

White Paper

PHYSICAL SECURITY



duostech

PHYSICAL SECURITY

WHITE PAPER

BY

CHARLES GOSLIN

“Charles Goslin, Vice President of International Operations for Duos Technologies, Inc., is an international expert in security threat and risk assessment. He developed his extensive security experience as a veteran operations officer for 27 years with the Central Intelligence Agency. He is skilled in developing and executing programs targeting terrorism, espionage, weapons proliferation, and other select U.S. national security objective. He brings a unique, ground-level perspective to security challenges that can only come from a lifetime spent mitigating risk, in all its forms, while living and working abroad.

His most recent assignment, before joining Duos, was as a senior advisor to the Regional Joint Terrorism Task Forces (JTTF) in the U.S. In addition to Mr. Goslin’s current work with international clients, he has authored professional articles and undertaken public speaking engagements regarding the evolution of physical security in the 21st century, and how it can better secure critical infrastructure for public and private enterprise.”

THIS PAGE INTENTIONALLY LEFT BLANK

INTRODUCTION

The perception that state-of-the-art security is represented by barbed-wire tipped fences, armed gate guards, electronically-locked steel doors, and a subterranean room crammed with CCTV displays filled with multiple, ever-changing scenes on flat-screen monitors is quietly disappearing. The fences, armed guards, rotating cameras, even the multiple displays, are still present, but that is where the resemblance ends.



Standard physical security systems and Information Technology (IT) networks have, for several years, been converging into new and stronger applications that substantially augment the traditional model for security design, the term of art being “security-in-depth.” Security-in-depth is a mainstay of physical security design used by security managers. It calls for increasingly robust and sophisticated security countermeasures embedded into rings around a facility, enterprise, or asset. This model is used in varying degrees and designs in many sectors world-wide, both private and public. In a generic sense, it works well as a template for security managers because it allows them to interpret the nature and level of threat, the key vulnerabilities of their facility, personnel, or existing countermeasures, and ultimately the risks that must be mitigated.

As with all designs, security-in-depth can be subject to misinterpretation and misuse. Understanding the strength of convergent technologies requires a critical look at physical security without the integration of new IT/convergent technologies and applications. Unfortunately, this is to a large degree still how security upgrades are implemented, today.



Critical Look at Traditional Physical Security Practice

The predictability inherent in the layered security-in-depth model allows, on the one hand, a new breed of terrorist and infiltrator to craft successful attack plans against embassies, hotels, compounds, national labs and other infrastructure or transportation targets around the world; and on the other hand it has lulled less-than-diligent security professionals still “fighting the last war” to respond with outdated, piecemeal countermeasures that do not adequately address the challenges of the 21st century. The logic chain in this is dangerous.

Nearly a decade after the attacks of 9/11, adversaries are still widely assumed to come in two basic types: the casual, petty criminal/intruder, and the more serious professional intruder, or terrorist. Until relatively recently, it is assumed that terrorists have

political motives and objectives which they wanted satisfied, and that they prefer to stay alive to ensure these goals are achieved. Airline hijackers are expected to have demands, such as for prisoner release, money, as well as an escape route. The tactic most often anticipated is infiltration of bad things: of the terrorist and a gun, the terrorist and an explosive (hidden on his person, or in/under a vehicle), or both. Professional intruders, unintimidated by guards, locks, and barriers, are expected to infiltrate a facility to commit sabotage, steal secrets or valuables, and escape – undetected. Evidence of these assumptions lie with the security tools chosen by security practitioners.

Using an extension of this flawed logic, detection or deterrence technology is selected that focuses on identifying bad things at checkpoints, or detecting the unauthorized person who has gotten into the facility itself. Motion detection sensors remain confined largely to interior spaces as outdoor detection sensors were considered too vulnerable to environmental factors and susceptible to nuisance alarms. CCTV's, theoretically capable of detecting incidents in real-time so long as an alert human is watching, are still used only as a deterrence measure, and for post-incident analysis and investigation. There is also an overreliance on magnetic-swipe access locks and/or code-entry pads, as systems that could “log” an individual's entry and exit, without corresponding authentication measures for verification. Combination locked vaults are susceptible to the same vulnerability – unverified, surreptitious entry.



Time and again in recent years, overreliance on identifying vulnerability within the security-in-depth design results in fatal flaws—in every sense of the word. Attackers no longer hide bombs under their vehicles or in the boot of a car; they fill every conceivable space with explosive material, wire the detonators to their chests, throw grenades as diversionary measures, and ram themselves and their lethal load as far into the premises of a facility as possible, at top speed, before detonating themselves. In their wake, are twisted and smoking bollards, barriers, fences, cameras, injured or dead guards with unused – expensive – explosives detection wands somewhere beneath the rubble. Clearly, this is a failed application of a design that emphasizes the detection of the explosive or gun, and not detecting – in time – the terrorist behavior itself. It is a good countermeasure, but designed for a different set of circumstances.



