

**Guidance
Note**



Fire Industry Association



Fire Alarm Management Systems (FAMS)

FIA Guidance document – Fire Alarm Management Systems (FAMS)

1. SCOPE	3
2. INTRODUCTION	3
3. OVERVIEW	3
4. SUMMARY	10
5. FURTHER RELEVANT PUBLICATIONS AND ONGOING WORK	10
6. FURTHER RESEARCH	11
7. BIBLIOGRAPHY	11



Created by experts' input from the Smart Project

1. SCOPE

These FIA guidance notes give an introduction to what a Fire Alarm Management System (FAMS) is, and varying capabilities, uses and benefits.

This guidance also discusses the interaction with FAMS and existing codes of practice and standards with particular emphasis on GDPR, the provision of adequate Cyber security and a correct management infrastructure.

These guidance notes are to be used in conjunction with the information contained in other codes of practices standards and guidance documents referred to directly within this file or detailed in the bibliography section.

2. INTRODUCTION

What are Fire Alarm Management Systems (FAMS)?

Fire Alarm Management Systems (FAMS) is a generic term used for a system providing control, monitoring and management of a sites fire alarm system.

FAMS solutions have varying capabilities, most can communicate fire and fault activity which is sent to a cloud hosted database. Users can then access their sites fire alarm panel information through the internet or be alerted to activations on site via their mobile phone, using apps or SMS (short message service).

The use of FAMS can be an advantage to servicing organizations and customers, where remote checks can be undertaken prior to an engineer visiting site. As an example, an engineer can ensure they have the correct parts in their van before attending a site, “first time fixes”. This also has the added benefit of reducing a company’s carbon footprint, where the time spend on the road by engineers will be significantly reduced, as well as making the business more efficient and leaner. If the size of the site requires two engineers to service a system, with FAMS it may now only need one. Assistance with compliance for parts of the fire safety orders, are also be a major benefit to organisations.

3. OVERVIEW

FAMS Compliance and Limitations

FAMS are not currently required to be compliant to any particular standard, but various manufacturers are considering making application for formal product performance criteria. One such standard is BS EN 54-21, which is the Alarm transmission and fault warning routing equipment standard.

IMPORTANT NOTE

If the early summoning of the fire and rescue service is considered critical to the safety of occupants, say based on a fire risk assessment, sites should be provided for automatic transmission of alarm signals to an Alarm Receiving Centre (ARC), unless there are reliable arrangements for summoning the fire and rescue service by persons in the building. This will mean providing a primary signalling signal compliant with BS EN 54-21.

An example where this is required is in residential care premises, facilities should be provided for automatic transmission of alarm signals to an ARC. Also, for Category P (Property) category systems unless they are continuously occupied, they should also incorporate a means for automatic transmission of fire signals to an ARC.

A FAMS without BS EN 54-21 compliance is providing complimentary signalling only or a secondary confirmation type signal, rather than primary signalling.

Primary signalling would only be achieved by an Alarm Receiving Centre through products compliant with BS EN 54-21.

There is also a standard BS EN 54-13 which is for the assessment of compatibility and connectability of fire detection and fire alarm system components. It specifies the requirements of the integrity of the fire detection and alarm system when connected to other systems. Should FAMS hardware be a type 2 component, so tested to ensure it has no adverse effect on a Type 1 component or potentially it could be used as a Type 1 component, if approved as an ancillary management product?

