Public Safety Technology: Advancing Mission Critical Communications

Introduction

People often imagine public safety as stalwart uniformed officers or emergency response teams. However, public safety is also a vast critical communications network operating 24/7/365 behind the scenes, ensuring civil security. This network is responsible for accurately and rapidly coordinating officers from animal control to the FBI. Its information management and operations control define public safety success. Failure is not an option.

Essential tasks in this network require technology that is reliable and configurable. In the last 15 years, public safety departments and national bodies have focused on modernizing these systems and updating infrastructure to modern needs. As population increases and security forces grow, mission critical communication teams face issues of volume, speed, location and cost, to name a few. Interoperability has become the new standard.

The following white paper will discuss the computing hardware that is bringing dispatch centers and network control centers into the modern era.

What is Public Safety?

Public safety is the information management, operations control and emergency responses carried out by government agencies that guarantee the day-to-day well-being of civilians. Local and federal task forces respond to emergency circumstances. These agencies include firefighters, animal control, law enforcement, crisis infrastructure teams, EMS and other personnel.

Their calls and orders are transmitted over government-specific frequency bands. These transmissions are monitored at network towers that operate on frequencies that can travel as far as 20 miles between towers. A state-wide public safety communication network may only have a few hundred towers ensuring total coverage. These towers may be in remote, hard-to-access areas. Communications traveling over this network are received and managed by dispatchers stationed in populated areas. These individuals receive calls and requests, carrying out actions and coordinating agency personnel on exclusive channels.

Public safety is not just response, however. Efforts are becoming more descriptive and prescriptive. Descriptive public safety means using data to describe the ongoing patterns and interrupt them with traditional surveillance. Prescriptive public safety means using data, software and intelligent coordinated initiatives to proactively prevent crime patterns from forming in the first place. These methodology changes result from three factors: improved technology hardware and software; diversified and changed demographics; and evolving social demands for less violence, less jail time and prejudice-free security.

These pressures and new responses are appearing in rapidly growing urban areas of the United States. Populations here tend to be diverse in age and be multicultural. There is more income disparity in these places and affordable housing tends to be an issue. Many of the circumstances that increase insecurity are present, requiring more supervision by public safety teams. Descriptive behavior in a place like this could be something as simple as identifying intersections with increased car accidents during peak traffic times and placing control barriers there. Prescriptive behavior would be taking smart city data, identifying patterns between citizen behavior and safety events, and adjusting community systems to prevent the circumstances from forming.

What concerns Public Safety innovation?

Computing hardware will continue to make a significant difference in future-oriented public safety communications networks. IoT devices and sensors that collect data must be reliable and durable. Computers will require greater processing power as they run larger software programs that use AI and real-time analytics. As governments will have more cloud programs to select for use, they will need increasingly configurable devices.

There are two umbrellas of concern when it comes to the backbone of Public Safety communications. First, technology solutions must be reliable. Reliable means two things: consistently works in use and remains in use for many years. Second, these technology solutions must be highly configurable. Configurable in this use means it interfaces with legacy infrastructure systems, interoperates with workstation equipment and can scale up or down to the needs of the operation.

Reliable Computing Hardware: A matter of cost, location and mission critical nature

When it comes to cost, there's a dual dilemma for public safety spending. On the one hand, no price is too great to guarantee public safety. On the other hand, no government body wants to pay high premiums year after year due to unreliable devices. Moreover, they do not want to budget for frequent, expensive maintenance. Thus, computing solutions designed for public safety must walk this balance of high quality, durability and affordability.

If a local authority upgrades their equipment and modernizes their infrastructure, a big consideration will be location. Network control and monitoring centers may be in a geographic area defined by mountains, swamps or deserts. Climates may have extreme temperatures or weather patterns. Areas may also be prone to natural or human disasters. All these considerations require the hardware to be durable and rugged, capable of being the "last man standing," because emergency teams depend on those machines to communicate.

The final matter of reliability affects the mission critical nature of public safety. These devices do not get one free pass to shut down due to errors. There is no "slow day." At any moment, someone may be relying on public safety communications channels for an emergency response. The conversation cannot bleep out, the network cannot fail and the system cannot freeze.

Configurable Computing Hardware: A Matter of Volume and Infrastructure

As population increases or concentrates in urban areas, local dispatch teams face issues of volume. One emergency call may demand the coordination of three different departments. Dispatch centers may need to house dozens of dispatchers and each could be fielding multiple calls. As a result, computers must be able to process the software and many tasks associated with that kind of volume.

Permanent infrastructure hugely affects the technology brought in to modernize the system. Although the term implies a single backbone or a united entity, the foundation of public safety encompasses many different systems. Of various ages and quality, the regional components can be based on analog technology and built with varying sized budgets. Computers must be equipped to anticipate any number of idiosyncrasies or possible constructions when being installed in a public safety network. This is especially true in network centers. Space may be at a premium in these places and computers cannot take it for granted.

