As a low voltage professional who does not install any network or IP devices, you may be saying to yourself “Why do I care about networking? I don’t work on networks.” You would certainly be correct – for now!

The future of low voltage, all low voltage systems, is not in the traditional products we use every day, but in the networked products. Low voltage and security products are either becoming network capable or even completely network based. In the future, possibly sooner than we think, network products will be the norm in professional installation, and non-network products (which are currently the bulk of the low voltage business) will be relegated to the low end and do-it-yourself markets.

Low voltage professionals who start to learn networking and IP now will be prepared for the change, and can cut their teeth as the market matures. Low voltage professionals who decide not to understand networking and IP will find themselves in the low end of the market. Once the tipping point is reached, and IP based products dominate the market share of a particular low voltage category, some will be ready, and some will be out of business.

Why IP?
Why is the market moving to IP and network products? It’s not just that we live in a “digital” world and “analog” is old technology. True, digital technologies have replaced analog in our daily lives. CDs and MP3s replaced records and tapes, DVDs and Blu-Ray replaced VHS, and GSM cellular phones have replaced our old AMPS analog cellular phones.

The change has occurred because digital brings many advantages to the products. CDs and MP3s produce higher quality sound records and tapes, DVDs and Blu-Ray discs produce high quality images than VHS, and GSM cellular phones provide better call clarity and security than AMPS phones did. The same is true with low voltage products, particularly ones dealing with audio and video.
IP and Security
IP is the future of security. IP cameras have been around since the mid-1990s. IP cameras have dropped significantly in price since their introduction, and have gained tremendously in features. In fact, many features available in IP cameras are not achievable with analog cameras.

Networks have been used as a communications option for access control systems for years, but now several vendors are offering products that use the network as their sole communications method, and even some that existing directly on the network as a network device.

Burglar and fire alarm communications were seriously impacted by the introduction of VOIP (voice over IP) when it was first introduced. VOIP offered cheap telephone service using their existing high speed internet connection. It also tended to not readily carry signals sent by digital communications built into and used with burglar and fire alarm panels. The result was spotty, and sometimes completely unsupported, communication to the monitoring stations.

Burglar and fire alarm professionals were forced to offer their customers alternative methods of communications so they could continue to offer monitoring services to their accounts. One method used was cellular, but IP (internet) communicators also began to be offered.

IP communicators have come a long way since their introduction. They have decreased drastically in price, and are now often used as the sole method of communication instead of as a back-up method. In fact, several vendors have their IP communicators listed for sole method of communication for fire alarm monitoring, which can replace two phone lines.

IP telephony has gained wide acceptance in the communications market. IP telephone systems are not common place, whether the system is a large or small implementation. Vendors have brought products to market design to serve all aspects of the telephone system market. Vendors now tout “unified communications” as a way of delivering data and voice over the same network.

Several vendors now offer IP intercom and PA (public address (paging)) over IP. Similar to the function of the IP telephone, these systems use the network to carry and deliver audio between devices and systems.

On the residential side, many low voltage installers currently pre-wire homes with structured cabling systems, capable of supporting a network. Some installers even install basic network switch hardware during the trim out phase. The home network may be used to share Internet access among multiple computers, but it does not end there.
Residential audio/video equipment is also moving to the network. Media servers and media center PCs are common place, even in small projects. These devices are often connected to the home network to distribute audio and video signals throughout the home. Many higher end A/V amplifiers now include a network connection for accessing signals over the home network and the Internet. Some vendors even offer systems that provide complete audio/video distribution to the entire home over the home network.

The Internet
Since the Internet was introduced to the public in the early 1990s, the number of people and businesses that access it and use its services has been booming. High speed connections (aka, broadband) has really driven the growth of the market. High speed internet has gone from being available to approximately 41% of the country in 2005 to almost 99% of the country in 2009. High speed internet is available from multiple sources, including telephone companies, cable companies, and satellite companies.