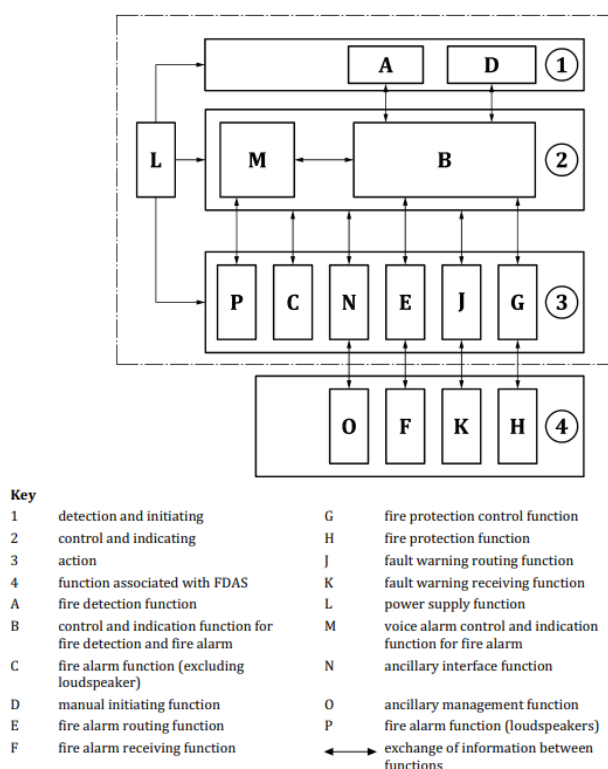


Figure 1. Fire detection and fire alarm systems and associated systems, functions and equipment

FAMS Benefits and Capabilities

Depending on the individual product concerned FAMS have the ability to be able to communicate full point identification for the whole of the sites Addressable Fire Detection & Alarm System, for a single panel to the complete fire alarm network. FAMS can also be used for Conventional Fire Alarm systems, where they are able to communicate Fire and Fault activity for a site, but there will be limitations of systems functionality.

Some of these FAMS products are also capable of remotely disabling fire alarm equipment, but these are mostly limited to FAMS offerings dedicated to a specific manufacturer, but potentially through technology enhancements and protocol sharing, further capabilities for these could be developed.

FAMS can generate reports, notify, and record Manual Call Point weekly tests, to assist clients for compliance with Articles 13 & 17 in the Regulatory Reform (Fire Safety) Order RRFSO. The Fire (Scotland) Act and the Fire & Rescue Services (Northern Ireland) Order have similar references.

FAMS can be used to provide independent evidence of maintenance testing, information communicated to FAMS can be stored in an infinite log.

The risk to life and property from fire is often dependant on the quality of fire safety management, and how records are kept and maintained is one of the biggest failings in premises. Digital records and remote service offerings can give that compliance with this part of a buildings Fire safety.

FAMS could potentially be used as part of a sites fire evacuation plan, where on receipt of notification of fire on a site an action is carried out, which might be to say isolate a gas valve manually on a site, or ensure other site fire safety management controls are undertaken.

Cyber security and correct managerial controls with a FAMS discussed later in these notes would be critically important.

FAMS Signalling, Power Supplies & Commissioning

FAMS have the capability of communicating either via the Ethernet wired or wirelessly via General Packet Radio Services (GPRS).

Ethernet is a wired connection and is generally much faster (depending on the speed of the internet connection), cable connections are also more secure. Sometimes in premises there will be no Ethernet port availability in the vicinity of the CIE and FAMS hardware.

For ease of installation and convenience GPRS signalling may be employed as an alternative.

GPRS is a packet switching technology that enable the transfer of data through cellular networks. Speeds can be an issue and the recording of signal strength and a thorough survey will be required for each site.

FAMS will require an adequate electrical supply to work. The question of if this should be sourced from the FD&A CIE is one for the designer of the system to make. If adding FAMS to an existing system then it will probably require an external dedicated power supply to power the FAMS. This in turn would need to report any power supply faults to the FD&A CIE.

During the commissioning it will be necessary to verify that the FAMS product is actually working. This will require testing the fire and fault signalling of a FAMS. The FAMS checks will be built into a company’s commissioning methodologies and will vary widely depending on the capabilities of the individual products. The recording of internet speeds, site GPRS signal strengths. The information from these checks could be added to the commissioning certificate in BS 5839-1:2017 or another dedicated form.

FAMS – Initial Data Proformas & Training

FAMS will require some client information for example, email addresses and telephone numbers. These will need to be stored in the system, to enable automatic notifications and alerts, and also to control and limit permissions for managers and users.

