

## The Role of Access Control in an IP World

Borer White Paper – 2007

**Like the fax and the mobile phone, card access control gained acceptance in the 80's and has become an everyday staple of corporate life**

**Borer Data Systems charts its technological evolution and explains the impact of networking architecture on the development of ATRACS**

Swiping a card to gain access to a company building is now a perfectly accepted feature of everyday corporate life. Over the years, we have all grown familiar with the routine and the advantages it brings to access control.

But where cards were once used exclusively to open doors, controlling who went where and when in a building, now they can be used for a wide variety of extra functions.

Developments in card technology allow for the card that gives you access at your workplace to be used for recording attendance, gaining access to your PC, as your identity card and even for cash-less transactions at a vending machine. The role of the multi-function card has evolved as card technology has developed. As ever, by pushing this technology envelope, we are seeing huge and dramatic gains in efficiency with more streamlined organisations and reduced staff numbers.

Today, IT systems across the world are connected via high speed Local Area Networks (LAN) and Wide Area Networks (WAN) and there is an increasing expectation that non-core applications such as security and access control - once the sole domain of the security manager - should share the corporate communications infrastructure.

This model also extends to the capture and dissemination of data. End-users have come to expect raw data such as staff details to be input only once and for this information to be inherited by all systems.

Organisations looking to eliminate inefficiency no longer find it acceptable to have to re-input the same information into the personnel system, the access control system and ID card system etc, with standalone applications - each with its own bespoke wiring requirements, unique database, dedicated PC and printer. Now market-proven these systems are more secure, easier to administer and more efficient overall than closed legacy systems.

In general the manufacturers and suppliers of security systems have been slow to design for enterprise wide applications, preferring instead to produce closed solutions. So that although technological advances have produced a range of proximity and smart cards, fingerprint recognition readers and high-speed networks, the fundamental layout of a typical access control system has not altered since 1977.

In the 1970's and 80's a control panel (a microprocessor based circuit board used to control access through a door and housed in a metal box together with a power supply) would service two card readers and one or two doors. A number of these control panels could be connected to a mini computer using low speed 2 or 4 wire data link (often erroneously referred to as a network). Today a control panel can be connected to a PC running a Windows program with capacity to accommodate 4 or even 8 doors. Little else has changed!



### **Legacy Architecture**

8 two door controller and power supplies, 16 reader heads and host PC



### **Network Architecture**

16 CAN based single door card reader controllers, power supply and combined site controller and PC with 250 door capacity running Windows 2000 Professional

Why change? Whilst it would be true to say that those elements make up a system that give an acceptable level of performance, other commercial pressures are forcing us to adopt alternative system architecture.

For example, one of the biggest property issues for commercial organisations today is space. How do we fit ourselves and all the necessary accoutrements of modern commercial life into the available workplace? And how can developers maximise the lettable or usable space within a commercial building to maximise their profit?

A large access control installation will require a significant amount of hardware to be accommodated into a building infrastructure. A typical installation will require all the door hardware (readers, locks etc) plus dedicated cabling, metal enclosures for power supplies and controllers - all to be situated as unobtrusively as possible. Once the computer network as well as fire alarm, air conditioning, telephone, intruder systems, etc. have been installed, few modern commercial premises have enough free closet space left to mount access control enclosures.

So door controller enclosures are typically installed in the ceiling void close to the door – this practice is fine – so long as there's room. But with office space at a premium, increasingly ceiling voids are becoming shallower, particularly so in new and refurbished buildings.

And what does the future hold? While an increasing number of architects and developers are keener than ever to reduce the amount of "wasted" space available for services in their buildings, tenants and occupiers are being more discerning about the high standard of services they expect from the building they work in. Lighting manufacturers reacted and developed low-profile luminaries, which occupy a much shallower space within the ceiling void, to overcome this situation. Now it is the time for the

security sector to meet the challenge and provide an access control solution that is smaller, smarter, and faster and with a lower cost of ownership.

## **NEW TECHNOLOGY**

Borer Data Systems took these facts into consideration when we embarked on the development of our new generation of products. We wanted systems which allow us to interact with other applications at the corporate level while providing an efficient means of monitoring and controlling disparate items of equipment such as card access readers, sensors and actuators at the building level. To meet these objectives we chose Ethernet and TCP/IP as our protocol for connecting to and running applications across the organisation's network and Controller Area Network (CAN) for monitoring and controlling devices within the building.

