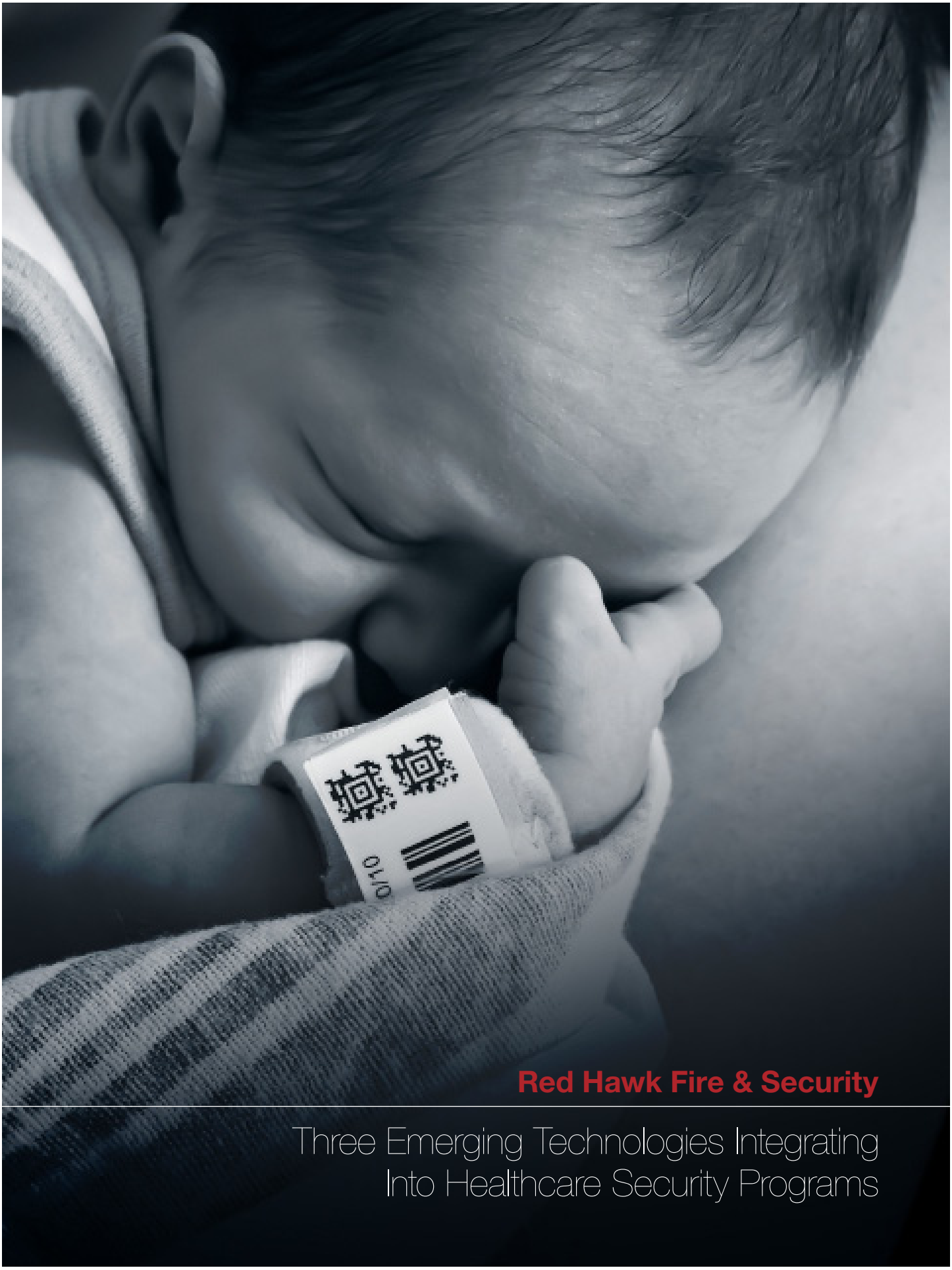

Red Hawk Fire & Security

Three Emerging Technologies Integrating Into Healthcare Security Programs

Three Emerging Technologies Integrating Into Healthcare Security Programs.

