Guideline
Alarm systems - Remote services
# Table of contents

Foreword ........................................................................................................................................... 2  
Introduction .................................................................................................................................. 3  
1. Scope .................................................................................................................................... 4  
2. Normative references ................................................................................................................. 4  
3. Definitions and Abbreviations .................................................................................................... 5  
    3.1. Definitions ........................................................................................................................ 5  
    3.2. Abbreviations ............................................................................................................... 7  
4. Use of remote access technology .............................................................................................. 7  
    4.1. General ........................................................................................................................ 7  
    4.2. Contractual responsibilities ........................................................................................... 7  
    4.3. Recommendations for the alarm system ....................................................................... 8  
    4.4. Recommendations for the secure computer platform ...................................................... 9  
    4.5. Recommendations for the information transmission system ........................................ 10  
    4.6. Recommendations for the operation of remote services .............................................. 12  
    4.7. Specific recommendations for use of remote services with fire & life safety alarm systems ..................................................................................................................... 12  
    4.8. Specific recommendations for use of remote services with security systems ................. 13  
5. Environmental statement ......................................................................................................... 13  
Annex A: Relationship with European standards ......................................................................... 14  
    A.1. Existing standardisation .............................................................................................. 14  
    A.2. Future standardisation ................................................................................................ 14  
ANNEX B: Summary of possible functionality of remote services .................................................. 15  
    Key: .......................................................................................................................................... 17  
Bibliography .................................................................................................................................... 18
Foreword

This document was prepared by Euralarm TG-Remote Services under the supervision of the members of the Services Section. It was approved by the SMM Services on 25th June 2013, and by the Euralarm Board on 26th June 2013.

These application guidelines were published by Euralarm on 01 July 2013. and supersede the document dated 1st October 2012.

This document is issued to supplement existing European Standards and Technical Specifications in an area not yet standardised. It is intended that interested parties use this document on a provisional basis to gain experience of its practical application as soon as possible.

This document takes the form of guidance and recommendations. It should not be quoted as if it is a formal specification and care should be taken to ensure that claims of compliance are not misleading.

Euralarm proposes to submit the core principles of this draft to the European Standardisation Bodies (CLC and CEN) for incorporation into relevant standardisation.

Any comments relevant to this will be appreciated – please contact Euralarm TG-RS via brian.harrington@euralarm.org.

<table>
<thead>
<tr>
<th>Change revision table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
</tr>
<tr>
<td>10.09.2013</td>
</tr>
</tbody>
</table>

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.

Copyright Euralarm

© 2013, Zug, Switzerland

Euralarm • Gubelstrasse 22 • CH-6301 Zug • Switzerland

T: +49 (0)89 8137 939655
E: secretariat@euralarm.org
W: www.euralarm.org
Introduction

It has been common practice for many years to monitor remotely the alarm and fault status of alarm systems installed in premises and their associated Alarm Transmission Systems from remote locations (whether directly by response authorities or by dedicated Alarm Receiving Centres). However, for more than 20 years, technology has also permitted access to those alarm (and other) systems from remote locations with a variety of available functionality. As in other areas, the trend to the use of IP technology for these services means that service providers will need to become familiar with the regulations and security concerns relevant to this technology.

The ability to access an installed system from a remote location makes it possible to enhance the service offered to a customer by an installation or maintenance service provider or by an Alarm Receiving Centre (ARC).

Note: The term “Monitoring and Alarm Receiving Centre” (MARC) is sometimes used to emphasise the additional monitoring functionality provided by such centres. For the purposes of this document, no differentiation is made, and the term “Alarm Receiving Centre” (ARC) is used throughout, as is done with existing European standards.

Whilst remote servicing and remote support cannot replace competent staff working at site, it can supplement and enhance it, to improve customer service, by the following means:

a) For the customer:

More effective support, based on improved understanding of the status and operating characteristics of the system, leading to faster response times, higher system reliability and availability, higher business continuity and less disruption from engineering staff at the supervised premises.

b) For service providers:

New and additional service opportunities, improved system interrogation ability leading to improved system and service quality and higher customer satisfaction, along with better staff utilisation.

It is, indeed, possible for end customers to be provided with remote access to certain agreed features of their systems.

Any problems with a system identified during remote access will need to be resolved – which in some cases may be possible remotely, or may require a site visit.

