YOUR CONTROLS INFORMATION OUTLET

SPRING 2002

Plugged IN

QUARTERLY

security | solutions

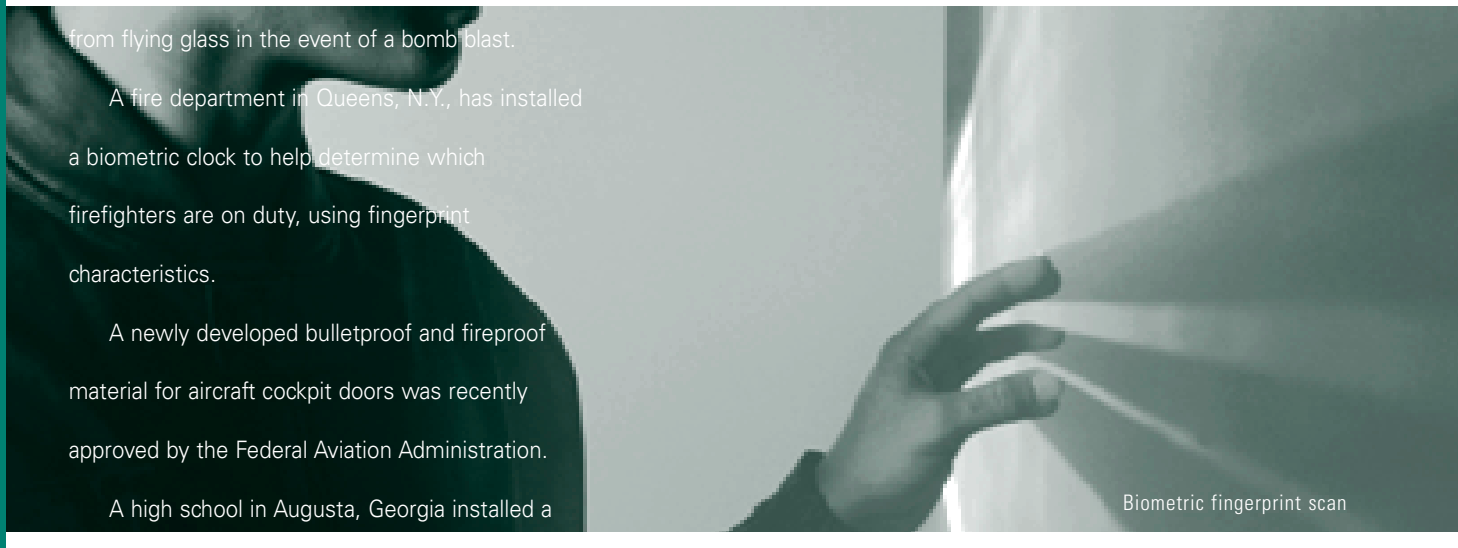
[safety]

The Hoover Dam recently installed a special glass protection film in its visitor center to protect people from flying glass in the event of a bomb blast.

A fire department in Queens, N.Y., has installed a biometric clock to help determine which firefighters are on duty, using fingerprint characteristics.

A newly developed bulletproof and fireproof material for aircraft cockpit doors was recently approved by the Federal Aviation Administration.

A high school in Augusta, Georgia installed a digital video surveillance system that allows law enforcement officials remote access to the school's cameras.



Biometric fingerprint scan

Who would have imagined that a common thread could be found between a fire department and an international tourist attraction? Before the September 11 terrorist attacks, it was unlikely. Since then security issues have become a top priority for organizations all over the world. Our customers are no exception.

Demand for commercial security systems has been on the rise for the past few years, as witnessed by the steady growth of Johnson Controls' security business. Today, our customers are asking for even more. In this issue of *Plugged In*, learn how we're stepping up to the plate to provide security solutions that do much more than keep a building and its occupants safe.

INSIDE

ALSO FEATURING global service | solutions

JOHNSON CONTROLS

Security Business [Stepped Up for Signific

With over a hundred years of building controls experience, Johnson Controls is a world leader in creating and managing quality building environments. It's only logical that Johnson Controls should strive to become a leader in providing integrated security solutions.

"We need to truly understand the security risks associated with the businesses of our clients, then develop security solutions using the appropriate technologies and processes."

Ross Shuster
Vice President of Security Sales

"Over time, customers have asked us to do more and more," said John Bobek, vice president, Strategy and Globalization. "Security ties in perfectly with our controls and facilities management work, so many of our customers are looking to us to provide security solutions as well. We can provide the customer a truly complete solution for his building, not just individual subsystems. Growing our security business is really a natural progression for us."

