

ISO/IEC JTC 1/SC 25/WG 1
Interconnection of Information Technology Equipment
Home Electronic System

- Title:** Model of a Security System for HES, revision 5
- Source:** ISO/IEC JTC 1/SC 25/WG 1
- Project:** Working Group 1, 25.01.04.02-04
- Requested Action:** Forwarded to JTC 1 for approval to be published as Technical Report Type 3
- Distribution:** SC 25/WG 1 and JTC 1
- Note:** Development of this TR is not included in the SC 25 Program of Work as presently endorsed by JTC 1. Nevertheless, at the last plenary of SC 25 the SC 25 Secretariat was instructed to progress this document based on the consideration that this work is integral to validating Project 25.01.04.02-01, *HES Application Model – Application Service and Protocol*. It complements two previous HES application models, already approved as TRs. Therefore, parallel to voting on this DTR, authorization by JTC 1 of a subdivision of the work item on HES application model is requested.

Draft Technical Report Type 3

Information technology -

**Home Electronic Systems (HES)
Application Model**

**Part 4: Model of a Security System for
HES**

TABLE OF CONTENTS

1	Scope	1
2	A Typical Security System	2
2.1	Modes of Operation.....	2
2.1.1	Intrusion detection.....	2
2.1.2	Restricted movement sensing.....	2
2.1.3	Activity monitoring	2
2.1.3.1	Elderly person monitoring	2
2.1.3.2	Latch-key child	2
2.1.4	Duress notification	2
2.1.4.1	Panic alarm	2
2.1.4.2	Medical alert	2
2.1.4.3	Forced disarm	2
2.1.5	Safety monitoring	3
2.1.5.1	Fire	3
2.1.5.2	Environmental pollutants	3
2.1.5.3	Water leaks	3
2.1.5.4	Over or under temperature	3
2.1.5.5	Earthquake	3
2.1.5.6	Machinery failure	3
2.2	Components of a Security System	4
2.2.1	Sensors	4
2.2.2	Control panels.....	5
2.2.3	Security System Controller	5
2.2.4	Alarms	6
3	The HES Security System Model	7
3.1	Physical Model.....	7
3.1.1	Fully HES compatible	7
3.1.2	Partial HES compatible.....	7
3.1.3	Isolated network	7
3.2	Logical Model.....	9
3.3	Message Flows	12
3.3.1	Sensors \leftrightarrow Zone Control	12
3.3.1.1	From sensor (according to sensor capabilities)	12
3.3.1.2	To sensor (not available with all sensors)	12
3.3.2	Zone Control \leftrightarrow Partition Control.....	12
3.3.2.1	From zone control	12
3.3.2.2	To zone control	12
3.3.3	Partition Control \rightarrow Alarm	13
3.3.4	Partition Control \leftrightarrow External	13
3.3.4.1	From partition control	13
3.3.4.2	To partition control	14

FOREWORD

ISO (the International Organization for Standardization) and the IEC (the International Electrotechnical Commission) form the specialized system for world-wide 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.

This Technical Report ISO/IEC TR 15067 was prepared by ISO/IEC JTC 1/SC 25, Interconnection of Information Technology Equipment.

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

- Part 1: Application Services and Protocol
- Part 2: Lighting Model for HES
- Part 3: Model of an Energy Management System for HES (under preparation)
- Part 4: Model of a Security System for HES (this document)

INTRODUCTION

This model of a security system for residences extends the set of HES (Home Electronic System) application models. 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 *HES Application Model – Application Services and Protocol*, WG 1 Project 25.01.04.02-01.

WG 1 has developed these models to foster interoperability among products from competing or complementary manufacturers. Product interoperability is essential when using home control standards, such as HES. This document defines a typical security system and describes the communications services needed. A high-level model for a security system using HES is presented.

1 Scope

Residential security systems are among the most popular applications included 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. Therefore, this generic model can be extended to describe commercial building security functions, as is explained.

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 Section 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, possible via telephone. The activation of the controller and choice of algorithm depends on user inputs from one or more control panels.

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 might indicate 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 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.

Most modern 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 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 cell, 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 NO_x.

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.

– 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 application 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 the previous section of this document. 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.

