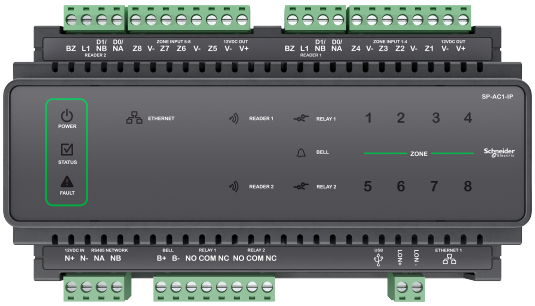
Security Purpose LON Controller (IP only)



The Security Expert Security Purpose LON Controller is the central processing unit responsible for the control of security, access control and building automation in the Security Expert system.

It communicates with all system modules, stores all configuration and transaction information, processes all system communication, and reports alarms and system activity to a monitoring station or remote computer.

Feature Highlights

- Built-in LON Interface
- Internal industry standard 10/100 Ethernet connection
- 32 Bit advanced RISC processor with 2Gb total memory
- Encrypted module network using RS-485 communication
- NIST Certified AES 128, 192 and 256 Bit Encryption
- Offsite communications via IP and cellular network connections
- Factory loaded HTTPS certificate
- 2 reader ports, independently configurable for either Wiegand or RS-485 operation
- OSDP configurable RS-485
- 8 high security monitored inputs
- 2 high current Form C relay outputs
- 1 high current monitored bell output
- Firmware upgradable directly from the software
- Designed for use with industry standard DIN Rail mounting

LON Interface

The two wire LON interface connects to the Schneider Electric Continuum range of I/O modules and provides high speed secure communication with up to 32 modules simultaneously. FTT-10, RS-485 and OSDP are supported, and the mode of operation can be switched programmatically.

The interface uses *Differential Manchester* encoding, which means the orientation of the 'A' and 'B' connections is not important - the interface works equally well wired in either configuration.

Communication

RS-485 communication interface, USB port and a 10/100 ethernet communications port provide a complete solution for system communication, expansion, offsite monitoring and integration.

Integrated Access Control

Providing a highly sophisticated access control solution with large user capacity and extensive features:

- Utilize multiple access levels to manage users over scheduled periods across multiple time zones.
- Assign door groups, menu groups, area groups, floor groups and elevator groups to an access level for flexible user management. Each user can be assigned multiple groups in multiple access levels.
- Monitor and control users' area status throughout the entire system with hard and soft anti-passback configuration options.
- Multiple card presentation options allow the use of access control cards, tags, mobile or other credentials to arm and disarm areas associated with doors.
- Count users entering an area and arm the area when the count reaches zero or deny access based on a maximum user count.

Connectivity and System Expansion

Extending the Security Expert system with onboard local inputs and outputs allows convenient and cost effective expansion without the increased cost of modules for simple system functions:

- 8 monitored onboard inputs can each be configured for EOL (End Of Line), dual EOL, or direct contact.
- 2 high current Form C relays onboard.
- 2 integrated reader ports, independently configurable for Wiegand or RS-485 reader operation.
- RS-485 connections support configuration for OSDP protocol.
- Bell/Siren output onboard with fully monitored operation.
- System expansion is achieved seamlessly by connecting additional expander modules.

Integrated Arming/Disarming

Featuring advanced integration of arming and disarming solutions for control of hundreds of alarm areas:

- Deny access to a user based on the status of the area and allow the user to control the area they are entering, in turn reducing false alarms.
- Implement vault control areas to manage time delayed access and unlocking of vault areas in banking facilities without the need for additional hardware control devices.
- Control access to a keypad using a card and PIN function, or allow card presentation to automatically log the user in at the associated keypad.
- Disarm an area associated with an elevator floor on access, or prevent the user from gaining access to the floor based on the area status associated with the floor.
- Arm large numbers of areas using area groups.

Flexible Reader Support

Provides 2 reader ports that can be independently configured for either Wiegand or RS-485 reader operation, allowing the connection of up to 4 readers controlling 2 doors.

Choose Wiegand readers for compatibility with all standard access control systems, or RS-485 for fast, secure communication.

