

Fault Tolerant CONTROLLERS

What they are and why we need them

By Steve Bowcut

It was the proverbial dark and stormy night. The access control and security system master controller located on the fifth floor of a high rise building just experienced a total failure. It's totally dead to the eight door interface modules for which it is supposed to provide intelligence and monitoring. In a world where security is a concern and system survivability matters, this could be a critical situation. A situation that many building managers have experienced and one for which they routinely lose sleep in anticipation.

In this situation, however, things are different. In fact, even in the morning when a call is placed to the security system service provider there is no excitement, no anxious rush to get a service technician dispatched to replace the dead processor. The dispatcher calmly tells the building manager that they will replace the controller on their next regularly scheduled maintenance call in a few weeks and at their standard labor rate. The building manager is calm and un-frazzled. What is going

on here? Is this a story about the indifference of a security system service provider, or something more? In this case, it's a story about how the newest innovation in the access control industry is changing how we look at critical equipment failures.

In the scenario depicted, the errant master controller is part of a Fault Tolerant system. As the name describes, this system is tolerant of equipment failures, in fact, it makes no difference to the performance of the system whether that particular master controller works or not. These new systems use a redundancy methodology that allows any master controller on the system to step up and take the place of any other master controller on the system. You could conceivably lose every master controller on the system except one and the system will continue with little or no perceptible degradation in performance.

Distributed vs. Subservient

There are two primary hardware architectures employed in the access control industry. One is the "dis-

tributed" architecture; named this because the intelligence of the system is distributed to each and every control panel in the system. With a distributed architecture, each card reader and its associated input and output points are connected directly to an intelligent controller.

The other common architecture is the master controller/door controller style (or what we used to call master/slave). With this configuration, the master controllers are the only intelligent component of the system and each door is connected to a "dumb," or at least "dumber," door interface module.

The advantage of the first type of system described here is that since the intelligence (database storage and decision making ability) is distributed to each panel and the number of doors connected to each panel is limited (commonly only 12 to 16 doors maximum), the risk of losing more than a few doors from the system due to any one hardware failure is very low. Even a catastrophic failure of a controller will result in the loss of only the 12 to 16 doors con-

nected to that panel, while all the other doors on the system would be unaffected. In contrast, the master controller/door controller configuration could conceivably put up to 128 doors in degrade mode if one master controller fails. The advantage of the master controller/door controller schema is the low cost associated with having fewer intelligent (and therefore more costly) controllers on the system.

Each service provider in the security industry has had to evaluate the pros and cons of these two architectures to arrive at the best solution to meet any specific access control application. Both are valid designs, and depending on how critical it is that the system stay up and operating or the size of the end-user's budget, either design could be more appropriate. In large part, manufacturers of access control hardware subscribe to either one or the other of these two architectural philosophies and will defend it vehemently.

Fault Tolerant Systems

New fault tolerant systems offer the service provider and the end-user the best of both worlds. They use the more cost-effective master controller/door controller architecture, yet offer system survivability that surpasses even the most conservatively designed distributed intelligence systems. Having the ability to fall back to any other master controller on the system is only the tip of the iceberg for these new systems. Their redundancy is really three-fold. A truly fault tolerant system offers redundant master controllers, redundant host computer and redundant communication paths. Redundant controllers were described above. Redundant host computers have been available for years with varying degrees of success. Sometimes done with third-party software and sometimes inherent to the access control software itself, this type of high-availability processing is not new. A very forward thinking designer might, however, incorporate today's new fault tolerant servers (up to "five-nines" availability using only one machine) with today's new fault tolerant controllers.

Although not altogether new in concept — since we have for years used such stratagems as auto dial backup — fault tolerant controllers bring new advances in redundant communications. With today's new fault tolerant access control systems, you can choose from several different backup or secondary communications protocols. You can opt to use a LAN as your primary communication path and then have another LAN, wireless network, hardwired RS485 or even a dialup

ers have to use the latest technologies available in every aspect of the design. This principle is manifest in fault tolerant access control systems. These new systems sport such advanced features as automatic data propagation. When a new fault-tolerant master controller is added to one of these systems, all the information the new controller needs to operate as an integral part of the system can automatically be transferred from either the host computer or from another master controller in



The Fault Tolerant controllers from PCSC use a redundancy methodology that allows any master controller on the system to step up and take the place of any failing master controller on the system.

modem serve as a secondary, tertiary or quaternary communication mode. This three-tiered redundancy of host, controller and communications offers a level of reliability that truly does make it seem as if the system will continue to work as it was programmed until the system is dismantled and put back in its box.

The Latest in New Technologies

One advantage of totally redesigning a product, as opposed to continually trying to modernize an existing product, is the ability the design-

the system. No human intervention is required to give the new controller the data and system parameters it needs to become a part of its new environment. Inputs and outputs are now global in their reach. Any input on the system can trigger any output and this can be based on any event, anywhere on the system — and none of this is dependant on the host computer or even any specific master controller.

This flexibility is an inherent consequence of the system's fault tolerant characteristics. These new

Although not altogether new in concept — since we have for years used such stratagems as auto dial backup — fault tolerant controllers bring new advances in redundant communications. With today's new fault tolerant access control systems, you can choose from several different backup or secondary communications protocols.

systems naturally incorporate 32 bit CPUs and can take advantage of today's advanced Power over Ethernet (PoE) technologies as well.

What Cost?

Possibly the most attractive feature of these new systems is the price. Fault tolerant systems are priced to compete with systems using standard designs. Thus far, the marketing scheme seems to be that these high-availability systems will be used as a tool to capture market share for

those manufacturers that offer them as opposed to becoming a high-priced optional feature, which is good news for the end-user. This marketing approach ensures that fault tolerant systems will become commonplace more quickly than if the new design remained a high-price option. If the end-user or system designer is faced with the question of whether or not to implement fault tolerant architecture and for little or no extra cost, it's a "no brainer."

It will take some getting used to,

but soon the days of frantic calls to dispatchers in the middle of the night to fix an access control and security system that has mysteriously dropped offline will be gone. Soon we can all have the luxury of knowing that even if the controller dies and the host computer goes offline and the communications fail, our facilities will remain secure. It will be hard, but I'm sure we can all get used to it. **ST&D**



Steve Bowcut is a 20 year veteran of the integrated security systems market. He has worked for both service providers and manufacturers. Mr. Bowcut is currently the business development manager for PCSC, an access control systems manufacturer in Torrance, Calif. He can be reached at sbowcut@lpsc.com

INSTANT, LIVE VIDEO



Introducing The Next Generation in Surveillance Technology

ICOP Guardian IP cameras provide cutting-edge surveillance JPEG 2000 video, with scalable frame and bit rates and the ability to stream LIVE video over the ICOP LIVE Platform.

With a strong pedigree in Law Enforcement mobile surveillance systems, these stationary cameras can provide first responders with access to instant, high quality, LIVE video that has the potential to change the outcome of crisis situations.

ICOP[®]

ADVANCING SURVEILLANCE TECHNOLOGY

866.210.ICOP (4267)

www.ICOP.com

(Nasdaq: ICOP)

16801 W. 116th St., Lenexa, KS 66219
Tel: 913.338.5550 Fax: 913.312.0264

Circle Inquiry No. 240 or visit www.st-and-d.com and click on e-Inquiry