GDPR is an important consideration when putting this personal data together and is considered in greater detail on page 7 of these guidance notes.

A proforma may need to be created and populated for the various options at the point of commissioning, so that the data can be correctly set up and it is recommended that this is agreed in writing.

Below may be considered as example data that is required to be inputted into a FAMS:

- Username, title (role or position)
- Email addresses
- Phone numbers and permission levels (Could be several defined access levels depending on the individual FAMS offering)
- What specific notifications are required and via what medium?

USERNAME	TITLE	EMAIL ADDRESS	TELEPHONE NUMBER (OPTIONAL IF YOU REQUIRE NOTIFICATION VIA SMS AND NOT JUST EMAIL)	PERMISSION MANAGER OR USER
Example – Julie Mann	Head	jm99999999@bt.com	07777 999999	Manager
Example – Will O’Connor	Deputy Head	woc88888888@bt.com	07777 888888	Manager
Example – Neil Jones	Site Facilities	nj77777777@bt.com	07777 777777	Manager
Example – Alison Quigley	Site Engineer	aq66666666@bt.com	07777 666666	User
Example – Hannah Boatswain	Teacher	hb55555555@bt.com	07777 555555	User
Example – Daniel Modasia	School Receptionist	dm44444444@bt.com	07777 444444	User
Example – Benjamin Leach	PE Head	bl44444444@bt.com	07777 333333	Manager

Figure 2. Example Proforma Information


NOTIFICATION	EMAIL  Y/N	SMS  Y/N	APP  Y/N
FIRE ALARM			
PRE-ALARM			
EVACUATE			
SILENCED			
MUTE			
TESTING			
RESET			
DISABLE			
ENABLE			
FAULT			

Figure 3. Notifications Email SMS or via an App

Information can be populated by clients after suitable training but may also be directly administered by the FAMS product provider or another third-party company selling the product. Will the system have shared control between the product supplier and end user?

Individual training requirements will depend on the capabilities and complexity of each FAMS and the individuals employed role as a manager or user.

If adequate training is not undertaken this could lead to problems. As an example, what if a user inadvertently removes a person through lack of understanding of the technology or through simple human error. This person will no longer receive an alert and for a Life safety system this could be a serious issue.

How do FAMS operate, is data recoverable?

A lot of the systems seen have dates and times from actions undertaken, be they alerts from sites or times when a system was last logged into. FAMS products reviewed so far do have reset capabilities if issues are identified or raised. What will be the product support if there is an issue to escalate for further support are questions to be considered?

Another consideration is the frequency at larger sites for members to be deleted or added. Would work email addresses and phone numbers only be the norm for adding into a particular FAMS managers/administrators/engineers, so that if they do leave the business for any reason the access capability is removed through an internal IT process?

FAMS Data Protection GDPR

An understanding of the implications of compliance with General Data Protection Regulations (GDPR) is required for FAMS. GDPR's primary aim is to give individuals control over their personal data. GDPR is important as it improves the protection of data subjects' rights and clarifies what companies must do who process this data in safeguarding those rights.

All FAMS will need to comply with all applicable data protection and privacy legislation in force at the time in the UK, including the General Data Protection Regulation ((EU) 2016/679), the Data Protection Act 2018, and the UK General Data Protection Regulation.

Controllers and processors of personal data must have in place appropriate technical and organizational measures to implement all of the required the GDPR principles. GDPR does not mandate a specific set of cyber security measures but expects you to take appropriate actions.

FAMS Cyber Security

Cyber security or information technology security is the protection of our computer systems from information disclosure, theft, or damage to the hardware, software, or electronic data as well as disruption or misdirection of the services being provided.

As we become more reliant on the Internet of Things (IoT) and Software as a Service (SaaS) cyber security needs to be carefully considered, for Life safety fire alarm systems, the consequences for an attack on design vulnerabilities in a fire alarm system would be intolerable, GDPR aside. The Control & Indicating Equipment) (CIE) could potentially be tampered with, passwords changed, controls and functionality could be lost. Depending on the specific capabilities of a FAMS, areas of detection and or sounders could be disabled.

