euralarm

White Paper

Fire safety in a connected world

Table of contents

Executive Summary 4

Introduction 4

Fire detection in the digital age 5

Remote services: from maintenance to continuous protection 5

Towards automated testing and digital documentation 6

Cloud connectivity and the emergence of smart buildings 7

Cybersecurity: safeguarding life in the digital realm 7

The European framework: standards, sustainability, and trust 8

From data to decisions: the power of integration 8

Challenges and the path forward 9

Conclusion 9

Foreword

Changes revision table			
Date	**Rev #**	**Paragraph / Page**	**Change**
6/2026			First publication

DISCLAIMER

This document is intended solely for guidance of Euralarm members, and, where applicable, their members, on the state of affairs concerning its subject. Whilst every effort has been made to ensure its accuracy, readers should not rely upon its completeness or correctness, nor rely on it as legal interpretation. Euralarm will not be liable for the provision of any incorrect or incomplete information.

Note: The English version of this document, [document number], is the approved Euralarm reference document.

Copyright Euralarm

Euralarm • Gubelstrasse 11 • CH-6300 Zug • Switzerland

E: secretariat@euralarm.org
W: www.euralarm.org

Fire safety in a connected world: Integrating detection, remote services, and cybersecurity

Executive Summary

The European fire safety industry is at a turning point. Digitalization, remote connectivity, and cybersecurity are converging to redefine how buildings are protected and maintained. This white paper outlines how these forces are transforming fire detection systems into intelligent, connected infrastructures — and what this means for service providers, building operators, and policymakers across Europe.

Across the continent, false alarms [1]remain a significant burden: studies such as Euralarm's 2022 False Alarm Study show that in some countries the false fire alarm ratio of FDAS (Fire Detection and Alarm Systems) is over 85% Unnecessary activations disrupt business continuity, erode confidence in fire protection systems and potentially waste emergency resources. At the same time, climate change, energy efficiency targets, and a shrinking pool of skilled labour are reshaping building operations and maintenance practices.

Digital transformation offers powerful answers. Through smart connectivity, cloud-based monitoring, and data analytics, fire detection systems can now provide real-time insights, enabling remote diagnosis, predictive maintenance, and data-driven decision-making. These capabilities reduce downtime, improve safety, and support sustainability goals by cutting travel and optimizing resource use.

However, with connectivity comes a new responsibility: cybersecurity. As fire systems are more often connected via the internet, they must be protected from digital threats that could compromise safety or availability. Standards such as EN 50710:2021 (for remote services), CLC/TS 50136-10 (for Remote Access Infrastructure), IEC 62443 (for industrial OT cybersecurity), and ISO/IEC 27001 (for IT information security management) provide the framework for building and operating secure systems that are designed to protect information, assets, and operations from unauthorized access, damage, or disruption. Such secure systems that follow Security by Design and Security by Default principles ensure that fire protection remains reliable, even in the connected era.

By integrating fire detection, remote services, and cybersecurity, European stakeholders can achieve safer, more resilient, and more sustainable buildings. Interconnected digital fire safety is already emerging as the new operating model and is expected to become standard practice across many new and modernised buildings during the second half of this decade, as connectivity, remote services and cybersecurity requirements become embedded in building operations and European regulatory frameworks. Those who act now will lead the market transformation, delivering smarter protection and stronger trust in the systems that safeguard lives and assets.

Introduction

Europe's building landscape is undergoing a digital transformation. As societies strive for sustainability, safety, and resilience, fire protection systems — traditionally ring-fenced and reactive — are being connected into intelligent

[1] A false alarm is defined as a fire alarm when there are no conditions that justify a fire intervention. They are divided intro equipment false alarms or technical failures, deceptive false alarms and malicious and good intent false alarms

networks providing pro-active solutions. The convergence of fire detection, remote digital services, and cybersecurity is reshaping how buildings are protected, operated, and maintained.