As we have seen in London, and more recently in Islamabad, and Mumbai, the CCTV cameras accurately and faithfully captured the faces of attackers, or the final seconds of a truck-bomber's run. These high-definition, day-night sophisticated cameras impassively detected the targets. However, since – within the existing security design – the CCTV cameras were relegated to roles as passive recording devices, they did nothing to alert in real-time or deter the attacks themselves. In London, we posthumously got to know the identities of the attackers,

where they came from, and a little about their motives, and neighbors. These interesting facts, though, did little to help those killed or wounded in the attack.

Within the U.S. Pentagon, in U.S. National Labs, or most recently in the White House itself – the most sophisticated mechanical or intrusion detection measures available do not deter innovative, relentless intruders adept at manipulating human weaknesses, or IT vulnerabilities, from thousands of miles away, to get at our nation’s most sensitive secrets. The information highway is broad, invisible and largely bypasses all of the physical security countermeasures designed to sequester cleared personnel, working at “cleared” computer terminals. Retrospectively, security in-depth is a classic design formula that favors the abstraction of “threat” and focuses instead on vulnerability; closing the vulnerabilities translates to mitigation of risk. Threat, when misapplied within this philosophy, remains in varying degrees a slowly evolving, amorphous entity that is just not in synch with rapidly changing circumstances.

Good Technology, poor design

For instance, Under-Vehicle Monitoring Systems (UVMS)—an excellent countermeasure to detect concealed explosives beneath a truck or car—cannot be the panacea for bomb detection at the gateway to a facility. It must be integrated with other explosive-detection technologies, designed to work in conjunction with robust barrier technology and not used as a substitute for measures to identify and neutralize vehicular (VBIED) bomb threats from outside the perimeter. In a design that takes into consideration today’s threat environment, UVMS systems are at best a secondary, and not the primary detection countermeasure for explosives. CCTV cameras in tough, armored, air-conditioned housings, with high-definition, day-night capabilities, are of little or no use when they convey so many images to the latest plasma flat-screen monitor in the Command and Control Center that overwhelmed, under-paid shift-workers stop watching. Metal detectors and explosives sniffers are incapable of detecting or deterring human desperation and will themselves become so much scrap metal if the suicide bomber detonates him/herself. The latest magnetic-swipe ID system is of no use at all if the badge is stolen or acquired outside of the facility, and used by the intruder. The point is that continuing to design in-depth security with a focus on vulnerabilities and detection of *bad things* only perpetuates the illusion of good security. This brings us to the convergence of IT and physical security disciplines.

Artist Rendering of Duos UVMS



Giving threat its due: Convergent Design and Tactics

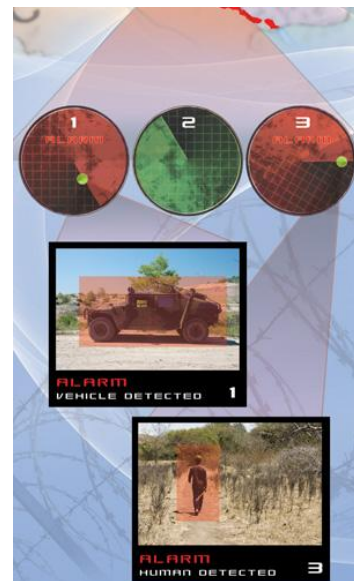
Security practitioners who interpret in-depth physical security with a threat-driven, “outside-in” design must of necessity give greater consideration to the specific tactics employed by today’s terrorist adversaries. These tactics include suicide bombings, as well as clandestine, armed teams infiltrating a hotel or resort to take hostages and inflict as much mayhem as possible. Traditional security design can be coupled with convergent IT and security technologies and applications to significantly strengthen the existing security investment because equal weight is given to designing for specific, current threat scenarios.

An illustration of this is standard perimeter security. Perimeter security is usually considered the outermost ring of “security in depth,” which follows a deterrence-through-design methodology that includes fences or walls, bollards, barriers, cameras, height-detectors at the gates, and lighting. The deterrent element of this design is presumed to be frustration or intimidation of the trivial (petty criminal looking for an easy way in), and delay of the serious (professional criminal, or terrorist infiltrator with an agenda). Using a threat-driven perspective, and taking into account today’s terrorist tactics, two additional needs for perimeter security immediately become paramount: real-time detection, and real-time – immediate - assessment of the threat. Simply using the technologies outlined above, even with a well-trained guard force, is not sufficient. On the other hand, using a network of robust, day-night fixed outdoor cameras, tied to long-range Pan-Tilt-Zoom cameras, enabled with a video intelligent-application, we have a marriage of IT/convergence technology with physical security measures that, by an order of magnitude, strengthens the perimeter.

The intelligence-enabled camera network on the fence-line detects and sends an alert about an approaching threat, in real time. This gives security personnel the time needed to assess and take action to neutralize or avoid the threat before it becomes a liability to everyone in the subject facility. On seaward facing properties, the perimeter can be secured using a virtual electronic “bubble” of security can secure approaches out to 12-kilometers, using ground-based radar and all-weather, day-night, laser illuminated PTZ cameras integrated to automatically vector-in, and track on approach unknown targets.

