PCSC FT Controller

PCSC's Fault Tolerant FT Controller is part of the company's FT solutions which include controllers, door modules and software designed specifically to stave off threats posed by single point failures in network-based access control and alarm systems.

In just a little more than a decade, the network component of most electronic security systems has become so integral as to be routine. Whether it's DVRs in a server room, IP cameras at the edge on a shared subnet, or IP-based access control, part of most security systems lives on a network.

It's a change that has major implications in a number of areas, not least the imperative that security infrastructure no longer resides on bullet proof solid state boards supported by serial data comms. Obviously, the swing to IP has come with great benefits but there are threats too, mostly notably a need to guarantee network support of vital electronic security systems.

Into this breach rides PCSC, the manufacturer of Fault Tolerant FT Controller, an automated solution that's designed to offer full systems recovery for access control, alarm monitoring and output control solutions. Importantly, FT Controller is designed to automatically recover regardless of communication or controller failure.

A typical PCSC FT system is either active/active or active/inactive in its architecture and the way this works is that if there's a faulty primary controller in a given system, an FT Controller takes over the running of the system with no system downtime.

In terms of hardware, the system comprises one or more Fault Tolerant Controllers and a network of Door Interface Modules (DIMs) made up of Dual Door Modules and Single Door Modules. FTCs and DIMS use peer-to-peer communication employing PCSC's robust Hydra Protocol.

PCSC's managing director Mas Kosaka believes network components are now an integral part of all electronic security systems, including networked access control and alarm monitoring solutions.

"Every aspect of the security industry now utilizes networks," he explains. "The main advantage of networking is that it has created a common communication standard for access control, alarm monitoring and CCTV. It's a standard that manufacture, integrators and end users understand.

"Network infrastructures simplify system design yet they also bring issues that need to be understood

before designing and implementing a networked security project."

Something that has been a growing cause for concern is that the involvement of network components – particularly shared components of dubious age and quality – can weaken the operational integrity of electronic security systems.

One of the things that bothers many security professionals is that network components may or may not be designed to report faults that impinge on the security system. They also report these issues to IT people – perhaps the mobile phone of an offsite tech or support company.

"Designing a network infrastructure security system is not a trivial task and should include the assistance of network specialist," says Kosaka.

"The network is the lifeline and if anything happens to it, it could be catastrophic. It is critical to understand the weaknesses and provide proactive measures and provide status notification to the appropriate IT and security staff. There are many ways to get failure notifications. Your operating system will be one of the first to notify the network caretakers by SMS or Emails.

"Network stability is one of the most important aspects of any system especially a security system. Without the network, most systems could completely fail. System providers need to be aware of the pitfalls and provide alternative solutions to ensure system stability."

OPERATIONAL REDUNDANCY

For many years networked security solutions have been sold as 'leveraging existing infrastructure' but if reliability cannot be assured this is not an advantage. Given the fundamental importance of electronic security systems there's an imperative to isolate and strengthen the performance of security related networks, over and above general data networks.

"When networked systems emerged, many touted leveraging existing infrastructure but in some cases this proved to be disastrous," says Kosaka. "When sharing a network, one needs to understand bandwidth.

> "Our FT controllers have the ability to support three communication ports including an Ethernet port as a primary communication path, a PoE (Power over Ethernet) port as a secondary communication and XBee Pro Digimesh wireless port"

"Today's networks are measured in network speed, such as GigaBit rates - though speed is important, access control systems need to measure bandwidth in terms of availability," he says. "Access control systems typically do not send large amounts of data but are required to send it frequently to maintain real-time status with many components. I believe data and security are equally important and should have separate networks to maintain system stability."

But what does building fault tolerant networks mean from the perspective of the security subnets we generally see in the real world? How does an integrator build a solution that is part of the overall network yet completely fault tolerant in its own right?

"Staying in contact with all components in a system requires you to have a robust network," explains Kosaka. "Depending on the end user, network stability, though important, may not be a

> "Network stability is one of the most important aspects of any system especially a security system. Without the network, most systems could completely fail. System providers need to be aware of its pitfalls and provide alternative solutions to ensure system stability"

high priority.

"What we have done is design a solution that utilizes the system network but provides a secured wireless network just in case the system network fails.