NOTE: The application of these points is currently more widely adopted in Security applications than for Fire & Life Safety systems. Whilst remote access can be implemented at an ARC, it is more commonly implemented by vendors or by installation and maintenance service providers.

Some countries have taken steps to regulate what (if any) functionality may be implemented remotely, and what (if any) precautions should be taken to deal with the issues that arise from doing so. This has resulted in disparate approaches to the use of this technology, thus jeopardising the benefits that could be reaped from full implementation of the European Services Directive (2006/123/EC) – including cross-border application of such technology.

These Application Guidelines therefore present recommendations for the definition and use of this technology by Euralarm members, and others who wish to take advantage of it, in order to provide experience to lead to standardisation throughout Europe.
1. Scope

These application guidelines are intended to provide advice relating to the design, installation, operation and maintenance of Fire & Life Safety and Security alarm systems to which remote access is required, along with recommendations concerning the systems used for such remote access. The guidance is equally applicable to services performed by ARCs and by installation / maintenance service providers.

These guidelines do not discuss the use of remote functionality by clients / end users, however, it is recommended that the principles contained should be applied if this is done.

These guidelines are applicable to the use of remote access to an installed and commissioned alarm system. However, certain measures (eg security of the communication link) are identified as applicable during the installation and commission stages to prevent this security being compromised.

For the purposes of these Application Guidelines, the scope of the electronic Fire & Life Safety and Security industries is considered as the combined scopes of CEN TC/72, CEN TC/191 and CENELEC TC/79, loosely coinciding with the scope of Euralarm.

The term “service” is used in this document in the same sense as in the European “Services Directive” and should not be confused with “maintenance.”

This document draws from existing standards where relevant to the use of this technology and makes recommendations for consideration in potential future standardisation.

An informative annex (Annex A) is provided to summarize the extent to which these guidelines impact on European standardisation. A further Annex (Annex B) summarises the functionality that is already, or is likely to become available for remote use.

The use of similar tools at the alarm system site is outside the scope of this document, but may draw on the principles established. In the case of Intruder & Hold-up alarm systems, Annex C of EN50131-3 is applicable in this case.

2. Normative references

The following European Standards and Technical Specifications are referred to within this document and will be found beneficial in following the Guidelines. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- EN 54-2 Fire detection and fire alarm systems. Part 2: Control and indicating equipment
- EN 54-21 Fire detection and fire alarm systems. Part 21: Alarm transmission and fault warning routing equipment
- ISO/IEC 2700X series Information technology - Security techniques - Information security management systems
- EN 50131-1 Alarm systems – Intrusion and hold-up systems - Part 1: System requirements
- EN 50131-3 Alarm systems – Intrusion and hold-up systems – Part 3: Control and indicating equipment
- EN 50136 series Alarm Systems – Alarm transmission systems
- CLC/TS 50398 Alarm systems - Combined and integrated alarm systems - General requirements
- EN 50518 series Monitoring and alarm receiving centres
3. Definitions and Abbreviations

For the purposes of this document, the following terms and definitions apply;

3.1. Definitions

3.1.1. Authentication

Exchange of a code (or codes) to identify that a supervised premises transceiver (SPT) has not been substituted by similar equipment without this code, or that the information message has not been modified.

[prEN50136-1]

3.1.2. Authorisation

Permission to gain access to the various control functions of a Fire & Life Safety or Security system.

[EN 50131-1]

3.1.3. Client

Individual or corporate body responsible for the alarm system. [TS50131-7]

3.1.4. Connection

Communication link between remote location and alarm system used for remote access.

3.1.5. Fault

Condition detected within an alarm system that prevents the system or part(s) thereof from functioning normally.

Note: Alarm system standards define a range of faults applicable to the relevant type of system.

3.1.6. Information transmission system

Equipment and network used to transfer information between one or more alarm systems and one or more alarm remote locations for diagnostic purposes.

NOTE 1: This may share equipment and network with an alarm transmission system.

NOTE 2: Information transmission systems exclude local direct connections, i.e. interconnections between parts of an alarm system which do not require an interface to transform the alarm system information into a form suitable for transmission.

3.1.7. Operating personnel

Trained technician(s) conducting any form of remote service.

