ZVEI | EXPLANATORY LEAFLET

ZVEI: Die Elektroindustrie

Explanatory Leaflet for the interaction of mobile devices with fire detection and fire alarm systems via IP networks

33010:2014-07

CONTENTS

1. FOREWORD

An application for remote access (in German: AFFZ) serves for the interaction of mobile devices with fire detection and fire alarm systems via untrustworthy networks, such as the Internet. In such networks, additional measures are necessary to ensure the principles of authenticity, confidentiality, and availability of the data and to ensure the unrestricted function of the fire detection and fire alarm system (FDAS). This gives rise to the need to take into account issues such as information security in relation to the area of application.

Additional risks (such as loss, theft, disclosure to unauthorized third parties) also arise from the use of mobile devices. These must be pointed out to the user and require special organisational regulations and technical measures.
This leaflet gives non-binding recommendations for the implementation of the above principles.

The application of this leaflet must take place in consideration of additional requirements also in other application scenarios. Requirements are specified, rather than concrete solutions, in order to be able to implement the security requirements in line with the latest state-of-the-art.

2. SCOPE

An AFFZ is used for the interaction between mobile devices and control and indicating equipment (CIE) via IP networks. An AFFZ is operated, for example, on a mobile smart device, laptop or other computer-assisted mobile system. The potential users of an AFFZ include operators, equipment installation, maintenance and service personnel as well as the fire service or other emergency services.

This leaflet takes into account safety aspects arising for control and indicating equipment in the context of connection to the Internet. The task of complete assessment of the information security extends beyond this guide to the manufacturer of control and indicating equipment CIE / AFFZ and other parties involved (e.g. planners and operators) with the overall system.

The use of technologies which are not within the responsibility of the manufacturer of the AFFZ can influence the availability, regardless of compliance with this leaflet.

This leaflet does not describe any requirements:

- for the availability of the IT infrastructure or the computer-assisted mobile systems. The availability must be ensured by the manufacturer and other parties involved, depending on the application area.
- for the hardware of the mobile systems mentioned in this context or their infrastructure (e.g. switches, servers) for user interfaces of the AFFZ
- for connections by service laptops to the control and indicating equipment, which use another communications channel (e.g. direct connection)

3. TERMS

3.1 Application fot the remote acces (AFFZ)

Application (programme) for a mobile device for communication with the CI.E

3.2 Authentification

Check of the information received in the course of authentification.

3.3 Authentication

Presentation of confirmation of a communications partner, that it is actually the one it is supposed to be.

3.4 Authenticity

Authenticity is the property that a communications partner is actually the one it is supposed to be. Authentic information ensures that it was created by the specified source

3.5 Control and indicating equipment (CIE)

Device in accordance with EN54-2 for the reception, evaluation, display and onward transmission of messages and information (e.g. fire alarm and fault messages).

3.6 Brute Force Attack

Method used in the field of cryptoanalysis for decryption by trial and error of all possible codes.

3.7 Denial-of-Service

Designates the non-availability of services, which occurs mostly as a result of an overload due to attacks on the basic infrastructure.

3.8 Integrity

Correctness (completeness) of data, i.e. it is complete and unchanged.

3.9 Secure Development LifeCycle (SDL)

Development cycle for trustworthy computer use unchanged.

3.10 Service application

Application (programme) for the communication of the CIE with the AFFZ. The service application provides the access point for the AFFZ to the CIE, and can also offer other services (e.g. web services).

Note: This can be integrated into the CIE. or on an independent system.

3.11 Smart device

Mobile device, typically a smartphone, tablet or similar on which the AFFZ runs.

3.12 Confidentiality

Confidentiality is the protection against unauthorised disclosure of information.

Note: Confidential data and information must be accessible only to authorised persons in the permitted way.

4. SYSTEM REQUIREMENTS

4.1 Reference to standards

This leaflet deals with the application for the interaction via IP network (AFFZ).
The AFFZ is no substitute for the obligatory display and operating elements of EN54-2, but rather a supplement. The AFFZ is not a component of the control and indicating equipment.

For further information, see Appendix A.

4.2 Access levels

The access levels of EN54-2 apply.

An authentication is required for all access levels (see 5.3.3).
This should be - personalized. The use of non-specific authentifications (e.g. person 1, access A), where users cannot be uniquely identified or share access, should be avoided. If this is not practicable, an organisational solution must ensure that users can also be identified at a later time.

Access and authorisations must be able to be withdrawn.

Restrictions within the access levels may arise with regard to the permitted functions, irrespective of the geographical location of the user.