The wide availability of high speed internet has helped drive the growth of the network inside the home and business as well. Not only do you have access to every conceivable piece of data known to man, you can also download it quickly. Additionally, high speed internet allows the user to remote access their own data (or system) from remote locations. Remote access to information (in the form of images, audio, data, or files) makes the system even more attractive the user.

Convergence
Low voltage devices are migrating to the network, and becoming an integral part of the network. IP (network) video is estimated to make up 20% of new large (16 or more cameras) CCTV installations. IP access control is estimated to make up 35% of all new installations. IP telephone systems are estimated to make up 95% of all new large telephone systems, and are gaining significant ground in smaller systems.

Network hardware vendors are aware of this trend and are structuring their hardware to be more low voltage and security product friendly. The vendors are marketing to the traditional low voltage and security market, as well as making their regular customer base aware of opportunities in IP based low voltage systems.

Standards
Low voltage and security equipment have compatibility issues. A piece of equipment from one manufacturer will often not interoperate with a piece from another. There are very few open standards in low voltage equipment; everyone does it their own way. This can make mixing and matching equipment very frustrating.
Network and IP products, on the other hand, operate on an open standard called Ethernet. A device designed to operate using Ethernet standards will interface and operate with any other device using Ethernet standards. The Ethernet standard covers the cabling, switching, hardware, and communication protocols.

Another great thing about an open standard like Ethernet is commoditization of products. Since everyone is building products to the same standard, there are more price pressures on the products. As in other industries, there are brand names that provide high performance and bring in a premium price, but competitive pressures even reach these as well. Intense competition also drives innovation. The profits that these vendors cannot make up in volume they make up by adding features to differentiate their products. A product with more features (particularly ones of interest to specific markets, like low voltage and security) can demand a few more dollars, adding to the manufacturer’s bottom line. These features may make the design and installation product easier on the installer, adding to his bottom line also.

**Existing Infrastructure**

One cost factor in conventional systems is the design and installation of the wiring infrastructure to support the system. Various types of cables, running in different directions, and serving different purposes increases the overall equipment and labor costs to install these systems. Additionally, each system installed within a building, would often own require its own specific cabling and wiring structure.

Using IP based systems significantly reduce the occurrence of this problem. IP based systems use a standardized infrastructure. Even better, this infrastructure often already exists in many buildings (commercial and residential alike). Most commercial buildings are wiring for an existing network, and many homes built since the mid 1990s are “network ready” as well.

Connecting IP based systems to an existing network is sometimes as simple as getting a network cable to the device. Sometime electronics (switch hardware) may need to added or expanded, and sometimes bandwidth usage is an issue/concern of the person managing the network.

**Long Distance**

When a conventional system needs to be extended over long distances (in the building, between buildings, across the street, or across the country) installation costs and continuing operation costs can increase dramatically. Significant investments in equipment are required to extend a signal intended to go a few hundred feet to be able to travel a few thousand. More significant investments in equipment and in continuing operation and service costs come up as the signal is required to travel over a distance of miles. All of this is because the cost burden of this signal transmission infrastructure is borne solely the installing company and their customer.
An IP system can eliminate or at least significantly reduce the cost of sending signals over long distance. IP systems even make sending signals over long distance easier than ever before thanks to an invention that changed the world: the Internet.

Using the Internet, IP based systems now have a worldwide reach. Any IP based device anywhere in the world can now communicate with another IP based device anywhere else in the world. IP eliminates the restrictions of wires by giving us an existing global infrastructure to use to send our signals.

99% of the country is now in areas served by high speed Internet. Almost every address in the United States has access to an on ramp to the information superhighway. The choice becomes do we use an existing connection and share our access with other devices, or do we want a dedicated connection of our own just for our system?

**IT Budget**

Companies live and die on data. Some data also has a shelf life, which can be very short for some types of data. Keeping the data flowing is prime concern of many organizations; it is often the life blood of their business. The IT (Information Technology) department is critical to keeping the blood flowing. Companies spend large amounts of their annual expenditures making sure this data keeps flowing, and that it is flowing in a timely manner. Business data is such an integral part of daily business operations that many companies have a top level executive position that is responsible for keeping it all moving. While the CEO may make decisions on how to run the business and the direction of the business, the CIO (Chief Information Officer) or CTO (Chief technology Officer) is responsible for providing the data and infrastructure to meet the business goals.