Executive Summary

Emerging technologies are changing the face of safety and security in the healthcare industry at a rapid pace. What wasn't even thought of last year is today's reality. Healthcare facilities are constantly faced with the desire to upgrade or enhance their program, but are challenged by the functionality of their older, existing system. So how do you get the newest technology without replacing the entire system? The easy answer is turnkey system integration. This white paper will look at three of the emerging technologies that need to be integrated into existing systems and that are transforming healthcare safety and security including advanced HD cameras with multi-function capabilities and the stretch technologies that allow them to run over existing coax lines, web-based physical access control, and evolving infant monitoring systems that help provide peace of mind for new moms.

System Integration: Working Together As One

The term "system integration" has been evolving right along with the technology that it is integrating. In 1965, when CCTV cameras were first being used by police as surveillance devices, the term "system integration" didn't exist because systems didn't integrate. Cameras were on one system, alarms on another and access control on another. If you needed to monitor them simultaneously, you wired them to the same room if possible. But as technologies advanced, companies and suppliers began to see the value add of interactions between subsystems. For the end user, integration was a pure and simple desire for cost savings–how can you do more with less? For the suppliers, it was an evolution of their offerings and a chance to provide better service. Although it is difficult to imagine systems as non-integrated elements, it wasn't that long ago that they were just that.

Today, "system integration" is defined as "the bringing together of the component subsystems into one system and ensuring that the subsystems function together as a system."[1] Successful system integration begins in the design phase of a project and is woven throughout the entire process. It must be thoughtfully designed, carefully installed and fully tested before determining that systems are operating together as they should.

The interesting challenge of system integration is that new technologies are constantly changing the way the pieces of the puzzle fit together. For example, the addition of megapixel cameras that we will discuss later in this paper, didn't just cause a change in the cameras themselves, but in the transmission needs and the storage needs as well. The new storage systems then interact differently with the existing alarm system. Engineers designing the system need to make the pieces fit together without tearing the whole thing apart.

Changing Regulations, Emerging Improvements

Another challenge to the constant evolution of healthcare security programs is the evolution of the needs surrounding data protection. Information security in the healthcare industry gets a great deal of attention and the regulations and requirements are vast. HIPPA, the Healthcare Portability and Availability Act, became law on August 21, 1996. The law brought with it much needed changes to the management and operation of security for healthcare operations and the data they possess and gives the right to privacy and establishes national standards for electronic healthcare transactions.

While HIPPA triggered obvious, immediate changes in electronic security, it also triggered needed changes in physical security. How would server rooms themselves be protected? Could there be access control in computer data areas? How do you manage asset location with laptops and other portable data processing equipment? The challenges needed to be solved and could all those emerging needs be fully integrated into existing systems? Today, HIPPA is part of the fabric of the healthcare security industry and so too are new security programs that help ensure its protection. New systems have been designed, installed and implemented that assist with the protection of data servers and other health information storage devices. An example of one of the latest is a networked wireless lock system which can be used for doors, medical lockers, IT racks and even secured dumpsters as they have a wireless padlock that can be used with this system. This system can monitor employees, contractors and temporary employees and is cost effective to install as it is wireless and therefore requires no wiring. The system meets HIPPA and Joint Commissions and it also eliminates the costs of re-keying for lost or stolen keys. As the healthcare system continues to see changing regulations and shifting requirements, the systems that protect it will need to evolve with those changes.

In addition to changing regulations, evolving science is also a factor in healthcare system integration. For example, infection control and reducing hospital-acquired infections (HAIs) have become a central concern. Controlling these infections requires specific dust control requirements for healthcare construction and renovation. Installation engineers must understand and meet these requirements.

Emerging Technologies

Now that we have identified some of the challenges to integration, what are some of the new technologies that are changing healthcare security? Let's take a look at three:

1. A Better Look: IP Cameras over Coaxial Lines
2. Better Controlled Access: Physical Access Control
3. Better Protection Where it Matters Most: Infant Monitoring

1. A Better Look: IP Cameras over Coaxial Lines

Today, with the evolution of technology, traditional analog cameras are being replaced by smaller megapixel cameras with greater capabilities. These capabilities include a wider viewing range and increased zoom that allows for more

detail such as reading license plates or identifying faces, all with a smaller camera that can be placed in a greater variety of places. By 2015, the megapixel cameras will dominate the market and IMS Research forecasts that more than 70% of all network camera shipments will be megapixel resolution. Megapixel cameras provide high definition resolution and can be equipped with face recognition software, zoom, intrusion detection, and motion detection. Any number of cameras can be combined into a single system and placed in multiple secure locations.