3 interaction categories are defined:

1. Visualisation without functional action (e.g. with additional information e.g. route cards, local information)
2. Visualisation with restricted functional action (e.g. switching off)
3. Visualisation with unrestricted action (e.g. remote support) taking particular account of Appendix A

Access level in accordance with EN54-2	**Interaction category of the AFFZ**		
	1	**2**	**3**
Information from access level 1	●	●	●
Information extending beyond access level 1	●	●	●
interaction with FDAS via access level 1		●	●
Action on the centre by access level 2 operating functions		●	●
Action on the centre by access level 3 operating functions			●
Action on the centre by access level 4 operating functions (taking into account Appendix A)			●

4.3 Display and operating functions at the AFFZ

The indication at the AFFZ must be consistent with those at the CIE. The arrangement, extent and presentation do not have to correspond to those of the CIE.

The possible and allowed indication and control functions of the AFFZ must be agreed between the parties involved on the basis of usage.

The operation of additional functions via the AFFZ, which do not belong to the mandatory functions of a CIE (e.g. technical controls), are possible at any time, provided that the availability of the mandatory functions according to EN54-2 is ensured.

4.4 AFFZ - CIE connection

The AFFZ establishes a connection via a defined access point (service application) to a CIE. This connection must fulfil the requirements defined below in this chapter. The following describes ways in which the access point can be located in different networks.

4.4.1 System layout

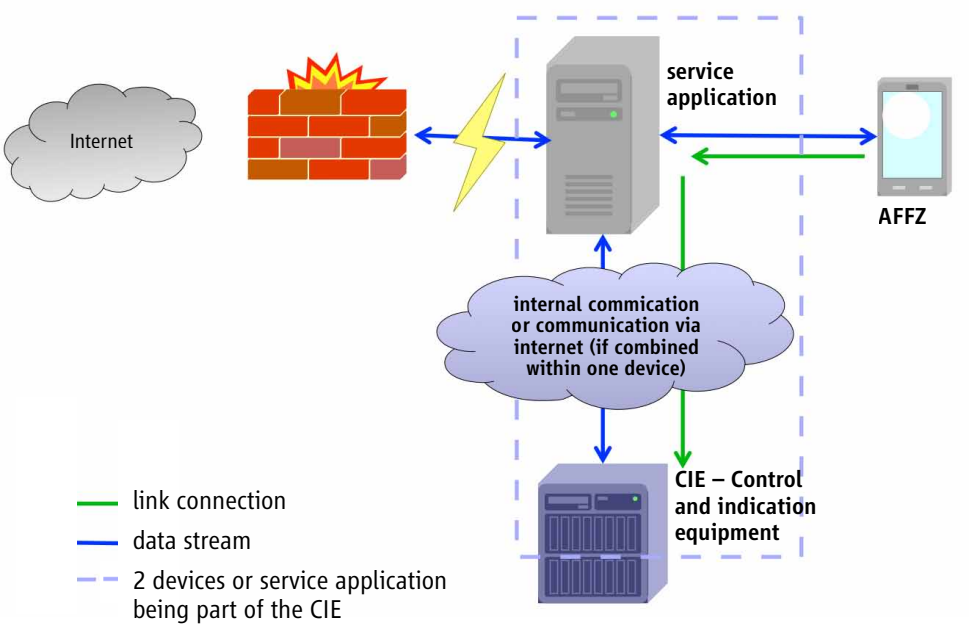
The system consists of the following system components:

- AFFZ
- Service application
- CIE application

which take part in the connection.

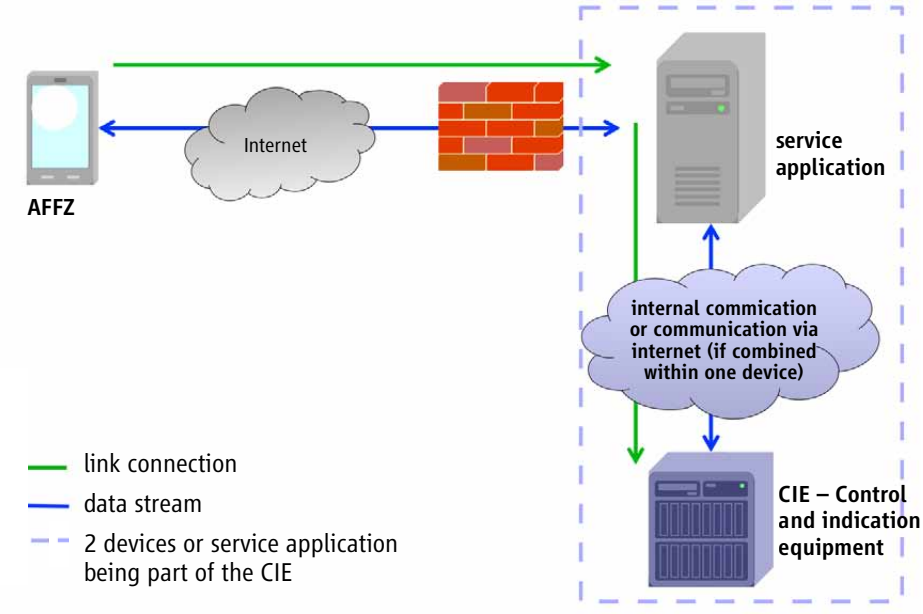
4.4.2 Direct connection in an internal network

The AFFZ and the service application are located on an internal network that is as well protected as possible against unauthorised access, e.g. corporate network, private network of fire alarm system. The AFFZ establishes a direct connection to the service application. No connection takes place via the Internet or other insecure networks.



