DATA SHEET

ESS-ACS

IRIZ ID
Technologies

WE INDENTIFY SECURE AND INTEGRATE

Introduction

ESS SOFT is a web based application built to centralize and organize the data that can be employed in various modules in an application. It acts as a vital tool for privileged users to access employee information, view reports in real time and perform necessary actions.

It provides users to access their personal data, send / receive requests via web portal enabled with email notification for essential actions. Decision making will be easy as all the information is automatically populated in real time.

ESS paves a way for an organization to empower the employees and use data (Access Control Information) as a conduit for better management decisions with accurate information whenever needed.

About ESS-ACS

It exerts a computerized control that is well organized to access the resources (building, small area or room in building, assets in a building etc.). It acts as a medium between operator and Hardware (Controller). Its core functionality is to send the commands, instructions, requests and data to controller and receive alarm responses from controller, and notify same to operator.

AccessSoft is a comprehensive access control management system designed to provide a user friendly environment in order to configure the controller, readers, schedules, access levels and several ACS features.

ACS Features

Device Management

CONFIGURE CONTROLLER

Discover Controller on Network

- HID VertX V-1000 32-Door controller
- HID VertX V-2000 1/2-Door Controller
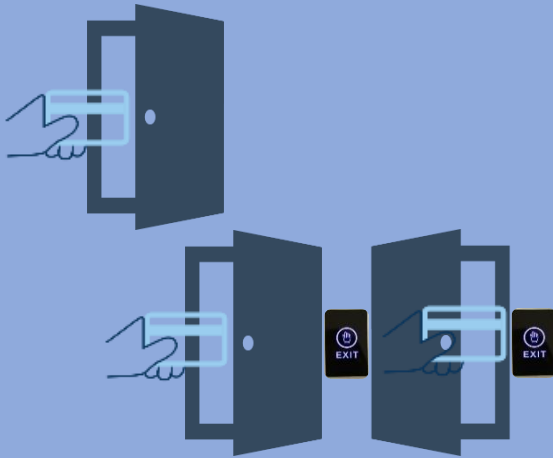- HID Edge EH-400 1 Door Controller

Option to Add Controller Manually

Discover Interface

- Door/Reader Interface V-100
- Input Status Interface V-200
- Output Interface V-300

Door Management

CICO / CIFO

Card-In Card-Out / Card-In Free-Out

Reader Interface (V-100) can be configured either for one door control or two door control.

CICO Supports single door with two readers, one at each sides of the door, one for Entry and the other for Exit.

CIFO: Supports two doors by connecting Reader-1 for Door-1 and Reader-2 for Door-2 and EXIT BUTTON for both the doors for free exit.

In the case of EDGE-EVO controller, it is always considered as one door control irrespective of CICO or CIFO.

PROTOCOL

Supports either WIEGAND or CLOCK & DATA reader protocol

ACCESS METHOD

There must be a proper association among the door configuration, physical reader connected and the credentials enrolled (Refer AM in card management)

Door configuration support following Access Methods

- CARD ONLY (Accept CARD Ignore PIN)
- PIN ONLY (Accept PIN Ignore CARD)
- CARD AND PIN (Accept CARD and then Pin)
- CARD OR PIN (Accept Either CARD or PIN)
- Free Exit (With Exit Switch)

Note: Biometric authentication is at reader level

PIN Authentication supports following options

- PIN Length (1-15)
- Attempt (0-10)
- Time Limit (0-60 Sec)
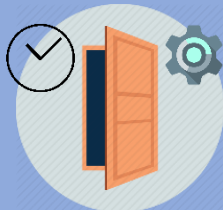- Lockout Time (0-300 Sec)

PIN COMMAND

PIN Commands allow a cardholder to lock and unlock readers from the reader unit directly.

- The desired reader(s) must be configured to accept PIN commands
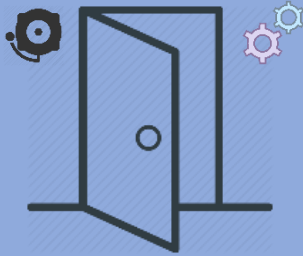- The card record(s) must be configured to allow the holder to issue PIN commands

DOOR TIMER SETTINGS

Following are the timer settings to enable/disable the output status with respect to the duration configured.

