## The Latest in Access Control Technologies

Fault Tolerant Controllers – Product Information

Fault Tolerant Security System U.S. Patent No. 7,644,299

(4 pages)

**In this article:**

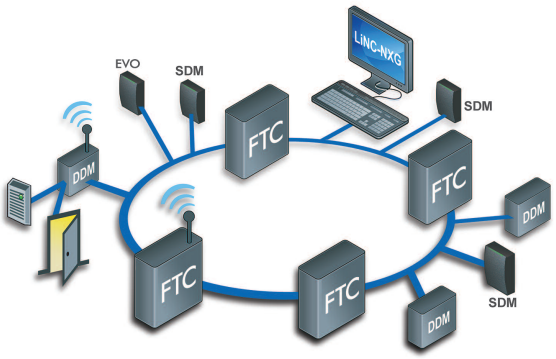


# INTRODUCTION

Security systems can be categorized into 2 types of network architecture:

**Type A** - Host to Distributed Intelligence Controller(s)
**Type B** - Host to Master Controller(s)-Sub Controller(s)

A "cluster" is defined as a controller or group of controllers with its peripherals (readers, lock, REX, door status, etc.). A cluster failure in Type "A" architecture would only affect the performance of the failed cluster. In the case of a Type "B" architecture, the Master Controller and the sub controllers is the "cluster". In either method, a failure of a cluster will degrade the performance of the system. In the case of a Type B architecture, the loss of the Master Controller is devastating, since the application services for the Sub Controllers are dependent on the operations of the Master Controller. The Type B architecture poses a high risk of a single point failure.




To increase the reliability and the responsiveness of existing security systems and networks, a Fault Tolerant Architecture (FTA) has been developed. The FTA is a system that supports redundancy with controllers, even with its communications for the highest level of operation, reliability and security.

**Fault Tolerant Systems (FTS)** Fault tolerance is available in LiNC-NXG™, LiNC-PLUS® and LiNC-XS™ providing the highest level of reliability and scalability for any security application. The FTS is comprised of a Host (LiNC-NXG, LiNC-Plus or LiNC-XS), a cluster or group of clusters comprising of a Controller (FTC) and Door Interface Module (DIM). If a Fault Tolerant Controller (FTC) becomes unavailable for any reason such as hardware or firmware failure, even during a routine maintenance, an alternate FTC immediately begins providing full service to the network of DIMs. Inherent in the FTA is the process of automatically transferring operations to another FTC is called a "hot fail-over". The FTC can be designed to support "active/active" or "active/passive" network topologies. The FTA utilizes "Peer-to-Peer" communication techniques, automatic database synchronization amongst the FTC within its network or "Clique". Features and processes like "Global Anti-passback", "Global Input/Output" control no longer require a "Host" to be available to make these decisions.

**FTC** – A controller with 100% distributed intelligence for Access Control, Alarm Monitoring, Output Control, Elevator Control and Building Management applications utilizing an "Open Standards" operating system. Each FTC is capable of maintaining the entire cardholder database, transaction logs and system parameters for all of the application designed for the FTC.

**DIM** – A sub controller designed to receive card reader information, manage and operate access authorization, entry exit logic, alarm monitoring and output control. DIMs are offered in 2 door and 1 door configurations. The 2 door configuration is the DDM (Dual Door Module) and the 1 door is the SDM (Single Door Module).

**Active/Active** – A system architecture having 2 or more FTCs. Each FTC having control and monitoring of DIMs, If one FTC fails, the operations of the failed FTC are automatically transferred to one or more of the remaining FTCs, providing seamless security operations.

**Active/Passive** – A system architecture where a FTC or a set of FTCs can be assigned as the "hot backup" to another. The duties of the "hot backup" FTC is strictly for the operational backup to the primary FTC. The "passive" FTC can be the backup to one or many FTCs.

**Fault Tolerant Communication Services (FTCS)** – Multiple communication options are available in the Fault Tolerant Architecture. Standard communication is Ethernet but upon primary communication failure, the FTC has the ability to automatically "switch" to an alternate communication mode. The FTC can support up to three simultaneous communication modes (Ethernet, PoE and ZigBee Pro Wireless) with each mode being the alternate communication for alternate communication routing.

**Network Load Balancing (NLB)** – The Fault Tolerant architecture enables security NLB utilizing FTC assignments for card authorization, Input and Output transaction handling increasing the security and responsiveness of the security network.

