Fault Tolerant Intelligence Controllers

A/E Guide Specification

January 4, 2015
Revision: 2.01

PCSC makes no representations or warranties with respect to the contents herein, and disclaims any implied warranties of operation for any particular purpose. Further, PCSC may modify this document without obligation to notify any person of any such changes or revisions.

Third Party Trademarks: All other trademarks, trade names, or company names referenced herein are used for identification only and are the property of their respective owners.

PCSC
3541 Challenger Street
Torrance, California  90503-1641
Phone: +1 (310) 303 3600
WEB:  www.pcscsecurity.com
E-Mail: Sales@1PCSC.COM
## Acronyms Used in this Document

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>DDM</td>
<td>Dual Door Module</td>
</tr>
<tr>
<td>DIM</td>
<td>Door Interface Modules</td>
</tr>
<tr>
<td>FTNA</td>
<td>Fault Tolerant Network Architecture</td>
</tr>
<tr>
<td>FTC</td>
<td>Fault Tolerant Controller</td>
</tr>
<tr>
<td>LED</td>
<td>Light Emitting Diode</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet</td>
</tr>
<tr>
<td>REX</td>
<td>Request to Exit</td>
</tr>
<tr>
<td>RISC</td>
<td>Redundant Instruction Set Computer</td>
</tr>
<tr>
<td>RDNA</td>
<td>Realtime Dynamic Network Architecture</td>
</tr>
<tr>
<td>SDM</td>
<td>Single Door Module</td>
</tr>
<tr>
<td>SMS</td>
<td>Security Management System</td>
</tr>
<tr>
<td>UPL</td>
<td>User Programmable Language</td>
</tr>
<tr>
<td>VDC</td>
<td>Volts Direct Current</td>
</tr>
<tr>
<td>VFD</td>
<td>Vacuum Florescent Display</td>
</tr>
</tbody>
</table>
1. **System Overview**

1.1. The System shall be designed to provide the highest means of reliability and incorporate an automated process of system recovery utilizing a Fault Tolerant Network Architecture (FTNA). The FTNA shall include Host, Fault Tolerant Controllers (FTC) and Door Interface Modules (DIM). The FTNA system may be designed with an “Active/Active” or “Active/Inactive” system architecture. An Active/Active architecture shall provide a “hot” redundant backup of a FTC. If for any reason, a primary controller fails, an “Active” FTC shall automatically take over the duties of the failed FTC. The progression of successors to a faulty FTC shall continue to provide security without any degradation. In an Active/Inactive Architecture, a backup FTC shall be included for the sole purpose as a backup controller.

1.2. A FTNA shall utilize Real-time Dynamic Network Architecture (RDNA) enabling automatic recover of the system due to:

- [x]... Communication Failure
- [x]... Controller or Firmware Failure
- [x]... Power Failure

2. **System Characteristics**

1. Fault Tolerant Controller

1.1. The FTC’s design shall incorporate open modular design techniques utilizing an Open Standards Operating System.

1.2. Communication between the Host, FTC and DIM shall be based on an “open standards” protocol utilizing “peer to peer” communications.

1.3. The DIM controllers shall be available in 2 configurations, a Dual Door Module (DDM) and Single Door Module (SDM).

1.4. Utilizing “Peer to Peer Communications” the FTNA shall provide an automated intelligent means to synchronize data between FTCs. New or existing FTCs shall not require the Host to be online to update their database and status information for card database, historical transactions, inputs and outputs.

1.5. The FTC shall be a 100% distributed intelligence architecture. Any requirements for Host intervention to process card authorization, Entry Exit, alarm processing or output linking shall not be accepted.

1.6. The FTC shall maintain the entire cardholder database. Host entry of a
Fault Tolerant Intelligent Controllers
cardholder shall automatically be downloaded to every appropriate
controller. Any system that requires Host intervention to make access decisions shall not be accepted.