- General Access Grant Time
- Extended Access Grant Time
- Door Held Open Alarm Time
- Auxiliary Relay/Output Time

DOOR ALRAM SETTINGS

- Door Force Alarm (Door Monitor must be connected)
- Door Held Alarm (Door Monitor must be connected)
- Access Alarm (configuration to generate Auxiliary relay based on following condition)
  - o When Access Granted
  - o When Access Denied Unknown Card
  - o When Access Denied
- REX/FREE EXIT (Exit switch must be connected)

ANTI-PASS-BACK

It supports two types of Anti-Passback namely;

- Timed: Uses a timer (in seconds 0-999) to determine the interval before a card holder can gain entry through the same reader
- Real: It is implemented through a system of entry and exit readers to defined areas within the controlled access area

Following are the actions after Anti-Passback violation

- Log Messages Only
- Log Messages and Deny Access
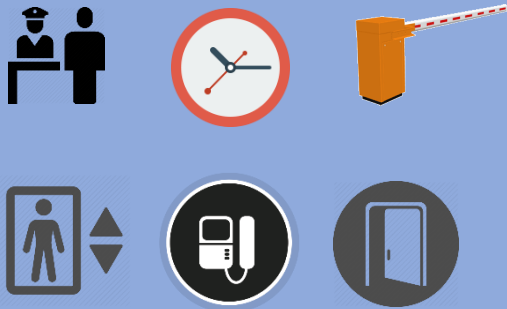- Log Message, Allow Entry and Deny Exit

MULTI-MAN ACCESS

It enables two or more card holders required to access the Door/Area with respect to the roles assigned with following options.

- Role Count/Card Holders (1 - 8)
- Preserve Sequence (Yes/No)
- Sequence Time-Out (1-256 Sec)
- Entry Type (Soft/Hard)

DOOR OPTIONS

Following are the optional door configurations for further reporting or action

- Guard Tour Check Point
- Attendance Reader
- Parking Gate/Barrier
- Elevator Reader
- Video Access Point
- Linked to Intercom
- Trace Door

Credential / Card Management

CREDENTIAL

A single user (Card holder) can have multiple cards/credentials

Credential comprises of following elements

- Unique ID/Enrollment ID
- Authentication Mode
- Card Number
- PIN
- Expiry Date
- Access Group/Level

CARD FORMAT

Supports multiple card formats including HID Standard Format, Proprietary Format, Corporate 1000 and Open/Custom Format along with various Facility codes.
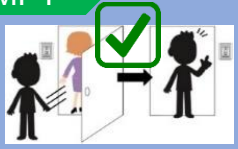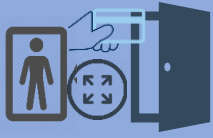
Example:

- H-10301
- H10302
- H10304
- Corporate-1000

PIN COMMAND

Enable card holder to input PIN Commands to LOCK or UNLOCK the Reader.

ACCESS TYPE

Access Type works in conjunction with Access Method configured at Door Reader

Following are the possible Access Methods

- CARD ONLY (Accept CARD Ignore PIN)
- PIN ONLY (Accept PIN Ignore CARD)
- CARD AND PIN (Accept CARD and then PIN)
- CARD OR PIN (Accept Either CARD or PIN)

PIN EXEMPT

Exempts a card holder from the PIN requirement at a PIN reader

ANTI-PASSBACK EXEMPT

Exempt or Underprivileged the card holder from the door if it is configured with Anti-Passback rule.

EXTENDED ACCESS

This is used in exceptional cases where required Access Grant Time (Door Unlock Period) is more than General Access Grant Time. Extended Access Time is configured at reader (Rages from 25msec to 27minutes).

CARD EXPIRY

Set Card Validity through START DATE TIME and END DATE TIME

ACCESS GROUP

Each card holder's record can support 1-8 Access Group(s), Value 0 indicates no Access Group.

Refer *Access Group Management* for more details.

CARD HOLDER OPTIONS

Card holder can be flagged with following options from reporting perspective

- Visitor Card
- Guard
- Trace Card

Access Group Management

ACCESS GROUP

Access Group defines the door privileges of a cardholder.