NOTE: These technicians may be ARC operators.

3.1.8. Remote access

Access to installed system at site carried out from a remote location to perform remote servicing, remote support or other activities.

3.1.9. Remote application

Software application running on a secure computer platform permitting remote access to one or more installed alarm systems, remote service functions or both.

NOTE: There may be more than one separate application to carry out all aspects of this functionality.
3.1.10. Remote location

Location from which remote services are carried out or processed.

NOTE: This may not be the same location as that of the secure computer platform.

3.1.11. Remote service

Any service for the client of an alarm system, carried out from a remote location.

NOTE: This may take the form of system checks or other support services.

3.1.12. Remote support

Actions other than contracted remote system checks performed from a remote location. (EXAMPLE: parameter / configuration change to meet customer requirement, view event log, access diagnostic features).

3.1.13. Remote system checks

Aspects of preventative maintenance, restricted to operations that can be performed electronically from a remote location.

3.1.14. Response authority

Designated authority with responsibility for attending the supervised premises following an alarm and taking the appropriate action (EXAMPLE: police force, fire brigade).

[TS50131-7]

3.1.15. Secure computer platform

Computer platform at a secure location running the remote application used for remote access to an installed system, not accessible without applying security measures so that unauthorised persons cannot gain access by normal means.

NOTE: This may be at the premises of the maintenance company or ARC, or at a third-party secure location.

3.1.16. Set

Status of an I&HAS or part thereof in which an intruder and/or hold-up alarm condition can be notified.

[EN50131-1]

3.1.17. Supervised premises transceiver

Equipment at the alarm system site, including the interface to the alarm system and the interface to the alarm transmission or information transmission networks.

3.1.18. Write function

Operation including the transfer of information to the alarm system at site (EXAMPLE: parameter change, test command, etc.).
3.2. Abbreviations

ARC            Alarm receiving centre
ATS            Alarm Transmission System
CEN / CLC      Standardisation bodies responsible for standardisation in this area
CIE            Control and Indicating Equipment
FDAS           Fire detection and fire alarm system
I&HAS          Intrusion and holdup alarm system
ISTS           Information transmission system
SPT            Supervised Premises Transceiver

4. Use of remote access technology

4.1. General

Implementation of the possible uses of remote communication technology should be governed by assessment of the level of risk. That is to say the operations permitted and the protection measures selected should be expected to vary between Fire & Life Safety and Security systems, as well as between systems designed to comply with the different security grades of I&HAS – or even between otherwise similar systems at different sites. In some cases, the level of risk may require that certain remote functionality should not be permitted or that certain security / safety measures become mandatory.

The assessment of risk should take into account any applicable local regulations.

System design features specified to meet the assessed level of risk should be included in the system documentation.

The equipment and systems installed for the purposes of remote services (the ITS) should themselves be the subject of rigorous testing, both prior to commissioning and as part of preventative maintenance.

Those responsible for the design planning, installation planning, installation, commissioning, operation and maintenance of alarm systems should also be conversant with European Standards and Technical Specifications relating to such systems (particularly those relating to system performance), Alarm Transmission Systems and Information & Communications Technologies.

NOTE: The summary of possible functionality included as Annex B should be considered as part of a risk assessment.

4.2. Contractual responsibilities

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

i) the specific alarm system involved

ii) the legal entity responsible for the remote location(s) from where the remote service(s) will be provided.

   NOTE: Where the connection crosses a national border, agreement should be reached on language(s) to be used.

iii) the operations or tests that may be conducted remotely, including when and under what circumstances

iv) the minimum frequency of site preventative maintenance relative to remote system checks

v) any operations or tests to be carried out automatically, whether under the control of CIE at site or of the remote secure computer platform
vi) the process of client authorisation required for each operation

   NOTE: This may take the form of contractual agreement that no specific authorisation process is required for certain or all operations

vii) the means of maintaining an audit trail of all remote actions (refer 4.4.4)

viii) how collected data will be handled and stored

ix) the specific technology security measures to be implemented

x) any special conditions required by the client’s insurer

xi) any special conditions required by the relevant response authority

xii) agreed time limitation(s) on active remote connection (refer 4.5.4)

The list of functionality at Annex B should be considered when defining contractual responsibilities.

