SECURITY TECHNOLOGY
EXECUTIVE

www.SecurityInfoWatch.com

ASIS Product Preview
More than 60 products direct from the show floor

Video Storage
What's new, from the cloud to self-encrypting drives

SECURITY TECHNOLOGY
EXECUTIVE
SECURITY INNOVATION AWARD
WINNER

The Hardened Hospital

How Jerry Forstater and Richard Warsh parlayed seven zones of technology into an innovative security system at St. Elizabeth's

**Also- Innovation Award Silver Medalist:
Hillsborough County Sheriff's Office**

Virtual 9/11?
POS Systems open a vulnerability

5 Steps to Greener Security

EXCLUSIVE SUPPLEMENT:
9/11 Lessons Learned

CYGNUS SECURITY MEDIA

Bring on the Innovation

This year's STE Innovation Awards covered a vast spectrum of the best the security industry has to offer

O nce again, the security industry's most innovative vendors and integrators have stepped up to showcase some impressive applications of security technology in the *2011 Security Innovation Awards*, presented by *Security Technology Executive*.

"The dozens of companies and vendors entering this year's competition spanned a vast spectrum of projects," says STE publisher/editor-in-chief Steve Lasky. "Each held unique merits and were certainly capable of earning high praise. Our panel of judges was hard-pressed to narrow the choices down to just four. We are thrilled to see the level of participation we had for this year's awards and are proud to present our top four."

This year's Gold Medal-winning project, St. Elizabeth's Hospital in Washington, D.C. (*on the next page of this issue*) featured nearly 25 technology providers. How did they integrate all those different technologies into a single, cohesive system?

The obvious answers are time and patience — but a unified, carefully crafted seven-zone security plan and the diligent efforts of submitting integrator Professional Systems Engineering LLC (PSE) probably had something to do with it as well.

"As it is every year, selecting the winner of the *2011 Security Innovation Awards* was extremely difficult," Lasky says. "This was perhaps our widest array of solutions ever; but one stood out in the eyes of our judges: the St. Elizabeth's Hospital project.

"The scope of this project was just as staggering as the array of technologies it incorporated," Lasky continues. "A project of this scope had to require a high-level of cooperation from vendors and service providers, all under the supervision of the project's system integrator. This was truly a masterful convergence of efforts and technologies."

Wrote one of the judges: "Too often, security directors may try to solve complex security issues with a single policy or a single technology; and it is common to see heralded security systems that are purely CCTV camera systems. The St. Elizabeth's project recognized layers of security and devoted the appropriate technology to that layer. From high-tech personal alarm units that can locate tracked patients to throw-over prevention fences, the level of security matched the level of concern. The project demonstrates adoption of a number of balanced technologies, meets stringent code requirements, and while expensive, the author clearly defines the value of this project."

Our silver-medal project (*also featured in this issue, page 60*) is the innovative Hillsborough County Sheriff's Office's "Eye on Crime" deployment. The rapidly growing IP surveillance project was submitted by Axis Communications, and end-user Craig McEntyre reports that the system has become a model for other community surveillance systems.

"This ambitious video project undertaken by the Hillsborough County Sheriff's Office really highlights the crime fighting potential of municipal surveillance network," one judge said. "The fact that the county saw such big decrease in crime can be directly attributed to the installation of this system. This would be a good case study for other municipalities to examine prior to installing their own surveillance networks."

Our bronze medal-winning project — Standard Aero — was submitted by Honeywell and will be featured in the Ocotber issue of *STE*. The company, which specializes in aircraft maintenance, used innovative access control and video surveillance technology not only to secure its operations, but also to save the company itself.

"Standard Aero solves a business challenge and a security challenge in the same step," one judge wrote. "They met a DHS security requirement for their business without frustrating their customers. Using an innovative technology application (RFID) tied into a pervasive video system, they showed that cameras could be more than forensic tools, and demonstrated new thinking that could possibly be adopted as a standard practice within the aviation services industry."

Louis Armstrong International Airport in New Orleans, which showcased its innovative use of NICE Systems' situation management technology, has been selected by the judging panel as an honorable mention project. It will be featured in the November/December issue of *STE*.