This information is referenced by the access control task when a grant or deny access decision is made.

Access Group is a permutation and combination of Door Groups and Schedules
- Door Group is a collection of Readers/Doors
- Schedule is a Collection of Time Intervals

DOOR GROUP
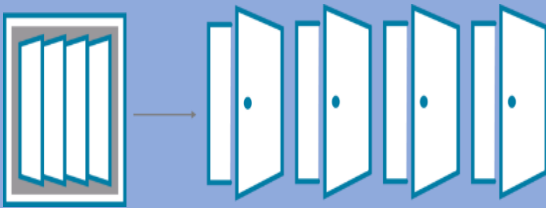
Door group is a collection of readers grouped together and added to desired access group to authorize door level access.

In the case of CICI (One Door Control), the entry and exit reader can independently be added in door group to decide whether to give access only to enter, exit, and both.

Door group can also be used as a filter option while generating the respective reports, for monitoring online access logs, etc.
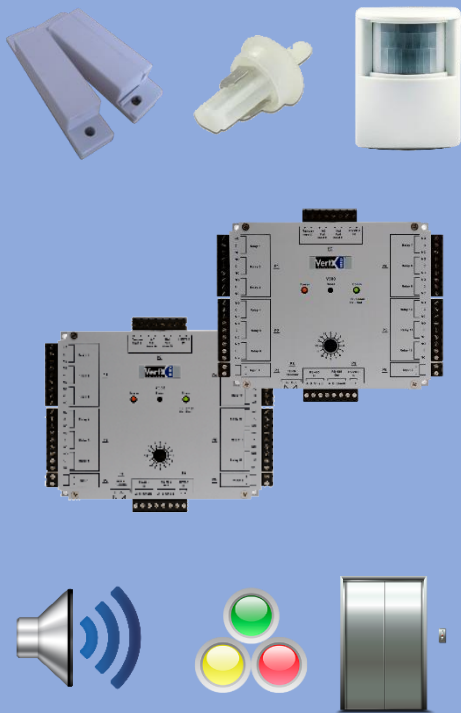
DOOR SCHEDULE

A schedule defines the set of intervals to be considered to grant or deny access, and to perform certain operations based on IN/OUT schedule interval like unlock door, elevator access, etc.

It is defined on week basis; each day can have up to 6 intervals.

Input and Output Management

I/O LINKER

The I/O Linker is a powerful tool allows the systems to generate event messages or to drive outputs based on a change in an input point value, a schedule or a logical input value.

It can perform following operations:

- Generate the output based on the input state change
- Generate output based on schedule
- Generate Alarm message based on certain events
- Monitor standard device status such as
    - AC Mains Power Fail (Provided monitored PSU)
    - Battery Fail
    - Tamper
    - Door Monitor etc.
- Drive device output states either individually or in a group
- Execute system commands

Above operations can be performed based on following conditions:

- Input status
- Schedules
- Timers
- Special logical variables (that are internal to I/O Linker itself)
- Receipt of events

FIRE ALARM

The same I/O tool can be used to configure the doors to release the lock when state change occurs on Input port where Dry Contact is connected from Fire Alarm Panel.

And door gets lock automatically once the status from fire panel input is back to normal.

A single signal from Fire Alarm Panel can be used to control one or more doors.

Note: All the Doors/Reader Interface must be connected to the same controller where Fire Alarm input is connected to either one of the input port belongs to the same controller where doors are connected or interface connected to same controller.

DOOR UNLOCK SCHEDUAL

It allows to configure the doors to LOCK or UNLOCK based on certain schedule, and doors can automatically get back to normal state, once the system time is out scheduled.

ELEVATOR CONTROL
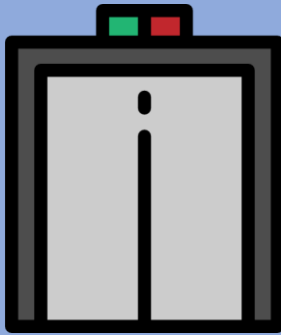
There are two approaches to control elevator.

- Reader Inside the Elevator (Cab Reader)
- Reader outside the Elevator

Out Reader: It works much like normal door; the Door Strike relay must be connected to Elevator panel unlike Door Lock.

