White Paper
Leveraging existing structured cabling
Infrastructure to deploy security systems

Infrastructure.
Networking.
Electronic Security.

All together.

MAYFLEX

+Background

The design of cabling systems for security applications has not changed radically over the last fifteen years. Bringing a video image or access control data back to a control room using conventional transmission methods is a simple and well-understood task. However, the move to IP based security products and the fast growth in business applications, now means that end users are demanding an increased level of integration between their video, audio and data. All of which need to be delivered over a single, standardised structured cabling system.

In contrast to traditional video and access control systems voice and data communications cabling systems have undergone many changes. Data networks run on structured cabling systems and have moved on from the original proprietary cabling of the 1980s to a standards based cabling system running on balanced twisted pair and optical-fiber. This means faster transmission speeds and much higher network bandwidth. Both of which enable the security installer to provide the level of integration required by their customers between CCTV, access control and other applications.

By embracing true structured cabling, installers can ultimately open up new revenue streams and deliver real benefits to end users by bringing together all of their systems onto the same cabling infrastructure.

The standards bodies acknowledged this shift in the usage and physical deployment of structured cabling systems with the publication of a new standard from CENELEC titled EN 50173-6 Information technology – Generic cabling systems – Part 6: Distributed building services. This standard has been written to include the requirements of the various established and developing systems that can utilise the infrastructure cabling that is installed in buildings. It is also being written to encompass Distributed building services that did not use the infrastructure cabling for historic, topographic, application or connector reasons.

The network infrastructure of a company plays a vital role in the distribution of information such as data, CCTV, access control, voice, and other electronic media. This distribution network runs across a structured cabling system. These cabling systems are designed for 24/7 flow of information, built with redundancy at its core and installed with a centralised topology, making the sharing of resources as easy as possible, with maximum flexibility and expandability.

Why do companies use Structured Cabling – What are the Benefits?

+ Standardisation

A structured cabling system uses the same cabling infrastructure for everything. This standardises all systems for phone, Ethernet, CCTV, access control and other data and communications systems.

True standardisation of structured cabling offers a promise. A promise, when installed and certified by a qualified engineer, that the system will work for a multitude of systems / protocols today and for the life-time of the installed (PL's) permanent links.

+ Reliability

Structured cabling systems support multi-vendor equipment which means they support applications and hardware even if the systems that run on them expand and the end user changes vendors. This support feature increases reliability and helps avoid the need to rework the cabling when a user upgrades to a technology and new devices can simply be added to the cabling system as required.

+ Flexibility

Whether a user needs to move a computer, a VoIP phone or a CCTV camera from one area to another, a structured cabling system can streamline the process and deliver a true plug and play backbone for all applications.

Moving to TCP/IP, IEE802. based packet transmission of data allows for agile networks that can communicate... Communication is the key. Once they can communicate the gateway is open to a multitude of bespoke, designed for purpose, "integrated systems".

+ Simplified Fault Diagnosis

Structured cabling allows for troubleshooting of problems to be fast and easy due to its segmented design which means there should be no single points of failure that could bring an entire network down. Diagnosing faults in the majority of cases is very easily done through a certified structured cabling tester. These devices often pinpoint issues within a cabling system quickly, however, these faults are normally found and rectified at the time the system was installed giving peace of mind that the infrastructure in place is ready to go.

+ Future Proofed

A structured cabling system will support future applications like multimedia, video conferencing, CCTV, access control and others with little or no upgrade problems as structured cabling is a long term investment and a fundamental foundation to any infrastructure.

+ Cabling can be re-used

The need to purchase and pull new cable into a building is diminished which means the end user can leverage his existing cable investment and thus make substantial cost savings. Added to this the impact of downtime and disruption is minimised since there is less cable to install allowing more of a building to remain operational.

+ Challenges

Many end users in the security market are being told the only way to deploy an IP video surveillance system or a new access control system is by removing all the existing coax or UTP cable and then installing a new Cat 5/6 structured cabling network.

An alternative method to this highly disruptive and costly scenario is to utilise the existing cable and employ a hybrid IP transmission system. There are many hybrid transmission systems available on the market that allow installers to take advantage of extended PoE power and Ethernet distances using legacy cable.

This hybrid technology allows an installer to reuse the cable that is in existence where necessary and to utilise unused capacity on the customers existing structured cabling systems and therefore avoid the need to install new cabling for every device. This robust IP technology allows installers to approach their customers with a whole new suite of choices when installing new systems or upgrading existing ones.

+ System Planning

A structured cabling system is a highly effective solution that supports all of the communication requirements of a business throughout their building or site with inbuilt flexibility for users to connect to CCTV cameras, access control points, data devices or telephone services via VoiP.

Prior to planning a security system upgrade a number of considerations should be thought about carefully including:

Applications

What does the system need to accommodate today in terms of data, voice, video and multimedia applications and which emerging technologies are on the horizon in the future?

Lifetime use

The structured cabling system will need to last 15 to 20 years as it will be the backbone of a business's communications.

Compatibility

The cabling system should be able to support all of the multiple applications that will be run on it in the foreseeable future.

Bandwidth

Bandwidth demand is only going to increase in a business which means providing enough bandwidth as possible for existing needs whilst considering and allowing for future needs.

Number of users

The numbers of users should be estimated for the future as the cabling will need to support them for the lifetime of the system (15 or 20 years) so that extra capacity is installed from the outset.

Moves and changes

The network should support new and regular changes. Category 5/6, fibre optic technologies are developing fast and the structured cabling network should be designed with flexibility to accommodate changes and additional users.

+ Benefits to installers of using cabling for multiple applications

By using existing structured cabling, the installer can open up a myriad of new revenue opportunities with his customer by adopting IP based security products in place of traditional analogue based systems. The installer can utilise the existing infrastructure to put in Video, Access control, alarms devices and offer his customer a truly integrated suite of hardware and software that controls all of the applications on a single network.

