Understanding Physical Access Control Architecture

A brief overview

Before exploring the architecture, it's important to define the system. A physical access control system (PACS) is a type of security platform that manages and controls who is allowed to enter a facility or environment. It identifies enrolled cardholders with credentials that have been granted specific access privileges. If the credentials are authenticated, a permission based access level will allow entry. The system is comprised of both hardware and software.

The typical Physical Access Control System (PACS) Architecture is a myriad of electronic hardware consisting of Access Controllers, Host PC's with Management Software and various types of Card or Biometric Readers connected to doors, gates, turnstiles, parking garage arms and other physical barriers.

This access control architecture is referred to as "distributed intelligence", with printed circuit board (PCB) panels termed "intelligent controllers". These controllers are networked to readers, which often contain their own level of onboard intelligence. Readers function as "edge" or peripheral devices, meaning they reside at the outer limits of the system, near doors for instance. Imagining spokes on a wheel, most PACS systems link back from their edge devices to the central hub, an intelligent controller. The controller is programmed and managed by a host computer using Physical Security Information Management (PSIM) software.

When a credential, whether a physical card, virtual card (mobile device), or form of biometrics is presented to a reader, the information is quickly analyzed by the system. The PSIM software grants or denies access, while also storing transactional data, referred to as "history". Historical data can generate "reports", and an audit trail is created. Today, this software and its corresponding data can also reside in the "Cloud", a virtual host, usually accessible through the internet. As a result, remote management and enterprise opportunities are further realized.

An access system can be integrated with other security sensory components such as motion detectors, video cameras, lights, sirens, burglar and fire alarms and more. The PSIM software is a critical component to manage these different resources. The software graphical user interface (GUI) aids in visually displaying and managing system statuses, real-time alerts, live and recorded video, reports and cardholder information.

Architectural weaknesses are present in nearly all typical access systems. The point of failure can reside anywhere in the system, from the software to the various hardware components. In a typical architecture, if one access controller fails, the whole system will fail. Mitigating failure points throughout will result in a more secure system.

One solution to lessen the impact of controller failure, is the patented Fault Tolerant Architecture (FTA). This type of

Continues…

Understanding Physical Access Control Architecture

A brief overview

Continued…

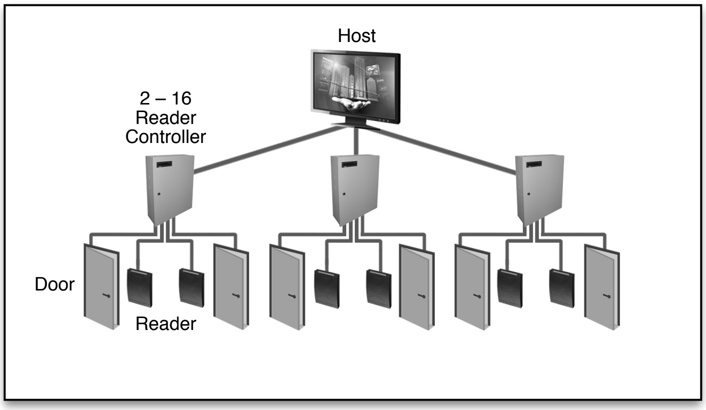
system is designed to increase “up time”, making the system extremely reliable.

The FTA may be designed with an “Active/ Active” or “Active/Inactive” architecture. If for any reason, a primary access controller fails, an alternate controller automatically takes over the duties of the failed controller. The system remains fully active, the progression of successors to a faulty controller continue to provide security without any degradation in system operations.

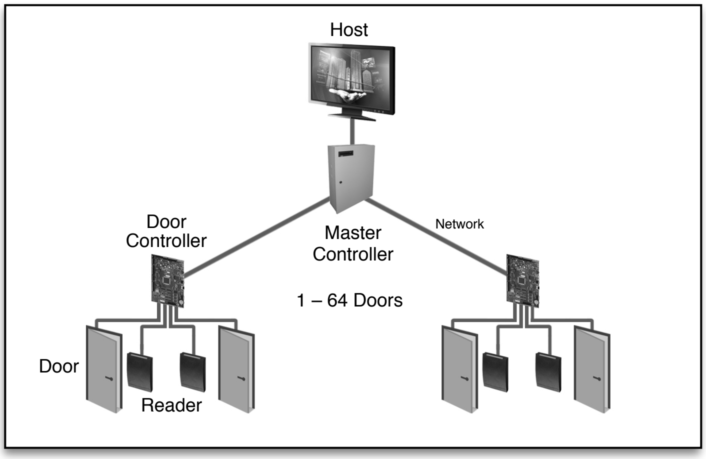
The FTA utilizes a series of Fault Tolerant Controllers (FTC) and sub-systems, termed Door Interface Modules (DIM) to ensure a higher level security architecture. Installation and maintenance costs are reduced due to the automatic hot cutover process and IP friendly hardware. In addition to Power-over-Ethernet, the FTC also features redundant communications, such as wireless.

To ensure the highest level of availability, it’s important to understand the advantages of redundancy at the controller level, which the FTA provides. This should not to be confused with the methodologies used for redundant servers operating the PSIM software. Without the true redundancy of the access controllers via the FTA, critical alarms could get ignored.

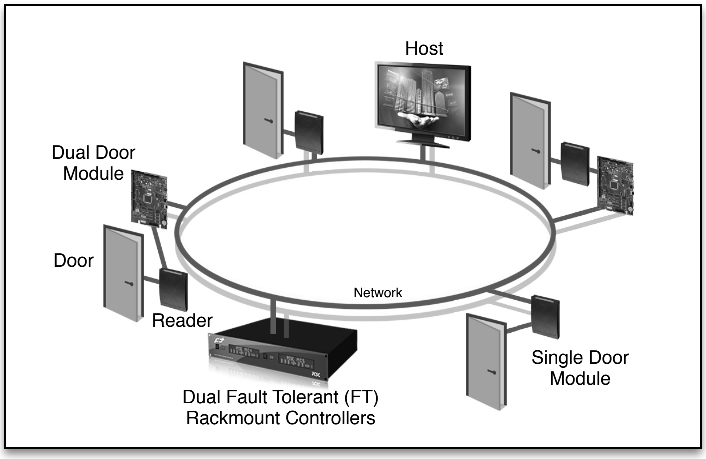
Distributed Intelligence Architecture



Master Controller Architecture



Fault Tolerant with Virtual Point Architecture


Host
Dual Door
Module
Door
Network
Reader
Single Door
Module
Dual Fault Tolerant (FT)
Rackmount Controllers