4.4.3 Direct connection via Internet

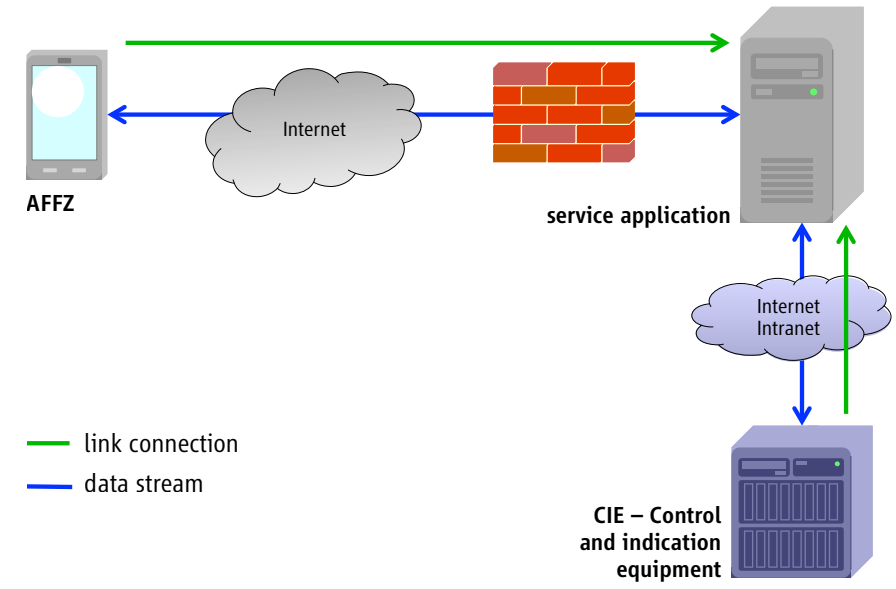
The service application is accessible directly from the Internet and integrated into the CIE or directly connected with it. Due to the possible direct availability of the CIE, this variant is exposed to greater risk of cyber attacks, and its use should be subjected to a prior risk assessment.



4.4.4 Indirect connection via Internet

The AFFZ on the smart device has a connection to a service application. The CIE also has its connection to the service application.

The CIE is in this case not accessible from the Internet.



5. REQUIREMENTS ON INFORMATION SECURITY

Since the AFFZ controls security-critical functions, high requirements must be placed on an information security concept.

In addition to technical measures, organisational measures should also be assessed by those involved by means of a risk assessment.[1]

5.1 Availability of the CIE

Functions of the AFFZ must not have any negative effects on the availability of the fire alarm system.

Suitable measures must be provided to ensure the absence of feedback from the network to the CIE. In this context, absence of feedback means that the functions required for handling the AFFZ connection have no effect on the obligatory functions of the CIE according to EN54-2.

5.2 Requirements on the development process

During the creation of the AFFZ and the service application for the access point, an SDL should be observed. This also includes subjecting the products to a fundamental technical security analysis (penetration or vulnerability tests) involving not only the testing of known weak points, but also new, unknown vulnerabilities.

In the case of security functions, the standard functions of the smart device and the relevant operating system should be used wherever possible and own implementations should be avoided. The use of security libraries is also recommended.

5.3 Requirements on the AFFZ

The security of the mobile device must be ensured for the secure use of the AFFZ.[2]

If there is no connection to the CIE, the AFFZ must not display any status information, or accept or cache operating steps relevant to the CIE.

All critical data stored on the AFFZ device must be encrypted.

An AFFZ should function on the smart device with the minimum possible rights. There should be no access for example to the address book.

[1] The contractual establishment of the following points is recommended:
- Possible and allowed indication and operating functions of the AFFZ
- Availability of the infrastructure / the IP network
- Access and usage rights

[2] The recommendations of the BSI must be taken into account.

5.3.1 Requirements on the integrity

The AFFZ must be protected against manipulation. This includes detection of manipulation of AFFZ as well as the denial of the execution of the AFFZ on an insecure smart device (for example, rooted/jailbreaked, debugger active). The solution used must correspond to the current status of the technology, and all critical data must be stored in encrypted form.