"We've heard a lot in the security industry over the past several years about the potential that physical security information management systems (PSIM) hold for streamlining operations. Until now, however, there have been few case studies that demonstrated the actual benefits of the technology," one judge wrote. "The fact that an airport of the size and scale of Louis Armstrong International was able to consolidate all of their security and life safety systems onto two screens in their security operations centers using the NICE PSIM platform is astonishing and truly innovative."

— *Paul Rothman, managing editor*

SECURITY INNOVATION AWARD GOLD MEDALIST

The Hardened Hospital

How historic St. Elizabeth's transformed six-plus years of work and seven zones of technology into the backbone of an innovative security system

By Richard Warsh

F ounded by Congress in 1852 to treat people living with mental illness, Saint Elizabeth's notably served as a hospital for wounded Union and Confederate alike, renowned writers, the biggest contributor to the Oxford dictionary, and three presidential assassins — with thankfully, only one having succeeded.

In April 2010, the Hospital moved into a new 450,000 square foot, state-of-the-art facility that incorporates best practices in patient mental health care with an environmentally sensitive design and sustainable strategies. The new building's therapeutic design includes bright and airy living and treatment areas, green spaces off each patient unit, and enclosed courtyards. A 28,000 square-foot green roof is likely the largest on any psychiatric facility in the country.

With a combination of community outpatients, both civil voluntary and involuntary commitments, and a large population of forensic patients — those adjudicated as "Not Guilty by Reason of Insanity" — the hospital needed a unique security plan that integrated patient safety, staff security and community access while keeping mindful of the urban, southeast Washington setting.

Because of the nature of the crimes or special needs of highly sensitive patients, the security and safety systems, physical barriers and operations were critical and inseparable to the integration philosophy of the design, construction, engineering, commissioning, training, daily operations, and emergency event planning and strategy.

Balancing the needs of patient and staff safety alike, while ensuring a maximum level of physical security, became the focus of the new Chief Administrator of the hospital, Dr. Patrick Canavan, while forensic patient responsibility was headed by Dr. Joseph Henneberry, and Facility Management responsibility was offered by Mr. Gilbert Taylor. Henneberry and Taylor worked with Professional Systems Engineering LLC (PSE), a systems strategy and design firm, at Patuxent Institution, a large behavioral management facility in Maryland.

PSE was hired by the architect to design all physical security such as hard and soft fencing, protected openings, K-rated barriers and lighting, as well as all security electronics, perimeter detection, wireless duress and access control. With more than 25 years of experience in psychiatric, forensic and maximum-security facility operations and technologies, PSE produced a security program integrating the security and public safety functions.

I charged the design team with establishing facilities which met U.S. District Court requirements and facility accreditation. New plans

Above: Jerry Forstater, CEO and chief engineer of Professional Systems Engineering was the principal-in-charge for the project. He is joined by St. Elizabeth's Hospital officers Pamela Belt, James Watson, Captain Colaya Stubbs, officer Terri Whiting; and Richard Warsh, Director of Facility Planning for the Department of Mental Health.

Right: Dr. Patrick Canavan, St. Elizabeth's executive administrator, addresses the crowd at the 2010 grand opening of the 450,000 square-foot, state-of-the-art facility.

Opposite page: CCTV, which is monitored by hospital security staff, consists of Pelco's Integral Technologies, digital video Sentry Enterprise recorders, and server management systems using Bosch cameras.

Integrator Professional Systems Engineering recommended extensive use of CCTV and fencing systems on the roof of the facility.

were developed by Mark Shaw, AIA, and Eric Kern, AIA, of Einhorn Yaffee Prescott Architects on behalf of the District of Columbia, Department of Mental Health.

Requiring a close collaborative effort, the Project Executive for the Construction Manager — Gilbane Company's Robert Poe with Project Manager William Millios — selected PSE to work directly with the hospital on transition requirements including fire code responsibility, master keying, mass evacuation and defend-in-place fire safety planning. PSE was also responsible for preparing fire and security evacuation maps, staff security and fire training. Jason Delp, Director of Projects and a partner with PSE, managed the integration of physical and electronic security while Thomas H. Pilson, IV, Director of Corrections and Public Safety, managed keying, life safety and security training. Frank Carpency, PE, CCP, Vice President with PSE during design, was responsible for security engineering from 2004 to 2005.

