

**Guidance
note**



Fire Industry Association

Leading Excellence in Fire Since 1916

**Guidance on IP connectivity and
remote services**

Contents

1. Introduction	3
2. Background	3
3. IP Connectivity	3
4. Remote Services	4
5. Relevant Guidance	5
6. Reference Documents	6
7. Implications.....	7
8. Appendix 1– Agreement and responsibilities of parties as defined in BS EN 50710:2021 section 4.2	8
Appendix 2 – BS EN 50710 Section 4.3.2 Security requirements of the Remote Access infrastructure (RAI)	9

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.

1. Introduction

This FIA guidance document is intended to support the Installers, Specifiers and Fire Engineers in identifying what is to be considered when providing remote connectivity using IP connections for signaling and for remote services.

Caution - The opportunity new technologies offer for provision of remote services can deliver some desirable benefits. However, it is important to note that all relevant, existing standards and codes of practice remain in place and should be followed. In particular, service providers should follow the recommendations of BS 5839-1 noting that the need for in-person visual inspection cannot be replaced by a remote connection¹.

2. Background

Historically, fire detection and fire alarm systems have been standalone with only periodic interaction during weekly tests or when there is a false/unwanted alarm, or a fault indicated on the panel. Remote connection was typically via alarm routing equipment to the Alarm Receiving Centre (ARC), and the information reported restricted to the notification of a fire or fault signal having been generated somewhere in the premises.

Recent developments in communications technology have resulted in the potential for the panel to transmit details of the origin of the fire or fault signal where such knowledge could improve the response time for an engineer to attend and resolve any issue.

Further opportunities for users to have real time visibility of the status of control equipment remotely via web applications or Mobile Apps and for system maintainers to interrogate systems and perform permitted operations remotely via the same connection.

Remote data connections today will commonly involve internet connectivity either by wireless, cellular or a hard-wired internet access point.

3. IP Connectivity

Internet Protocol is the normal method of connecting and communicating with many building systems. Fire safety systems are no exception. The range of options for connectivity means that a cost-effective solution is available for almost all systems both current and legacy. There is a general, growing expectation that the functionality and ease of use associated with connected systems is made available for fire safety systems and a number of commercial offerings are available in the UK fire industry offered by manufacturers and third parties. At the same time there are concerns that end users and service providers take the correct measures to ensure the integrity of the system is protected from malicious and accidental interference associated with remote connection. This includes adherence to clause 43.4 of BS 5839-1:2025.

¹ The 2025 release of BS 5839-1 recommends that visual inspection of devices should include verifying the correct operation of the LED indicator

4. Remote Services

The note to clause 43.4.2 of BS 5839-1:2025 refers to BS EN 50710:2021 which defines **any service provided for a client of a Fire Safety and/or security system (FSSS) carried out via a remote connection**. With current technology it is feasible to access a range of system functions and data remotely. These capabilities can be used to improve the effectiveness of the system and the services provided to end users as well as introducing efficiencies in the way service providers deliver their services.

It is important to understand what is permissible and the precautions that should be taken to ensure the operation of the fire safety system is not compromised, risking the safety of buildings and occupants.

Subject to suitable contractual arrangement being in place (see section 7) the range of services that may be provided remotely include:

- Read Only:
 - Monitoring and logging of non-alarm events such as faults, disablements
 - Monitoring of alarm events for informing response of the end user (not alarm routing to an ARC – nor routing of signals to sound the evacuation locally)
 - Provision of data to improve the effectiveness of the system (e.g. supporting investigation of unwanted alarms, monitoring device contamination, report on PSE/battery status)

Read only access may be made available to end users as well as service providers to improve the way the system is managed on a daily basis.

- Control of the live system
 - Enablement and disabling of part of the system
 - Reset of alarms
- Remote Services provided by a qualified service provider
 - Fault finding and troubleshooting
 - Testing of functionality of different elements of the system.
 - Re-programming of the system
 - Device sensitivity
 - Cause and effect

In all cases of remote services, it is imperative that an appropriate contract is in place (see appendix 1) and that sufficient control of access to view the systems and data is in place. It shall employ Cyber secure measures to prevent unauthorised access or hacking of systems that can lead to compromised safety of buildings and occupants as well as potential breach of regulations relating to protection of data (see Appendix 2).

If remote control or testing of the system is provided, the service provider and end user must also ensure that compliance with existing standards and regulations is maintained such as visual inspection as recommended by BS 5839-1. Any risks associated with remote access must be identified and mitigations in place so that there is no reduction in effectiveness and safety to buildings and occupants.

Remote services do not replace the recommendations for periodic inspection of fire detection and alarm systems set out in BS 5839-1.

5. Relevant Guidance

Euralarm Guidance on Remote Services – November 2022

The guidance provides an explanation of the main elements of Remote Access Infrastructure, and checklists that help service companies to make a self-assessment of their readiness and compliance with the provisions laid down in EN 50710, EN 16763 and CLC/TS 50136-10.

Readers may find it useful to refer to the guidance alongside this document. Follow the link below to view or download from the Euralarm website:

<https://www.euralarm.org/resource/guidance-on-remote-services---final-xlsx.html>

6. Reference Documents

Below are listed the documents that are most likely to be considered in the context of remote connectivity:

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

Note - It is important to understand that this does not override the requirements set out in other documents that govern Fire Detection and Fire Alarm systems e.g. BS 5839-1.