An important step toward growing the security business was the acquisition in 1998 of Cardkey®, a widely recognized brand in the access control business. "In acquiring Cardkey, we made a conscious decision to begin to focus on building the security business at Johnson Controls," said Patrick Young, president, Security Solutions. "The Cardkey product, people and installed customer base that came with this strategic acquisition were a seed for growth."

The integration of the Cardkey field organization with JCI field offices was completed in mid-2001. "We are now focused on building the security business and core competency with all of our field offices throughout Johnson Controls worldwide," added Young. "The ability to deliver security solutions globally will be a key competitive advantage with global customers."

Integrated Solutions

System integration is an important part of Johnson Control's growth strategy. Today, customers are looking for solutions that work for their particular building, not simply products out of a box.

"The security industry has become very focused on technologies almost to a fault," said Ross Shuster, vice president of security sales. "Our approach must be consultative. We need to truly understand the security risks associated with the businesses of our clients, then develop security solutions using the appropriate technologies and processes."

The recent acquisition of SCIENTECH Security Services, now called Johnson Controls Security Systems (JCSS) demonstrates our commitment to offering integrated security solutions on a worldwide basis, particularly in the federal government marketplace. "They are the best security system integrator for high-end market needs such as federal buildings," said Bobek. "They work with the customer to assess what is needed, design a system that meets these needs, and ensure it is installed properly and continues to work well."

JCSS's focus is on the Federal Government market, although its skills, capabilities, and knowledge could also be applied to

Published by Employee Communications in Milwaukee, editor Kerri Grote, M19, 414-524-4337, Kerri.A.Grote@jci.com

FAN 168.1
To submit story ideas or suggestions contact the editor or write to *Plugged In*/M19

other markets, which is a future challenge for our company.

Growth Strategies

Many large customers have locations throughout the world and are looking for a company that can provide a security solution for their entire enterprise. "The security industry is very fragmented, with most providers being local or regional organizations," said Shuster. "We're one of the few companies organized who can provide consistent security solutions on a global basis."

Johnson Controls is in the process of building the infrastructure to deliver the security business globally. This includes developing a business model, which provides a road map each area office can use to plan the security business and build an organization to sell and deliver it. Coinciding with this is a major hiring initiative, which will more than double the security sales force in North America by the end of the year.

Growing the security business will demand a very clear focus across the entire organization. "Because of the acquisition of Cardkey and the strong name association of 'Cardkey' with access control systems, people think we are purely an access control company," explained Shuster. "But our focus is on comprehensive security solutions."

All offices worldwide need to develop a core competency in security. Johnson Controls is developing a standard sales approach to help security sales personnel and their support teams to analyze security threats customers are facing, and then apply the appropriate processes and technologies.

"We're one of the few companies organized who can provide consistent security solutions on a global basis."

The Centers of Excellence for Security will provide support for these efforts by planning the business globally, establishing relationships with key partners, and following up with technical support to ensure customer satisfaction.

"Security was a growth market even before September 11, but what September 11 did was reshuffle our customers' priorities," Young said. "It created an atmosphere where our customers really want to go back and reassess their security needs. This complements our consultative sales approach, where we go in and help them do threat and vulnerability assessments and offer complete security solutions that protect their people, assets and intellectual property." PI

New Products for a Growing Market

The emphasis on complete security solutions has driven product development. Johnson Controls is broadening its product portfolio to include a whole range of products that weren't part of the core offering three or four years ago. Access control continues to be the central part of a security system, but we continue to expand our offerings to include CCTV, video badging, intrusion detection, and perimeter protection.

We are also investing heavily to integrate biometric technologies with our systems, which provides a more secure environment by positively identifying an individual using a nontransferable physical characteristic such as a fingerprint. The technology is gaining wide acceptance, as it has become much easier to implement and cost effective in recent years. (see *Invent*, page 6).

Demand for biometrics is being driven in part by airports, one of the largest security markets. Airports must comply with the Aviation and Transportation Security Act passed January 3, which requires airports to upgrade their systems to include biometrics.

Johnson Controls expects significant activity in this market over the next several years and is creating a team to specifically address its needs. We recently won contracts to provide integrated security measures to over 1,000 FAA sites and 60 airports around the country.

Young believes security is very much a growth market. Johnson Controls has doubled its security business over the last two years, and expects to double it again in 2002. PI

THE FACE OF THE CUSTOMER

Commanding Performance

in fact

Sept. 11, 1941

Date the groundbreaking ceremony took place for the Pentagon.

How do you control energy costs in a 7.2 million square foot building occupied by over 29,000 people at any given time? "Not by merely telling people to turn their lights off before they leave their offices," said Steve Carter, assistant building manager, Pentagon. "We needed to reduce our electric bill, which was $1.1 million per month, and we felt controls were the way to go."

Over the last five years, Johnson Controls has been retrofitting the entire building with new controls and a centralized control system, including constructing a Building Operations Command Center (BOCC). Until recently, many of the controls in the 60-year-old landmark were manual.

