



iWorX ACU-1

Specification & Submittal Data

ACU-1

Overview

The ACU-1 is a self-contained controller for single door access control. Use the ACU-1 to electrically control passage through a physical barrier such as a door or gate.

The controller monitors contacts and controls actuators via its 2 card reader/keypad interfaces, 4 digital outputs, 4 supervised inputs, and 1 relay output. LED indicators, field wiring terminal blocks, and panel mounting ability are other features of this controller. It functions as part of an Echelon LonWorks® Network using the integral FTT-10 Free Topology communications transceiver.

A Local Database Module (LDM) enables the controller to locally validate access attempts in the case of a loss of network communication.

Features

- Controls access to one barrier (door or gate)
- Compatible with 26-bit Wiegand card readers
- Interfaces with entry and exit (optional) card readers
- Local storage of card database in case of network failure
- Battery backup of local memory
- On-board relay used to control door strike
- Free access set by schedule or manual override
- Door Propped and Door Forced detection
- Two supervised inputs for additional tamper detection (glass break, etc.)
- Maximum of 500 access cards (system wide)
- Occupancy status tracking to interface with HVAC equipment
- Three door access modes (card only, card + PIN, cipher)
- LONWORKS interface to building automation systems and host products
- Automatic configuration via the LCI
- Alarm/Event reporting



Innovex Technologies
511 Braddock Avenue
Turtle Creek, PA 15145
www.innovextechnologies.com

iWorX is a trademark of Innovex Technologies
LON, LonWORKS, & LonMARK are trademarks of Echelon Corporation

Specifications

Electrical

Inputs

- Cabling: twisted shielded pair (use multi-core for Card Reader Data Inputs), 18 AWG recommended—500 feet max. (152 meters)

Supervised Inputs (TB5-26 through TB5-33)

- 0-5 Volt
- Resolution: 8 bit

Card Reader Data Inputs (TB3-12, TB3-13, TB4-20, and TB4-21)

- Compatible with Wiegand 26-bit electrical interface standards

Outputs

Digital Outputs (TB3-14, TB3-15, TB4-22, and TB4-23)

- 50 mA maximum load
- Current sinking to DC common when on

Relay Output (TB6-37 through TB6-39)

- 2 amps @ 30 VDC or VAC
- SPDT, form-C contact

Power Outputs (TB3-10 and TB4-18)

- 5 VDC, 100 mA maximum load
- Individually short-circuit protected using a PTC.

FTT10-A Network

- Speed: 78KBPS
- Cabling: Maximum node-to-node distance: 1312 feet (400 meters)
- Maximum total distance: 1640 feet (500 meters)

Table 1: Network Wire Specifications

Cable Type	Pairs	Details	Connect Air Catalog No.
Level 4 22AWG (0.65mm)	1	Unshielded, Plenum, U.L. Type CMP	W221P-2001
Level 4 22AWG (0.65mm)	1	Unshielded, Non-Plenum, U.L. Type CM	W221P-1002

For detailed specifications, refer to the FTT-10A Free-Topology Transceiver User's Guide published by Echelon Corporation. For information on ordering Connect Air items, contact Connect Air International; 4240 B Street; Auburn, WA 98001 <www.connect-air.com>.

Power Requirements

- 12 to 24 VAC or 12 to 24 VDC power (requires an external supply)

Power Consumption

- With no external loads: 6 VA

Mechanical

Enclosure

- Dimensions: 10.5" (267mm) wide, 5.64" (143mm) high, 2.52" (64mm) deep
- Material: 0.063" thick Aluminum
- Surface preparation: black, semi-gloss paint

LDM Battery

- Battery Life: 5 years
- Memory retention: 1440 hours (60 days) of accumulated power off
- Battery type: BR1/3N primary lithium (removable)

Electronics

- Base board dimensions: 9.0" wide, 4.0" high
- Terminals: Removable screw terminal blocks. Rated for 12 to 24 AWG wire

Environmental

- Temperature: 32 to 104 degrees F (0 to 40 degrees C)
- Humidity: 0 to 90 percent, non-condensing
- Altitude: 0 to 10,000 feet (3048m)

Agency Listings

- UL916 PAZX
- CSA 22.2 No. 205-M1983 P PAZX7

Agency Compliances

- (CE) EMC Directive
- EN5022
- EN50082-1
- FCC Part 15 Class B

Application Description

Overview

The controller monitors and controls access to a single entry barrier through the use of an entrance card reader. An exit card reader may also be used to monitor and control exit access. Supervised inputs are provided for tamper detection.