RS-485 readers provide the added benefits of being easier and more cost effective to wire and deploy, and allow for direct integration with Security Expert systems, enabling you to make changes on the fly once readers are installed. RS-485 also allows for longer cable runs and offers a simpler firmware update process.

OSDP protocol configuration in RS-485 offers additional security and adds scalability, flexibility and ease of implementation.*

* The Schneider Electric implementation of OSDP conforms to a subset of the OSDP functionality. For specifications and reader configuration, refer to *Application Note 254: Configuring OSDP Readers*.

Multifunction Reporting Services

The controller incorporates a host of offsite reporting options.

- Implement IP based reporting using the encrypted ArmorIP protocol or other common IP reporting standards.
- For complete peace of mind, set up multi-channel reporting using a combination of local ethernet and 4G network (via the Security Expert Security Purpose DIN Rail Cellular Modem).
- Communicate with third party applications using ASCII or HEX directly from the controller.

Integrations

The Security Expert controller offers integration with a wide range of third party systems:

- Link the Security Expert system with intelligent locking solutions through comprehensive world class solution partners Salto, Aperio, and Cencon.
- High level interface for control of modern elevator systems.
- Integrated biometric identification systems provide superior user identification options.
- Other third party integrations such as building and lighting control systems.

Secure By Design

Schneider Electric controllers are cyber secure, supporting emerging cybersecurity requirements through advanced security features.

With secure encrypted communication, resilience to outages, secure storage of security parameters and no universal default passwords, Schneider Electric controllers are inherently designed to protect devices, networks and data from unauthorized access.

Mandatory cybersecurity regulations on connected devices are defining requirements in terms of data & cryptography, logical security, system management and privacy protection.

Schneider Electric controllers feature essential requirements of newly introduced standards and legislation aimed at regulating the Internet of Things and IoT devices, along with specifications of emerging new laws.

Schneider Electric controllers are Secure By Design.

Secure Encrypted Web Connection

Equipped with a factory loaded HTTPS certificate, ensuring a secure encrypted web connection straight out of the box.

The default certificate provides automatic TLS encryption of data transmissions, secure identity authentication, and message signing to assure data integrity.

Output Follows Input Programming

The Security Expert system's advanced programming features provide endless opportunities for customized automation. Output follows input programming allows any output or output group in the system to be intelligently controlled by any input or input type. This has a wide variety of applications: from turning on lights and climate control when motion is detected, to unlocking a specific door with a key switch, or auto arming an area after a period of inactivity.

Programmable Functions

Programmable functions are special applications that implement logical control of outputs, doors, areas and other devices.

- Perform actions when a particular event or operation occurs, such as setting the room temperature based on the number of people in an area, adjusting internal lighting levels based on a sensor reading, or unlocking doors in the event of a fire alarm.
- Process logic functions to allow complex equations to be evaluated using internal memory data values and output status .
- Control of doors, areas, elevators and outputs can be easily programmed and managed.

Ethernet 10/100 Connection

Onboard ethernet communication allowing direct connection from a local PC or interconnection to an existing LAN/WAN:

- Directly connect the Security Expert system across a LAN or WAN interface for high speed upload and download.
- IP reporting functionality using the ArmorIP protocol, Contact ID over IP, SIA over IP and full text reporting methods.
- Full 10/100 compliant network interface allows connection of the controller to all networks at the maximum capable signaling rate.

Upgradable Firmware

Firmware can be upgraded directly from the Security Expert software.

