to traditional lead-acid batteries, LIBs offer higher energy density, compact form factor, longer lifespan, faster charging, and greater efficiency. However, these advantages come with increased fire and safety risks, particularly due to the potential for thermal runaway and battery fires if anomalies occur. Following are the major risks associated with Lithium-Ion batteries.

Thermal Risk

Lithium-ion batteries are highly sensitive to temperature variations. Extreme heat or cold can degrade performance and compromise safety. External heat sources—such as fire can elevate internal temperatures, increasing the risk of failure. Internal short circuits caused by contact between electrodes, or manufacturing defects like electrode misalignment, contamination, or improper assembly, can also trigger thermal instability.

Electrical Risk

Electrical hazards include power fluctuations, overcharging (often due to Battery Management System (BMS) failure), overvoltage (which can cause lithium plating on the anode), undervoltage, and repeated over-discharge cycles. Ground faults and other electrical anomalies can lead to excessive heat buildup, capacity degradation, and in severe cases, battery failure.

Environmental Risk

Environmental conditions play a critical role in battery safety. High humidity can corrode terminals and degrade insulation, leading to short circuits. Water submersion causes irreversible

damage, including electrolyte leakage. Exposure to acids or alkalis can erode internal components, while excessive vibration may damage internal connections. These factors, if unaddressed, can result in serious battery malfunctions.

Mechanical Risks

Mechanical damage such as punctures, dents, or crushing can compromise the battery casing, exposing internal components to external elements. Overpressure, physical stress, or manufacturing flaws can also lead to casing rupture, increasing the risk of fire or explosion

Lithium ion battery comes with increased fire and safety risks, particularly due to the potential for thermal runaway and battery fires.

Electrical faults, overheating, and the degradation of insulation are major risk.

TRANSFORMERS, UPS, SWITCHGEAR & POWER DISTRIBUTION UNITS

Fire risks associated with transformers, UPS systems, switchgear are driven by electrical faults, overheating, and the degradation of insulation materials.

Transformers use flammable insulating oil for cooling and insulation. Oil leaks when exposed to high temperatures or electrical arcs can cause ignition & fire. Winding failures or insulation breakdowns generate significant heat, and it may lead to ignition. Overheating caused by overloading accelerates insulation degradation and increases fire risk. Mechanical failures, including loose connections or structural damage are potential fire risks as well.

In the case of UPS systems battery failures are among the most common issues. Short circuits within the UPS comes second followed by UPS overload. For switchgear faulty wiring due to poor installation or wear and tear over time leads to electrical faults. Overloaded circuits cause components to operate beyond their thermal limits. Aging components such as insulation materials degrade, and mechanical parts can lead to arc flashes. Arc flashes are sudden, high-energy discharges that can ignite surrounding materials.

BACKUP GENERATORS

Generators run on flammable fuels such as gasoline or diesel, which can leak or spill during storage, handling, or operation. Such leaks create vapors that are highly ignitable. The engine of a generator produces substantial heat while running. Flammable materials stored in vicinity of running generator is a fire hazard. If generator unit lacks adequate ventilation, this heat can build up and potentially lead to ignition. Electrical faults in generator caused by damaged wiring, short circuit or overload may lead to fire & combustion.

CABLE

Datacenter has extensive networks of power and data cables. They are routed through raised floors or overhead pathways and acts as fuel load. These bundled cables can facilitate the rapid spread of fire and the production of dense, potentially toxic smoke, posing serious risks to both equipment and personnel. Fire incidents involving cables are primarily associated with power cables. Power cables carry enough electrical energy which in fault conditions can generate sufficient heat to ignite the surrounding insulation or jacketing materials.

Cables require an external or internal heat source to initiate combustion, once ignited it can sustain burning and contribute to fire growth specially in densely packed and limited ventilation conditions.