Cab Reader: In this case, the Reader and Reader Interface will be installed inside the Elevator, Group Output/Multiple Relays will be generated though Output Interface (V-300) based on the Elevator Group authenticated.

Following are the major elements involved

- Elevator Reader
- Elevator Group
- Card Access to Elevator Group
- Group Output with Output Interface (V-300)

Alarm Management

ALARM MONITOR

Event/Alarm Messages generated real-time on hardware are displayed on screen for operator to view and take appropriate action with respect to the message.

The messages are broadly categorized into following

- Access Grants or Denials
- Doors Held or Forced
- Input Point state changes
- Hardware Alarm state changes
- Task start, stop, or restart status

LIST VIEW BASED UI

List based UI provides a rich and easy interface for operator to monitor the logs in real time.

It is divided into two parts, one for Access related logs and the other is for rest of the alarms

It also provides an option for operator to send real time commands to perform access related operations such as open door, unlock door and reset card/door status etc.

LIST OF ACS ALARMS

Following are the list of ACS alarms generated in real time

GRANT ACCESS
GRANT ACCESS EXTENDED
DENY ACCESS NO DOOR ACCESS
DENY ACCESS DOOR SCHEDULE
DENY ACCESS UNKNOWN READER
DENY ACCESS CARD / PIN DELETED
DENY ACCESS WRONG PIN
TIMED ANTI-PASS BACK VIOLATION
REAL ANTI-PASS BACK VIOLATION
AREA VIOLATION
REAL ANTI-PASS BACK VIOLATION EXIT
AREA VIOLATION EXIT
DENY ACCESS-DOOR GROUPS/SCHEDULES NOT CONFIGURED
DENY ACCESS NOT ACTIVE

LIST OF OTHER ALARMS

Following is the most common door or I/O alarms

DOOR STATUS	
DOOR IS OPEN	
DOOR IS CLOSED	
DOOR HELD OPEN	
DOOR HELD CLOSED	
DOOR FORCE OPEN	
DOOR FORCE CLOSED	

| DOOR COMMANDS	
DOOR OPEN COMMAND	DOOR UNLOCK/GRANT
FREE EXIT / REX ON	FREE EXIT / REX OFF
TAMPER ALARM ON	TAMPER ALARM OFF
AC POWER FAIL ON	AC POWER FAIL OFF
BATTERY FAIL ON	BATTERY FAIL OFF
FIRE INPUT ALARM ON	FIRE INPUT ALARM OFF
INTERCOM ALARM ON	INTERCOM ALARM OFF
EMERGENCY GLASS BREAK ON	EMERGENCY GLASS BREAK OFF
BUZZER ON	BUZZER OFF
LED INDICATOR ON	LED INDICATOR OFF

Health Check-Up
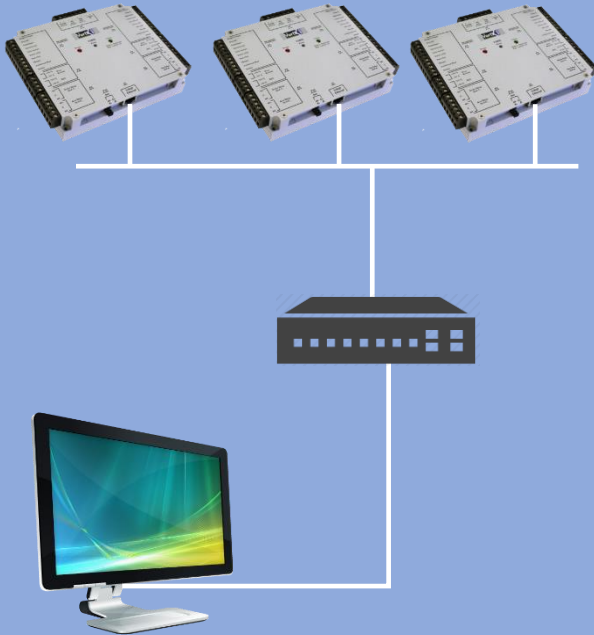
As the name implies it helps to identify the controller communication status and address if any issue persists. It is divided into two parts based on mode of request and response between host and controller.