1.7. The FTC shall be designed to facilitate a “Virtual Point Definition” network.

1.8. The FTC is used as the sub-system to the Security Management System (SMS) for the purpose of initiating all decisions based on parameters and criteria as it relates to the cardholders and associated hardware connected devices. Decisions and events transpired at the FTC are uploaded to the Host System as transactions events. All transactions shall be logged with transaction type and the time of occurrence (Date and Time (HH:MM:SS)).

1.9. The SMS shall record all transactions with a “received” time stamp. This time stamp shall record when the transaction was “stored” at the SMS. Transactions reports shall be available to be sorted by the “Stored” or “Occurred” time stamp.

1.10. The system shall operate with 100% intelligence without the need for the host to be on-line. All parameters such as holidays, daylight savings, automatic door openings, automatic card activations, deactivations and output schedules shall be stored within each FTC to process decisions for up to 1 year without the need for Host intervention.

1.11. The FTC shall have a vacuum florescent display interface (VFD) to display the Fault Tolerant Network Status. Communication status of the Master Controllers and DIMs shall be displayed and updated in real-time.

1.12. The FTC series controller shall incorporate automatic firmware management. The FTC shall keep all DDM and SDM components of the system updated to the "approved" firmware version for the site without manual intervention.

1.13. Communications

1.13.1. Utilize the Hydra Communication Protocol

1.13.2. Provide a “Self Healing” Communication Architecture

1.13.3. Primary communications for FTNA network shall be Ethernet or PoE

1.13.4. Optional secondary communication path shall be available with:

   2.1.13.4.1Ethernet
   2.1.13.4.2XB Pro Digi Mesh

3. Card Authorization

3.1. The system shall provide the highest level of card authentication and cardholder authorization logic. Authorization of a card shall be determined with a minimum of the following:

3.1.1. Card Validity

3.1.2. Door Location

3.1.3. Date, Day and Time

3.1.4. Stale Time

3.1.5. Long Access

3.1.6. Entry Exit – Building, Department and Parking

3.1.7. Supervisory Access

3.1.8. Event Control
5. Escort requirements
5.1.1. Card Action Output

4. Features

1. Cardholders shall have the ability to be automatically “Activated” or “De-Activated” by date and time (mm-dd-yy hh:mm).
2. Cards shall automatically be de-activated from lack of use. A user specified “stale” time shall be available for automatic means of deactivating cards due to the lack of use.
3. Each Controller shall support up to 128 time periods
   3.1. A total of 12 start/12 stop intervals, per time period, shall be included.
   3.2. Support up to 4,000 authorization groups
   3.3. Each authorization group shall include one (1) time period.
   3.4. Each cardholder shall support four authorization groups.
   3.5. Each authorization group shall have an alphanumeric name description.
4. Support 365 user selected holidays.
5. Supervised inputs shall have the ability to be programmed to send alarms as they occur or provide a “latch” mode. A software latching circuit shall provide “1” transaction of the alarm per occurrence until acknowledged by the Host. Systems that can not throttle alarm transactions are not acceptable.
6. Ability to detect and differentiate “forced entry” and “door left open”. A separate output action is required for each door status.
7. Provide the ability for “local door alarm” processing. When a door is “left open too long”, a local door left open alarm shall enunciate. If the door is not properly closed within a user defined time, a “Door Left Open Too Long” transaction message shall be sent to the Host for alarm processing and user action.
8. Allow unused door logic, such as door strike relays, request-to-exit inputs, and door status inputs to be assigned as general-purpose points.
9. Automatically adjusts for daylight savings time and leap year independent of the host system.
10. Support a minimum of three (3) “Card Classes” which can be utilized with User Programmable Logic to interact with external devices or functions, such as lights, sirens, or HVAC.
11. Integrate each physical input independent of its polarity.
12. Support Local Door Left Open Alarm
13. Provide “2 Stage Alarm Monitoring”. To prevent nuisance alarms, local door left open alarm shall be activated prior to sending the door left open alarm to the host.
14. Maintain a second expiration date for each cardholder. This date shall be used to prevent access to a unique group of readers, such as parking lots or recreational facilities. Once the date has expired the card shall be disabled only for this group of readers.
Fault Tolerant Intelligent Controllers
Fault Tolerant Intelligent Controllers