A large factor in keeping the business moving, and getting time sensitive data into the right hands, is the speed and reliability of the data system. Companies with high volume or high speed delivery requirements are always looking for ways to speed up the process. In the world of networking, more volume or higher speed usually means an upgrade. An upgrade usually means spending more money for the latest and greatest gear to do the job.

A company considering a medium to large physical security system for its facility is usually looking at a large investment. But the word “large” is a relative term, depending upon what you compare it to and whose budget it is coming out of. A “large” physical security system coming out of a security, operation, or maintenance budget will likely be significant. It may even be a deal killer, or at least require some scaling back to fit within the budget.

A “large” IP based physical security system coming out of an IT budget may be a different story. The cost of the IP based physical security system may likely be insignificant compared to the yearly or even monthly outlay to keep the data humming along. It’s all a matter of scale.
Wiring
When a new system is installed in a building it typically requires new wires. The more types of systems installed, the more wires required. To further complicate matters, if an equipment change occurred between wiring and installation, or if the project was a retrofit application, compatibility issues may arise as many systems use proprietary cabling.

IP based systems can be installed with less wires, or even use existing wiring as their wiring structure. The existing network structure may be able to be used to support the new system. Even if new wiring is required, because of existing network issues or concerns of the installer or customer, wiring is still simpler than conventional systems because standard network cabling, typically Category 5e or Category 6, can be used almost completely.

Wiring with Category 5e or Category 6 cables is typically more economical than the cables used by most conventional systems. Category cables are standardized, so they can be manufactured by a wide variety of cable vendors. Category cables are sold in high volume due to the demands of the data and communications industry. The wide availability of manufacturers, and the sheer volume of sales, helps keep Category cable pricing low, even as copper prices rise.

Expansion
While most conventional systems can be expanded, the actual expansion of an existing conventional system can be labor and equipment intensive. New cabling will need to be brought to the new parts of the system, and existing cable may need to be rerouted or reconfigured to accommodate the new system configuration. Head end hardware may also need to be changed or upgrade to accommodate the additional capacity as well.

With IP based systems, expansion can be as simple as adding capacity to the existing systems. Network hardware may need to be expanded, but many networks are designed and installed with possible expansion in mind. Since the head end hardware of IP systems is typically electronic and/or software based, the expansion can be as simple as a software upgrade.

Intelligence
Convention systems have some or no intelligence in the local device. Conventional systems rely on communication to the head end equipment for commands and decision making. While many access control systems can function with loss of communications to its host PC, the PC itself is required to collect the data from the control unit and manage it. The access control system continues to function, but in a degraded mode.

CCTV systems, however, are not so forgiving. The loss of communication between the camera and the head end equipment means no control over the cameras, and no recording of video. Additionally, most conventional CCTV systems rely on the head end for decision making regarding alarm triggering and reaction.
IP based systems by nature have the ability to be more intelligent and self supporting. Intelligent IP based access control system can not only log data at the control unit, but also manage data at the control as well. Some systems operate without the requirement of any software installed on the PC to communicate with the device.

Intelligent IP based cameras have the ability to manage their video. They can store it and send it later at a time more convenient to the network usage requirements. The can even decide when to record video, and when not to based on what the camera sees, not what the recording device decides. Some can even act on alarm conditions completely independent of the recording device or head end equipment.

Summary
The world is moving to the network. The traditional, conventional systems that most low voltage installers are used to dealing with are become intelligent, network based product. The low voltage professional can start now to prepare by beginning to design and install IP based systems and products, or he can take the “wait and see” attitude as the market passes him by. The change is coming, you are either ahead of it or overcome by it.

Networking and IP Training
National Training Center offers several options to help you get the networking and IP training you need. Live training classes are offered around the country, webinar training is available on a regular basis, and available 24/7 in Training Department, our online training solution. Our NTC Professional Reference Books feature sections covering networking and IP as well.