4.3. Recommendations for the alarm system

4.3.1. General

These recommendations are additional to those shown in relevant system standards, application guidelines, etc.

Siting and protection of any additional equipment required to permit remote access should be equivalent to the SPT for the associated ATS.

The use of remote services should not be considered as a total replacement for site maintenance. Certain checks can be made only at site, hence regular visits to site are essential – the frequency of which should be determined contractually (4.2 iv) except where defined by local regulations, etc.

4.3.2. Indications

It is recommended that an indication should be available at site when a remote connection has been authenticated, and until it has been disconnected.

NOTE: This is not a requirement of current European standards.

4.3.3. Event logging (I&HAS only)

It is recommended that the CIE event log should identify each occasion that a remote connection is made, including time, date, and whether configuration / parameter changes were made.

NOTE: Identification of a remote connection is not currently a requirement of relevant standards, so this may not be available in all equipment (see EN50131-1, EN50131-3).

Commensurate with the level of risk (4.1), consideration should be given to including all parameter change information in the CIE log (see also 4.4.4) and to generating an activity report (including source of changes) to the ARC and remote location.

The event log should be retained as required by EN50131-1.

4.3.4. Test functionality

Activation of alarm system outputs from a remote location should be kept to a minimum.

In certain specific situations, a responsible person should be present at the site when such testing is carried out; examples of such situations include:

  i) where fire suppression / extinguishing systems are activated automatically by the alarm system

  ii) where automatic triggering of external equipment such as air conditioning systems, elevators, key safes, etc. takes place.
4.3.5. Privacy issues

Where equipment capable of transmitting sound or visual images from site is installed, care should be taken to ensure that this is possible only under specific conditions, to prevent breaches of privacy legislation (EXAMPLE: as a result of an alarm, during controlled test conditions).

NOTE: where practicable, this should be controlled by the alarm system firmware.

4.3.6. Combined and Integrated Systems

Where various systems at the same site are combined or integrated, the recommendations of CLC/TS50398 should be implemented. Remote access may be restricted to certain of the combined or integrated systems only.

NOTE: Integration may take place through equipment installed at site, or at a different location.

4.4. Recommendations for the secure computer platform

4.4.1. General

Equipment should be sited such that unauthorised persons cannot view displayed information.

Note: The secure computer platform and associated application may be located in part of the premises of an installation or maintenance service provider, of an ARC or of a suitably contracted third party.

4.4.2. Management of the secure computer platform

The remote location should be managed to ensure that only authorized personnel are permitted access to the secure computer platform and the remote application running on it. In particular, codes to authorise access to the secure computer platform / remote application should be unique to each authorised user, changed routinely and authorisation removed promptly from personnel leaving employment.

The remote operations permitted to be performed by each authorised user and the sites they are permitted to access should be restricted according to the needs of their role and to their training, using levels of access reflecting those specified in the standards relevant to the alarm system. Access to the software application controlling remote services should not be left open when the computer terminal used for access is left unattended.

Corresponding procedures should be in place to manage the use of remote services from a location other than that of the secure computer platform (EXAMPLE: access by “on-call” maintenance technician).

NOTE: Further recommendations are contained in the ISO/IEC 2700x series of standards.

4.4.3. Operating personnel

Personnel operating the secure computer platform, including those operating via a secure link from a remote location, should be properly trained on the use of the application.

Personnel authorised to carry out write functions should have competence specific to the equipment installed at site and equivalent to that of personnel who would carry out equivalent operations at site.

Competence should be demonstrated by a suitable training scheme.

NOTE: Whilst it is desirable that this should be by a certification scheme based upon European standards, appropriate national or manufacturers’ schemes may be used until such becomes available.

4.4.4. Audit trail

A record should be maintained of:

i) all remote services performed, including date, time, duration, authorised personnel involved and a normal maintenance report of all actions performed;

ii) any configuration / parameter change (EXAMPLE: temporary isolation of part of the alarm system), including reasons. Consideration should be given to this information being stored additionally at the alarm system CIE (4.3.3);
iii) the person authorising any change, where this is contractually agreed (4.2 (vi)).

As far as is practical, this audit trail should be maintained automatically by the secure computer platform / application. Where this is not possible, it may be preserved in any appropriate format.

The audit trail should be retained for a minimum of two years.

NOTE: This period is derived from EN50518-2 clause 9.

