**Honeywell Security Product Group**

**Galaxy DIMENSION**

**Technical Submission**

**800-16174**

**Version 3.0**

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Summary of Change** | **By** |
| 1.0 | 26 May 2010 | Initial Revision. | Liam Smith |
| 2.0 | 11 Jun 2010 | Second Revision | Liam Smith |
| 2.1 | 13 May 2011 | Addition of TouchCenter | Drew Aitken |
| 3.0 | 10/9/13 | Re-write in line with generic A&E specs | Martin Pacitti |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

###

**Table of Contents**

Contents

[Scope 4](#_Toc366698971)

[System overview 4](#_Toc366698972)

[System Architecture 5](#_Toc366698973)

[System functionality 5](#_Toc366698974)

[1.1 Zone input circuits for detection points: 5](#_Toc366698975)

[1.2 Area control (Partition or Group control) 6](#_Toc366698976)

[1.3 System users 6](#_Toc366698977)

[1.4 Event log 6](#_Toc366698978)

[1.5 Outputs for signalling and control 6](#_Toc366698979)

[1.6 Timers and Scheduling 6](#_Toc366698980)

[1.7 Automatic system Diagnostics 6](#_Toc366698981)

[1.8 Communications 7](#_Toc366698982)

[1.9 Wireless sensor capability 7](#_Toc366698983)

[1.10 Access Control 8](#_Toc366698984)

[1.11 Remote Servicing 8](#_Toc366698985)

[1.12 Compliance and Approvals 9](#_Toc366698986)

[Appendix 1 – System Peripherals 10](#_Toc366698987)

# Scope

This specification defines the requirements for an Intruder alarm system range which can deliver the security needs for Mid to Large size commercial applications.

# System overview

The following is a summary of the minimum specifications for the control panel range.

* 16 multi-state detection circuits on-board the standard control panel
* Expandability capability up to 520 detection circuits
* Capability for 32 independent areas (partitions or groups)
* Capability for 1000 users
* Intruder Event log Capacity of 1500 events
* Independent Access event log capacity of 1000 events
* 7 switching outputs on-board the standard control panel capable of switching 400mA each
* One relay output on-board the standard control panel capable of switching 1A @ 30v DC
* Capability for 67 independent weekly schedules, each with 28 on/off events
* 67 independent holiday schedules, with 32 holiday periods
* Schedule driven auto-arm for each area (partition or group)
* Lockout schedule capability to prevent disarming during secure periods
* Capability for voltage substitution detection on the detection circuits
* Full diagnostics monitoring of all detection circuits and power supplies
* Automatic scheduled reporting capability of diagnostic information
* Communication capability over PSTN, Ethernet, GPRS and ISDN
* Wireless sensor capacity for 198 sensors
* Bidirectional communication for all wireless sensors for message delivery confirmation
* Agile-routing capability for all wireless sensors to provide wireless-path redundancy
* 32 channel Bi-directional audio capability with 10 second pre-alarm per channel
* Access control capability for 64 doors each with Wiegand card readers/PIN pads
* Schedule controlled user rights for door access
* Door access rights controlled per system area (partition or group) with automatic blocking for armed areas
* Secure remote Servicing capability for configuration and remote maintenance
* Full range of system peripherals including Colour, Graphical, Touch-screen user interface
* Full compliance to En50131 at Grade 3 level plus communications compliant to Grade 4 level, ATS 5

# System Architecture

The System must consist of a centralised control panel which contains all the configuration settings and system control authority. The system must have the following minimum specification:

# System functionality

## Zone input circuits for detection points:

Zone input circuits are multi-state analogue detection circuits which allow connection of conventional alarm sensors or wireless detection inputs which are individually identified.

The system shall have 16 on-board, zone input circuits with an upgrade path to 520 zone inputs circuits. All zone input circuits must have fully configurable system responses.

Each wired zone input circuit must be capable of full supervision using an end of line resistor plus contact resistor to detect the following states:

Zone short circuit

Zone low resistance

Zone Closed (Normal)

Zone high resistance

Zone Open (Alarm)

Zone Fault

Zone masked

Zone Open circuit

It must be possible to enable certain circuits with voltage tamper detection to detect if an attempt has been made to bypass the zone input circuit by substitution of the circuit with a voltage source

Each Wireless zone must use two-way communications with transceiver modules. There must be the capability to use multiple transceiver modules to provide alternate paths to each sensor. The system shall monitor the signal level on each path to maintain the strongest two-way route to each sensor.