This transformation brings vast opportunities. Smart connectivity and data-driven insights can dramatically reduce false alarms, enhance maintenance efficiency, and improve life safety outcomes. Yet it also brings new vulnerabilities, especially when fire safety systems are connected to the cloud and external networks. Understanding and managing this interplay between digital opportunity and digital risk is now essential for every stakeholder in the fire safety ecosystem — from manufacturers and service providers to building owners, operators, and regulators.

This white paper explores how digitalization, remote services, and cybersecurity form an integrated framework for modern fire detection. It reflects the European perspective and regulatory landscape, providing an outlook on how businesses can adapt to a future of connected, cyber-secure, and sustainable fire safety.

Fire detection in the digital age

Fire safety has traditionally relied on hardware-based systems that required periodic manual inspection and had a stand-alone operation. Today, as buildings become more complex and multifunctional, these legacy systems no longer suffice. Across Europe, false alarm rates remain high, disrupting operations, burdening emergency services, and eroding trust in safety systems.

The transition toward digital fire detection is driven by the need for reliability, operational continuity, and resource efficiency. Modern sensors and control panels are not only detectors; they are data nodes capable of self-diagnosis, communication, and integration with wider building systems. When combined with cloud connectivity and data analytics, these devices can help to distinguish between real and false alarms, adapt to environmental conditions, and even predict potential failures before they occur.

This transformation is taking place against the backdrop of profound global and European trends: decarbonization targets under the European Green Deal, new fire risks from renewable technologies like photovoltaic systems and electric vehicle charging, and a chronic shortage of skilled technicians. Digitalization offers a means to address all these challenges at once — reducing emissions through remote diagnostics, enhancing safety through predictive maintenance, and optimizing scarce technical resources.

Remote services: from maintenance to continuous protection

One of the most visible manifestations of digitalization in fire safety is the rise of remote services. Such services, whether provided by point-to-point connections or leveraging cloud connectivity, enable monitoring, diagnostics, and may even support maintenance actions in some circumstances

Traditionally, maintenance followed a reactive model: a fault occurred, a technician was dispatched, and downtime ensued. Over time, the industry introduced preventive maintenance, replacing purely reactive service models with scheduled inspections and testing. In this approach, systems are maintained at predefined intervals, typically based on regulatory requirements or manufacturer recommendations. While this represented a

significant improvement over reactive maintenance, it still relies largely on fixed schedules rather than the actual condition of system components. Detectors, control panels, and communication interfaces may therefore be serviced too early, before any deterioration has occurred, or too late, after performance has already been affected. Preventive maintenance reduces the risk of failure but does not eliminate inefficiencies or unexpected disruptions.

The growing connectivity of fire safety systems now enables a further step in the evolution of maintenance strategies. Through secure remote connections and cloud-based monitoring platforms, fire detection systems can continuously transmit operational data such as detector status, contamination levels, environmental conditions, and system events. Service providers and facility managers are able to analyse this data in real time and identify irregularities that might otherwise remain unnoticed during periodic inspections.

This capability enables predictive maintenance, in which maintenance activities are based on the actual condition of system components rather than predetermined schedules. For example, detectors can automatically report contamination levels or changes in sensitivity, allowing maintenance to be scheduled precisely when cleaning or replacement is required. Similarly, system diagnostics can detect early signs of component degradation, communication faults, or abnormal environmental influences. By addressing these issues before they lead to alarms, faults, or system downtime, predictive maintenance significantly improves reliability while optimizing service resources.

Beyond prediction lies an even more advanced concept: prescriptive maintenance. In this model, the system not only identifies potential issues but also recommends specific actions based on data analysis and historical performance patterns. By combining large datasets from multiple buildings with machine learning algorithms, digital platforms can determine the most effective intervention strategy, recommend spare parts, and prioritize service actions across multiple sites. In some cases, corrective measures can even be executed remotely, such as adjusting configuration parameters or updating system software.

Towards automated testing and digital documentation

A further advantage of connected fire safety systems lies in the ability to automate routine inspection and testing procedures while digitally documenting the results. Traditionally, periodic testing of fire detection systems has required significant manual effort. Technicians often need to work in teams to activate detectors, verify signals at the control panel, and record results in paper-based logbooks or separate documentation systems. This process can be time-consuming, disruptive to building operations, and prone to inconsistencies in documentation.