There is no question that megapixel cameras are excellent investments and offer enhanced capabilities, but what if a customer can't find a way to invest in a digital cable infrastructure? Two technologies have emerged to solve the problem. One is a "hybrid" camera that can simultaneously transmit both IP and analog signals on a single coaxial cable. This allows easy migration from an analog CCTV system to an IP network-based system utilizing the existing camera infrastructure. The new camera sends its video signal over the coax to a hybrid receiver that delivers both analog video and digital video.

The second is the use of devices that allow customers to replace an analog camera with a digital camera using the existing coaxial cables. These devices, referred to as "extenders or encoders," stretch IP cameras beyond cable distance limitations and also act as a PoE inserter. This new hybrid camera and extender receiver means that customers can keep their cabling infrastructure and their video management system (if they choose) while they start to migrate to digital IP solutions that provide better video, better storage, better analytics, and mobile apps. This hybrid technology helps customers minimize investment, making the most of existing surveillance equipment such as coaxial cables, local power supplies, matrix switchers, controllers, and video wall monitors. The re-use of legacy coax cable also helps cut labor costs which can be as much as 25% of an IP upgrade. And integration of this new system is easily done–it's almost as simple as plugging it in.

In addition to maximizing current systems without total replacement, this new system allows for end users to choose when they would like to install IP equipment because the migration can be done incrementally. Legacy coax can be migrated from analog cameras to IP/megapixel cameras at the time chosen by the end user. This can help healthcare security managers manage interruptions that can be extremely difficult and even costly in the healthcare environment that is often up and running 24 hours a day, seven days a week.

Finally, there is one additional cost consideration that is often overlooked and that is unused cable. In some regions, leaving unused cable in place that is not connected at both ends (or not properly tagged for future use) is illegal due to fire and smoke fuel load safety. The US National Electrical Code rules 800.2 and 770.2 prohibit the abandonment of unused cable. Removing cable can also create issues of its own such as an asbestos contamination situation that can be both time-consuming and costly, not to mention potentially hazardous. Any way you look at it, removal and disposal or recycling of existing cable is expensive, sometimes impossibly so. In fact, in some cases, it is more expensive to pull out old cable than it is to install new!

2. Better Controlled Access: Physical Access Control

Access control presents a variety of unique challenges to hospitals and other healthcare facilities. From sensitive areas and operating rooms to data storage areas and parking facilities, physical access is a constant concern. How do you let the right people in at the right times? And in many situations, the stakes are high: lives are on the line. Advances in technology have begun to solve many of the challenges.

One of the biggest concerns with access control is the need for 24/7, vigilant control. Many facilities staff entrances around the clock, but what if your facility has multiple doors? Multiple sensitive areas? And multiple buildings? The costs can be enormous. Oftentimes areas are simply locked to avoid unauthorized access, creating difficulties for those who need to enter the area. The latest technologies solve these concerns with biometric readers or even a physical access control system that utilizes facial recognition, voice recognition and even movement recognition. A camera can be programmed to identify faces and allow or restrict entry. The system can be set up to greet the approaching person and ask them to state their name and analyze their movement patterns. It can detect speech patterns or stress, count people and provide any number of behavioral analytics. A camera can also be used to capture additional types of analytics that play an important role in a total security program. License plate capture, object left behind, loitering detection, speed monitoring, and wrong way detection are just a few examples that healthcare systems are currently using today.

In addition to the traditional technologies, a new breed of physical access control that utilizes web-based (cloud) rather than server-based systems is also growing at a rapid pace. These physical access control systems (PACS) offer a number of advantages over traditional systems. Most importantly, there is no local server with local outages and downtime. Instead, systems utilize network appliances that can connect with a virtual server and can synchronize identities, roles and polices across all doors and buildings in real time. The cost of a private virtual server or "cloud" is also oftentimes much less: not only in the straight-up cost of server versus server, but also in the operating costs of set-up, deployment, maintenance, and downtime.

Another advantage to cloud-based PACS lies in the security of the system. Building and facility managers may feel comfortable that the doors are locked, but the IT security people are constantly worried about a costly virtual breach. IT managers often utilize "dedicated" servers for access control to minimize the concerns. Controlling the system instead through a secure web-based browser can eliminate the need for the on-site server.