ELECTRONIC EQUIPMENT

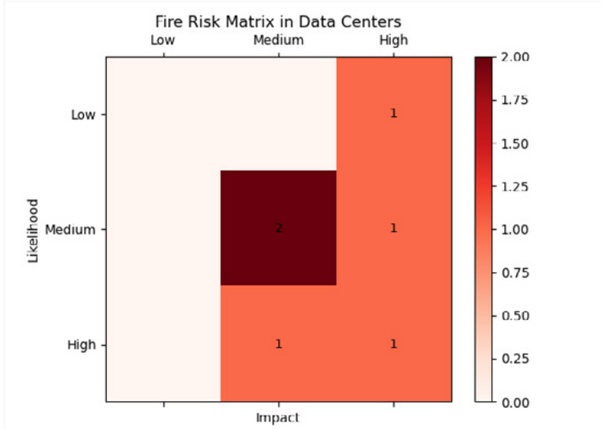
Servers, storage devices, networking hardware within a data center creates a significant fuel load in a relatively confined space. These components include combustible materials such as plastics, circuit boards and insulation which can contribute to fire development and propagation if ignition occurs. Power supplies within servers and networking hardware possess a higher potential as ignition source compared to semiconductor units.

VENTILATION SYSTEM

Data centers rely on advanced HVAC systems to maintain the precise temperature and humidity conditions. A significant proportion of data center fires comes from HVAC systems and their associated support equipment. Within these systems, several components are particularly susceptible to becoming ignition sources under certain conditions.
Air filters over time accumulate dust, lint, and other particulate matter, which can serve as a combustible fuel source. If this buildup is exposed to an ignition source such as an overheated motor or electrical fault it can ignite and potentially lead to a fire.
Fan motors within HVAC system are subject to both mechanical and electrical stresses, and faults in either domain can result in overheating. When a fan motor overheats, it can ignite nearby combustible materials, especially if those materials include accumulated dust or insulation.
Airflow patterns created by HVAC systems plays a crucial role in the behavior of smoke during a fire event. These patterns can influence smoke flow towards smoke detectors. Inaccurate airflow dynamics cause delayed smoke detection.

RAISED FLOOR & PLENUM

Accumulation of dust and debris in raised floor or suspended ceiling over time such as small particles, paper scraps, or packaging materials. A spark or heat source such as a faulty cable or overheating equipment can ignite and start a fire that spreads quickly through the concealed space. Another risk involves the power and data cables that run through these areas. If power cables are overloaded or damaged, they can overheat and cause the insulation to melt or catch fire. For example, a bundle of cables under the raised floor might be carrying more current than they are rated for. If one of them fails, it could generate enough heat to ignite nearby materials, especially if airflow is restricted and heat builds up. Fires in raised floors or ceilings are particularly dangerous because they are hidden from view. A fire could start and grow without being immediately detected, especially if smoke detectors are not properly placed or if airflow patterns from HVAC systems push smoke away from sensors.



RISK MATRIX

Among the highest risks are lithium-ion batteries, which pose a significant threat due to their high likelihood of thermal runaway and off-gassing incidents. In the category of medium likelihood but high impact, UPS systems are notable for their susceptibility to battery and electrical faults, while raised floor fires, though rare, can be catastrophic due to hidden ignition sources that are difficult to detect and manage. On the other hand, cables represent a high likelihood but medium impact risk, frequently acting as ignition sources, particularly when bundled densely. Lastly, in the medium likelihood and medium impact category, HVAC systems can be problematic due to dust accumulation and motor faults, and electronic equipment, including power supplies and circuit boards, also presents a moderate risk profile..

Risk Assessment

According to NFPA 72 (Chapter 4), a comprehensive fire risk assessment is a fundamental prerequisite for designing effective fire detection systems, particularly in specialized environments like data centers.

- **Identification of Ignition Sources:**
A detailed analysis of potential ignition sources within the data center, including Battery banks, power supplies, UPS systems, electrical wiring, and transient combustibles introduced during maintenance activities.

- Fuel Load Analysis:
Quantifying the type and distribution of combustible materials within the IT spaces, including equipment components, cabling, and any temporary storage, is essential for understanding the potential fire intensity and smoke production.

- Ventilation System Analysis:
The impact of the data center's HVAC system on smoke movement and detector response must be thoroughly evaluated. This includes analyzing airflow patterns, air change rates, and the potential for smoke stratification.

- Consequence Analysis:
Understanding the potential consequences of a fire, including equipment damage, data loss (although often mitigated by mirroring), and operational downtime, helps to define the required level of fire protection and the criticality of early detection. The primary objective in modern data centers often shifts from life safety (due to low occupancy in IT areas) to mitigating the loss of data storage and retrieval capacity.