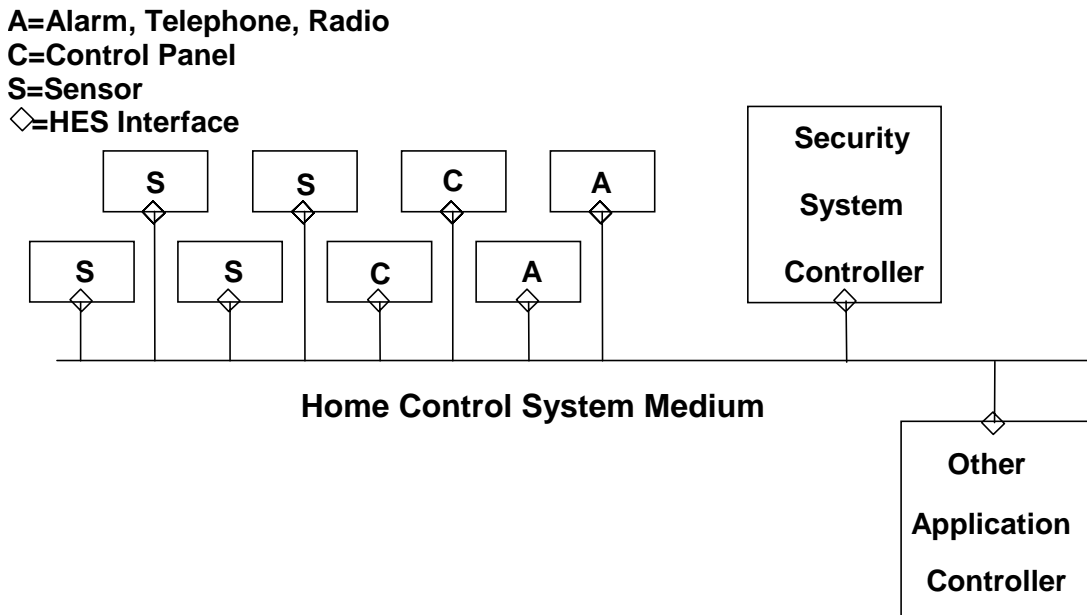


Figure 1 – Physical HES Security System Model

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.

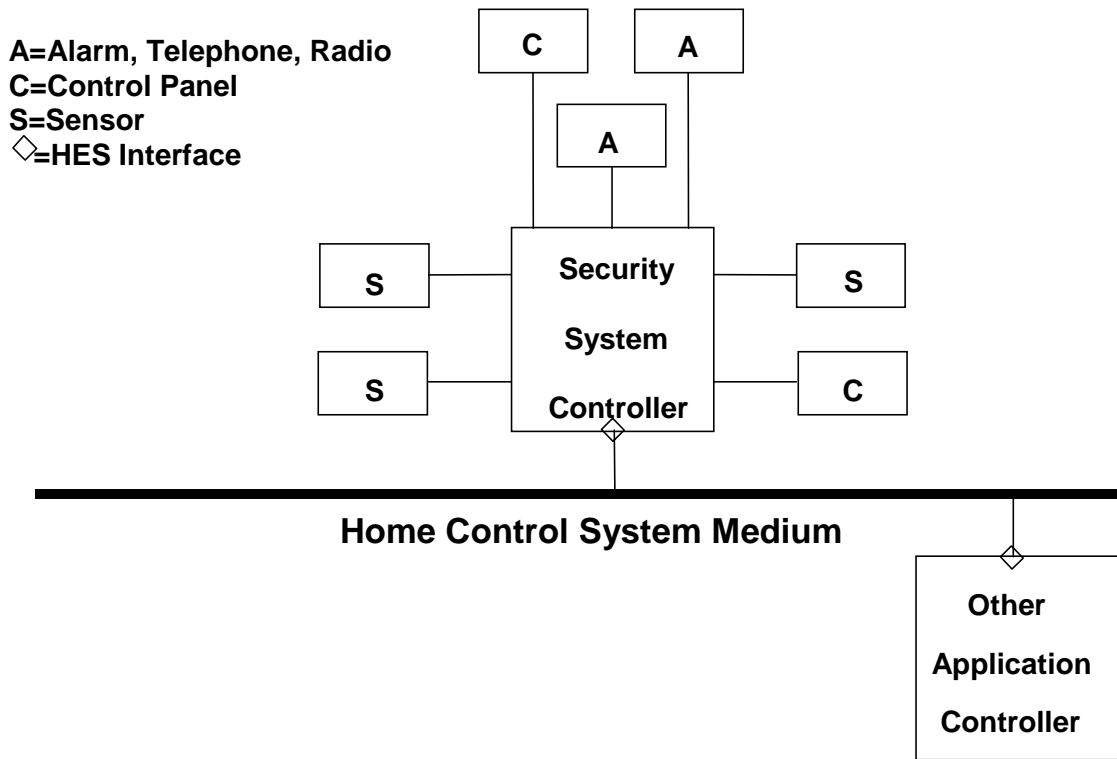


Figure 2 – Physical HES Security System Model with Isolated Components

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 application domains 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.