Public Safety Computing Solutions

Two Sealevel devices have achieved great success in their public safety applications. Both industrial computers, the equipment is designed with anticipating public safety needs and long-term field placement. Some of these computers have been in operation for as long as 12 years, a remarkable milestone given the modern tendency to obsolescence. One computer is an emergency wireless communications system manager. The other is a dispatch console.

The Last Computer Standing: Emergency Wireless Communications System Manager

When it comes to network monitoring, the computer managing this task has the most important role. It detects when communications are not being received or transmitted over the network and sends continuous updates about network status. From both a public safety standpoint and a liability standpoint, ensuring these calls go through and that they are documented has a high priority for public safety teams. These devices are self-sufficient and indicate necessary repairs, minimizing the number of expensive trips to remote centers. The Sealevel solution is based on our Relio R4 industrial computer.

Designed for Durability

From start to finish, this computer is designed to be durable and reliable, regardless of the circumstances. The enclosure and interior is resistant to shock and vibration. The computer is fanless, the system cableless and its COM express board construction is solid state. It is tough and equipped to stay tough.

It can withstand extreme climates, with a wide temperature operating range, functioning from -30°C to 60° C. The wide surface area dissipates heat quickly and efficiently, allowing for fanless operation over the accepted temperature range. The components are chosen for their cold resistance. The computer is built for energy efficiency, so it does not generate much heat.

Ready for Remote Locations

Its 1U size fits the standard Telco racks that populate the sites requiring these devices, which means it is universally applicable equipment. It is also equipped with an internal battery backup. If power to the device is disrupted, this computer can continue to monitor network communications until the battery runs out. It will flag these outages in its reports and record equipment failures until it shuts down.

Configured for Communication

The server replaces devices that communicate serially and converts analog and digital inputs into IP communication, an essential upgrade in modern telecommunications, guaranteeing connection. Moreover, previously existing infrastructure may vary between locations, requiring plenty of I/O options. The device is designed to interface with the most complicated tower sites.

The Queen of Control: Dispatch Console

In dispatch centers across the United States, computing systems can be the difference between life or death in an incident. These consoles process information, run the software that manages emergency phone calls and power the equipment that dispatchers use for their cases. These computers are highly configurable and reliable. Again, the Sealevel solution is a Relio industrial computer.

Perfect for All Preferences

Dispatchers may use many peripheral devices to accomplish their jobs and their consoles must be equipped with plenty of I/O to accommodate them. For example, USB ports, optically isolated digital outputs and dry contact inputs enable devices such as flagging lights and press-to-talk footswitches. Dispatchers multitask and manage communications coming from multiple talk groups and channels. These coordinators need I/O to configure their workstations.

Compact for Comfort

The initial introduction of computers to public safety was not a smooth transition. Technology systems ran on standard PC towers that were prone to obsolescence with bulky desktop screens and monitors. These first machines were loud, required graphics and audio cards, and added heat to the rooms. New consoles are compact and fanless. They can be mounted underneath desks, out of sight and out of mind. Desk space can include other tools and still have room for large screens.

These computers also eliminate the need for audio cards. They include a Digital Signal Processor for audio processing and two audio codecs that convert microphone audio to digital packets. These elements ensure packets of information are encoded and transmitted in a way that enhances understanding. For example, a dispatcher receiving a call from a yelling police officer and a quietly speaking animal control officer will hear the same volume and speed from each of them.

What is the future of Public Safety technology?

The future of public safety technology continues to be modernization and reliability; however, as data harnessing becomes a primary tool for improving the industry, innovative networks and systems will become a priority. Cutting edge solutions must eventually be applied to the modernized infrastructure. IoT and big data management will enhance civil security if done on equipped hardware.

For example, consider a smart city that uses IIoT technology to add a layer of intelligence to their governance. Light poles, parking meters and even traffic lights have been incorporated into their networks. These structures can be automated, but they can also be used to collect anonymized data and create non-specific surveillance of d angerous activity.

Light poles may be built with low-power, long-range (LPWAN) sensors that detect acoustic activity, such as gunshots. Their sensors would relay their data over the internet to a cloud network, similarly managed as phone calls, in dispatch centers. These same sensors and data management could also be used for those prescriptive public safety initiatives that are proactive instead of reactive.

Similarly, edge computing devices could be installed at these locations and communicate with the same high-processing consoles that dispatch centers currently use. Public safety coordination could happen in real time, on-site to mitigate the risk associated with latent information.

Constant pressures, consistent solutions

The public safety field continues to have the same goal: deliver information rapidly in every crisis. The pressures that affect it will always be the same. However, modernization as an added goal will change as the available technology continues to improve. At Sealevel, we take pride in our dedication to quality and a commitment to innovation. If our technology could help meet your public safety needs or you would like to discuss how our IoT products could make your operations smarter, please contact us.