A third advantage to utilizing cloud-based PACS is the mobility that comes with it. Although many types of new systems now offer a web browser option, there are still legacy systems that can keep building and facility managers tied to their desks, controlling a server. The newer technology takes the control of the system mobile–users can manage building security from any web browser in any location with Internet access. Mobile access lets a manager freely move about a building or even a campus while maintaining centralized control. There are no costly, frustrating software updates or down time, systems can be updated in real time from virtually anywhere.

As you can see, between facial recognition and other analytics changing the way we look at visitors and their behaviors, and PACS moving to web-based control, the world of access control is rapidly advancing.

3. Better Protection Where it Matters Most: Infant Monitoring

A third evolving technology that is changing healthcare safety and security is infant monitoring. While infant abduction is not on the rise nor is it of epidemic proportions, abduction of infants in a healthcare facility is certainly a tremendous concern for parents, nurses, healthcare security, and risk-management administrators. According to the National Center for Missing and Exploited Children, a best estimate for the nationwide incidence of infant abductions by nonfamily members between 1983 and 2008 ranges between 0 and 10 per year,[2] with just more than half occurring in a healthcare facility. The important thing to take into account, however, is that infant abduction needs to be a zero-event. Not one is acceptable. Anecdotal evidence also suggests the statistics may be misleading, as there may be numerous attempts that go unreported or are thwarted by hospital security.

The newest technologies to prevent abduction involve advanced wireless radio frequency technology (RFIS). Every infant wears a small, tamper-proof infant protection tag that is placed on him or her immediately after birth, with a matching tag on the mother, and is immediately entered into the system. The system can provide exit protection, triggering an event if there is an unauthorized movement of a baby toward a door and tamper protection that triggers an event if there is any attempt to detach, cut or disconnect the tag. The system can also prevent any infant-mother mismatch. The tag can be monitored on multiple floors and set to activate not only an alarm, but also door locks and elevator holds. This valuable system gives nurses and other staff the information they need to do their jobs and gives new parents unmatched peace of mind.

In terms of integration with an existing system, the new infant protection devices can be easily integrated with nurse call, electronic access control systems and surveillance systems such as CCTV or IP Cameras. They simply add capabilities and do not require any advanced integration upgrades.

Summary

In conclusion, healthcare facilities and hospitals are faced with numerous security challenges simply by the nature of their business. Healthcare facilities are places where lives are saved or made better and the best safety and security is of the utmost importance. In today's changing and often challenging world, the reality of new security needs must be met. Just a few months back, who would have thought that a hospital would need to lock down to allow for emergency surgery of an alleged terrorist? Or that a facility would need to protect kidnapping victims while they healed? Our reality is changing and so are the systems we require. The three technologies discussed are allowing healthcare security managers new ways to improve their programs without depleting their budgets with a complete system replacement. Integration is now seen as a "must-have" rather than a "nice-to-have" and manufacturers of equipment are working to meet those needs by creating solutions that utilize existing technologies and easily integrate with a variety of systems. In the next few years, look for the phrase "system integration" to become less of a promise and more of a way of doing business.

1. (via Wikipedia). Gilkey, Herbert T (1960), "New Air Heating Methods," New methods of heating buildings: a research correlation conference conducted by the Building Research Institute, Division of Engineering and Industrial Research, as one of the programs of the BRI fall conferences, November 1959. Washington: National Research Council (U.S.). Building Research Institute, p. 60, OCLC 184031

2. "Guidelines on Prevention of and Response to Infant Abductions." National Center for Missing and Exploited Children, 9th edition. 2009

Authored By Red Hawk Fire & Security

Red Hawk Fire & Security is an industry leader with more than 1,400 employees and 50,000 clients across the country. Relentlessly dedicated to helping protect businesses from the risks they face every day, Red Hawk's comprehensive portfolio of life safety and security offerings employs cutting-edge technologies and advanced systems integration to create flexible solutions for companies of all sizes. The Red Hawk team of industry experts brings an unmatched breadth of expertise and years of hands-on experience to every solution. The company serves clients in banking and financial services, retail, education, health care and manufacturing and is headquartered in Boca Raton, Florida.

the power of experience™

RED HAWK
Fire & Security

Boca Center Tower II, 5100 Town Center Circle, Suite 350, Boca Raton, FL 33486
877-744-HAWK(4295) | info@redhawkus.com | **www.RedHawkUS.com**