FIRE DETECTION STRATEGIES

PREVENT | **DETECT** | **SUPPRESS**

Autronica's approach goes beyond detection technology. Our execution model includes detailed risk assessment, custom system design, factory acceptance testing, on-site commissioning, and post-installation support.

This turnkey delivery ensures seamless integration with BMS, ESD, and IT infrastructure, reducing project risk and accelerating go-live timelines. Autronica strategy to address data center fire involves three main stages prevention, detection and suppression.

PREVENTION

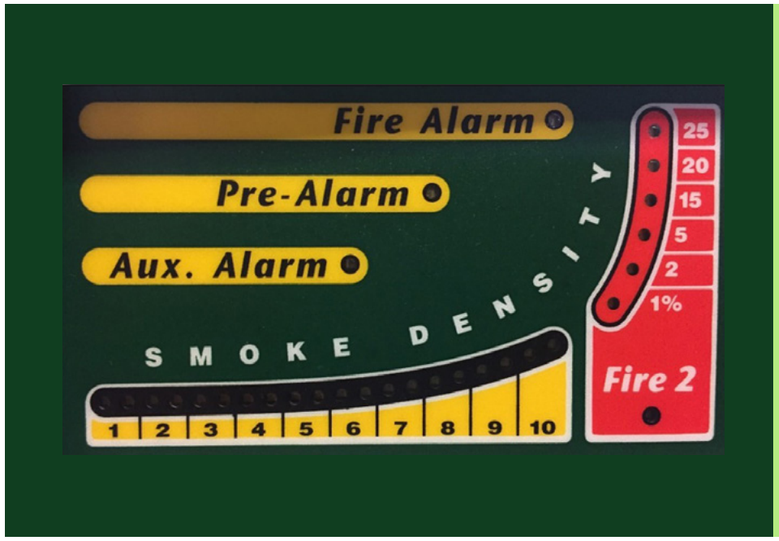
The prevention phase in fire safety for data centers is centered around the early identification of anomalies. The goal is to detect potential issues at their very beginning, allowing enough time to take corrective action and avoid downtime. This proactive approach is essential in datacenter environments where even minor disruptions can result in significant operational and financial consequences.

During this phase, attention is primarily directed toward high-risk areas such as computer rooms and battery storage. These zones house equipment that is not only expensive but also vital to the continuous operation of the data center.

Computer rooms contain servers which hosts all the applications and data. Battery storage areas are in continuous service and can pose fire risks due to chemical reactions or thermal runaway.

Computer rooms

Computer rooms in data centers rely on very high-sensitivity smoke detection systems, commonly known as aspirating detectors, to ensure early warning. These systems work by actively drawing air samples from the environment through a network of sampling pipes.
The air is then filtered and analyzed in a highly sensitive laser detection chamber capable of identifying microscopic smoke particles and combustion aerosols long before they become visible to the human eye.



These detectors send warning minutes or even hours before a fire becomes critical. This picture outlines sensitivity level for different technologies. Aspirating HSSD systems can detect very small particles produced early stages of anomalies.

The design of the ASD system takes into account the airflow patterns within the data center. Cold air is usually directed to flow from the front of server racks, sometimes from below through raised floors, while hot air is extracted from the rear and vented out through hot aisles. Sampling points are strategically placed throughout the data hall to ensure comprehensive coverage. These include locations inside server racks, often using specialized probes, beneath raised floors where power and cabling are routed, and above suspended ceilings.

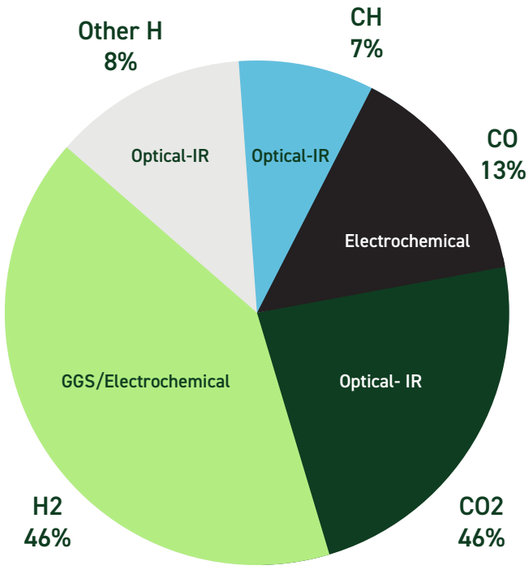
The pipe network is highly flexible and can be routed to monitor critical zones directly. ASD systems are designed with multiple configurable alarm thresholds, allowing for a staged response to potential fire events. These thresholds are typically categorized into three main groups: auxiliary alarm, pre-alarm, and fire alarm, each with further sub-levels. This tiered approach enables personnel to investigate minor anomalies before they escalate into full fire alarms, thereby reducing the risk of unnecessary disruptions to operations.