The Pentagon Team. First row: Season Hickcox, Dan Delgados, Rohollah Mahboobi, Behrooz Mahboobi, Stanley Carl Berry; Second row: Robert Andrews, Jarvis Cain, Chad Hensen, Mike Hallberg, Carols Alfaro, Stephen Bauman; Third row: Mike Ganskopp, Dave Nichols, Ed Decker, Kevin Hensen

"We are in the process of putting every building system – access, fire, life safety, lighting, mechanical, electrical, and HVAC – under control of one command center," explained Rohollah Mahboobi, Pentagon site manager, Johnson Controls. "Everything is being integrated into one network so every system could be monitored from a single seat."

The retrofit work – ongoing since October 1997 – includes major renovations of segments of the building referred to as wedges. The main command center, the BOCC, was completed in June 2001.

Major Renovation

The wedge retrofit is part of a seven-phase, 20-year, $1.1 billion Pentagon renovation project, which will ensure that the building complies with current health, fire, and life safety codes. During the 60-year history of the Pentagon, the building has not undergone any major renovations.

Renovation to Wedge 1 area, which represents about one-fifth the total area of the Pentagon, is being completed in phases. The first phase was completed early in 2001, and Wedge 1 officially reopened for occupancy on March 8. The remaining areas and the rest of the wedges are to be renovated one section at a time to ensure all systems are maintained during the renovation.

As the renovation continues, Johnson Controls will provide a variety of solutions, including upgrading safety systems, lighting retrofits, and communications support features.

Not Just Any Normal Work Day

September 11, 2001, began like any other workday for Steve Carter. This date is a significant one for the Pentagon. Construction began that day in 1941, which made September 11, 2001, the Pentagon's sixtieth birthday.

As they made routine system checks from the BOCC, Carter and his team watched the events at the World Trade Center unfold on one of the center's 90-inch monitors. When the second plane hit the second tower of the World Trade Center, the team immediately began lockdowns, securing mechanical and electrical areas and searching for unauthorized people and unusual packages.

One hour after the first Trade Center tower was hit, Carter felt a jolt. The fire alarm and HVAC systems completely lit up the command center's huge screens, indicat-

Inside the Building Operations Command Center at the Pentagon.

ing everything on the newly completed Wedge 1 was on fire. Fortunately, the plane had hit the section of the Pentagon that had just finished renovation and near another section where renovation was just beginning, so few people occupied the area, greatly reducing casualties.

Sixteen Johnson Controls team members were working near the area of impact when the plane hit and all made it out of the building safely. Chad Hensen, systems applications engineer, Johnson Controls, was only a few hundred feet from the impact site. He immediately went to the BOCC to offer his help.

Carter had Hensen use the system to control the air pressurization in different parts of the building, get system fans running, and determine where equipment was down. This helped contain the fire and minimize the spread of smoke. "You can't imagine how important it was to have a programmer on hand to make all of this happen automatically," recalled Carter. "Chad was invaluable."

"We can't imagine having to struggle through these events without the Johnson Controls team."

As part of the renovation, Johnson Controls installed a new fire system, which has smoke control features. On September 11 it worked exactly as designed. "The systems we put in place were instrumental in getting smoke out and keeping the fire contained," explained Carter.

For the next several weeks, the Johnson Controls team worked 12-hour days, setting up a remote monitoring site, going through the entire building to monitor equipment, opening and closing air dampers as necessary, and pumping fresh air into areas of the building that could still be occupied. The team also monitored levels of combustible gases and toxic fumes.

Symbol of Freedom

The team's efforts helped keep 4.5 million square feet operational while the fire continued to burn in 1 million square feet of the building. By the second day, many of the Pentagon's occupants were back to work. Key military command centers remained in the building and did not have to relocate to other sites.

"The Pentagon is a symbol of freedom, a security blanket for people around the world, and in light of the attacks, it was important that we minimized the area that had to be evacuated and kept the building operational," said Carter. "We can't imagine having to struggle through these events without the Johnson Controls team. It's not just a contract to them. They're a committed team that feels as much ownership of our place as we do – they're really quite amazing."

Carter and his team learned a lot from the events of September 11. "What we did in a manner of hours was to take systems that were installed to save energy and improve indoor environments and used them to provide air barriers," Carter explained. "This stopped smoke infiltration, minimized the spread of damage, and, most importantly, potentially saved lives. If there is a silver lining in this very dark cloud, it's that the experience gained will provide us with a system second to none."

Despite the events of September 11, the renovation is proceeding according to schedule. Contractors have partnered together to work around the clock to ensure Wedge 1 will reopen on September 11, 2002. PI

in fact

$83 million | Amount appropriated by Congress to construct the Pentagon in 1941.