Each zone must have full programming capability of the following attributes:

* Function (or Zone Type. The complete list of zone functions is shown in Table 1)
* Descriptor (16 alphanumeric characters)
* Chime Attribute (Chime effect, enable/disable)
* Omit Attribute (Zone can be omitted, enable/disable)
* Part Attribute (Zone included in part arm, enable/disable)
* Response Time (Fast or slow)
* Custom SIA (SIA format mnemonic for alarm signalling)
* Activity Monitor (Check for zone activity in the dis-armed state)
* Resistance Select (Resistance windows of the zone)
* Group (Assignment of zone to Galaxy Group)
* Wireless sensor programming and signal strength

## Area control (Partition or Group control)

The system must have the option to be configured to have up to 32 fully independent areas (partitions or groups). Each area must be capable of being armed independently. Each system user must be capable of having authority to one or any combination of areas

Every zone on the system must be assigned to one area only. Certain zone types such as Keyswitch and Exit Terminate (Push To Set) zones must have the configuration ability to assign additional areas that their function will also affect for shared entrance areas.

There must be configurable logic to allow multiple areas to arm at the same time but to hold off common lobby areas from arming if all the surrounding areas are not armed or not currently in the process of arming yet.

## System users

The system must be able to be configured to have up to 1000 users. Each user must be able to have a variable authority level to govern rights to arm, disarm and reset the system following alarms. Each user must have separate assignment of arm/disarm control and access control rights. Each user must have the ability to be programmed with a PIN code up to 6 digits long plus an Access control card up to 40 bits long.

## Event log

## Outputs for signalling and control

The control panel shall have at least 7 high-current (400mA) switched-negative outputs, one relay output capable of switching 1A at 30V DC and at least 6 low current signal outputs. There must be an upgrade path to allow at least 260 outputs to be configured on the system.

## Timers and Scheduling

The system must have multiple independent timer schedules which run on a weekly cycle. Each weekly cycle must have the capability to program at least 28 events (on and off switches).

The schedules must be able to be assigned to control the following system events:

Autoarm/disarm

Arming monitor

Output control for electrical switching

Activity control of user profile for arming/disarming restrictions

Access control profile restrictions

## Automatic system Diagnostics

The system must have comprehensive self-diagnostics and reporting sufficient to have full visibility of the current health and trends on the system.

The system must be able to record the following system health data:

Status of every system power supply including:

 Output voltage

 Output voltage history (minimum and maximum)

 Output current

 AC mains Input Status

 Battery charge status

 Battery presence status

 Battery load test status

The status of every zone input on the system including

 Circuit loop resistance for wired zones

 Resistance history (minimum and maximum in the closed/normal state)

 Signal strength from every wireless sensor

 Signal strength history for each sensor (minimum and maximum)

 Activation history in the disarmed state for detector operation checking

The system must be capable of being configured for periodic transmission of the self-diagnostic information to the remote management software. The remote management software must be capable of generating a report, automatically, for each installation which will highlight all the areas where the measurements are outside spec or where there is trend where the measurements are drifting significantly.

## Communications

The system must be able to communicate over the following media

PSTN, Analogue telephone lines

ISDN Telephone lines

Ethernet WAN and LAN connections

Each of these media must allow for alarm signalling and Remote Servicing

## Wireless sensor capability

It must be possible to install up to 8 transceiver interface modules in order to allow use of wireless sensors and user control ‘keyfobs’. The system must accept an incoming message from any sensor via any transceiver interface.

Wireless communication must be two-way with the system delivering an acknowledge reply to each message from a wireless sensor or keyfob. The system must allow for intelligent routing of the acknowledge signals so that the reply is sent only from the transceiver interface which has the strongest reception of the original signal.

Wireless keyfobs must give user feedback on arming command status and must be capable of showing the armed status of the system upon request

The wireless sub system must meet the requirements of EN50131-5-3 to Grade 2 level.

## Access Control

The system must be capable of controlling up to 64 doors. Access through the doors must be restricted to users who have access rights to those specific areas of the building at specific times. The system must not allow access to an area which is armed to avoid false alarm activation.

It must be possible to define rights for users to disarm or arm areas of the building using their access control card at a door control reader.