5.3.2 Registration of the AFFZ

Every mobile device which uses the AFFZ should be individually registered on the service application. The service application must offer the possibility of administration of various smart devices or assigned users, so that previously authorised devices or users can be blocked.

5.3.3 Requirements on the authenticity

Every user must authenticate himself over the AFFZ at the access point. This applies for all interaction levels.

After a defined period of inactivity, renewed authentication must be necessary

5.4 Requirements on the communication

5.4.1 Requirements on the integrity and authenticity

The integrity and authenticity of the data exchange must be ensured by a suitable procedure.

5.4.2 Encryption

Since sensitive data is being transmitted, the transmission must take place in encrypted form.
This applies for all interaction levels.

5.5 Requirements on the access point in the Internet (service application)

Due to the accessibility of the access point by the Internet. procedures for its security are necessary. The application within the access point with which the AFFZ communicates must be secured by suitable procedures

5.5.1 Web application

If an Internet application with web interface is to run on the access point, this must be secured in accordance with the latest status of the technology.

5.5.2 Login / Authentication

General Best Practices must be applied. See BSI recommendations.

5.5.3 Logging

Important operations such as connections, logins, failed logins or changes to the configuration data must be reported/documented.

5.5.4 Network services

In the area of network services, the corresponding measures for system hardening must be used, such as the switching off of unused services.
Precautions must be provided against attacks (e.g. denial of service or brute force attacks).

5.6 Documentation

Manufacturers should take the following points into account in the documentation, in order to ensure secure use by the customer.

- Target groups of an integrator or user who have to be informed for security-specific considerations about the information contained in the documentation must be defined
- Security characteristics and functions of the components
- Risks / threats which are covered by the components themselves
- Threats which arise in the course of security assessment or security management
- What measures have been taken in order to secure the product against such threats
- Services which cannot be secured (with the mechanisms integrated into the product), and therefore require supplementary technical or organisational security measures
- All interfaces and functions documented
- No back doors or concealed functions
- Recommendations with regard to configuration for secure operation
  - Adequate instructions for the change of standard passwords and for the deactivation of unneeded accounts
  - Configuration options / alternatives, with the corresponding consequences
  - Settings which are critical or which can lead to an increased risk
- Checklist for overview of the configuration and its specific security implications
  Specification of the configuration for other components of the infrastructure used (e.g. routers & switches)
- References to further information on security and secure operation

APPENDIX A
IT RECOMMENDATIONS

A.1 BSI recommendations

- BSI IT basic protection
- Secure remote access to the internal network (ISi-Fern)
- Secure provision of web services (ISi-Web-Server)
- Requirements on network-capable industrial components
- Secure passwords in Embedded Devices
- Development of secure web applications
- Secure software development under Android
- Industrial Control System Security: Top 10 threats and countermeasures

A.2 IEC 62443

International standards series on "IT security for industrial control systems – Network and system protection"

- Part 1-1: Terminology, concepts and models
- Part 2-1: Establishing an industrial automation and control system security program
- Part 3-1: Security technologies for industrial automation and control systems
- Part 3-3: Security for industrial process measurement and control network and system security

A.3 VDI Guideline 2182

Information security in industrial automation

A.4 BDEW White Paper Requirements on secure control and telecommunications systems

Basic security measures for control and telecommunications Requirements on systems for companies in the energy industry

APPENDIX B
NATIONAL APPLICATION REGULATIONS

Reference list on application guidelines. The list is not necessarily complete.

B.1 Germany
VDE 0833-1 Article 5.1.4

B.2 Netherlands
NEN 2654-1 Appendix F

B.3 Austria
ÖNORM F3000

This explanatory leaflet was produced by the members of the ad hoc APP working group of the Specialist Security Association

Claus Caspari, Bosch Sicherheitssysteme
Philip Dürringer, Bosch Sicherheitssysteme
Frank Herstix, Novar GmbH a Honeywell Company
Markus Ibba, Bosch Sicherheitssysteme
Michael Jäntsch, Siemens
Andreas Kahl, Bosch Sicherheitssysteme
Thomas Kern, Schrack Seconet
Christian Kühn, Schlentzek & Kühn
Christian Lais, Siemens
Oliver Lenz, Detectomat
Lukas Linke, ZVEI
Andreas Schneckener, Hekatron

We would like to thank the Federal Office of Security in Information Technology (BSI) for the content support and comments by Jens Wiesner.

Imprint

ZVEI Explanatory Leaflet for the interaction of mobile end-devices with fire detection and fire alarm systems via IP networks

Publisher:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
Lyoner Straße 9
60528 Frankfurt am Main

Telephone: 069 6302-245
Fax: 069 6302-1245
E-Mail: krapp@zvei.org
www.zvei.org

Responsible:
Peter Krapp
Geschäftsführer Fachverband Sicherheit
und Arge Errichter und Planer

July 2014