TECHNICAL
REPORT

ISO/IEC TR 15067-4

First edition
2001-06

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM (HES) APPLICATION MODEL

Part 4: Security system for HES

Reference number
ISO/IEC TR 15067-4:2001(E)

TECHNICAL REPORT

ISO/IEC TR 15067-4

First edition
2001-06

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM (HES) APPLICATION MODEL

Part 4: Security system for HES

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

PRICE CODE F

For price, see current catalogue

CONTENTS

INFORMATION TECHNOLOGY –
HOME ELECTRONIC SYSTEM (HES) APPLICATION MODEL

Part 4: Security system for HES

FOREWORD

1) ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

2) In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

3) Attention is drawn to the possibility that some of the elements of this Technical Report may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC and ISO technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical report of one of the following types:

- type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;
- type 2, when the subject is still under technical development or where, for any other reason, there is the future but not immediate possibility of an agreement on an International Standard;
- type 3, when the technical committee has collected data of a different kind from that which is normally published as an International Standard, for example ‘state of the art’.

Technical reports of types 1 and 2 are subject to review within three years of publication to decide whether they can be transformed into International Standards. Technical reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

ISO/IEC 15067, which is a technical report of type 3, was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

This publication has been drafted in accordance with ISO/IEC directives, Part 3.

This document is not to be regarded as an International Standard. It is proposed for provisional application so that information and experience of its use in practice may be gathered. Comments on the content of this document should be sent to IEC Central Office.

Technical Report ISO/IEC TR 15067 currently consists of four parts:

- *Part 1: Application services and protocol (under consideration)*
- *Part 2: Lighting model for HES*
- *Part 3: Model of an energy management system for HES (under consideration)*
- *Part 4: Model of a security system for HES*

INTRODUCTION

This model of a security system for residences extends the set of HES (Home Electronic System) application models. ISO/IEC JTC 1/SC 25, WG 1 has already developed and SC 25 has accepted models for lighting and energy management. These models are intended to facilitate validation of the language being specified for HES in ISO/IEC TR 15067-1: *Information technology - Home Electronic System (HES) application model – Application services and protocol*.

These models have been developed to foster interoperability among products from competing or complementary manufacturers. Product interoperability is essential when using home control standards, such as HES. This Technical Report defines a typical security system and describes the communications services needed. A high-level model for a security system using HES is presented.

INFORMATION TECHNOLOGY –
HOME ELECTRONIC SYSTEM (HES) APPLICATION MODEL

Part 4: Security system for HES

1 Scope

Residential security systems are among the most popular applications in a home automation system. This model is intended to be generic. It is applicable to a wide variety of security functions that extend well-beyond traditional intrusion detection. Potential applications of home security as represented in this model include activity monitoring, duress monitoring, and safety monitoring of personal well-being.

The intrusion and safety applications of a security system are similar for commercial buildings. This generic model can therefore be extended to commercial building security functions.

2 A typical security system

2.1 Modes of operation

A modern security system provides more than detection of unauthorized entry into a building. The range of applications of a security system spans:

2.1.1 Intrusion detection

Sensor devices are installed to detect intrusion at particular locations in a building. The sensor types are described in 2.2.1. Sensors are connected to a security controller that is programmed with various algorithms. When a sensor is armed and tripped, the controller may sound an audible alarm locally and/or may issue a notification to a remote site, for example via telephone. The activation of the controller and choice of algorithm depends on user inputs from one or more control panels (user interfaces).

2.1.2 Restricted movement sensing

Typically, this mode of operating a security system is chosen when the occupants are sleeping. Sensors at the perimeter of the house and in selected rooms are armed. Activity and movement in the bedroom will not trip the alarm. Therefore, one or more motion detectors in the bedroom and possibly some window sensors are not monitored. All other sensors are monitored as for intrusion detection.

2.1.3 Activity monitoring

This is a relatively new application of a security system. The system is specifically programmed to alert a monitoring station or place a call to a family member upon the absence of internal motion. Examples where this scheme is used include:

2.1.3.1 Elderly person monitoring

The objective is to determine if the person is moving about the house while home. The absence of motion over a period of an hour or two when the person is not expected to be sleeping might indicate that the person needs help.

2.1.3.2 Latch-key child

The term latch-key child describes a young child who returns from school to an empty house because both parents are working. The child carries a key to the house, called the latch-key. Upon returning home from school, the child enters a unique security code, different from the one the parents use. This sets the system to call a parent at work when the child enters the house. Alternatively, the system might be programmed to alert the parents if the child has not returned home on time.