"To achieve this, our FT controllers have the ability to support three communication ports. They have an Ethernet port as a primary communication path, a PoE (Power over Ethernet) port as a secondary communication and XBee Pro Digimesh as the alternative wireless communication port.

"PCSC's architecture is designed to meet the needs of users and does not confine the designer to specific system architecture," Kosaka explains.

"Unlike a fixed definition for inputs and outputs, we allow the user to define their own use for our fault tolerant controllers."

A core element of PCSC's FT solutions is their ability to not just resist failure but to recover from failures. But how can a system be designed in such a way as to self manage its own recovery?

"Our FT architecture provides Real-time Dynamic Architecture (DNA), which is an automatic means of self healing a communication failure or even a controller failure," Kosaka explains.

"Those 3 communication ports I mentioned earlier ensure the stability of the communication network and we automatically switch communications to alternate ports until we establish communications. "With our DNA process, our FT controllers automatically take over the duties of a failed FT. The security system continues to operate perfectly as long as one FTC is available on the network."

Cost is an increasingly important issue for security departments but Kosaka believes reliability is the more important fundamental.

"Our competitors provide that reliability through redundant PC servers and though that architecture meets the needs of operating system, it does not answer the needs at the security system controller level.

"When a competitor's controller fails, it could create a total failure even if they have redundant servers, while card and alarm transactions would not be able to be processed. In comparison, our FT systems provide a higher level of performance and security at a lower cost for redundancy."

According to Kosaka, OCSC's FT architecture provides 100 per cent availability and processing as

long as one FT controller is operational.

"Card access authorizations or alarm processing are not degraded during communication failures or controller failures like other systems. We also offer global anti-pass back and global input output linking without the need for the PC. Basically, our system is 100 per cent distributed intelligence and provide access processing and alarm monitoring, without the need for PC intervention."

Along with fault tolerance the system also reports incidents to security management and control room operators.

"The FT architecture provides real-time status information to host systems, while communication failures or controller failures are reported to the user through graphics, SMS and/or Email," says Kosaka.

So - what is the reaction of IT departments to fault tolerant controllers like PCSC's FT Controller?

"Interestingly, our biggest supporters are IT departments," Kosaka explains.

"We were the first to provide access controllers in standard 2U rack mount which can be installed in the IT room. End users can also buy our very bright vacuum florescent display (VFD) which provides a real-time display of the FTC and sub-controllers. This allows IT teams to see the security system status without having to query our system software."

A key part of PCSC's solutions is Hydra Protocol.

"The Hydra Protocol is not just a protocol but a network manager, utilizing peer to peer techniques," explains Kosaka. "It manages and controls communication from the Host, FTC and sub controllers. The Hydra Protocol manages and controls security data, communication and is the firmware manager.

"It ensures that the system data and security data is identical at all FTCs. It even controls the firmware level of its network. If you install a controller with an older firmware level, it will automatically download and update the firmware to the correct levels, ensuring system stability and security."

Fault Tolerant FT Controllers have many alarm and reporting parameters – importantly the FTC network is managed by PCSC's LiNC-NXG (next generation) application software making staying on top of alarm reporting functionality very easy.

"LiNC-NXG has the ability to properly manage alarms through our alarm management software using graphics and the ability to have multiple work stations," Kosaka explains.

"Our software allows the user to send alarms to appropriate workstations and provide alternate routing for alarms that are have not been responded within a user defined time period.

"Basically, our system is 100 per cent distributed intelligence and provide access processing and alarm monitoring, without the need for PC intervention."