Seven Zones of Technology

The security program defined the security and public safety functions of the site into seven zones of security — protected from both internal and external breach.

Zone 1 is the housing unit into which the highest level, maximum security forensic patients are assigned. Generally speaking, an individual remains at this housing unit floor location except for therapeutic and recreational activities in a secure courtyard and visits for extended health care.

Zone 2 is the secure corridor using the Andover Continuum Access Control System from Schneider Electric, Critical Systems Division. Also covering personal protection are Senstar Flare RF wireless duress transmitters and receivers for the coverage of Zones 1 and 2 and virtually all facilities under patient control. The personal alarm system is able to locate personal duress transmitters with an indoor accuracy on the correct floor within 20 feet of the true location, and on the outside of the buildings, within 50 feet on all sides of the exterior walls. The alarm system must annunciate within three seconds of the activation of an alarm with better than 97-percent accuracy.

Zone 3 encompasses the building's exterior envelope and includes further access controls including full-height stainless turnstiles and ADA access devices from Boon Edam. A full exchange-based electronic intercom system by TOA was provided for security use to provide private channel communications and full security compliance. Security Zone 3 also includes X-ray machines by L3; and metal detection meeting the FAA "Three Gun Rule," and National Institute of Law Enforcement and Criminal Justice Standard 0601-00 with stainless multi-zone floor standing detectors and handheld detectors by CEIA USA.

CCTV is used in a deliberate security manner and consists of Pelco's Integral Technologies, digital video Sentry Enterprise recorders, and server management systems using Bosch cameras.

Zone 4 includes liberal use of CCTV on the roof and on the exterior grounds along with specified security lighting, including high pressure sodium wall packs, floors, street lights and roadway luminaires — all by General Electric. Specifications required a minimum of 2 footcandles (FC) at ground level with a max:min ratio not exceeding 5 FC.

Zone 5 consists of a "soft fence" — DeTekion's taut-wire detection system. Appearing as a physical fence, its "wires" are actually tensioned to allow actuation of alarms by slackening or stretching the tendons of the individual sensing cables. Alarms are received on separate system

St. Elizabeth's Hospital Project Technology Providers

Access Control System: Andover Continuum from Schneider Electric
Card Readers and Access Cards: HID Global
CCTV System: Allegiant Matrix from Bosch Security Systems
CCTV Multiplexors: Pelco
Digital Video Recording: Integral Technologies Digital Sentry Enterprise by Pelco
Security Intercom System: TOA Electronics
Personal Wireless Duress System: Senstar Flare
Uninterruptable Power Supplies: American Power Conversion (APC)
Fiber Optic Transceivers: UTC Fire & Security (IFS) and AFI by American Fibertek Inc.
Fiber Optic Cabling: Corning Cable Systems
Fiber Data Repeaters: Black Box
Fencing: First Defence
Fiber Optic Perimeter Intrusion Detection System: DeTekion Security Systems
Gate Sensors: GE Security
Taut Wire Intrusion Detection System: DeTekion Security Systems
Servers: Dell
Security Lighting: General Electric
Network Switchers: HP Procurve
Metal Detectors: CEIA USA
Monitors: Orion (19"), LG (42")
X-Ray Package Search Equipment: L3 Communications
Turnstiles: Boon Edam
Fire Alarm/Smoke Detection/Mass Evacuation: Siemens
Microwave Transmitters/Receivers: Senstar

Corning Cable Systems, UTC Fire & Security, American Fibertek and Black Box provided the hospital's fiber optic infrastructure.

computers and registered on the access control system while CCTV integration provides alarm video and event storage.