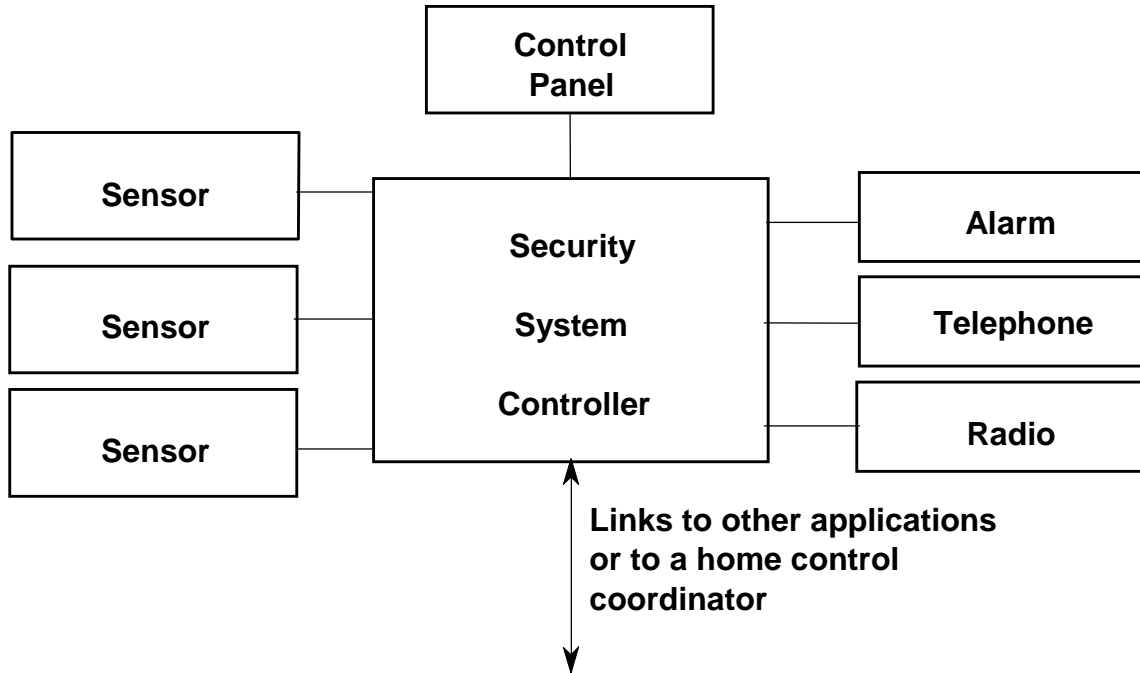


Figure 3 – Logical Model for HES Security System

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:

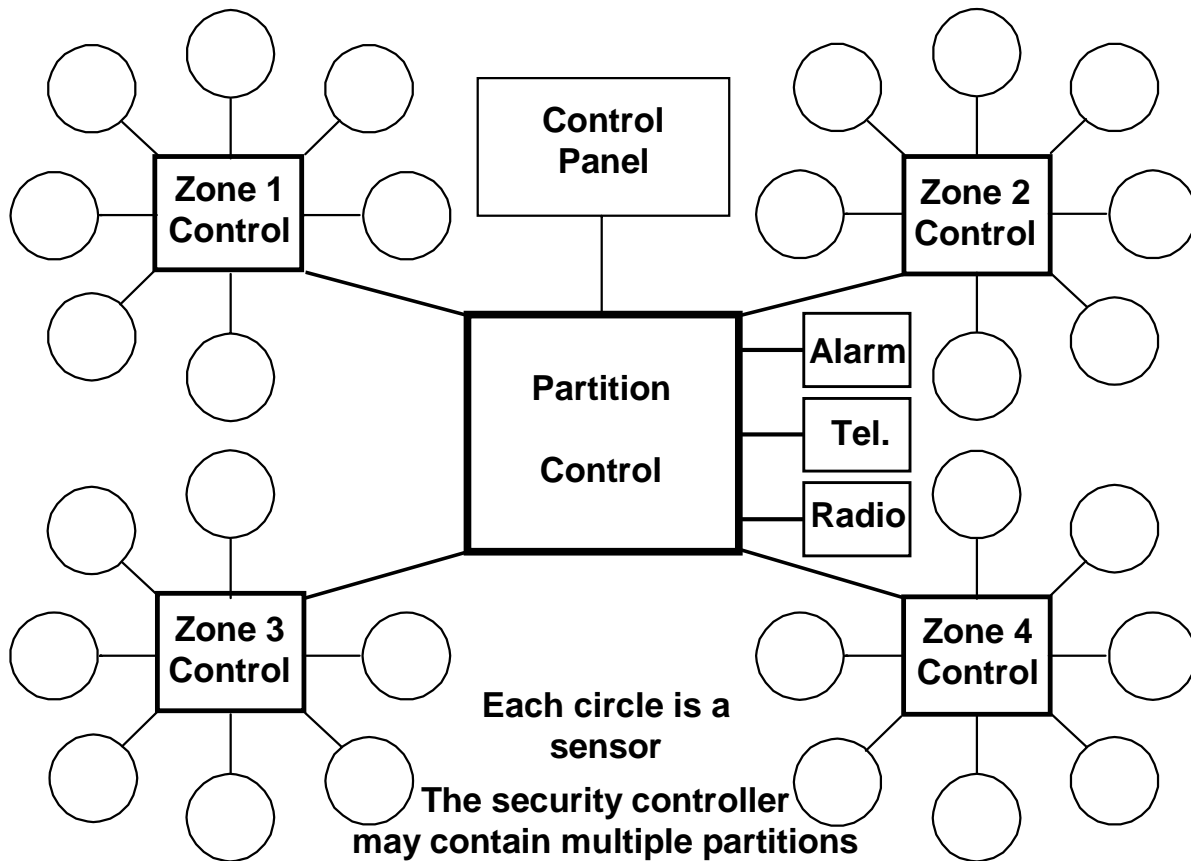


Figure 4 – Logical Constituents of a Security Controller

- *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 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 on-line 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 in the beginning of the previous section.
- 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.

Security is one of many application domains possible in a home control network. As shown in Figure 3, the security controller may be linked to other home control applications or to a home control coordinator. The coordinator might be responsible for providing common scheduling and application domain interaction. This coordination function may be distributed among the system controllers through sophisticated software, thereby eliminating the coordinating controller.

3.3 Message Flows

3.3.1 Sensors ↔ Zone Control

3.3.1.1 From sensor (according to sensor capabilities)

- Sensor ID, name, location, etc.
- Self-test results
- Sensitivity level setting
- Tamper indication
- Battery low indication
- Specified trouble code
- In reset mode
- Operating properly
- Alarm state

3.3.1.2 To sensor (not available with all sensors)

- Change sensor identification and location parameters
- Initiate self-test
- Set sensitivity level
- Reset
- Operate

3.3.2 Zone Control ↔ Partition Control

3.3.2.1 From zone control

- Zone ID, name, location, number of sensors in zone, etc.
- Sensor IDs, names, locations, etc. in this zone
- Zone off-line, not operating
- Zone on-line, no alarm
- Zone in bypass condition
- Zone on-line and in alarm
- Zone bypassed and in alarm
- Sensor with specified ID is issuing a specified alarm code
- Location of sensor issuing current alarm code
- Specified sensor issuing specified trouble code

3.3.2.2 To zone control

- Set zone off-line, not operating
- Set zone on-line

- Set zone in bypass condition

3.3.3 Partition Control → Alarm

The alarm may be a bell, siren, telephone, radio, or message pad according to the type of alarm. The following types of alarms may be issued.

- Intrusion
- Elderly monitor
- Latch-key child monitor
- Panic alarm monitor
- Medical alert monitor
- Force disarm monitor
- Fire
- Environmental pollutants
- Water leaks
- Over or under temperature
- Earthquake
- Machinery failure

Where appropriate, the alarm message includes an alarm condition, code, and location.

3.3.4 Partition Control ↔ External

External refers to another controller or control panel.

3.3.4.1 From partition control

- Partition ID, name, location, number of zones in partition, etc.
- Zone IDs, names, locations, etc. in this partition
- Partition off-line
- Partition on-line
- Partition unarmed
- Specified zones armed (may describe as a macro: home, away, in bed, etc.)
- Reporting mode: issue alarm, call specific numbers (for latch key or medical monitoring)
- Battery charged
- Battery charging
- Battery charge level: dead/missing, critical, low, normal, overcharged
- Event history (listed with date, time, and event code)
- Zone & sensor with specified IDs issuing specified alarm code
- Location of zone & sensor issuing current alarm code
- Specified zone & sensor issuing specified trouble code

3.3.4.2 To partition control

- Set partition off-line
- Set partition on-line
- Disarm partition
- Arm specified modes (may be specified as a macro)
- Set reporting mode: alarm, specified call
- Set exit timing: delay before partition is armed
- Set entry timing: delay before partition alarms after trip
- Set access control: user names and codes, valid times and dates, authorization level