When designing a security system for a site, the question of how it should be interconnected is often one of the first you need to answer. Should you choose a system that has its own proprietary bus network, which might require twisted pair cabling, or perhaps one based on an ethernet backbone? Both types of network have their advantages and disadvantages as discussed below.

**Ethernet connectivity**

Some security systems are based on a number of modules, and each module is connected to its own ethernet connection. One big advantage of a system like this is that in many cases it can be much more convenient, allowing the installer to utilize existing network cabling and other
infrastructure, rather than needing to install new cabling.

On the other hand, if a security system relies entirely on networking infrastructure controlled by others – typically the IT department, then the stability and reliability of the security system is dependent on that network being available when your system needs it.

"The stability and reliability of the security system is dependent on that network being available"

Another potential disadvantage is that certain areas of the premises may not be equipped with a nearby network outlet, and if the network in question is not managed by you, it might be necessary to request the IT department add an outlet for you to use.

**Proprietary bus connectivity**

A system with its own proprietary bus network can also have advantages. Perhaps the first and most important difference is that because the network cabling is installed specifically for the security system, the designer has the luxury of being able to decide exactly where the wiring should be placed and terminated.

Another advantage is that the cabling would only be used by the security system, so the installation company can be sure the network will always be available, and there would be very little chance part of it could be accidentally unplugged.

Another potential advantage is that some systems are able to run bus cabling of distances well over 1,000 metres, whereas individual ethernet connections are typically limited to 100 metres or less.

Another consideration, which applies particularly to intruder and holdup alarm systems, is that communications between elements of the security system should not be prevented by other factors, such as a power failure. Obviously, if a part of such a network is formed by ethernet infrastructure, such as network switches and / or media converters, then that infrastructure
needs to be battery backed, and the power supply must be monitored. In some cases, the equipment must be able to withstand a power failure of 24 or even 60 hours. Such long standby times are unusual in IT infrastructure, but are quite common in the case of security systems.

The equipment must be able to withstand a power failure of 24 or even 60 hours

How this all fits together

When selecting a system, it is usually most helpful to have a flexible system that can support a number of different deployment options. This is especially true if the system in question can support a combination of different interconnection types. For example, a single system that can contain a variety of interconnections can then be deployed in a very wide variety of systems where existing infrastructure may be used to aid in the design and deployment:

- **Fiber connections** – Many modern sites are pre-cabled with existing fiber connections which can be used to form a dedicated interconnection between system components which can be of the order of kilometres apart.

- **Ethernet connectivity** – With the increasing ubiquity of networking within premises, some elements of a security system can be deployed using the existing infrastructure.

- **Repeater** - For very large or densely packed systems, a device that can be used as a form of “repeater” can be extremely useful to permit very long interconnect cabling distances.

Systems can be formed by utilising a fusion of all of the above connectivity methods

Some security systems can be set up to enable multiple discrete access control modules to be deployed, connected to an existing ethernet network, and treated as a single ‘system’ by the
management software, while retaining full offline functionality in the event the network becomes
unavailable. Further, some systems can be formed by utilising a fusion of all of the above
connectivity methods.

In practice, of course some applications would suit a deployment that relied solely on ethernet
connectivity. Some other applications, especially systems or parts of systems that are part of an
intruder and/or holdup alarm system, would better suit a deployment using a dedicated
proprietary bus network, and other systems would suit a combination of these communications
options. Selecting a system that can be deployed in a variety of ways can be enormously helpful
in providing the flexibility projects might demand.

Author Profile
You may also be interested in...

**Power Over Ethernet - First Choice Of Security Installers For Powering...**

The security industry’s continued migration to networked IP-based systems ensures that PoE will be integral in their design.

**Choosing The Right Cable For Networking Infrastructure**

The use of multiple wires has advantages for network transmission. Network connection to a remote device begins by considering...

**The Digital Transformation Of Modern Access Control Solutions**

The safeguarding of premises through the monitoring of entrance and exit points has traditionally been a very manual aspect of security. Hum...

**Automatic Gates: Making The Right Investment For Access Control**

The experience of the COVID-19 pandemic has made us all more conscious of who is coming and going from our property. Whether it is a family...