There may be phishing attempts to acquire sensitive customer or our managers/ administrators /engineer's information such as usernames, addresses phone numbers. Malware could be installed, and data permanently deleted.

Large corporations can be targeted for financial gain or attacks can simply be malicious, depending on the nature of the customers involved attacks may be politically motivated.

In the UK, the National Cyber Security Council was set up to help protect critical services from cyber-attacks and to improve the underlying security of the UK internet. Its aim is to make the UK a safe place to live and be able to conduct business online.

Most countries have their own versions, as another example in America there is the National Institute of Standards & Technology (NIST) which provides frameworks for improving critical infrastructure cyber security.

Considerations may also need to be made to each product manufacturers individual requirements for data security and this could mean adhering to specific management standards and processes that have been produced and accepted as good practice.

It is appreciated that Cyber security technologies and standards are complex. One way a product manufacturer can demonstrate how secure its product is, is by having what is known as a Penetration test or “Pen test” completed of its system. Penetration Testing, otherwise known as Pen testing, is where attempts are made to compromise or gain unauthorized access to a particular network or application. The process is sometimes referred to as “white hat hacking” or “Ethical hacking”. This is where a qualified professional will attempt to uncover vulnerabilities and misconfigurations that present themselves as a cyber security risk.

This will give product manufacturers an overview of their security, highlighting flaws so they can be sorted before they are picked up by malicious hackers. Penetration tests evidence will be mandatory for some companies and compliance schemes.

It may be a possibility that a product manufacturer may not want to share results of a Pen test highlighting its flaws and vulnerabilities. A Non-Disclosure Agreement (NDA) or confidentiality agreement contract may need to be agreed between parties to protect this information.

Now in addition to Pen tests control processes are extremely important. Businesses may ask a company to provide proof of compliance. There are two similar frameworks for this, ISO 27001 certification or a SOC 2 report.

BS EN ISO/IEC 27001:2017 is a generic standard applicable to all organizations, regardless of type size or nature which specifies Information Security Management System (ISMS) requirements for establishing, implementing, maintaining, and continually improving an information management systems.

A security management system preserves confidentiality, integrity, and availability by creating a risk management process so clients/customer’s, insurers and third parties can see they are being looked after against the threat of cyber-attacks.

It is expected that an organization considers this and has a process in place, scaled to the size and needs of the organization.

Now if a product manufacturer is not specifically accredited to ISO 27001 another route to demonstrating compliance is by providing a SOC 2 Type 2 report.

A SOC 2 TYPE 2 report is created by an external auditor who will assess the effectiveness of an organizations controls regarding security, availability, processing integrity, confidentiality and or privacy. It captures how a company will safeguard a customer’s data, and how well those controls are working.

ISO 27001 accreditation and a SOC 2 Type 2* report is fundamentally the same. The only difference is who conducts the audit. A recognized accreditation body completes ISO 27001 certification whereas SOC 2 reports are completed by a licensed company or individual.

***NOTE:** Sometimes 2 written as “II” instead of 2.

If you are a service provider, or a service organization, which stores, processes, or transmits any kind of information, you may be required to have either ISO 27001 or a SOC 2 Type 2 to remain in a competitive market. Some companies are demanding such accreditation.

IMPORTANT NOTE

When hosting customer data as part of your overall product architecture, it is important to use a reputable and cyber security certified cloud hosting provider. But that is only the beginning of your cloud security responsibilities. When leveraging Infrastructure as a Service (IaaS), you hold the responsibility for the servers and cloud configuration management within your tenant space.

The providers of these services work as shared responsibility models between themselves and the customer. Shared models help to relieve operational burdens, but limitations are to the infrastructure, hardware, software, and networking specific to the cloud service. Customers responsibilities is defined by the services they require but there will always be some level of shared responsibility in the guest space.