4.5. Recommendations for the information transmission system

4.5.1. General

The recommendations for the ITS should be applied to all remote services – including those performed prior to or as part of commissioning, in order to ensure the security of the communication link.

4.5.2. ITS Performance

The ITS should meet performance and security characteristics equivalent to, or better than, those of the ATS associated with the alarm system.

NOTE: This is currently an equivalent requirement of EN50136-1 applicable only if changes are made to ATS parameters. As these are often inseparable from Alarm system parameters in the context of remote connection, it is recommended that this be specified for the ITS as a whole.

4.5.3. Initialization of connection

Where required by the assessed risk or by local regulations, a responsible person should be present at site before a remote connection is made.

A connection between the alarm system and the secure computer platform should be initiated by one of the following methods, selected as appropriate to the assessed risk (4.1):

i) Automatic, from site:

The alarm system initiates the connection, either in response to a system event or at a pre-programmed time for scheduled checks.

ii) Automatic, from remote location:

The secure computer platform / application initiates the connection at a pre-programmed time for scheduled checks.

iii) Manual, from site:

The client or his representative, or an alarm company technician manually initiates the connection at the alarm system CIE.

iv) Manual, from remote location

Authorized personnel at the remote location manually initiate the connection via the secure computer platform. Where appropriate, this may be configured to require acceptance from a responsible person at site before the connection is made.

v) Manual, from remote location, with “ring-back”

Authorized personnel at the remote location manually initiate the connection via the secure computer platform. On receipt of the incoming call, the alarm system “drops” the connection and initiates an automatic “ring-back” call to the secure computer platform before any information is exchanged.

This procedure may also be triggered by utilising a cloud message service to request the alarm system to initiate the connection.
Commensurate with the risk (4.1), consideration should be given to the ARC being informed of a connection being made from a location other than the ARC.

NOTE 1: Different methods may be used at different times, or for different purposes, for the same alarm system. Regardless of the method used, initialization is not complete until the security measures described in 4.5.4 have been completed successfully.

NOTE 2: It is not intended that this clause should restrict future development – other methods may be developed equivalent to the above and providing comparable degrees of functionality / security.

4.5.4. Security measures

Remote access to the CIE of the alarm system should be possible only to / from a secure computer platform running the software application that makes the remote connection.

NOTE: There may be more than one secure computer platform and / or remote location associated with any given alarm system.

If control is by a device not at the same location as the secure computer platform, access to this device should require the same level of security as the secure computer platform. Connection to the secure computer platform should be by secure means including encryption, substitution protection and traceability (EXAMPLE: VPN or SSH) – see a) in Figure 1. Alternatively, the secure computer platform may be used to authorise a direct connection with equivalent security between the control device and the alarm system. In this case measures should be in place to ensure that the database for the alarm system held in the remote device is up to date (EXAMPLE: database held on secure computer platform downloaded to remote device or database uploaded from alarm system to remote device) before the connection can be used.

Access to the software remote application at the secure computer platform should require authorisation by secure means appropriate to the assessed risk (4.1) and at least equivalent to that specified by the relevant standard for use at site, or 1 million differs, whichever is greater – see b) in Figure 1. This authorisation should identify the individual performing the remote services.

The communication link between the secure computer platform and the CIE of the alarm system requires authentication by a successful exchange of secure codes of at least 1 million differs, before data is exchanged – see c) in Figure 1. These codes should be generated non-sequentially and be unique within each secure computer platform.

![Fig 1: Information transmission system - security measures](image)

NOTE: The remote location may be the same location as the secure computer platform / application.

Measures should be in place to prevent an authenticated remote service connection being left “open” accidentally (EXAMPLE: time-limited connection – see 4.2 xii).
4.5.5. Alarm conditions whilst a remote service is being performed

In the event that a condition notifiable to an ARC arises whilst a remote service is being performed, the transmission to the ARC should be prioritised to comply with the transmission requirements of the relevant standard. Consideration should be given to the use of multiple signalling paths using diverse technologies to facilitate such compliance.

In such circumstances, the remote services being performed should be aborted.

4.6. Recommendations for the operation of remote services

4.6.1. General

Agreement should be obtained from the client before any write functions not authorised by 4.2 (vi) are performed, in particular agreement for any configuration / parameter changes.