+Improved system management

By deploying security devices on the network, management of devices is centralised as part of an overall network management process. This means that network or security managers can check security remotely using a laptop. The security information can be interrogated via a central control point, such as a control room, which can result in manpower cost savings through centralised control.

+Scalable systems

It is standard practice in most network installations to add in extra capacity which means using the existing network and cabling infrastructure allows a high degree of scalability. IP cameras or door readers can be easily added or relocated with little impact on the network.

Despite the many new IP and PoE-based solutions in the security market, there are still many traditional access control systems which are still in place and working. As a result, many manufacturers also offer hybrid solutions that bridge the gap between legacy cabling and structured cabling systems.

+ How should an installer approach system planning?

Implementing an IP based system can only be successfully achieved as part of a well-designed, high quality passive cabling solution, an Ethernet based network. If an installer does not have in-house expertise in this area, then a distributor who focuses on product performance and customer support of IP based security solutions should be partnered with and then they can advise on how best to utilise existing structured cabling systems for new or upgraded security systems. See http://www.mayflex.com/electronic-security for more information on the support available from Mayflex.

+System design on structured cabling networks

Designing separate systems to support CCTV and access control data is no longer considered to be acceptable. System designers now have to plan communications networks without knowing how many voice and data ports any user position will require. For example, does the user at position "A" need two voice ports, for phone and fax, one port for data or voice or two data ports, for Ethernet and video? The need for this kind of flexibility means that planning is essential.

+Access control systems are finally becoming standard network devices

In recent years, the security and IT industries have been moving toward each other as a result of IP convergence. Whilst CCTV has converged quickly access control systems have been much slower to evolve. However, access control systems are finally catching up due to the convergence of physical and logical security.

Security devices are becoming network appliances with all the standards and protocols that IT professionals need to see when deploying a device on their networks. With network-based access control, users can do a lot more than they previously could and end users are becoming quick to catch on with the benefits of deploying access control as part of their network enabling them to use access control data in other non-security processes, such as time and attendance, or cashless vending.

These benefits improve efficiencies outside of traditional security and increase the value of security systems that provide real ROI (return on investment).

While IP convergence is the biggest trend in access control, other advances are being made in the use of smart cards that can store and process information, and can be read with radio-frequency identification (RFID) technology. Smart card technology works well and as more applications are converged over the network the use of smart cards is set to grow.

+The importance of Standards

Access control systems have historically been proprietary closed systems, but IP convergence and new manufacturers entering the marketplace, along with end user demand are driving the need for more open systems and interoperability. Datacom's infrastructures are standards based, and some consultants believe that access control manufacturers will have to adopt more open based systems in much the same way that the CCTV manufacturers have had to comply if they are to remain competitive.

As early as 2014 ONVIF™, www.onvif.org. the leading global standards organisations for IP-based physical security products, announced the final release of Profile C, which brings the functionality of the ONVIF global interface specification into the physical access control arena. The purpose

+ Summary

of this was to enable system designers to achieve interoperability between clients and devices of physical access control systems and network-based video systems.

As more and more manufacturers adopt these standards the deployment of proprietary based systems will reduce as end users will demand greater Interoperability and open standards. This is evident in the recent evolution of access control systems and the many new devices entering the security marketplace that take advantage of the IP and Power over Ethernet (PoE) standards.

Some of these products use the structured cabling network to connect directly to a network switch and receive PoE to provide 750 mA of continuous power at the door. Whereas in the past systems needed several separate cores for the lock, request to exit and door status monitoring, and then more pairs for the reader which means the installer can now just bring one network cable back to a controller located near the door and run short cables to the various door functions.

The benefits of using existing structured cabling networks are significant both from a cost saving perspective as well as enabling more flexible, reliable and future proofed systems for the end customer.

The use of this infrastructure for video is now commonplace however the recent developments in the access control sector are also significant. From reduced installation and maintenance costs to the ability to leverage the corporate network. What IP and PoE security devices mean to the end customer is large savings on cabling and labour which means security can now fit in within the IT infrastructure, and take advantage of the scalability and all the other benefits of a converged network such as backup power, efficient use of rack space and data back up and redundancy.

Most manufacturers and industry professionals believe that as access control products are designed to leverage the existing IP infrastructure that we will see even more technological advancements and more integration opportunities. And with the next generation of PoE products we'll be able to deliver even more power to the door and further reduce costs and simplify installations.

As IP convergence and open standards become more common, manufacturers and vendors will be investing even more in the new technologies which will in turn benefit installers, consultants and end users alike. As the amount of available products increases and the cost and flexibility of deploying systems on existing structured cabling infrastructure will become the new standard and driving force for convergence of access control in much the same way network based surveillance systems have evolved.

Mayflex UK
Excel House
Junction Six Industrial Park
Electric Avenue
Birmingham B6 7JJ
United Kingdom

Tel +44 (0)121 326 7557
Email sales@mayflex.com
Website www.mayflex.com

Mayflex MEA DMCC
Office 22A/B
AU (Gold) Tower
Cluster I
Jumeirah Lake Towers (JLT)
Dubai
United Arab Emirates
PO Box 293695

Tel +971 4 421 4352
Email mesales@mayflex.com
Website www.mayflex.com

Certificate No. FS 547274

Certificate No. EMS 542663

Investor in Customers®

CCTV User Group
Leading, Working, Delivering, for ALL CCTV Users

UserGroup
Affiliate Member

FIA
The Fire Industry Association
CORPORATE MEMBER

BICSI
CORPORATE MEMBER

All together.

Printed on paper made from 75% recycled fibres.

MF1079_10/16

MAYFLEX