To maintain reliability and accuracy, ASD systems incorporate multi-stage filtration to remove dust and contaminants before the air reaches the detection chamber. This, combined with clean-air barriers and stable optical components, helps maintain calibration and reduces the likelihood of false alarms. Some detectors also use short-wavelength lasers, which offer improved stability across varying temperatures and better resistance to false triggers. These systems can be integrated with the main fire alarm or data center management systems through standard protocols, or relay connections. Additionally, onboard diagnostics monitor dust accumulation and filter life, enabling predictive maintenance and ensuring the system remains effective over time.

Battery Rooms

The dynamics of fire detection differ significantly in battery energy storage systems. Unlike conventional fires, where smoke precedes flames, fires in BESS often involve simultaneous smoke and fire occurrence, providing little to no warning. This is particularly challenging because the rapid escalation leaves minimal time for intervention.

A crucial distinction between battery energy storage fires and general fires is the occurrence of off-gassing events. Depending on the battery type, off-gassing can precede a fire, offering an early warning sign. Off-gassing involves the release of volatile gases from the battery, which can be detected using specialized sensors. Early detection through off-gas and smoke detection technologies provides a critical advantage in preventing fires.



According to data from NFPA 855, the off gas generated from LIB comprises several key components.

One of the primary gases released during off-gassing is ***carbon monoxide (CO)***, which remains present for an extended period. The release of CO is typically accompanied by a rise in temperature within the compartment, indicating a potential hazard. CO constitutes approximately 13% of the off-gas composition.

Hydrogen (H_2) is another significant component, making up around 50% of the off gas. This high concentration of hydrogen poses a substantial flammability risk, necessitating stringent safety measures. ***Carbon dioxide (CO_2)*** is also present, accounting for about 26% of the off gas. Additionally, ***methane (CH_2)*** is found at a concentration of 7%, and other hydrocarbons constitute around 8% of the off-gas mixture.

Monitoring of these gases are crucial to prevent accidents and maintain a safe operating environment. Off-gas release is observed in ***lithium-ion (Li-ion)*** batteries, serving as a predictor of potential thermal runaway events and indicating that the battery is not operating within suggested parameters.

Detecting early off-gas release is of vital significance in battery safety. Off-gas release refers to the emission of gases from battery cells during specific operating conditions or failure modes. These gases are primarily generated due to chemical reactions occurring within the battery, with key scenarios including charging, discharging, and thermal runaway events.

Electrochemical detection technology relies on chemical reactions between the target gas and an electrode within the sensor. This interaction generates an electrical signal proportional to the concentration of the gas. Electrochemical sensors are highly sensitive and selective, making them effective for detecting specific gases such as carbon monoxide (CO) and hydrogen (H2), which are commonly released during off-gassing events in lithium-ion batteries.

Optical infrared (IR) detection technology uses infrared light to detect the presence of gases. When a gas absorbs IR light at specific wavelengths, it causes a measurable change in the light's intensity. This change is detected and analyzed to determine the concentration of the gas. Optical IR sensors are advantageous due to their ability to provide continuous, real-time monitoring and their high sensitivity to a wide range of gases, including combustible gases and carbon dioxide (CO2).

Catalytic gas sensor (CGS) detection technology involves the oxidation of combustible gases on a catalytic surface, which generates heat. This heat change is then measured and correlated to the concentration of the gas. CGS sensors are particularly effective for detecting flammable gases such as Hydrogen (H2) methane (CH4) and lighter hydrocarbons such as C2, C3 and C4. They are robust and reliable, making them suitable for harsh environments where other sensor types might fail.