$145 million | Value of the Johnson Controls contract award for the Pentagon renovation.

$1.1 billion | Cost, as required by Congress, that cannot be exceeded for Pentagon renovation.

Biometrics

Gaining access to high-security areas using facial recognition, fingerprint, or retinal scan sounds like something out of a James Bond movie or futuristic espionage thriller. As it turns out, those movies could be imitating reality sooner than you think.

voice patterns
fingerprints
retinal scans

INVENT

Industry experts agree that biometric technology is becoming more reliable, cost effective, and easy to use and integrate. Technologies such as smart cards and biometric readers provide Johnson Controls' customers with a viable alternative to previous security technologies.

"Biometric input provides the highest return on your security dollar you can get right now," said John Hooper, global product manager, Johnson Controls Cardkey® Solutions Security Products. "Security data output is more secure than older technologies such as magnetic stripe cards and proximity readers, because even when PIN numbers are used you can never be certain that the person gaining access is the actual owner of the card."

Biometric technology can more accurately verify the identity of an individual. Biometric readers measure actual physical characteristics, which are unique to each individual and nontransferable. Because these characteristics cannot be lost, stolen, or forgotten, biometrics is more convenient for the user, and greatly reduces the potential for collusion and fraud.

How it Works

The Biometric Consortium defines biometrics as "automatically recognizing a person using distinguishing traits." In terms of security technology, this means taking an individual sample of hand geometry, voice pattern, fingerprint, retina scan, facial pattern, or signature to create an electronic template against which the user can be identified. A biometric reader compares a live sample to the stored template to make a match.

"This technology is available on the market now and works for virtually any type of security application," reported Hooper. "For example, a thumb print reader that requires two separate fingerprints could be installed in a hospital to control illegal use of narcotics. One

person could never be alone in the area where the drugs are stored; two people would always have to be there together in order to gain access."

Biometric input is compared two different ways. Recognition answers the question, "Are you who you say you are?" Authentication occurs when the user's actual biometric – a fingerprint, for example – is compared one to one with the template stored on a smart card.

Verification occurs when a live biometric is compared electronically to a large database and secures a match. In comparing one to many, it attempts to verify the person uniquely among a large population and answer the question, "Who are you?" An example would be using facial recognition technology at a large sporting event or airports to identify possible criminal elements. Because it requires a large database, verification is more expensive and complex than recognition. Verification also increases the likelihood of false acceptance or false rejections, weakening security.

Get Smart

Smart cards resemble credit cards and contain a microprocessor chip that stores biometric templates as well as other electronic data. "Johnson Controls offers six different smart card technologies from vendors around the world," said Hooper. "This really expands our customers' options in terms of meeting their application or the type of technology needed for biometric input."

Smart cards employ an electronic filing cabinet system, which typically includes sixteen "drawers" of information. Some drawers could store facial templates for use with one type of reader, other drawers could store finger print templates for another reader, while other drawers could include text or raw data for cashless vending.

Enterprise-wide Solutions

Smart cards can carry virtually any information, including employee, medical, or academic records or financial balances. This makes them suitable for a number of campus- and corporate-wide solutions, and makes it easier for a student or employee to travel from location to location. "By putting security and other pertinent data on a smart card, you greatly reduce an organization's internal communications, personnel time expenditure, and database storage," explained Hooper.

Another major potential market for biometric security technology is the airline industry. The Federal Aviation Administration's benchmark specifications require the use of proximity smart cards (smart cards that don't require contact with a reader) at security points in airports. Johnson Controls recently contracted with several major airports to install over 500 thumb print readers. This installation will meet the FAA Part 107 Regulation that mandates biometric application updates to normal access control security systems.

Other smart card applications such as loyalty cards have enormous market potential. Airlines, for example, could present frequent fliers with loyalty cards that carry a passenger's biometric along with proof of registration with the members of the International Air Transport Association, enabling these passengers to bypass long security lines. E-purse technology allows users to store financial balances and authorize purchases, allowing a parent to set a student's spending limit, say, at the campus bookstore or local McDonald's.

"Smart cards are the way things are headed," said Hooper. "And smart cards with biometrics are going to get a lot cheaper. They offer a pretty wide range of solutions that work in a variety of climates and work environments." PI

in fact

Nearly 0% | False accept rate of retina scans, the best biometric performer on the market.

100 | Number of patents that have been issued for signature dynamics, a hot biometric field of development.

1975 | Year the first commercial biometric device was introduced when finger measuring machines were installed on Wall Street.

20,000 | Number of areas to which access is controlled using biometric technology.

$6,000 | Average cost per access point for a biometrics reader in 1993.

$500 | Average cost per access point for a biometrics reader in 1999.