Zone 6 consists of an arched 15-foot fence using First Defence posts. Buried into the ground to prevent tunneling, the fabric is topped with 3/8 inch non-climbable fencing. The mesh is 14-gauge and is difficult to cut with normal hand tools. The fence framework has a high-yield strength of 50,000 psi with the posts meeting ASTM F1083 and complying with rated wind gusts of almost 100 mph. Gate operators in Zone 6 consist of Southern Steel operators with maximum security 9100A locks.

Zone 7 — the final zone — consists of a contraband fence using fence fabric extended to a 22 ft. height. This fence was requested by Dr. Henneberry, who had personal experience at former institutions with weapons and contraband breaching the secure perimeter. This effort provides practical resistance to weapons, drugs or other paraphernalia from crossing into the highly secure patient zones.

Extensive use of fiber transceivers by IFS, AFI and Black Box and fiber optic cabling by Corning was used as communication media for all external communications, which was significant. Digital communications were required for taut-wire monitoring, as well as fiber optic perimeter intrusion detection on the hard fence which is double-looped on the hard perimeter fence. All communications for alarm, monitoring, CCTV and controlled access are established on multiple graphical user workstations throughout the facility.

As digital video recorders are usually extremely sensitive to power shifts and especially loss of power, extensive use of localized APC uninterruptible power supplies are used throughout the project.

Every system within the seven security zones is integrated to establish a unified Command, Control and Communications hierarchy and for implementing new security and life safety strategies.

The Code Approval Process

With original specifications produced in May 2005, a revamping of the specs occurred in June 2006 due to delay in construction funding. While this was a straightforward process, the code approval process during construction from 2006 to April 2010 required substantial consulting engineering services, again performed by PSE. There were design reviews and permitting, functional code review of systems and equipment, fire safety planning, fire/incident evacuation planning with both mass evacuation and shelter-in-place meeting NFPA and IBC I-3, Condition IV requirements. By 2009, evacuation maps and training were also in the planning process.

The thousands of hours spent by Gilbane, the construction manager, the architects, engineers and security designers was impressive in order to open a facility with a smooth transition process.

"Many owners and even construction managers underestimate the amount of due diligence required for functional code review of systems and equipment," says Jerry "Dutch" Forstater, CEO and chief engineer PSE. "The review of a complicated, massive structure such as Saint Elizabeth's must account for HVAC control, fire alarm messaging, fire alarm zoning, horizontal exiting and smoke partition conformance, mass evacuation procedures and shelter-in-place compliance. All hospitals, small and large, need an effective program to manage critical events to provide a safe emergency management program."

Training and Acceptance of New Technologies

With upwards of 1,000 people on site during active community periods and more than 600 occupants 24 hours a day, the facility sees 30 years of wear-and-tear in 10 years time compared to an average building. With this compression of life cycle comes substantial cost to maintain the systems to provide the utmost in reliability and patient control.

There are critical aspects to appropriate transitioning of new security technologies with staff that were transfixed with technologies dating to the 1960s that

St. Elizabeth's Hospital Project Key Contributors

DC Department of Mental Health:
• Richard Warsh – Director of Facility Planning

Saint Elizabeth's Hospital:
• Dr. Patrick Canavan – Executive Administrator
• Dr. Joseph Henneberry – Director of Hospital's Forensics Services (Retired)
• Gilbert Taylor – Director Facilities and Environment (Former)
• Tamil Perry – Public Affairs Officer

Architect, MEP Engineers: Einhorn Yaffee Prescott Architecture & Engineering P.C.
• Marc Shaw, RA, LEED AP – Project Executive, Principal (Former)
• Eric Kern, AIA, LEED – Senior Project Director, Principal

Security Consultant: Professional Systems Engineering LLC
• Jason Delp, EIT – Project Mngr
• Frank Carpency, PE, CPP – V.P. Engineering (Former)
• Richard Suhar, PE – Commissioning Engineer

Evacuation Planning and Security Procedures Consultant: Professional Systems Engineering LLC
• Jerry "Dutch" Forstater, PE – Principal-in-Charge
• Thomas H. Pilson, IV – Director of Correctional Services and Public Safety

Construction Manager: Gilbane Building Company
• Robert E. Poe, III, LEED AP – Project Mgr.
• William Millios – MEP Engineer
• Christopher White – Area Engineer

General Contractor: Tompkins Builders Inc.
• James H. Payne – Director of Construction Coordination

Electrical Contractor: Freestate Electrical Construction Co.
• Susan Gaughan – Project Manager

Security Contractor: Critical Systems by Schneider Electric (formerly TAC Critical Systems)
• Bob Boden – Project Manager

Fencing Contractor: Hercules Fence
• Steve McLaughlin – Project Manager

looked more like a group of old submarine turrets — with little information compared to what appears today in modern security control centers.