So vulnerability scanning and patching, central logging and monitoring, antivirus, and cloud configuration hardening, as well as ensuring your code is vulnerability free and all third-party components are properly licensed, are critical steps to provide end to end security of your product. In a nutshell, an individual product manufacturer also needs to be operating under an ISO 27001 accreditation scheme or have a SOC 2 Type 2 report to demonstrate its compliance.

4. SUMMARY

With the turning off of the Public Switched Telephone Network (PSTN) in 2025 and the switch to a data focused network rather than a voice network. FAMS will have a huge potential in helping to improve fire safety, assisting duty holders of premises, reducing our carbon footprint and will improve the quality of service to clients.

As we become more reliant on these innovative product offerings and through technological developments, it may be possible that existing codes of practice are changed or amended to accept these as viable alternatives or the accepted solution.

Where FAMS are used, the controls and processes need to be stringent for the Life safety and or Property protection. Cyber security cannot be an afterthought and must be addressed for confidence in the integrity of a product.

5. FURTHER RELEVANT PUBLICATIONS AND ONGOING WORK

EN 50710 Remote services Standard – This is currently in a draft format. When this standard is released more guidance will be available and we will know definitively industry expected standard requirements. The introduction of EN 16763 and the services directive already requires a pan European approach for remote access, so all tasks will need to be completed by qualified person as one example. The EN 50710 document specifies the minimum requirements for the provision of secure remote services via a remote access infrastructure (RAI) carried out either at site or off-site (e.g. via IP connections) to fire safety systems including, but not limited to, fire detection and fire alarm systems, fixed firefighting systems, smoke and heat control systems. Aware that remote access infrastructure is in EN 50136 series and there is being the IOT cyber security considerations.

6. FURTHER RESEARCH

CEN TECHNICAL COMMITTEE NO 79: ALARM SYSTEMS

7. BIBLIOGRAPHY

BS ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems.

BS 5839-1:2017 – Code of practice for design, installation, commissioning, and maintenance of systems in non-domestic premises.

CREST – Council for Registered Ethical Security Testers- International not for profit accreditation & certification body.

Data Protection Act 2018 and UK General Data Protection Regulation (GDPR).

EN 54 – 13 Non-harmonized Assessment of compatibility & connectivity of fire detection systems.

EN 54-21 Harmonised Alarm transmission & fault warning routing equipment.

EN 50710 Requirements for the provision of secure remote services for fire safety systems and security systems.

EN 16763 Services for fire safety systems and security systems.

EN 50136-1:2012+A1:2018 – Alarm systems – Alarm transmission systems and equipment – Part 1: General requirements for alarm transmission systems.

ETSI – European Telecommunications Standards Institute – Cyber Security for Consumer Internet of Things.

Fire (Scotland) Act 2005.

Fire & Rescue Services (Northern Ireland) Order 2006 & The Fire Safety Regulation (Northern Ireland) 2010.

ISO/IEC 27000 (series), Information technology – Security techniques – Information security management systems – Overview and vocabulary.

NCSC – National Cyber Security Centre – MCSS Minimum Cyber Security Standards.

NISTIR 8259 – Foundational Cybersecurity Activities for IoT Device Manufacturers.

PAS 555 – Cyber Security Risk – Governance & Management.

PAS 79-1 Fire risk assessment – Part 1: Premises other than housing – Code of practice.

Regulatory Reform (Fire Safety) Order RRFSO 2005.

SOC 2 TYPE 2 – Systems & Organizational controls. Type 2 assess controls.

UL 2900 – Series of Standards for Cybersecurity assurance program.

DISCLAIMER

The information set out in this document is believed to be correct in the light of information currently available but it is not guaranteed and neither the Fire Industry Association nor its officers can accept any responsibility in respect of the contents or any events arising from use of the information contained within this document.



Fire Industry Association

Tudor House, Kingsway Business Park, Oldfield Road, Hampton, Middlesex TW12 2HD

Tel: +44 (0)20 3166 5002 • www.fia.uk.com