Significant standoff distance can be achieved using this technology by using the space outside of the perimeter, not just between the perimeter and the facility itself. With intelligent video and sensor applications, a dumb perimeter can be transformed from a physical “deterrence-through-design” countermeasure to an interactive virtual barrier with depth that can actually allow real-time denial of lethal attackers. In this application, the CCTV camera array is transformed from being a deterrent or investigative tool to a real-time intrusion-detection and assessment tool providing advance alerts that allows security time to react, save guest and employee lives, and secure valuable property and assets.

Artist Rendering of Border Security



Addressing the threat of the Insider

Using convergent technologies within the perimeter, the “insider” threat can be addressed, head-on. Once inside sensitive areas, electro-mechanical entry technology such as magnetic swipe access can be augmented by facial geometry/recognition or biometric access applications that provide the crucial authentication needed to verify access into sensitive areas. Insider-enabled clandestine access into sensitive areas is significantly reduced using convergent technology to supplement traditional locks and alarms. In public transit chokepoints, rapidly developing facial recognition software technology, scanning for known threat

profiles, can give law enforcement or national security authorities a real-time edge in detecting the proverbial “needle in a haystack.” Combined with live intelligence reports, even a 70-percent recognition reliability factor helps analysts narrow the odds for police in the middle of a manhunt.

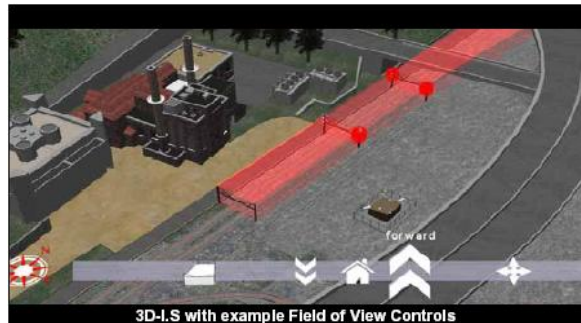
Streamlining Command and Control

An important shift in emphasis, when incorporating convergent IT/Security applications into overall security design for the hospitality industry, is the Command and Control (C&C) Center and its operation. The application platform used to integrate intelligence-enabled sensors, cameras, and ground-radar, and the displays used to present the information to the operators, must be significantly upgraded from the traditional security operations center used to direct operations. In the old C&C Center design, display monitors use sequential CCTV switchers, rotating through potentially hundreds of CCTV cameras and showing them as multiple camera scenes on a single monitor... with perhaps a dozen or more monitors in the room. This is illusory security; in reality, no operator can reliably focus on the scenes displayed for a significant amount of time.



Command and Control Center

Convergent IT/Security transforms the nature and utility of the C&C Center. Using intelligent video, monitors can be replaced by flat video walls that can be used to display Internet screens and video-enabled conference calls, as well as three-dimensional displays of the facility and its environment. Gone are multiple camera scenes – they are no longer needed. With the CCTV camera activated as a sensor/detection device, enabled by a robust, server-based application centralized within a hardened equipment room, a video display comes up only when the camera detects an intrusion and an alarm is sent to the C&C Center. On a three-dimensional (3D) display of the facility (inside and out), the location of the intrusion and camera field of view (FOV) glows red; only then does the operator need to react, bring up the display, and – using a Pan-Tilt-Zoom (PTZ) in the vicinity – investigate and assess the threat, in real time. Sophisticated intelligent video software will detect and generate alerts for multiple alarms and prioritize them. In this way, a security crisis can be efficiently managed by trained security personnel, much as a Combat Controller manages force-protection, or live battle developments within the Combat Control (C&C) room on a naval ship. This capability, with the



Sophisticated Duos 3D Graphical User Interface (GUI)



3D-I.S with example camera drill down selector

technology available today, enables security managers, guard force personnel on the perimeter, and first-responders to control crisis situations in the homeland just as efficiently.

Duos Technologies

Duos Technologies, Inc. epitomizes the transformation taking place in convergent technologies and applications for today's security market. We believe that careful design of security solutions, taking into account existing measures, and the known threat environment, are an absolute requirement. We take a holistic approach to each client's security needs and as a first step, require a full security and engineering assessment with equal emphasis on security threat as well as vulnerability, before issuing a proposal. Our R&D team tests existing technologies to assess their capabilities and suitability in our overall solutions. Commercially, we are a full-service integrator that is lean and nimble enough to respond quickly and efficiently to large infrastructure security needs, at a fraction of the price quoted by our larger, but less agile, industry counterparts.



Most important, Duos Technologies is composed of a team of dedicated security professionals who are at the vanguard of cutting edge security, making intelligent video and sensor-based technologies, and Command and Control software platforms, the new standard for security design.



duostech
Duos Technologies , Inc.

6622 Southpoint Dr. S. | Suite 310 | Jacksonville, FL 32216
P/ 904.296.2807 | F/ 904.296.4103 | www.duostech.com | info@duostech.com