Digitalized fire safety systems enable a more efficient approach through automated testing and integrated digital documentation. Detectors and system components can perform self-tests or remotely triggered functional tests, with the results automatically transmitted to a central platform. Service engineers can monitor these tests in real time or review them afterwards through secure dashboards. Because the system records each event, test action, and system response automatically, the results are documented consistently and with a level of detail that is difficult to achieve through manual reporting.

The use of digital logbooks and inspection records provides additional operational and compliance benefits. All maintenance activities, system events, and inspection results can be stored in a structured and searchable digital environment. This enables building operators, service providers, and authorities having jurisdiction to easily access

historical records, verify compliance with inspection requirements, and generate standardized reports. Digital documentation also improves transparency across multi-site portfolios, allowing organizations to maintain a clear overview of the status and maintenance history of their fire safety systems.

For service providers and building operators alike, these capabilities significantly reduce administrative workload while improving traceability and accountability. Automated testing can shorten maintenance visits, enable single-technician inspections in some cases, and reduce disruption to building occupants. At the same time, digital documentation ensures that inspection and maintenance activities are reliably recorded and readily available for audits or regulatory verification. As fire safety systems become increasingly connected, automated testing and digital recordkeeping will play a growing role in supporting both operational efficiency and regulatory compliance.

Cloud connectivity and the emergence of smart buildings

The foundation of remote services is secure cloud connectivity. Fire safety systems increasingly form part of a building's broader digital ecosystem, where data from sensors, HVAC systems, lighting, and security devices converge into a unified platform. In this context, fire detection becomes a core element of smart building operation.

In a connected environment, every event in a fire system — an alarm, fault, or maintenance notification — can be transmitted instantly to a cloud-based dashboard. Facility managers gain a panoramic overview of multiple sites, while service companies can remotely access control panels, review system logs, and even execute configuration changes. These capabilities are now made available through specialized web portals and mobile applications, making professional fire system management more agile and transparent.

For building operators, the benefits are tangible: reduced downtime, optimized scheduling, improved resource use, and compliance documentation that is automatically generated and securely stored. Moreover, connectivity allows coordination between systems — for example, linking fire detection with emergency communication, lighting, and HVAC to enable dynamic evacuation guidance.

However, with this interconnectivity comes a critical dependency: the security of data and networks. As soon as fire safety systems are connected to the Internet, cybersecurity becomes integral to life safety.

Cybersecurity: safeguarding life in the digital realm

Cybersecurity in fire safety is fundamentally about protecting life, assets, and operational continuity from digital threats. The digital transformation that enables remote access and intelligent analysis also expands the attack surface. A compromised fire system could lead to unauthorized access, data manipulation, or disruption of critical safety functions. As hybrid warfare, ransomware, and industrial espionage intensify globally, these risks can no longer be ignored.

European standards already provide a framework for secure digital services in fire safety. The EN 50710: standard and CLC/TS 50136-10 define requirements for remote services for fire safety and security systems, ensuring that only authorized personnel access systems through secure connections. At the same time, international standards

such as ISO/IEC 27001 and IEC 62443 define requirements for information security and industrial cybersecurity. Systems certified under these frameworks demonstrate that they are built on Security by Design principles — embedding protection throughout the product lifecycle rather than adding it as an afterthought.

In practice, Security by Design means that devices and software are conceived with secure architectures, strong encryption, and rigorous testing. Several manufacturers apply multiple principles including;
- Security by Default, ensuring that protective measures are active from the moment of installation;
- the Principle of Least Privilege, which limits user access strictly to what is necessary; and
- the Separation of Duties, which prevents any individual from having complete control over critical functions.

Equally important is the recognition that cybersecurity is a shared responsibility. Manufacturers must design secure products; service providers must follow hardening guidelines and update systems regularly; and end users must implement strong policies for access control, password management, and network segregation. Cloud service providers, such as those hosting European fire safety platforms, must comply with stringent data protection standards, including the EU General Data Protection Regulation (GDPR), to ensure confidentiality and privacy.