Originally developed by the German Company Robert Bosch for use in the automotive industry, CAN provides a cost-effective communications bus for automotive electronics as an alternative to expensive and cumbersome wiring looms. CAN have been adopted by ISO as an open communication standard for intelligent devices and is now increasingly being used in industrial control and building automation systems. In all cases, the major requirements are cost-effectiveness, the ability to function in a difficult electrical environment, high-speed communications and ease of installation and maintenance.

The CAN network is up to 100 times faster than traditional solutions. For example, a CAN based system can process a card access transaction in 4 thousandths of a second in contrast to the industry norm of a quarter of a second. This faster communication provides a higher degree of system flexibility, which allows for even the biggest of projects to be undertaken with greater efficiency.

The CAN protocol also allows any device on the network to talk to any other device. All CAN devices have local intelligence with all messages being received by all devices on the network. In this way, the detection of a fire alarm by an input device can cause all or selected access readers on the network to release doors – even if the controlling PC is not connected. Should a number of devices attempt to access the network simultaneously all messages are prioritised so that the highest priority message will always take precedence over other data.

## **THE FUTURE**

It is clear that the future will see more integration between an organisation's communications network, telephone system, IT infrastructure and the division between services such as CCTV, intruder monitoring and access control becoming increasingly blurred. In producing access control systems for the 21st Century, several facets need to be addressed.

Firstly, field devices such as access readers, alarm inputs and enunciators need to be small for ease of mounting and should be able to share a common communications and power buss.

Secondly, the access control database and software should be able to run on the corporate network infrastructure without having to install bespoke communications and dedicated PC workstations.

Thirdly, applications will be required to be integrated, bringing together such functions as access control, alarm monitoring, attendance recording, guard tour, visitor management, cashless-vending and CCTV. This third level of integration will provide the greatest efficiency gains as it allows for previously stand-alone applications to share data and work together.

For instance, by integrating the CCTV, access control and intruder alarm system onto the same network one security guard can oversee a number of locations from his desktop PC.

The access control system can check for approved members of staff, resetting or activating alarms depending on whether the site is occupied or has been vacated. Images from cameras transmitted over the corporate Intranet or Internet can be used for visual verification of alarms.

Out of offices' hours' alarms detected by the access control equipment and/or movement detected by processing the images received from cameras on the network will cause the event to be logged on the custodian's PC allowing an immediate video replay of the event.

This application of already available technology allows manpower to be used more efficiently as it transforms a proactive system (where the guard constantly has to monitor the CCTV) into a reactive system (one where events are drawn to the guard's attention as they occur). The communications revolution is here to stay and the new technology is capable of delivering real benefits to organisations everywhere.

**The application of true Networking technology to access control has many advantages over legacy technology including:**

- The application of 'Plug and Play' technology, ensures devices can be installed onto a CAN network without special programming and with the minimum of fuss
- Different devices (door access readers, attendance terminals, alarm monitors) all share the CAN network, thus requiring less hardware and bespoke cabling to fulfil a project
- Less power is taken by a CAN based device - 'the green effect', compared to an equivalent legacy device enabling one power supply to support a number of doors. A legacy reader and controller will typically need 280mA at 12 Volts dc while the equivalent CAN based reader controller needs only 90mA)
- Power over LAN technology allows for both electrical power and data to pass over the LAN. The whole job can be completed by the installer, instead of having to employ an electrician to connect power and an installer to set up the network. Hence fewer power adapters and a more economical installation
- Fewer cables are required to terminate. A typical full featured 8 door legacy system requires in the order of 392 cable ends terminated compared to 160 using CAN

**These features allow access control installation to be undertaken rapidly with less equipment required. This reduces the overall cost of ownership for a true network based access control system in comparison to equivalent legacy solutions.**

Tel: +44 (0)118 979 1137 UK Tel: (0)845 155 9623 Fax: +44 (0) 118 977 3526 Email: [info@borer.co.uk](mailto:info@borer.co.uk)

[Borer Data Systems Ltd](#), Crown House, Toutley Road, Wokingham, Berkshire, RG41 1QN

Web: <http://www.borer.co.uk> Registered in England No. 1207085