Technical Specifications

Ordering Information	
SP-AC1-IP	Security Expert Security Purpose LON Controller (IP only)
Power Supply	
Operating Voltage	11-14V DC
Operating Current	120mA (Typical)
DC Output (Auxiliary)	10.45-13.85V DC 0.7A (Typical) electronic shutdown at 1.1A
Bell DC Output (Continuous)	10.4-13.45V DC 8 ohm 30W Siren or 1.1A (Typical) Electronic Shutdown at 1.6A
Bell DC Output (Inrush)	1500mA
Total Combined Current*	3.4A (max)
Electronic Disconnection	9.0V DC
Communication	
Ethernet	10/100Mbps ethernet communication link
RS-485	3 RS-485 communication interface ports - 1 for module communication, 2 for reader communication
USB	Type-A
LON Interface	
LON Interface	The two wire LON interface connects to the Schneider Electric Continuum range of I/O modules and provides high speed secure communication with up to 32 modules simultaneously. FTT-10, RS-485 and OSDP are supported
Readers	
Readers	2 reader ports that can be independently configured for either Wiegand (up to 1024 bits configurable) or RS-485, allowing connection of up to 4 readers providing entry/exit control for two doors **
	RS-485 reader port connections support configuration for OSDP protocol
Inputs	
Inputs (System Inputs)	8 high security monitored inputs
Outputs	
Outputs	4 (50mA max) open collector outputs for reader LED and beeper or general functions
Relay Outputs	2 Form C relays - 7A N.O/N.C. at 30V AC/DC resistive/inductive
Dimensions	
Dimensions (L x W x H)	156 x 90 x 60mm (6.14 x 3.54 x 2.36")
Net Weight	348g (12.3oz)
Gross Weight	418g (14.7oz)
Operating Conditions	
Operating Temperature	UL/ULC 0° to 49°C (32° to 120°F) : EU EN -10° to 55°C (14° to 131°F)
Storage Temperature	-10˚ to 85˚C (14˚ to 185˚F)
Humidity	0%-93% non-condensing, indoor use only (relative humidity)
Mean Time Between Failures (MTBF)	560,421 hours (calculated using RFD 2000 (UTE C 80-810) Standard)

***** The total combined current refers to the current that will be drawn from the external power supply to supply the expander *and* any devices connected to its outputs. The auxiliary outputs are directly connected via thermal resettable fuses to the N+ N- input terminals, and the maximum current is governed by the trip level of these fuses. The Bell output is connected in the same way.

** Each reader port supports either Wiegand or RS-485 reader operation, but *not both at the same time*. If combining reader technologies, they must be connected on separate ports.

The Schneider Electric implementation of OSDP conforms to a subset of the OSDP functionality. For specifications and reader configuration, refer to *Application Note 254: Configuring OSDP Readers*.

Regulatory Notices

RCM (Australian Communications and Media Authority (ACMA))

This equipment carries the RCM label and complies with EMC and radio communications regulations of the Australian Communications and Media Authority (ACMA) governing the Australian and New Zealand (AS/NZS) communities.

CE – Compliance with European Union (EU)

Conforms where applicable to European Union (EU) Low Voltage Directive (LVD) 2014/35/EU, Electromagnetic Compatibility (EMC) Directive 2014/30/EU, Radio Equipment Directive (RED)2014/53/EU and RoHS Recast (RoHS2) Directive: 2011/65/EU + Amendment Directive (EU) 2015/863.

This equipment complies with the rules of the Official Journal of the European Union, for governing the Self Declaration of the CE Marking for the European Union as specified in the above directives.

Security Grade 4, Environmental Class II, EN 50131-1:2006+A2:2017, EN 50131-3:2009, EN 50131-6:2008+A1:2014, EN 50131-10:2014, EN 50136-1:2012, EN 50136-2:2013, EN 60839-11-1:2013, Power frequency magnetic field immunity tests EN 61000-4-8, Readers Environmental Class: IVA, IK07, SSF 1014 Larmklass 4.

UK Conformity Assessment (UKCA) Mark

This equipment carries the UKCA label and complies with all applicable standards.

UK PD 6662:2017 and BS 8243

Security Expert systems conform to PD 6662:2017 and BS 8243 at the security grade and notification option applicable to the system.

UL/ULC (Underwriters Laboratories)

- UL1076 for Proprietary Burglar Alarm Units and Systems
- UL1610 for Central-Station Burglar-Alarm Units
- UL294 for Access Control System Units
- CAN/ULC S304 for Signal Receiving Centre and Premise Burglar Alarm Control Units
- CAN/ULC S319 for Electronic Access Control Systems
- CAN/ULC S559 for Fire Signal Receiving Centres and Systems

Industry Canada

ICES-003

This is a Class A digital device that meets all requirements of the Canadian Interference-Causing Equipment Regulations.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CAN ICES-3 (A)/NMB-3(A)

Federal Communications Commission (FCC)

FCC Rules and Regulations CFR 47, Part 15, Class A.

This equipment complies with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference; (2) This device must accept any interference received, including interference that may cause undesired operation.