Electrochemical sensors provide high specificity and sensitivity, optical IR sensors offer continuous monitoring and reliability with least intervention, and CGS sensors provides broad range to detect Hydrogen (H2) methane (CH4) together. Together, these technologies form a comprehensive approach to off-gas detection, enhancing the safety and reliability of lithium-ion battery systems.

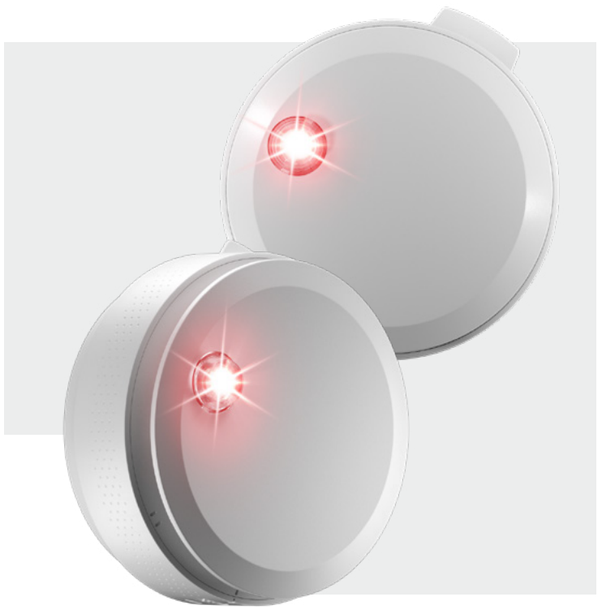
Sounde r with high soun d pressure

Smoke Detection

Heat Detection

Visual alarm device (VAD)

Carbon Monoxide detector



DETECTION

Fixed Smoke Detectors

Fixed smoke detectors are commonly used in fire safety systems to detect visible smoke particles through a method known as light scattering. These detectors are particularly effective at identifying smoldering fires, which tend to produce larger smoke particles that are more easily detected by this technology. While they are not as sensitive as early warning smoke detection systems, fixed smoke detectors serve an important role as a secondary layer of protection, especially in areas that are considered less critical within datacenter facility. Typical locations for these detectors include offices, hallways, and electrical rooms that are situated outside the main data hall.

For datacenters smoke detection combined with sounders, visual beacons, temperature sensors, and carbon monoxide monitoring provides a good solution. Due to high uptime requirement detectors are expected to meet Safety Integrity Level 2 (SIL2) standards, which ensure a high level of reliability and performance. Integrating multiple features into a single unit not only enhances detection capabilities, reduces false alarm but also simplifies the overall system architecture, reduces the amount of wiring required, and minimizes installation complexity. Another key requirement in today's data centers is the inclusion of self-diagnostic capabilities in fire detection systems. These features help reduce the time, effort, and cost associated with manual testing and maintenance. By continuously monitoring their own performance, these detectors can alert facility managers to issues such as sensor degradation or contamination.

Heat Detectors

Heat detectors respond to a rapid rise in temperature (rate-of-rise) or a fixed temperature threshold. They are Less common in the main data hall as primary detectors because they react only after a fire has generated significant heat, which might be too late for sensitive equipment. They are more suitable for areas like generator rooms, battery rooms, or any room where high heat is an expected fire characteristic.

Flame Detectors

Flame detectors are specialized fire detection devices that identify the presence of flames by sensing the specific radiant energy. Flame detectors respond to the unique light signatures produced by combustion, making them highly effective in detecting flames. Multi-spectrum IR tuned for general fire is most suitable flame detector for datacenter application due to its immunity to false alarming.
Flame detectors are not commonly used for general protection in data halls however they find application in areas such as fuel storage rooms, generator enclosures, and outdoor chiller areas.

SUPPRESSION

The primary challenge is to extinguish a fire without damaging expensive electronic equipment or compromising data integrity. Below are suppression methods used in datacenter.

Clean Agent Gaseous Suppression Systems

Clean agent system deploys a gas that extinguishes fire by either removing heat from the fire tetrahedron, displacing oxygen, or interrupting the chemical chain reaction of combustion. They leave no residue, are non-conductive, and are generally safe for electronic equipment and personnel. Clean agents allow for quicker recovery after a fire event. The suppression system activated from fire detection system. There's usually a pre-discharge alarm and a timed delay to allow personnel to evacuate.

