COMITÉ EUROPÉEN DES ASSURANCES

SECRETARIAT GENERAL
3bis, rue de la Chaussée d'Antin F 75009 Paris
Tél. : +33 1 44 83 11 73 Fax : +33 1 44 83 11 85
Web : cea.assur.org

DELEGATION A BRUXELLES
Square de Meeûs, 29 B 1000 Bruxelles
Tél. : +32 2 547 58 11 Fax : +32 2 547 58 19
Web : cea.assur.org

PROPERTY INSURANCE COMMITTEE
Prevention Specifications

Centralised Technical Management

CEA 4018: February1998 (en)

(EFSAC endorsed)

Centralised Technical Management

Part A

1. Foreword

These specifications embody CEA's considerations on the subject of Centralised Technical Management.

The basis for the specifications is the EURALARM Position Paper "Combined/Integrated Alarm Systems" identified under the number EUR (SC5) e21/95 of October 1995. This document is reproduced in part B.

The supplementary specifications are given below.

2. Supplementary specifications

2.1 General

The Insurer shall be consulted at an early stage prior to the designing of the installation of a Centralised Technical management system (combined and integrated alarm systems).

Part 6 of the EURALARM position paper is mandatory.

In regard to clause 6.2.3 of Part B, any fire detection system shall normally have priority over other property protection alarm systems.

The Insurer's confirmation of the order of priority shall be obtained on a case by case basis.

In high risk situations requiring fire and theft protection, type 1 configuration (see clause 2.3) shall be applied.

Periodic inspection shall be carried out in accordance with clause 6.3.4 of the EURALARM position paper.

2.2 All Configurations

Interconnections between applications are permitted.

In the case of interconnections only between "security systems", two-way communication (output and input) is permitted and any failure in the interconnection would not have the effect of impairing any of the systems.

Where common facilities include the display of information, the display associated with "security systems" shall always have the highest priority unless circumstances dictate otherwise. Supplementary information may be accessible on demand providing the display of any "security system" alarm signal is not adversely affected. Alternatively, the supplementary information may be displayed separately.

The transfer and processing of data shall be protected to ensure that alarms and other signals from the "security system" are not delayed, corrupted or lost.

The working of other applications, or functional parts of other applications, shall not adversely influence the functions of the "security system".

Access to the operation of non-security functions shall not allow access to a "security system" without authorisation.

All necessary corrective and preventative maintenance services shall be available for at least the first year of the life of the installation.

Periodical inspection shall be carried out at least twice a year.

A record of all preventative maintenance carried out shall be maintained in the relevant system log book.

2.3 Configuration Type 1

Type 1 configuration may include applications or the functional parts of the following applications:

- Fire detection and alarm system
- Intrusion alarm system
- Personal attack alarm system
- Closed-circuit television (CCTV)
- Access control system
- Non- security system

Indications concerned with specific functions of a "security system" shall be clearly and unambiguously associated with that system.

A failure in the common facilities shall not affect any mandatory function of the independent systems or the main functions of the "security systems" and a failure in any independent system or sub-system shall not affect the functionality of any mandatory function of the other independent systems or sub-systems.

The operation of any independent system or sub-system shall have no effect on the operation of any other independent system or sub-system. A tamper condition present in one independent system shall have no effect on the other independent systems. No failure, operation or tamper condition in a part of one of the sub-systems shall affect any other sub-system.

Each security sub-system shall have provision for signal outputs associated with the main functions of that sub-system. This provision shall be integral with the security sub-system and shall not be part of the common facilities or any other security sub-system.

2.4 Configuration Type 2

Type 2 configuration shall include applications or the functional parts of the following applications:

- Fire detection and alarm system
- Intrusion alarm system
- Personal attack alarm system
- Closed-circuit television (CCTV)
- Access control system
- Non- security system

In order to give any fire extinguishing system autonomy, the functions associated with such a system shall not be included in a Type 2 configuration.

Common facilities shall meet the most severe requirements of the sub-system or functional parts of the system.

Indication and outputs concerned with the specific functions of a "security system" shall be clearly and unambiguously linked with that system.

When a common processing unit is used, the running of the processing program shall be monitored so that a failure of a "security function" shall initiate a fault warning.

When a common power supply (main power and/or stand-by power) is used, the specification of the power supply shall be in accordance with the relevant standard for each part of the "security system" and shall also take into account the operation of the non-security systems.

The power supply to each application shall be separately and independently protected.