1. **Controller to host**: in this case all the controllers are enabled to send a message to host at certain interval to indicate its working status. The status of the controller is presumed to be online, offline or suspected. if there is a delay in receiving the message from controller than the predefined interval then it is marked as suspected, and wait for some more time (configured interval) and then it marks as offline if there is no message from respective controller, or else online.

2. **Host to controller**: this works like that of ping, operator can send a ping command to select all controllers, either online or offline status will be marked based on the result of ping command.

The list of controllers(s) with status (only suspected/offline) shall be notified to concerned security operator or admin via email to take necessary corrective action.

Mustering
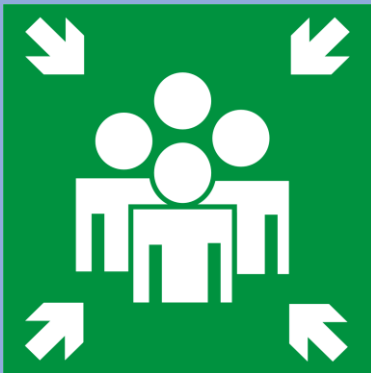
Mustering process utilizes the access control readers that are installed at designated mustering points to generate the list of card holders at any point of time segregated based on area. The card holders in the building can be consulted and checked off as they're accounted for.

The readers in mustering system are categorized into three different types such as **Head Count, Assembly Point** and **Roll Call**.

Roll call: List of card holders at danger zone need to be evacuated on higher priority
Head Count helps to track the number of people at designated area such as canteen, library etc.
Assembly Point indicates the list of people who are at safe place.

Guard Tour
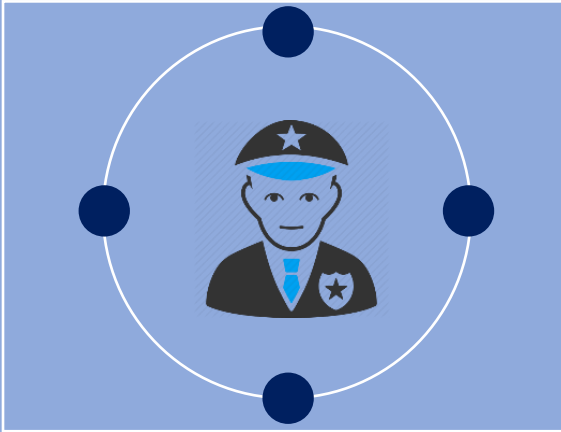
Guard tour system helps organizations to execute the patrolling process and to track that the officers will accomplish their tasks within the predefined time intervals.

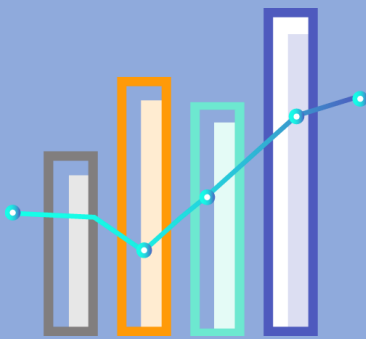Patrol plan includes Route, Interval, and Rounds in a day.

Route: List of checkpoints in an order

Interval: A time difference b/n each check point

Rounds: One or more cycle in a day (different starting interval)

Roster: A day on which guard will be assigned with a patrol plan

Reporting

ESS application generates sophisticated grid or template based reports grouped into respective categories with various filter options.
• EMPLOYEE DETAILS
• CARD DETAILS
• READER DETAILS
• ACCESS DETAILS
• MUSTERING
• GUARD TOUR
Reports can be filtered based on
• DATE RANGE
• DOOR GROUP
• COMPANY, DEPARTMENT and DESIGNATION   Many More...

The generated report can be exported to Excel and PDF format

ACS Reporting List

Cards List	Roll Call
ACS Logs	Head Count
Door List	Assembly Point
Door Group List	Guard Tour
Door Group Details	Guard Tour Reader List
Schedule List	Guard Tour Checkpoint list
Access Group List	Fire Alarm Report
Access Group Details	Mobile Punch Location
Trace Access	Alarms
Parking	
Video Access Point	
Intercom	
Visitors	
Track Recent Location	

END OF STATEMENT

IRIZ ID

Technologies

WE INDENTIFY SECURE AND INTEGRATE