The elements of transition included commissioning of security and fire alarm systems to provide as close to 100-percent accuracy, reliability and functionality as possible. With this came the production of the security policies, procedures and post orders along with security training during two weeks of highly intensive shift training. As-records were provided in CAD format to be able to drill down and magnify site elements and equipment through a Help Desk, or Knowledge Center, as Gilbane Company calls it. PSE and Gilbane worked with our staff to provide these staff-sensitive transition services over the course of 18 months.

Leveraging Advanced Technology

Here are some of the advantages of innovating behavioral health by incorporating maximum security and life safety management:

• Multiple zoned security levels with contiguous life safety protection for mass evacuation and shelter-in-place.

• Clear and concise reporting, recording and response.

• Systems integration based on each system being independent from the access control and monitoring system to increase reliability in unexpected events.

• Improved patient care, staff safety and community/consumer involvement.

• Facilitation of mental health management to the community-at-large in the event of a natural disaster or terrorist action.

Return on Investment
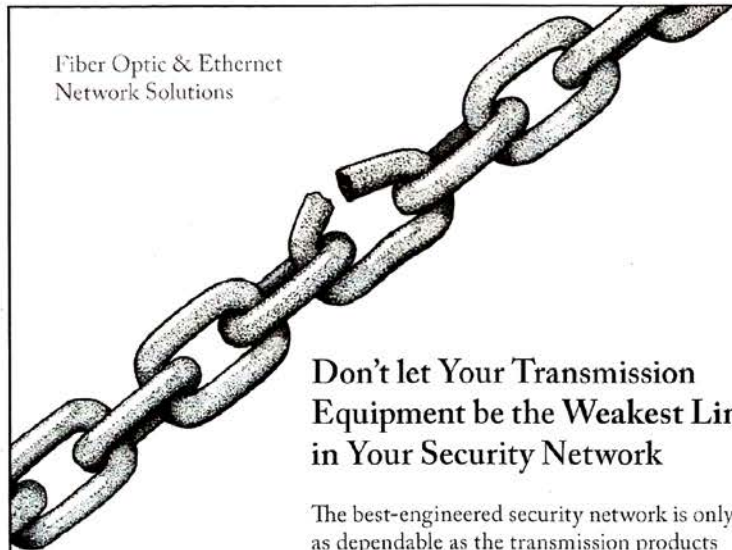
For every opportunity, there is a cost. The opportunity was to provide an infrastructure and facility that replaced buildings that were from mid-20th century and even post-Civil War structures while incorporating new behavioral strategies. The return on investment probably cannot be measured against any strict rule based on its technology cost or other hard physical security or life safety cost. In fact, most facilities' operational costs far outweigh the traditional "bricks and sticks" values placed on buildings.

Because the return on investment is both relative and easily justifiable, a percentage cost of approximately 9 percent of the project's value for the physical security, electronic security, fire alarm and installation cost does not seem unreasonable. In this case, the hard costs for facility were $165 million with a system materials and installation cost approaching $15 million.

Saint Elizabeth's and the Department of Mental Health's management is ecstatic with the results of almost six years of planning, design and construction of an innovative facility. This is reflected in the unprecedented number of requests for tours to mark its success. ∎

Richard Warsh is Director of Facility Planning for the Washington D.C. Department of Mental Health. The Security Innovation Award is an annual competition held by STE magazine. The winning projects are chosen by a panel of security industry experts. For more details or to learn about entering next year's competition, contact editor Steve Lasky at steve.lasky@cygnus.com.

Visit www.securityinfowatch.com/ste/einquiry and select einquiry #224 for more information