2.1.4 Duress notification

2.1.4.1 Panic alarm

Many security systems provide panic switches that are wall mounted in one or more locations. If under duress or physical threat, the occupant can issue an alert through the security system by operating this switch. A special duress notification is sent to the monitoring station.

2.1.4.2 Medical alert

An adjunct to a security system might be a pendant switch worn by an ill, disabled, or elderly person. When a switch on this pendant is pressed, an alert is issued to summon medical help.

2.1.4.3 Forced disarm

A forced disarm might be a situation where the occupant is forced under threat of physical assault to enter the house with an aggressor and warned not to trip the security system. Some security systems offer a method of disarming a security system and simultaneously indicating silently that this action was done under force. A special disarm code is entered into the security control panel.

2.1.5 Safety monitoring

2.1.5.1 Fire

Among the system sensors might be smoke and heat detectors to monitor for fire. Whether a safety system and security system are embodied in one network may depend on local fire codes. Such codes may differ between residential and commercial buildings.

2.1.5.2 Environmental pollutants

Monitors for environmental pollutants may be installed in heavily-insulated buildings or as part of a safety system when using gas for heating or cooking. The security system might link to the ventilation system to clear any accumulating gases, such as carbon dioxide, carbon monoxide, or oxides of nitrogen.

2.1.5.3 Water leaks

This may include pipe breaks, seepage, or building sprinkler activation.

2.1.5.4 Over or under temperature

This may be offered in climates with extreme temperatures or in commercial establishments selling or manufacturing perishable products.

2.1.5.5 Earthquake

2.1.5.6 Machinery failure

2.2 Components of a security system

In early-developed security systems, many sensors were wired in a series loop from the controller. The sensors were normally closed. Each series loop is called a zone. If any one sensor in a series loop opened, the controller issued an alarm and possibly indicated which zone had a tripped sensor. However, it was not possible to determine which sensor in the loop tripped.

The most recent systems wire each sensor individually to the controller. Alternatively, some sensors may share a bus that allows individual communications to each sensor. Nevertheless, the term *zone* is still used, but now refers to a logical grouping of sensors that are armed or disarmed as a unit. However, it is now possible to determine which sensor in a zone tripped. Also, each sensor in a zone may be accessed for diagnostic purposes.

In a home automation environment, the security system might provide information to other home systems. For example, a lighting system or heating/cooling system might query the security controller about room occupancy. The controller would determine occupancy from sensor inputs. Also, the controller might adjust various sensor sensitivities appropriately for each system task. Therefore, the concept of disabling a zone logically for security purposes should not physically disable the sensor for other applications.

Some security controllers have sufficient capacity to serve multiple independent security systems. Applications might include apartments or offices in a building. Also, a section of a house, such as an in-law apartment or a home office, might be programmed with separate algorithms. Each independent subsystem is called a *partition*.

Following are the physical elements of a generic security system:

2.2.1 Sensors

- Contact sensor: a switch trips if a door or window is opened. A contact sensor may be placed below a mat so that it is tripped by someone walking across the mat.
- Acoustic sensor (also called a shock sensor): a sensor attached to a window is tripped by the sound of breaking glass.
- Glass break sensor: a conductive foil used commercially near the edge of a glass pane. If the glass break cuts the foil, a current flow is interrupted indicating a problem to the controller.
- Motion detector: an infrared device detects temperature changes caused by a person passing across a cone-shaped field in front of the detector.
- Pick-up coil: an electrical coil buried in a driveway detects large metal objects passing, specifically a car.
- Photo-electric cell: a photocell detects the interruption of light (visible or infrared) from a source. The photocell is installed at a position where a passing person would interrupt the light.
- Smoke detectors: the common varieties are photo-electric cells, to detect smoke particles, and ionization, to detect smoke.
- Heat detectors: these sensors trip upon a pre-wired or programmed rise in temperature.
- Water detector: usually placed on the floor to sense flooding.
- Various gas detectors: these sensors may monitor CO, CO2, or NOX.

Some of the sensors listed may be offered with various levels of complexity. For example, there are now “dual-tech” sensors. Conventional passive infrared sensors can only sense movement tangential to the detector. These sensors rely on focusing infrared radiation from the body by means of a number of Fresnel lenses onto a pyrolytic detector. They therefore detect movement of the heat source into and out of a number of zones, each of which extends from the detector head out into the protected space.