4.6.2. Remotely conducted tests

When tests are carried out from a remote location, the client, ARC personnel and (where local regulations require it) response authorities should be advised of the operations to be performed. See also 4.3.4.

Remote tests should not be carried out whilst an alarm condition is present and should be aborted in the event that an alarm condition arises during the tests (see 4.5.5)

4.6.3. Configuration / parameter changes

Configuration / parameter changes should not be carried out whilst an alarm condition is present.

After configuration / parameter changes, an assessment should be made of the potential impact on the operation of the alarm system. If there is any possibility that the operation has been affected detrimentally or errors introduced into any part of the system configuration, the person responsible should ensure that the system is tested without delay. This check should be made mandatory for all changes where commensurate with risk (4.1).

In any event, a check of correct operation should be carried out as soon as practicable, and not later than the next planned maintenance visit.

Where local regulations are more stringent, these must be followed.

4.6.4. Remote system checks

Subject to compliance with local regulations or codes of practice, agreement with the client, response authorities and (if relevant) the client’s insurer, remote system checks may be carried out as an alternative to an agreed proportion of the specified site preventative maintenance visits. Where this is done, the level of checks to be carried out should be agreed in advance.

NOTE: Remote system checks may be used to supplement site preventative maintenance visits.

If remote system checks identify a fault that cannot be corrected remotely, arrangements should be made with the client for a site visit to correct this as soon as practicable.

4.6.5. Automated system checks

Where system checks for a security system are to be carried out and the results passed to the secure computer platform automatically by the alarm system CIE, the recommendations of 4.5 should be met.

The nature and timing of such tests should be agreed in advance with the client.

4.7. Specific recommendations for use of remote services with fire & life safety alarm systems

All local regulations and fire brigade policies must be adhered to.

When tests are to be carried out remotely, the recommendations of clause 4.3.4 should be applied.
Configuration / parameter changes should not be made remotely if the operation will render the system non-operational for more than 300s unless local measures for fire safety are implemented.

NOTE: This time limitation is derived from EN54-2 clauses 12.5.2 and 12.5.3.

If changes are required to be made that may cause the alarm system to be non-operational (EXAMPLE: firmware upgrade, system reconfiguration) the following recommendations should be applied:

i) local regulations for fire watching or other means of protection of the premises should be in place before the remote connection is made and remain in force until the operation is completed and checked;

ii) a check should be made of correct operation before the alarm system is returned to normal operation;

iii) consideration should be given to implementing a means of “roll back” to the previous firmware version or system configuration in the event of failure of the update.

If correcting a fault that renders the alarm system non-operational, any operations may be performed without waiting for protection measures to be implemented at site, but correct operation should be checked at site immediately.

4.8. Specific recommendations for use of remote services with security systems

Remotely setting and unseting of an I&HAS should be permitted only with the specific approval of the client.

Except as permitted by 4.6.5, write functions (including tests) should not be carried out whilst the system is “set.”

NOTE: where practicable, this should be prevented by the alarm system firmware.

For I&HAS of Security Grade 4, consideration should be given to implementing a means of “roll back” to the previous firmware version or system configuration in the event of failure of the update.

5. Environmental statement

Service providers offering services for alarm systems should consider:

i) how use of remote checks instead of or as an adjunct to preventative maintenance can reduce the number of journeys to site;

ii) how the prior use of remote diagnostic and test capabilities can be used to ensure that all necessary equipment and spares are carried to site for corrective maintenance purposes.

- thus effecting a reduction in their “carbon footprint.”
Annex A: Relationship with European standards
(Informative)

A.1. Existing standardisation

In implementing these application guidelines, it should be noted that the following factors include enhancements to existing standards, hence equipment may not be available to fully comply with all of the recommendations.

- Indications – additional to CIE standards (EN54-2, EN50131-3, etc.) - see 4.3.2

- Event log (I&HAS) – additional to CIE standards (EN50131-1, etc.) - see 4.3.3

- Consideration should be given to extending event logging requirements for remote operations to CIE for FD&FAS (EN54-2)

- Characteristics and performance of ITS – addition to scope and content of ATS standards (EN50136 series and EN54-21) - see 4.5.2

- Provision of “roll back” facility – addition to CIE standard (EN54-2, EN50131-3) - see 4.7 iii), 4.8

A.2. Future standardisation

Whilst presented as integrated application guidelines for the current purpose, eventual standardisation should take into account the varying requirements for Fire & Life Safety and Security systems, as well as segregating requirements for the alarm system, the ITS and the remote centre equipment and operating factors.
This annex summarises functions that are, or may become possible for remote services for alarm systems. This should be taken into account when risk is being assessed (See 4.1) and when contractual responsibilities are being defined (See 4.2).