Entrance (required) and exit (optional) card readers may be used to control door access. The controller supports card readers that use 26-bit Wiegand encoding. Up to 500 access cards are supported system-wide.

An LCI must be used to configure all of the controller's access parameters. You can download a database of cards to the LCI or add the cards by putting the controller into auto-add mode and presenting cards to the reader. A local database of card information provides secure access in case the network communication is lost. The memory containing the local database is maintained by a backup battery.

One input is dedicated to monitoring the door status, and one is dedicated to monitoring the exit request pushbutton. Two non-dedicated supervised inputs can be used for monitoring other tamper devices such as a glass break detector or a motion sensor.

Digital outputs are provided to control card reader indicators such as LEDs and audible sounders. 5 VDC outputs are provided to power the card readers. If the readers that are used require a different voltage, they must be powered with a separate supply. A relay output is provided to control a barrier locking device such as a door strike or magnetic lock. Both normally open and normally closed contacts are provided to accommodate devices that lock when power is applied or devices that lock when powered off.

Alarms are generated when the controller detects that a door has been propped or when a door has been forced. Alarms are also generated if the two spare supervised inputs have been tampered with.

Sequence of Operation

Door Access Modes

A door can be set to allow free access or to require a card, card + PIN, or cipher code for access. Use a schedule to set different access modes for the ON and OFF periods of the schedule. Set the door access mode manually, and it will remain in that mode until you change it or return it to automatic mode.

Use a separate schedule to set a door to allow free access during certain times of the day. The door will allow free access during the ON part of the specified schedule, and will resort to the access mode specified by its normal schedule for the OFF part of the free access schedule. Manually placing a door in or out of free access mode is also supported. Use the LCI to set these parameters for each ACU-1.

Door Groups

A Door Group defines whether access is permitted or denied to particular doors for the cards in that door group. Define up to 16 different door groups. Door groups can also use schedules to specify when cards are allowed access.

As an example, one door group may be set up to allow engineers access to the building entry doors and the engineering labs. Another door group may be set up for human resources employees that only allows access to the building entry doors.

When defining a door group, all doors in the system are denied access by default. Change the access to permitted for the appropriate doors in this door group.

When deleting a door group, do not delete a door group that is currently being used by some cards. Doing so will remove that door group limitation from those cards, and those cards will be permitted access to all doors.

Cards

An iWorX system may have a maximum of 500 access cards in its database (kept in the LCI). Add cards to the system through an LCI, or through the LCI's SCS software. To use the LCI, put an ACU-1 in auto add mode, and specify whether the normal access mode will be card only or card + PIN. When the ACU-1 is in auto add mode, present cards to the reader. If you selected card + PIN as the normal access mode, you will need to enter a 4 digit PIN for each card after you present it to the reader. This PIN will be valid system wide at any permitted ACU-1 that requires a PIN, and can be changed at a later date from the LCI. If a door in the system has an exit reader, and the access mode for the door is card + PIN, occupants must use the PIN when exiting the door as well as entering it.

Specifying a door group for a card defines the doors that are accessible by that card. If you designate a default door group on the LCI, all cards will be assigned to that door group when they are added. After the card is added, change a card's door group using the LCI.



You must be sure to take the LCI out of auto-add mode after you are finished adding all cards. Otherwise, any card that is presented to the reader will be added to the database instead of checked to see if access should be granted.

Use the LCI to view the following card attributes:

- Name
- PIN
- Door Group
- Card Number,
- Last Time Used
- Last Door Used

Use the LCI to change the Name, PIN, and door group for a card after it is added to the system. You can also use the LCI to delete cards from the system.

Local Card Database

The controller keeps a local database of all cards that are permitted access to its door. This enables the door to provide appropriate access even if the ACU-1 loses its network connection. When a card is added to the system through an LCI, it is also added to the local database of the ACU-1 that was used to add the card. When a card is added to the system through the System Configuration Software (SCS) utility, it is automatically added to the local database on the proper ACU-1s.

After a card is added to the system, when it is presented to a reader and granted access to that door by the LCI, it will be added to the local database of that door's ACU-1. If a card is presented to a reader and denied access by the LCI, it will be deleted from that ACU-1's local database if it was previously included.

Ciphers

An ACU-1 can be set to allow the use of cipher codes rather than cards to grant access. Use the LCI to set up to four 4-digit cipher codes that can be used at any ACU-1 in the system that is in cipher mode. Cipher access can be limited to certain times of the day through the use of schedules.