By contrast, devices using Doppler-shift techniques detect motion towards and away from the detector. Such devices may be based on ultra-sonic sound or on microwave radar. Combining passive infrared and, say microwave, Doppler techniques in a single device and processing the resulting signals provides a good way of improving the discrimination of sensors.

Some sensors may be programmable to adjust for various application requirements. For example, there may be different sensitivity levels and timing characteristics according to the application. Although some of this processing could be done by the controller, the low cost of electronics frequently permits a considerable degree of signal processing to be done within the sensor.

2.2.2 Control panels

- Wall-mounted keypad

  Typically, this is a numeric key-pad. Additional keys may be provided for special functions. Among these functions are:

  - Enabling or disabling sensors in a particular zone.
  - Selecting the operating mode of the system

  Some panels include separate keys for each function. Others require a special sequence of function and numeric keys. The keying procedure affects user convenience and product cost. This technical report makes no value-judgement on these market issues.

- Portable remote control device

  This may be a wearable device for issuing emergency calls by pressing one key.

- Keypad with voice response

  Confirmation of user selection at a keypad may be done by a tone, a sequence of tones, or a spoken voice drawn from a synthesized or pre-recorded vocabulary.

- Computer keyboard

  A few security systems can now be programmed from a personal computer (PC). The system configuration may be entered at the PC and down-loaded into the security controller.

- Another controller

  It is possible to program another home automation subsystem controller to set operating parameters in the security system. This mode has not been implemented in systems for sale.

2.2.3 Security system controller

The controller is responsible for:

- Configuring the sensors into zones and partitions
- Communicating with the user via the control panels
- Establishing an operating mode for each partition
- Monitoring the sensors
- Issuing the appropriate notification or alarms
- Establishing a telephone or radio link to a monitoring station
- Monitoring sensor and system integrity
- Miscellaneous network management and testing
- Communicating with other home automation controllers

- Varieties of controllers include:
- Specialized computer with embedded microcode
- Personal computer

  The PC must be kept running all the time to monitor the security sensors and issue alerts according the security mode selected.
- Fully distributed controller

  It is possible, though not common, to distribute the functions of a controller among the other elements of security system (sensors, control panels, and alarms). In this case, the controller is a virtual function, not a physical component. The physical model in this document is based on the usual practice of designing a physical controller for a security system.

2.2.4 Alarms

- A siren or bells
- A telephone or radio call to a monitoring service or to a specified list of persons
- Types of alarms:
  - Intrusion
  - Notification about elderly or latch-key child
  - Medical emergency
  - Panic alarm
  - Forced disarm
  - Fire
  - Gas detection
  - Water leak
  - Temperature extreme
  - Earthquake
  - Machinery failure
  - System trouble

3 The HES security system model

3.1 Physical model

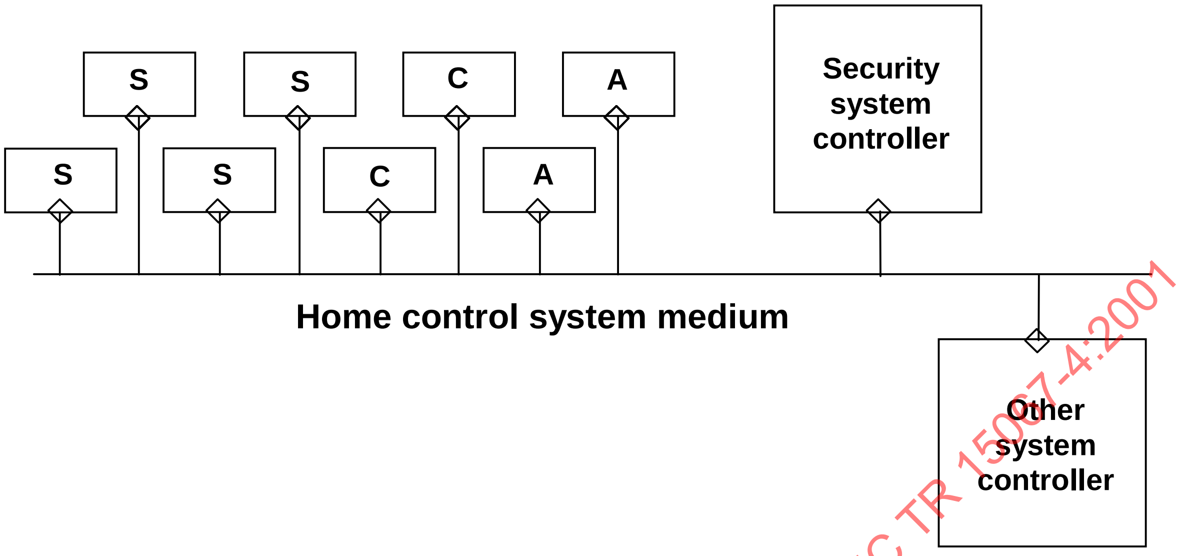
The physical elements of the HES security system model are shown in Figure 1. The components have been described in clause 2. A key decision for manufacturers is whether the HES network forms the basis for linking together the security components. Choices include:

3.1.1 Fully HES compatible

Every sensor, every alarm, and the controller contain an HES interface.

3.1.2 Partial HES compatible

A group of sensors or alarms shares a network concentrator. The concentrator includes the HES interface. The concentrators and the controller comprise the HES network.



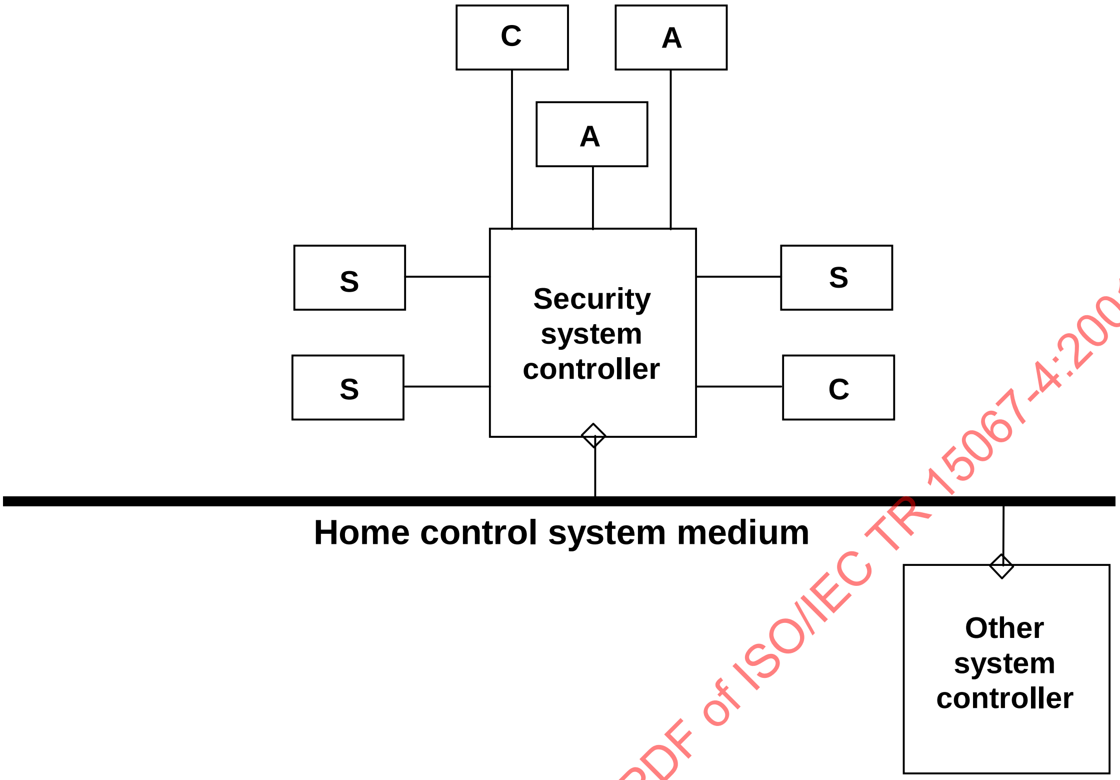
Components

A	alarm, telephone, radio
C	control panel
S	sensor
◊	HES interface

Figure 1 – Physical HES security system model

3.1.3 Isolated network

Only the security controller contains an HES interface. The sensors link to the controller via a proprietary network. The communications network interconnecting most security system components sold now is proprietary. Security manufacturers are concerned that connections to other systems via a common network will degrade reliability. Most security systems are designed as isolated networks because of concerns for system integrity. Thus, Figure 2 is a physical model according to current practice.