Table B.1 Remote functionality possible, or likely to become possible

<table>
<thead>
<tr>
<th>Function</th>
<th>FDAS</th>
<th>I&amp;HAS</th>
<th>Video Surv</th>
<th>Audio Surv</th>
<th>Access Control</th>
<th>Inte-</th>
<th>Vehicle track</th>
<th>Social alarms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic alarm signalling</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>NOTE normally to ARC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access to pre-alarm info – INTRUSION §</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access to pre-alarm info – FIRE §</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote interrogation of:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Currentstatus</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>System event logs</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Remote servicing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Automation of aspects of remote servicing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Remote access to system diagnostics</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Power supply characteristics</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Status of inputs / outputs</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Status of Detectors</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Storage equip **</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setting parameters</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Basic system programming before</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

* ALL ITEMS RELEVANT TO THE INDIVIDUAL SYSTEMS BEING INTEGRATED. PLUS:
<table>
<thead>
<tr>
<th><strong>Function</strong></th>
<th><strong>Function Type</strong></th>
<th><strong>FDAS</strong></th>
<th><strong>I&amp;HAS</strong></th>
<th><strong>Video Surv</strong></th>
<th><strong>Audio Surv</strong></th>
<th><strong>Access Control</strong></th>
<th><strong>Integrated</strong></th>
<th><strong>Vehicle</strong></th>
<th><strong>Social alarms</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>commissioning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Changing config after commissioning†</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Adjusting parameters after commissioning†</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Detection range, etc</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>De-activate and re-activate transmission line by device or by line †</td>
<td></td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Remote access to test facilities</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Detectors</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cameras</td>
<td></td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td></td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microphones</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td></td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outputs</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning devices or other peripherals</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Powersupplies (inc batteries)</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarm transmission systems</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote control of system</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setting / unsetting</td>
<td></td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Restore (reset) following alarm</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>-</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Pan / zoom cameras</td>
<td></td>
<td>-</td>
<td>✓</td>
<td></td>
<td>-</td>
<td></td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Video smoke detection</td>
<td></td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audio challenge</td>
<td></td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td></td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice recognition</td>
<td></td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td></td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function</td>
<td>FDAS</td>
<td>I&amp;HAS</td>
<td>Video Surv</td>
<td>Audio Surv</td>
<td>Access Control</td>
<td>Integrated</td>
<td>Vehicle track</td>
<td>Social alarms</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>-------</td>
<td>------------</td>
<td>------------</td>
<td>----------------</td>
<td>-------------</td>
<td>---------------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td>Hosting (with server in ARC)</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Update / upgrade system firmware</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Time &amp; Attendance Records</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Monitoring and control of non-alarm functionality</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Optimisation of non-alarm parameters</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Fault warnings from othersystems</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

Key:

§ - pre-alarm:

Although the term is used differently in Fire and Security systems, it has been retained for familiarity, rather than invent new terms. It may be defined as follows:

In FIRE:
The period **after** an alarm condition has been generated during which action is taken to differentiate between the activation of a single device and a full alarm.

In SECURITY:
The period **prior to** the generation of an alarm condition, during which images or sounds are recorded and stored for review after an alarm condition is generated in order to determine the action to be taken.

* - The term “storage equipt” relates to equipment used for storage of visual or audio information

‡ In Security applications, the term “Changing configuration” will usually be synonymous with “adjusting parameters,” but in FDAS, the terms have different significance.

† The term “transmission line” used in FDAS is equivalent to “interconnection” in I&HAS and should not be confused with an “alarm transmission path” forming part of an ATS or ITS.
Bibliography

EN 50132 series  Alarm Systems – CCTV surveillance systems for use in security applications

EN 50133 series  Alarm Systems – Access control systems for use in security applications - General requirements for components