- BS 5839-1 Fire detection and fire alarm systems for buildings. Code of practice for design, installation, commissioning and maintenance of systems in non-domestic premises
- BS 5839-6 Code of practice for the design, installation, commissioning and maintenance of fire detection and fire alarm systems in domestic premises
- BS 5839-8 Fire detection and fire alarm systems for buildings. Design, installation, commissioning and maintenance of voice alarm systems.
- EN 50136-1 General requirements for alarm transmission systems
- PD CLC/TS 50136-10 Alarm systems. Alarm transmission systems and equipment
- BS EN 16763 Services for fire safety systems and security systems
- EN 54-21 2006 Alarm transmission and fault warning routing equipment
- BS EN 54-2 Fire detection and fire alarm systems. Control and indicating equipment
- BS EN 54-16 Fire detection and fire alarm systems. Voice alarm control and indicating equipment
- Product Security and Telecommunications Infrastructure Act 2022 (PSTI)

FIA Guidance on Product Security and Telecommunications Infrastructure (PSTI) regulation - UK

- BS 8644-1:2022 Digital management of fire safety information. Design, construction, handover, asset management and emergency response.

7. Implications

When undertaking services remotely, the following points are recommended:

	Read Only	Diagnose	Function Test	Control
Design of Remote Services Infrastructure				
Risk Assessment	✓	✓	✓	✓
Contractual Agreement between end user and service provider of remote connection	✓	✓	✓	✓
Definition of responsibilities	✓	✓	✓	✓
Measures to protect integrity of site and personal data	✓	✓	✓	✓
Clear definition of scope of permitted actions	✓	✓	✓	✓
Access control and User management for Service provider and end User organisations	✓	✓	✓	✓
Site Specific Awareness Training	✓	✓	✓	✓
Cyber Security audit at design and regularly post installation	✓	✓	✓	✓
Procedure for regular software updates	✓	✓	✓	✓
Ensure compatibility with hardware and software	✓	✓	✓	✓
Provision of control functions only if included in contract	✓	✓	✓	✓
During Remote connection				
Provide Impact assessment ahead of performing service		✓	✓	✓
Personnel performing remote services to be familiar with the site and local regulations in force		✓	✓	✓
CIE to indicate services are in progress		✓	✓	✓
Notify end user and ARC at start and end of service intervention		✓	✓	✓
On site, in person verification of system health by competent person following intervention		✓	✓	✓
Record of user logins and activity	✓	✓	✓	✓
Provide audit trail of changes available to end user		✓	✓	✓
Periodic Testing of Remote connection as part of planned maintenance	✓	✓	✓	✓
Ensure compatibility of hardware with any software changes		✓	✓	✓
Visual Inspection in accordance with BS5839-1			✓	
Control during Remote connection				
On-site, in person verification at site shall be performed before any alarm is silenced or reset				✓
Remote Disablement of devices shall be performed only after consultation with the responsible person and must be indicated on the local CIE				✓

8. Appendix 1– Agreement and responsibilities of parties as defined in BS EN 50710:2021 section 4.2

Contractual agreements between the organization providing the remote service(s) (RSP) and the client should include identification of:

- 1) the specific FSSS and the site in which it is installed
- 2) the scope of the services provided, the operations or tests to be conducted remotely, including when and under what circumstances and the possible further actions to be conducted based on the results of the remote service
- 3) legal entity responsible for the RAS (Remote access system)
- 4) transparency as to where and how system and site data are handled and stored
- 5) the process of client authorization required for each operation and how the communication (see 4.4.2) to the client is made and evidenced
- 6) NOTE This may take the form of contractual agreement where no specific authorization process is required for certain or all operations.
- 7) use and handling of credentials
- 8) the means of maintaining an audit trail of all remote actions and the retaining period
- 9) any conditions required by the client's insurer
- 10) any conditions required by e.g. police, fire brigade etc. if applicable
- 11) the agreed time limitation(s) on active remote sessions with regards to the read, control and write functions according to the risk assessment
- 12) use and handling of automated connections/sessions and
- 13) the limit of responsibility of the Remote Service Provider.

Appendix 2 – BS EN 50710 Section 4.3.2 Security requirements of the Remote Access infrastructure (RAI)

In order to ensure the security of the communication link, the following requirements shall be applied to all remote connections established via the RAI to perform remote services carried out either at site or off-site including those performed prior to or as part of commissioning.

- The Security of the RAI shall be supported by state-of-the-art security measures such as authentication, authorization, encryption, substitution protection, event logging and traceability.
- The physical and logical connections shall be monitored securely for internet cyber security. The platform is to be audited regularly for effective protection and continuous improvement.
- Remote access to the FSSS shall only be possible via a remote access server (RAS).
- Remote access requires authorisation by secure means appropriate to the risk assessment and be at least equivalent to that required for direct access on site. This authorisation shall identify the authorised person / automation system performing the remote services.
- The remote access session shall be terminated after a defined period of inactivity.
- Information related to the sessions (login, logout, user, operations) shall be logged at the RAS with timestamps.
- The communication links between the Remote Access Client and the RAS and between the RAS and the Remote Access End-point of the FSSS shall require authentication before remote functions are executed.



Fire Industry Association
Leading Excellence in Fire Since 1916

Tudor House, Kingsway Business Park, Oldfield Road, Hampton, Middlesex TW12 2HD
Tel: +44 (0)20 3166 5002 • www.fia.uk.com