When executed correctly, cybersecurity does not hinder connectivity — it enables it. It builds the trust necessary for digital fire safety to reach its full potential.

The European framework: standards, sustainability, and trust

Europe provides a unique environment for advancing integrated fire safety. The region's regulatory culture emphasizes both safety and sustainability, aligning closely with digital innovation. Initiatives such as the Corporate Sustainability Reporting Directive (CSRD) are expanding the definition of responsible business, making environmental, social, and governance (ESG) performance a core obligation. Digital fire systems directly contribute to these goals amongst others by reducing travel emissions and supporting efficient maintenance.

At the same time, the European cybersecurity landscape — including regulations such as the NIS2 Directive and the Cyber Resilience Act — is setting higher expectations on products and for critical infrastructure operators, including building and safety systems. Euralarm's role as an industry voice is crucial in ensuring that standards like EN 54 (for fire detection and alarm systems), EN 50710 (for remote services), CLC/TS 50136-10 (for Remote Access Infrastructure) and IEC 62443 (for cybersecurity) evolve coherently, avoiding overlaps and ensuring practical interoperability.

Trust in this context is built through transparency, certification, and collaboration. Certification demonstrates compliance, but continuous dialogue between manufacturers, service providers, and regulators ensures that standards keep pace with technological evolution.

From data to decisions: the power of integration

The convergence of fire detection, remote services, and cybersecurity yields a new paradigm: data-driven fire safety. When information from detectors, control panels, and connected devices is aggregated and analysed in real time, it becomes possible to identify patterns and predict risks that would otherwise remain invisible.

Machine learning and artificial intelligence are beginning to play a role in this process. Algorithms can correlate environmental data — such as temperature, humidity, or particulate concentration — with historical alarm patterns to distinguish genuine fire events from false triggers. This intelligent orchestration transforms fire safety from a static, reactive function into a living system that learns and adapts. It enables prescriptive maintenance planning, continuous compliance monitoring, and faster emergency response. The result is a safer, more efficient, and more sustainable built environment.

In the future, AI has the potential to dynamically adjust detection thresholds, optimize suppression responses, and coordinate evacuation routes based on live building occupancy data. However, such adaptive techniques are not compatible with current prescriptive product standards.

Challenges and the path forward

Despite rapid progress, challenges remain. Legacy infrastructure across Europe often lacks the connectivity or interoperability required for digital integration. Upgrading these systems requires investment and a clear strategy for data governance and cybersecurity. The diversity of national regulations and approval processes can also slow adoption, underscoring the need for harmonization and mutual recognition of digital standards.

Another challenge is workforce transformation. As digital fire systems proliferate, technicians must evolve into data-literate professionals capable of managing software updates, cloud dashboards, and cybersecurity configurations. Education and certification programs will be vital to bridge this skills gap.

Finally, the growing reliance on digital ecosystems makes resilience a key concern. Redundancy, secure network architecture, and clear contingency plans are essential to ensure that digital dependence does not create single points of failure.

Conclusion

The intersection of fire detection, remote services, and cybersecurity defines the next frontier of fire safety in Europe. Digitalization is not a passing trend but a structural shift — one that will determine how effectively societies can protect people, assets, and the environment in the decades to come.

By embracing secure connectivity, industry stakeholders can achieve unprecedented efficiency, accuracy, and sustainability. But this requires commitment to common standards, continuous investment in cybersecurity, and collaboration across the value chain.

Fire safety is, at its core, about trust. In a digital world, that trust must extend beyond the reliability of sensors and alarms to encompass the integrity of data and networks. Through secure, connected, and intelligent systems, Europe can lead the way toward a future where fire protection is not only smarter, but also safer.

Publication date: DD-MM-YYYY

Euralarm
Gubelstrasse 22
CH-6301 Zug (Switzerland)

Swiss Commercial Registration No: CHE-222.522.503

E secretariat@euralarm.org
W www.euralarm.org