15. Maintain three (3) access times for each door location; Standard, Long, and Egress.
   15.1. STANDARD access time shall be used for the majority of the cardholders and shall support a range from 0-254 seconds.
   15.2. LONG access time shall be assigned to cardholders who require extra time to enter/exit a location, such as delivery persons, or to meet American with Disabilities Act (ADA) requirements. The Long access time shall support from 0-254 seconds. A Long shunt time shall also be required to prevent a door held open alarm exceeding the standard shunt time. The time shall not require additional hardware nor be dependent on the host for the decision.
   15.3. EGRESS time shall be used for request to exit devices and support a time between 0 - 254 seconds.

16. Shall have the ability to maintain an automatic door unlock during specific hours and days. Opening and closures shall be independent of the Host.

17. Be required to activate the automatic unlock only after the first valid card access at that location within a pre-defined period of time to prevent false openings.

18. Support three (3) “zones” of Anti-Passback; Building, Department, Parking.

   19.1. Support three (3) “levels” of Anti-Passback; Strict, Soft, and Lenient.
   19.2. STRICT Anti-Passback will deny access to a cardholder if they attempt to reenter the same door. An alarm must be triggered to alert the Entry Exit error condition.
   19.3. SOFT Anti-Passback authorizes access with the use of the card on the second attempt at the same reader. An event message shall be forwarded to the host indicating entry/exit error.
   19.4. LENIENT Anti-Passback follows the Entry/Exit criteria and denies access upon detection of status violation but allows entry on subsequent attempt, while automatically synchronizing entry Status.

20. Utilize User Programmable Logic (UPL) for the manipulation of inputs, card status, outputs, and event control.

21. Each FTC shall allow the following inputs to trigger UPL:
   21.2. Physical Input Point
   21.3. Time periods
   21.4. Each FTC shall support the following computations for UPL:
       21.4.1. Activate or Deactivate
       21.4.2. Increment Count (range 0-65,000)
       21.4.3. Decrement Count (range 0-65,000)
       21.4.4. Increment by Seconds or Minutes (0-65,000)
       21.4.5. Decrement by Seconds or Minutes (0-65,000)
       21.4.6. Flip Flop Output Control
       21.4.7. Time Period Override
21.4.8. Generating “Events”

22. Threat Level Access Control
   22.1. The system shall incorporate 4 levels of “Security Threats”. Each level of threat will “automatically” provide a different set of access permissions for individual cardholders.

23. Escort/Visitor Control
   23.1. Maintain the assignment of access cards for Visitor Control. Each visitor shall be assigned an “Escort Required” status requiring an employee or “Escort Capable” cardholder to grant a valid entry. The decision shall not be dependent on the host.
   23.2. All visitor badges shall expire automatically at midnight of the date issued without operator intervention based on programmed expiration.

24. Two-Person Minimum Occupancy Rule (TPMOR) for high security applications.
   24.1. TPMOR shall be host independent. Any system requiring the host to maintain access decisions shall not be accepted.
   24.2. The TPMOR feature requires the first two- (2) people to badge into an area at the same time before access is granted. Once the area gains the 2 person occupancy, subsequent access shall be granted on an individual basis. Exiting the area shall require that the last 2 occupants exit at the same time. An exit reader shall be incorporated for decrementing the count.
   24.3. The TPMOR feature shall have the ability to determine the proper occupancy count during access by Escort Required and Escort Capable. The last 2 occupants shall not be the Escort Required and Escort Capable personnel.