Components	
A	alarm, telephone, radio
C	control panel
S	sensor
◊	HES interface

Figure 2 – Physical HES security system model with isolated components

In fact, an HES security network could be isolated from all other networks via appropriate choices of private messages or physical routers that isolate subnetworks, each of which uses HES. The security controller may be on a separate bus joined to other home automation subsystems via a router. The router is interposed to provide electrical isolation for an auxiliary power source, such as a battery, supplying part or all of the security system if the mains fail.

Power isolation might be limited to critical portions of the security systems. It may not be economical to maintain all sensors active during a power failure. For example, a system might offer both volumetric protection (usually via motion detectors) and peripheral protection (with contact, acoustic, and pick-up coil sensors). In a mains failure, only the peripheral sensors would be battery-backed to manage the cost of auxiliary power.

3.2 Logical model

The logical relationship among these components is illustrated in Figure 3. If the physical model of Figure 2 is implemented, the controller may make the attached components logically visible to the HES network, so Figure 3 still applies.

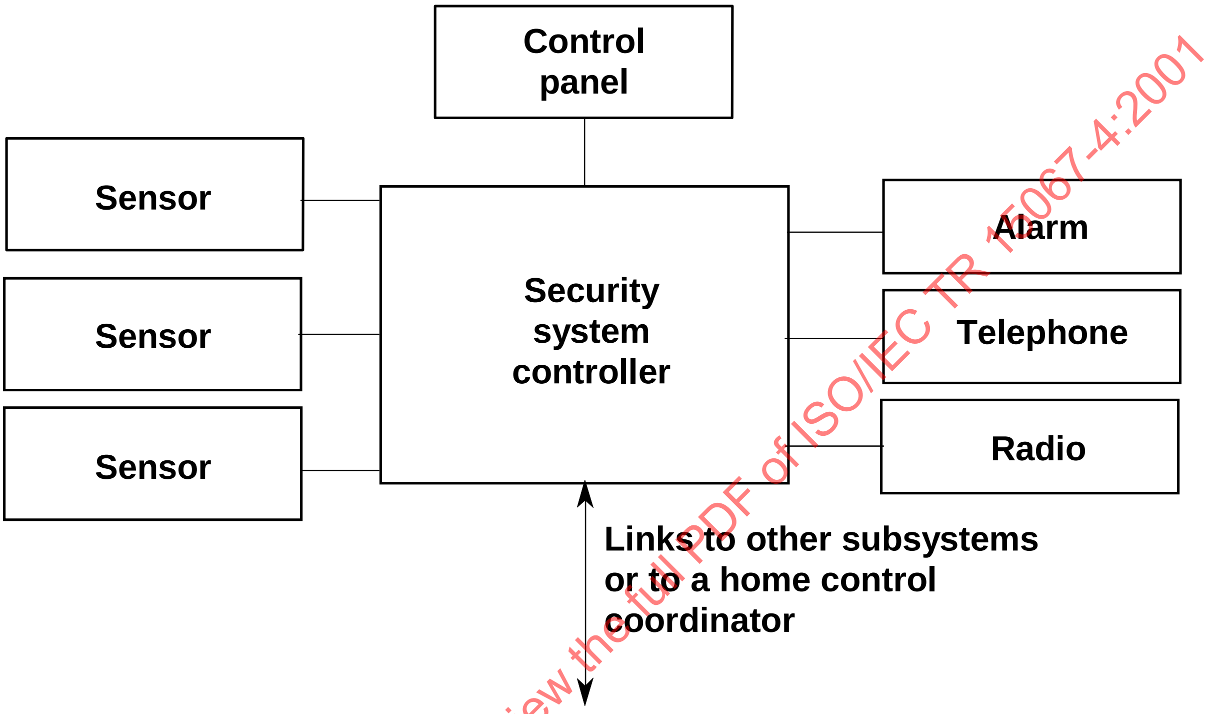

Control panel
Sensor
Sensor
Sensor
Security system controller
Alarm
Telephone
Radio
Links to other subsystems or to a home control coordinator

Figure 3 – Logical model for HES security system

The telephone connection is included because some alarms are issued by calling a pre-programmed telephone number and annunciating the alarm, or using the telephone to report a latch-key child. A radio link could substitute for, or back up the telephone. Figure 4 presents more details about the logical structure of a typical security system. Note that sensors are grouped into zones logically within the physical controller. The controller contains information about the sensors composing each zone. A zone may be in the following states:

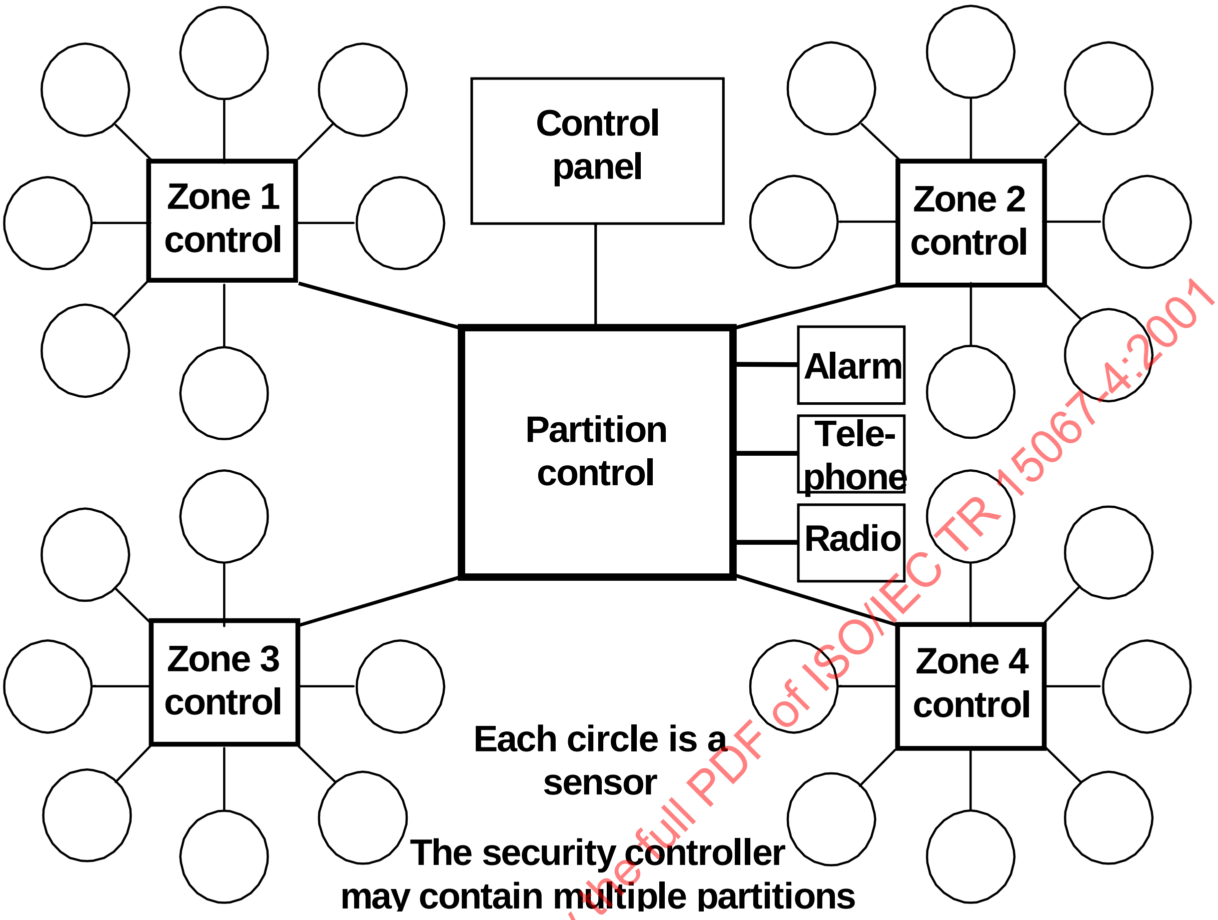


Figure 4 – Logical constituents of a security controller

- *On-line*, meaning the sensors are operating
- *Alarm*, meaning a sensor is tripped.
- *Bypass*, meaning the sensors are operating, but any sensor trips are being ignored. This applies, for example, when the occupants are at home and the system is disarmed.

As noted, zones are grouped into partitions to form logically independent security systems. The partition logic is responsible for:

- configuring the online and bypass states of each zone. The timing of zone state changes to and from bypassed is critical. For example, arming the zone that is monitoring the exit might be delayed for a specified time until the occupants leave the house after setting the security system;
- defining the operating modes listed at the beginning of clause 2;
- maintaining the security codes for arming and disarming the various system modes. Separate codes may be assigned for selected persons, such as a repair person or a guest, who may be allowed in only during certain hours on designated days;
- retaining a historical usage log to record each system event. Typically, each code entry into the security panel is recorded along with the time and location of any alarms;
- recording the system operational and maintenance status of each zone.