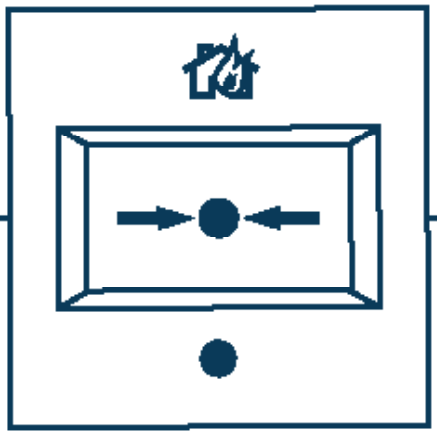
Guidance Note

Fire Industry Association



Guidance Policy on the Remote Access and Control of Fire Detection and Alarm Systems

Note that the purpose of this policy is to prevent the accidental downgrading of system functionality or effectiveness resulting from remote access.

Guidance Policy on the Remote Access and Control of Fire Detection and Alarm Systems

BACKGROUND

The subject of remote configuration/access to fire detection and alarm systems (FD&A) has been considered by the FIA on a number of occasions and a paper outlining the options available had been prepared by BFPSA in 2000. Since then, the technological advances in fire alarm control and indicating equipment (CIE) and telecommunications mean that more and more of the functionality of FD&A systems is capable of being interrogated and amended remotely from the CIE.

This FIA policy statement gives recommendations on those factors that FIA members should consider when considering requests for remote access to and management of FD&A systems.

For the purposes of the policy, remote access is defined as where the control and functions of the CIE are carried out by an engineer off-site. Providing instructions to the responsible person/s via a phone line is not considered remote access or considered appropriate by the FIA due to the potential for misunderstanding.

AGREEMENT OF PROTOCOL

It is imperative that a procedure be agreed, in writing, between the responsible person (RP) for the fire alarm systems as defined in BS 5839-1 and the service provider, as to which parties shall have remote access authority and to what level.

ACTIVITIES THAT ARE 'ALLOWED' (IE READ ONLY)

The remote access should not replace the physical on-site inspections required by BS 5839-1. Remote interrogation and diagnostic activities may, however, be fully allowed.

These should be fully controlled in an appropriate manner.

Examples of these 'read only' activities are:

- Review of fault conditions.
- Review of the sensitivity drift of sensors.
- Viewing the system logs.
- Viewing the status of devices in preparation for service visits.
- Detector condition monitoring.

All of these examples may help the service provider to assist the RP in deciding on further action to be taken. This may involve a site attendance to carry out work 'not allowed' under this policy.

ACTIVITIES THAT ARE 'PERMITTED IF NECESSARY'

These are activities that may be implemented under appropriate procedural controls and risk assessment, if site requirements dictate them necessary and are instructed in writing by the RP.

Examples of these activities are:

- Remote isolation of a zone may be permissible if a system was in fault due to water leaking in a zone.
- Urgent hot work that will require immediate action.

The procedural controls should include but are not limited to:

- Identity checks on personnel, eg passwords.
- Qualifiers defined for each action, ie a set list of questions to ask for each task.
- A disclaimer to be read each time.

Following each occurrence of a permitted task, a site visit should be scheduled to confirm the actions taken and ensure that the system is returned to a quiescent state

For the purpose of clarity, activities that are 'permitted if necessary' are site specific and agreed between the RP and the service provider for that specific site. There may not be any 'permitted if necessary' activities agreed for many sites.

EXAMPLES OF FUNCTIONS THAT ARE 'NOT ALLOWED'

The remote access should never replace the physical annual on-site inspection.

The following are examples of activities that must not be carried out remotely, unless they have been agreed in writing for a specific site under 'permitted if necessary':

- The remote testing of the detectors to the physical phenomena that they are designed to detect (ie electronically), unless provision is made to provide the actual physical phenomena automatically.
- The remote testing of auxiliary devices or control functions.
- Alteration of the performance of sounders, ie dB changes, unless a definitive method of reading audio output is available on the device on-site, and then only if agreed for that site under 'permitted if necessary'.
- Alteration of the performance of voice alarm systems,
- Anything that alters system configuration, ie cause and effect,
- Anything that alters system certification and/or the site fire risk assessment,
- Anything that alters system design, ie the removal of a device or change of detection mode.
- The permanent isolation of electrical circuits, loops, detection and alarm zones.
- The isolation of associated fire protection equipment, ie suppression systems.
- The isolation of remote monitoring connections.
- The initiating or silencing of alarms.
- The initiating or silencing of the evacuation signal.
- Re-booting of the system or part thereof.
- Software modifications.

It is noted that all of the above may be possible remotely and if the client insists then they can be done. However, neither the FIA nor its member companies should recommend them, and if they are requested by the client, the client should confirm his instructions and the acceptance of responsibility in writing.

The prime reason for advising against remote changes other than 'read only', is that without being present on-site it is not always possible to see if a remote activity has been effective or whether it has compromised any other parameters of the system.

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