## Remote Servicing

A PC software suite must be available to service installed systems from a remote, centralised location. This package must have the following capabilities:

* Centralised database for storing site data for at least 100,000 configured installations
* Ability to have up to 32 operators accessing the database, simultaneously, via a client browser application across a local or wide area network.
* Ability to have up to 64 remote systems connected to the database simultaneously via a communications server application
* Ability for the communications server to accept incoming connections from remote systems, automatically, even when no operator is active on a client browser.
* Choice of Communication Media
	+ Ethernet TCP/IP
	+ RS232 Serial Interface
	+ PSTN
* Full Audit trail log of activity in accessing the database
* Connection log of all remote, installed systems which are connected to the database
* Ability to define scripts to make mass updates to groups of accounts to roll out a common change across many installed systems

**Operator Features include:-**

* Creating/Open of system accounts
* Printing account information
* Copying account information to new accounts
* Real-Time control of remote systems via virtual Keypad Operation
* Upload data from installed systems
* Download data to installed systems
* Off-line programming of all aspects of installed system configuration
* Rolling back panel programming data to a previous, saved version
* Mimic Panel display of system status in real-time
* Diagnostics indication of installed systems’ health
* Event log display
* Event log filters
* Ability to set time and date
* Initiate connections to installed systems
* Copying of event log data
* Printing of installed system data
* Printing of event log
* Automatic generation of detailed system health status reports using uploaded diagnostic data

## Compliance and Approvals

The product must be independently tested to the following directives and standards:

**R&TTE 99/5/EC**

**EN50131-3: 2009 security grade 3, environmental class II**

The product must be suitable for use in systems designed to comply with EN50131-3:2009:

* Security Grade: 3
* Environmental Class: II
* Power Supply Type: A
* Alarm Transmission System: ATS2=D2, M2, T2, S0, I0

The control panel must be compatible with the relevant parts of the following standards:

**EN50131-1:2006+A1:2009** Alarm systems – Intrusion systems – General requirements (grade 3).

**EN50131-6:2008** Alarm systems – Intrusion systems – Power supplies (grade 3).

**PD6662:2010** Scheme for the application of European Standards for intruder alarm systems.

**BS8243: 2010** Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions - code of practice.

# Appendix 1 – System Peripherals

The following peripherals must be available for system design:

**User Interfaces**

**Standard keypad for programming and user control**

* Stylish design
* 32 (2 x 16) alphanumeric backlit LCD display
* Tamper protection
* Tactile backlit rubber buttons
* Full system control
* Addressable
* Can be connected directly to the system databus at distances up to 1,000 m from the control panel
* Arm/Disarm with PIN and/or optional proximity tag
* Easy installation
* Self learn capability for proximity tags

**TouchCenter Keypad with Prox tag reader**

* ¼ VGA TFT Touchscreen keypad
* Graphical icons for end user control
* Engineer access and control capability
* Plastic enclosure
* Lid and mounting tamper protection
* Can be connected directly to the panel up to distances of 1,000 m
* Integrated proximity reader for arm/disarm capability
* Self learn capability for proximity tags
* Dual action functionality, simple arm/disarm operation removes the need for PIN entry

**Self contained single door controller**

* Proximity Door Control Unit
* Connects directly to peripheral data bus
* Monitors the status of one door
* Able to control a door lock and request to exit button directly
* Can be used to arm/disarm with Prox Card/Tag
* Addressable
* Intended for Internal use or External use

**System Expansion**

**Zone & output extension module**

* Connects directly to peripheral data bus at up to 1000 m from the control panel
* Addressable
* 8 zone input circuits with voltage tamper protection
* 4 transistorised outputs
* Lid and surface removal tamper protection

**Intelligent Power Supply Range**

* EN50131-1/EN50131-6 Grade 2 or 3 compliant
* Total capacity 2.75 A
	+ Rating dependent upon grade selected and battery capacity
	+ RS485 communication support
	+ 8 zones/4 outputs

**Wireless transceiver portal or Gateway**

* Wireless transceiver providing support for wireless sensors and keyfobs
* Comprehensive wireless diagnostics, testing and monitoring functionality
	+ - Low battery
		- Programmable supervision
		- Jam detection (interference)
* Centralised programming mode via system keypad
* Walk test automatically logs the signal strength of each zone
* Full signaling of RF status

**Wireless sensor portfolio**

The following wireless sensor types must be available for system design:

10m PIR sensor

12m Dual-Tech microwave & PIR sensor

Magnetic door contact

Shock sensor

Audio glass-break detector

Smoke sensor

Carbon Monoxide sensor

Flood and temperature sensor

Wireless sensor must have a typically battery life exceeding 3 years.

Sensors must have an open field transmission range of 2km.

This page is intentionally blank