5. Cardholder Parameters and Control
   5.1. Card Capacity and Features
      5.1.1. Support up to a 24 digit Card Number
      5.1.2. Support Department of Defense (DOD) Common Access Cards (CAC)
      5.1.3. Support FIPS-201 Card Format Requirements
      5.1.4. Support TWIC Card Formats and capacities
      5.1.5. Support a minimum of 10,000 and expandable to 100,000 cardholders
      5.1.6. Support a minimum of 10,000 and expandable to 100,000 historical transactions in the event communications to the host is disrupted.
      5.1.7. Provide Four Levels of Authorizations Groups per cardholder.
         5.1.7.1. Each level will shall provide four authorizations groups
      5.1.8. Card Activation and Deactivation by Date and Time
      5.1.9. Provide an “automated” means to deactivate cardholders from “lack of use” or “Stale” times definable in Days and minutes.
         5.1.9.1. Provide user selectable “Lack of Use” variables per individual reader.
Fault Tolerant Intelligent Controllers

5.1.10. Provide individual or group “Card Action” control for Output Control
5.1.11. Card Actions by Access denied
5.1.12. Individual “Event Override” capabilities for Supervisory Control
5.1.13. Escort Control by reader
5.1.14. TPMOR
5.1.15. Each FTC card transaction shall be time-stamped with the following:
    • Date (MMDDYYYY - DDMMYYYY) minimally
    • Time (Hours, Minutes, Seconds)
5.1.16. Message Text (Description of transaction)
5.1.17. Support cardholder names in addition to the cardholder ID number

6. FTC Hardware Requirements
6.1. The FTC and DIM shall utilize a 32 Bit CPU architecture utilizing Redundant Instruction Set Computer (RISC) for higher reliability and performance.
6.2. The operating system of the FTC shall be Open Systems Architecture. Proprietary operating systems shall not be acceptable.
6.3. FTC shall have standard LED arrays for Status Display with optional text display capabilities with Vacuum Florescent Display (VFD).
6.4. The Controller will provide a visual means to indicate connection status to the Host.
6.5. Reader’s Visual User Interface
6.5.1. Reader shall provide transaction “Status” utilizing the red and green LEDs.
   6.5.1.1. Power - Constant display of the Red LED
   6.5.1.2. Card data being processed - Fast blink Red and Green LEDs
   6.5.1.3. Access authorized - Solid Green LED
   6.5.1.4. Denied access - Constant Red LED after card data processing
   6.5.1.5. Escort Required - Slow blink Red/Green LED’s until the second card is read.
   6.5.1.6. Two Man Rule - Slow blink Red/Green LED’s until the second card is read.
6.6. Card data read errors of four (4) or more within one minute shall be reported back to the host.
6.7. Support the following minimum card/reader technologies:
   1. Multi-Technology (Proximity and Smart)
   2. Proximity
   3. Smart Card
   4. Biometrics
      4.1. Finger Print
      4.2. Finger Vein
      4.3. Hand Geometry
      4.4. Iris Scan
Fault Tolerant Intelligent Controllers

4.5. Palm Vein
4.6. Facial Recognition

2. Magnetic Stripe
3. Vehicle Identification
4. Bar Code
5. Keypad

8. Simultaneous support of multiple card technologies.
9. Simultaneous support of multiple card formats without card number duplication.
10. Support Card plus PIN, card or PIN only type readers.
11. Standard LED displays to represent:
   11.1. Power
   11.2. Host Online status indicator
   11.3. Input Status
   11.4. System Status and Diagnostics
   11.5. Real-time Error Displays in “text” format

12. Power
   12.1. Power for the FTC shall be provided by:
       12.1.1. Internal Power Supply
       12.1.2. External Power Supply
       12.1.3. PoE

13. Power shall be monitored by the FTC and provide alarm notification upon:
   13.1. AC Power Fail
   13.2. Low Battery Conditions

14. Battery protection for the onboard memory for programmed data and history transactions for a minimum of one (1) year without power.
15. Provide accurate Date and Time for up to one (1) year where no power is being supplied to the controller.
16. Maintain historical information for a minimum of one (1) year where no power is being supplied to the controller.
17. Installation and Enclosures
   17.1. The FTC controllers shall have the option for wall mount and standard rack mount enclosure (2U).
   17.2. Enclosure shall be equipped with an overall “power” LED on the outside of the cabinet for safety.