**Cluster (Clique) Topologies** – Unlike current systems, the FTA enables FTCs to create virtual connections between "points" and controller. The inherent flexibility within the architecture can provide a robust enterprise network solution to meet any security configuration.

## BENEFITS

| | |
|---|---|
| **Higher Reliability** | The FTA is designed to eliminate a single point-of-failure. Security applications are distributed over multiple FTCs, achieving a redundant application network at the controller level. |
| **Scalability** | One can increase the population of FTCs, increasing reliability and responsiveness with each addition FTC within a Clique. |
| **Manageability** | The FTA architecture appears to the user as "One" single-system image and provides a single point of control to administer, whether it is locally or remotely accomplished. |

## FEATURES

### System Features

- Fault Tolerant Process
- Automatic Hot Cutover
- Fail Safe Operations
- Open Systems Platform
- Open Architecture Protocol
- Peer-to-Peer Communications
- Homeland Security Threat Level Control
- Automatic Alternate Communication Routing - up to 3
- Access Action for Disabled Persons
- Supervisory Controlled Entry Authorization

(Features cont'd)

- Event Control Card Logic
- Cardholder or Card Group Action
- Stale Card Processing
- User Programmable Input Action
- Dynamic Input to Output or Group Output Linking
- 3 Levels of Anti-Passback Control
- Automatic Card Activation and Deactivation by Date and Time
- User Configurable Cardholder and History Capacity
- User Selectable Input Monitoring Modes

**High Security Features**

- "Threat Level" Card Authorization Logic Two
- Person Minimum Occupancy Rule Escort Capable
- and/or Required
- 5 State Alarm Monitoring
- 2 Stage Alarm Control
- Alarm Latching
- AC Power Fail Notification
- DC Low Power Notification Supervised Readers
- Supervised Tamper
- Supervised REX
- Designed to be 99.9999% reliable and available

## Hardware Features

**FT System Controller**

- 32 Bit Processor and Architecture
- Onboard 10/100 TCP/IP communication
- 3 Communication Ports
- 7 Segment Real-time Status Display
- Host Online Status Notification LEDs
- Electronically Protected Power Input
- 3 - USB 2 Ports
- FLASH Memory
- Up to 16 MB RAM
- Optional Vacuum Florescent or LCD Display
- Real-time FTC and DIM Status Display
- Optional SD Memory (up to 16 Giga Bytes)
- Supervised Tamper Switch
- Battery Charger Output
- 1 Year Battery Backed Memory and Clock Calendar

**DDM Sub System Controller**

- 32 Bit Processor and Architecture
- Onboard 10/100 TCP/IP Communication
- 3 Communication Ports
- Host Online Status Notification
- Electronically Protected Power Input
- 3 - USB 2 Ports
- FLASH Memory
- 2 Wiegand Reader Ports
- 2 Door Status Inputs
- 2 REX Inputs
- 2 Form C Relay Outputs
- 2 Voltage Outputs
- Supervised Tamper Switch
- Battery Charger Output (12 VDC)

**SDM Sub System Controller**

- 32 Bit Processor and Architecture
- Onboard 10/100 TCP/IP communication
- FLASH Memory
- 1 Wiegand Reader Port
- 1 Door Status Input
- 1 REX Input
- 1 Form C Relay Outputs
- 1 Voltage Outputs
- Supervised Tamper Switch

## Reader Technologies

- Multi-Technology Reader (Proximity, Mifare, DESFire, compatible with ISO 15693 and 14443)
- HSPD Card Formats
- Proximity
- Smart Card
- Magnetic Stripe
- Biometric
- Bar Code
- Keypad

## Capacities

- 20,000 - 250,000+ Cardholders (user configurable)
- 20,000 - 60,000+ History Transactions (user configurable)
- 1 to 32 DIMs per FTC
- Simultaneous Multi Card Format Recognition
- Multiple Site Codes (16)
- 16 - 512 Five State Inputs Supervision*
- 16 - 512 Temperature Monitoring*
- 16 - 512 Relay Outputs*

* Please consult your PCSC representative for configuration availability

## Communications

- 10/100 TCP/IP (Standard)
- PoE (Power over Ethernet)
- ZigBee™ Pro Wireless with MESH technology

## SUMMARY

The Fault Tolerant Architecture offers the highest level of reliability thus providing the highest level of security. The enhanced network and controller features provide automatic failover capabilities to enhance system reliability which are not available on any other system.

The FTA system can be designed and implemented to prevent any loss of security. The system configuration is not limited to the “fixed” architectures found in today’s systems.