“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.”
INTRODUCTION

Hotels are not designed with high-security in mind and, in normal times, they don’t need to be. They are built to accommodate the traveling public, and high-end resorts and facilities around the world have aesthetics and comfort, not security and safety, in mind. As diplomatic missions are hardened into virtual fortresses around the world, and airports scan every item the traveling public carries, from toenail clippers to toothpaste, it is almost axiomatic that terrorists focus their tactical planning increasingly towards the softer target.

The most recent deadly terrorist attack in Mumbai, India are the latest in a growing trend of attacks on luxury hotels and resort facilities. Paradoxically, these attacks are not on just any hotel, or resort. They are hotels that cater to western diplomats, military personnel, or wealthy businessmen. The resorts are attractive targets because an aggregate of tourists can be found at these locations. If the nationality of the tourists corresponds to the target set on a terrorist’s agenda, they invite attack.

Individuals in their own countries are relatively secure behind protected borders with vigilant border guards. Diplomats or on-duty military personnel are relatively safe in guarded compounds with thick, bomb-resistant walls. Off-duty or on vacation, when diplomats, soldiers, or tourists on holiday leave the security of their homes or workplaces, they become accessible targets and are acutely vulnerable to attack. That vulnerability, unfortunately, is passed on to the hotel or resort where they stay.

Vulnerability: the “Maginot Line” Syndrome

An example of failed security tactics—designed to fight the last war—is France’s Maginot Line. This massive and expensive system of defenses was built to hold off a German invasion of France. The German tacticians, knowing it was impregnable, simply went around it. France fell, within weeks.

Security practitioners in today’s hotel and resort industry have a tremendous challenge in considering all of the scenarios that might be used to compromise their facilities and jeopardize the safety of their guests. Unfortunately, the “Maginot Line” syndrome plagues security design in hotels and resorts, despite the use of tactics by terrorists in recent years that consistently overcome the security countermeasures in place.
The predictability inherent in the traditional “security-in-depth” model of design, has allowed a new breed of terrorist and infiltrator to craft spectacularly successful attacks against hotels and resorts. 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. With regard to the latter, the tactic most often anticipated by terrorists 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. The extension of this logic is that detection and deterrence technology is focused on finding bad things at checkpoints. All too often, these checkpoints are aggregated at the main entrance to a facility, more to make guests feel better than for real security. The back door of the hotel, service entrances, and loading docks are only lightly guarded, if at all.

This is the Maginot Line Syndrome, all over again. Recognizing hardened security, the terrorists either blast their way through with automatic weapons and grenades, or elect a suicide attack with a massive bomb over infiltration and hostages. In their wake lie twisted and smoking bollards, barriers, fences, cameras, explosives detectors or portals, and – most unfortunate of all – dead guards. All technically good countermeasures, miscast in their design for a different set of circumstances, and different type of terrorist, in a more innocent era.

Security countermeasures that are built into a traditional “security-in-depth” design, with a focus on bad things only perpetuate the illusion of good security. It does not take into account the changing tactics of terror today, and the human element. This brings us to the convergence of information technology and physical security design and measures.

Convergent Security Design for the hotel and resort industry

Security practitioners who interpret in-depth physical security with a threat-driven, “outside-in” design must 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 threat.
An illustration of this is standard perimeter security for coastal resort facilities. 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, 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.

A security challenge for large hotels and resorts are the maze of interior labyrinthine corridors, floors, and multiple exits where criminal intruders can hide or escape. While traditional CCTV can provide “after-action” video images of events, the DVRs recording these images are of little use in the real-time tracking of intruders or hostage-takers as they move from one sector of the facility to another. Using convergent IT technologies and existing CCTV networks, a traditional “event recording” physical security element can be transformed into a real-time security application. CCTV’s are stitched together for seamless, live tracking of images. RFID technology is integrated into the network to create a “tag and track” system within the hotel environment that allows security authorities in protected command and control centers to track intruders. Counter-terrorism forces or SWAT teams responding to a
threatening situation can have these images streamed, live, to portable devices so that they know exactly where intruders are and where they are going. As a day-to-day application for hotel security officers, this application can be used to augment guest security and safety measures. In either case, having an integrated, tag-and-track network can significantly reduce insurance premiums for the hotel as it can provide real-time alerts for theft from guests or on-premise shops (such as jewelry), track the thieves, or provide real-time alert for assault of a guest, within the hotel.

Networks can be configured, in select locations within the hotel, to alert automatically for objects left behind or taken, for loitering activity in areas where it is not allowed, or for intrusion in restricted areas. Within “employee-only” 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. This is particularly important, within the hospitality industry, in the food-storage locker area. These areas can be secured with biometric access, restricted for only individuals who are authorized to enter. All entry/exit into these sensitive areas can be logged for audit purposes when required.

21st Century Command and Control, for Hotels

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.
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 hotel 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 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 for today’s hotels and resorts. 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.