Water Mist Systems

Discharges a very fine mist of water droplets. The tiny droplets rapidly absorb heat, reducing the temperature, and the vapor displaces oxygen. It uses significantly less water than traditional sprinklers, minimizing potential water damage. It is gaining popularity as an alternative to gaseous systems in datacenter applications. Water mist is rapid and cost efficient to rearm.

Rack-Level Fire Suppression

These are small, localized clean agent systems or even aerosol-based systems directly integrated into individual server cabinets. It can extinguish a fire at its source within a rack, preventing it from spreading to other equipment or requiring a full room discharge. Often used in high-density racks or for added protection of extremely critical equipment.

Emergency Shutdown (ESD) Systems

The F&G system is integrated with the building management system and emergency power off systems. In a potential fire event, the ESD system can automatically shut down power to affected areas, activate fire suppression, and isolate critical systems to prevent further damage or hazards. Manual call points are located throughout the facility for any emergency activation needs.

AUTRONICA IN DATA CENTER

KEY FEATURES

Multi-Technology Gas Detection
Integration of electrochemical, optical IR, and catalytic gas sensors for detecting off-gassing from lithium-ion batteries.

High-Sensitivity Smoke Detection (ASD)

Laser-based aspirating smoke detection that samples air from multiple zones, detecting microscopic particles long before visible smoke appears.

SelfVerify Technology

Automatically tests every detector, interface, and alarm device every 24 hours, reducing manual testing and maintenance costs.

Smart Zoning and Tiered Alarm

Configurable alarm with zone-specific strategies such as operational zone , detection zone and alarm zone for staged response to anomalies.

Integrated Emergency Shutdown (ESD) and BMS Connectivity

Seamless integration with Building Management Systems (BMS) and Emergency Power Off (EPO) systems.

Compliance with Global and Local Standards

Alignment with NFPA 72, 75, 76, and new Norwegian data center safety regulations (2025).

BENEFITS

Enables early intervention, reducing risk of equipment loss and operational disruption.
Detects early-stage thermal runaway in lithium-ion batteries, preventing fires.
Ensures continuous operation and reduces downtime.
Reduces false alarms and unnecessary evacuations with staged response.
Automates shutdown only of affected zones.
Optimal technology selection based on detection capability, maintenance requirement & cost.
Reduces risk of non-compliance penalties and ensures regulatory readiness.

AUTRONICA ADVANTAGES

Most systems rely on periodic manual testing, which can miss faults or cause downtime.
Autronica's SelfVerify Technology ensures continuous operational readiness.
Many systems use point detectors that are slower and less effective in high-airflow environments.
Autronica's ASD detects microscopic particles long before visible smoke appears.
Most systems rely on smoke detection alone, which is too late for battery fires. Autronica's multi-technology gas detection detects early-stage thermal runaway.
Many systems use binary alarm logic, lacking the nuance of Autronica's smart zoning and tiered alarm thresholds.
Many systems does not provide advance ESD integration features. Autronica's ESD and BMS connectivity at SIL2 certified level provides reliable shutdown and recovery.
Some systems may not meet the latest or region-specific standards. Autronica ensures full compliance with global and local standards.

TECHNICAL DIFFERENTIATORS

SIL2 Certified Systems – Proven safety integrity for Datacenter environments
Dual Safety Architecture – Redundant system design ensures no single point of failure.
In-Built Isolators – Every device is protected, reducing fault propagation.
Automatic Addressing – Faster commissioning and reduced human error.
False Alarm Immunity – High reliability in complex environments.
Hazardous Area Equipment – Certified for harsh and high-risk zones.

WHY WE WIN IN DATA CENTERS?

- Proven Performance
Trusted in critical infrastructure worldwide for 50+ years.
- Lifecycle Support
Fast response and expert service.
Dedicated Fire Detection Focus
From R&D to Aftersales and services full value chain.
- Tailored Solutions
Tailored for data center needs.
Reputation & References – Extensive install base and customer trust.
Regulatory Approvals – Worldwide.
- Turnkey delivery model
Autronica delivers complete fire and gas safety systems as a single-source provider.
From concept to commissioning, our in-house engineering, project management, and service teams ensure flawless execution. This reduces coordination complexity and ensures accountability across the project lifecycle.

www.autronicagroup.com