FACT FILE

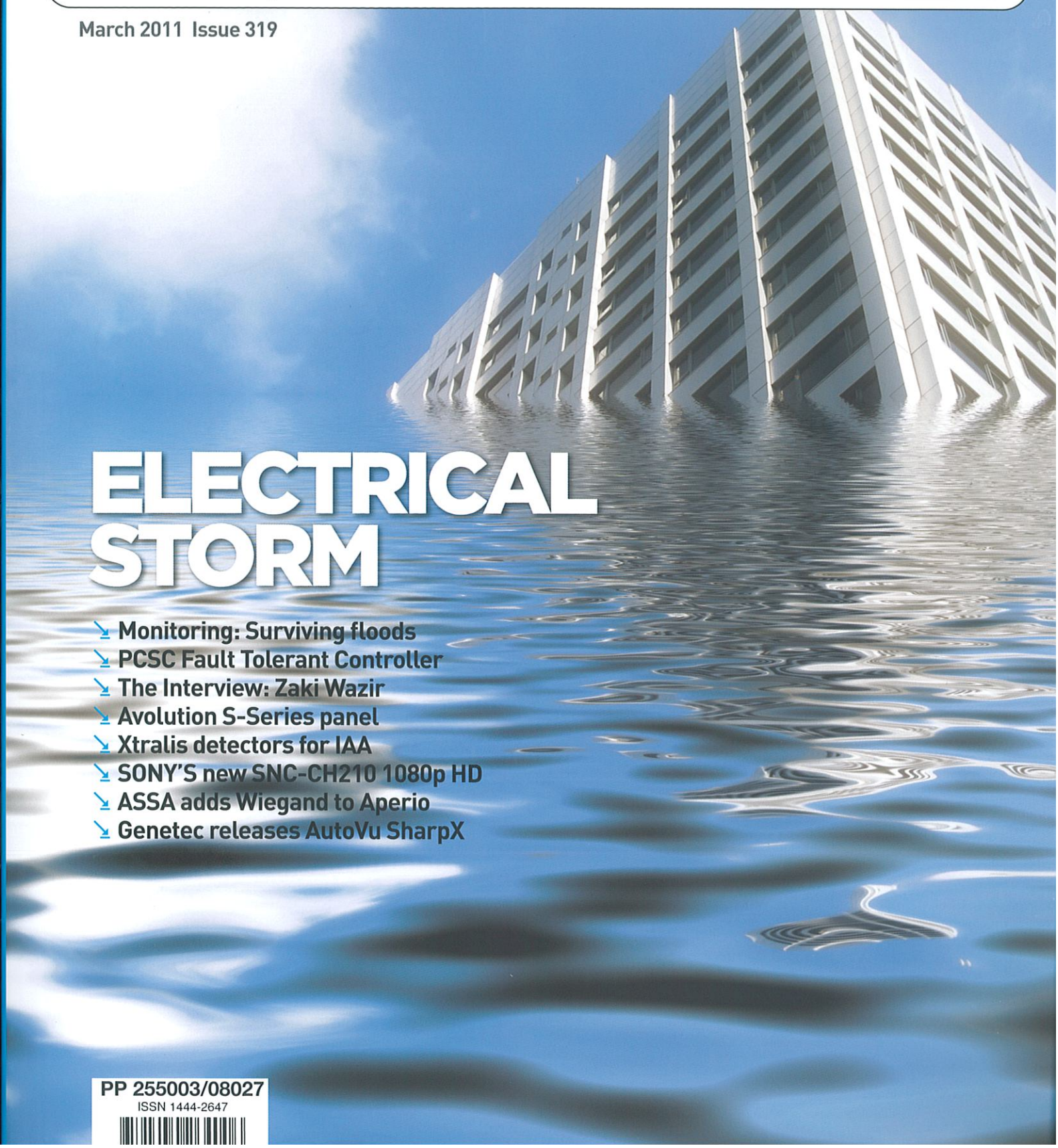
FEATURES OF PCSC'S FAULT TOLERANT FT CONTROLLER:

- Fault Tolerant Process
- Automatic Hot Cutover
- Fail Safe Operations
- Open Systems Platform
- Open Architecture Protocol
- Peer-to-Peer Communications
- Homeland Security Threat Level Control
- Auto Alternate Communication Routing-3 Types
- Access Action for Disabled Persons
- Supervisory Controlled Entry Authorization
- Cardholder or Card Group Action
- User Programmable Input Action
- Global Anti-Passback
- 3 Levels of Anti-Passback Control
- "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

Security Electronics & Networks

Security Managers ◆ Integrators ◆ IT Managers

March 2011 Issue 319



ELECTRICAL STORM

- Monitoring: Surviving floods
- PCSC Fault Tolerant Controller
- The Interview: Zaki Wazir
- Avolution S-Series panel
- Xtralis detectors for IAA
- SONY'S new SNC-CH210 1080p HD
- ASSA adds Wiegand to Aperio
- Genetec releases AutoVu SharpX

PP 255003/08027
ISSN 1444-2647