18. Managed Firmware Update of Door Interface Modules
   18.1. The current version of the DIM firmware will be automatically managed and updated by the FTC. Firmware versions will be displayed by the Host System to ensure firmware compatibility.
   18.2. In the event of a “new” or replaced DIM, the FTC system will automatically, check, verify and update the firmware as needed.
7. Door Interface Module (DIM)

7.1. Door Interface Modules shall be available in a minimum of 2 types, Dual Door (DDM) and Single Door Modules (SDM)

7.2. Each DIM shall support the appropriate minimum of interfaces:
   7.2.1. Wiegand interface reader port
   7.2.2. Door Position Status
   7.2.3. Request to Exit (REX)
   7.2.4. Relay outputs for 12 or 24 VDC locks
   7.2.5. Additional general purpose inputs and outputs

7.3. Support a variety of reader technologies. Only non-proprietary readers shall be approved. Include manufacturer, model number and cut sheet with proposal.

7.4. All readers shall be electronically supervised on the Wiegand interface. The DIM shall automatically notify the host upon reader failure or vandalism to the reader. Mechanical or optical detection methods shall not be accepted.

7.5. The DIM shall have the ability to assign different reader technologies and formats for each reader. The controller shall not be limited to any one type of reader technology. Each DIM shall support a minimum of technologies as reader ports.

7.6. High Security Alarm Monitoring
   7.6.1. DIM inputs shall have the ability to have software configurable input selection (dry contact, supervised input or temperature).
   7.6.2. All supervised inputs shall provide 5 states of supervision (Normal, Alarm, Short, Open and Calibration fault). The system must be capable to detect when an input point is about to “false” due to weather elements such as corrosion.
   7.6.3. Supervised points must automatically calculate a 5% variance from normal. Mechanical adjustments of alarm points are not acceptable.
   7.6.4. Supervised calibration of each point must be “automatically” calculated. The resistance caused by the size of cable or distance from the controller shall not impede the alarm detection circuit.
   7.6.5. The system shall provide an “Adaptive Supervised Calibration Mode” to incorporate the use of existing end of line resistors (EOL).

7.7. Standard LED displays to represent:
   7.7.1. Power
   7.7.2. Communication
   7.7.3. MC “Online” Status indicator
   7.7.4. System Status and Diagnostics
   7.7.5. Real-time Error Displays in Text
   7.7.6. Adaptive Calibration Notification

7.8 Power
   1. Power for the FTC shall be provided by:
      1.1. PoE
      1.2. UL Listed External Power Supply
2. Power shall be monitored by the FTC and provide notification upon:
   2.1. Primary Power Fail
   2.2. Low Battery Conditions

8. Execution
   8.1. The supplier shall install all system components and appurtenances in accordance with the manufacturer’s instructions, and shall furnish all necessary interconnections, services, and adjustments required for a complete and operable system as specified and shown. Control signal, communications, and data transmission lines grounding shall be installed as necessary to preclude ground loops, noise, and surges from adversely affecting system operation. Provide mounting hardware as required. Installation shall be in accordance with State and Local laws governing security system installations.
   8.2. All low voltage wiring outside the control console, cabinets, boxes and similar enclosures, shall be plenum rated where required by code. Cable not pulled through conduits or placed in raceways, outlet boxes, junction boxes, or similar fittings with other building wiring.
   8.3. The supplier shall perform system testing to ensure it is operable to the manufacturer’s specifications. The test report shall be submitted to the customer for approval and sign-off.

9. Warranty
   9.1. The access control system shall be warranted for a period of one (1) year from the date of acceptance.
   9.2. The supplier shall provide all services required to maintain the system in an operational state as specified by the manufacturer for a period of one (1) year after acceptance.
   9.3. The system supplier shall include a line item bill of materials included in the project and the warranty associated with each.
   9.4. The system supplier shall maintain equipment stock for any high-usage equipment.