ATLAS SAFETY & SECURITY DESIGN, INC.

SITE SECURITY PLANNING AND DESIGN CRITERIA

As presented at the **American Society of Industrial Security** Convention, Sept 1999

By Randall Atlas Ph.D., AIA and Anthony DiGreggario
Atlas Safety & Security Design, Inc.
Miami, Florida

1. Statement of the Problem

While architects have to design buildings that are fire resistant and be accessible to persons with disabilities, they don't have to make buildings resistant to crime. Designing for fire resistance and accessibility means complying with building codes and industry standards. The purpose of building codes around the United States is the protection of the health, safety, and welfare of the building occupants. Thus, architects and designers need to design for the safety and security of the users of the environment. The architects of the future must design against threats of criminal behavior, workplace violence, and acts of terrorism as part of their commitment to designing buildings that protect the building users.

The first contact a person has with a particular architectural project is accessing the site to gain entry to a property or building. With the increasing threats to persons and property, from acts of terrorism, workplace violence, and street crime, the first and most important line of defense is securing the site perimeter and the careful placement of the building/s on the given site.

Architects design buildings that serve a particular function for the users and clients of a building and hopefully do it in a pleasing aesthetic manner. But also important in fulfilling this task, this design should protect that user, ensuring their safety and security in the environment. The main guardian of health and safety for building designs are building codes, but these only address architectural features, such as egress design, fire safety, structural integrity, stair proportions, and railing design while ignoring the considerations of crime or terrorism. As safety is a prime consideration of building codes, security of the site and of building users should be considered a high priority.

2. Assessment Process

Achieving the correct level of protection against site-based threats may be very expensive and is highly dependent on the nature of the protected assets and the threat against which they require protection. Determining what is required is a matter of managing the perceived risks. If the designer is to assist in providing protection in the design of the site, an assessment of the security requirements must be accomplished preferably before the design begins, but certainly no later than the beginning of the architectural programming phase. This assessment is the responsibility of the owner; however, it is incumbent on the designer to assure that the nature of the security requirements is determined before the design begins. Failing to obtain a definitive answer will certainly result in design changes, delays, and cost increases to the owner and the architect if the owner "discovers" their security needs later in the design process.

The site assessment will answer the following four questions:

- What are the assets (persons, places, information, property) that require security protection?
- What are the criminal or other threats (street crime, workplace violence, terrorism, sabotage) against which the assets must be protected?
- What are the ruinerabilities of the assets to the threats (for example, if workplace violence is a threat, can uncontrolled persons enter private workspace unchallenged)?
- What are the countermeasures (for example, does the design channel visitors through controlled site access portals) required to mitigate the threat?

DESIGN CRITERIA

- Threat: Tactics; weapons, explosives, tools
- Assets
- Levels of protection
- Constraints

The result of the assessment will be a set of recommended countermeasures that may be priced and presented to the owner in a priority order so selections may be made of those recommendations that are prudent and cost effective. In the case of the government standards, the assessment results in the assignment of a defined Level of Protection (LOP) with specified countermeasures. When the LOP is defined, the specified countermeasures are priced and again the owner may select appropriate measures depending on a prudent level of protection and the cost effectiveness of the measure.

3. Security Layering: the Onion Philosophy

The first layer is the outside skin of the onion which translates to the site perimeter of the property. The building skin of the architecture is the next layer. Sensitive areas within a building are deeper layers requiring protection, and finally special persons, information, or property may require point protection or the center of the onion. The site perimeter is the first, not last, line of defense. The State Department seeks setbacks of at least 100 feet for new buildings and even that distance is difficult to obtain in most urban settings. While most perimeter fences and walls are designed to discourage intruders, they are of little use against a determined person or bomb vehicle.

Designs are now available for vehicle-stopping capabilities. The building skin is the next layer of protection. It is possible but never easy or inexpensive to minimize openings, orient them away from the perimeter, raise them above the ground, and provide windows, doors, grilles, and other devices that resist ballistic weapons, explosives, and forced entry all the while trying to retain a sense of openness, operable sashes, unobstructed views, and adequate natural lighting. The next layer is the interior space planning security. The most sensitive areas should be located high and away from exterior zones. Thought must be given to the use of spaces behind or near windows.

New developments in blast curtains, window films, and break resistant and bullet resistant glazing provide the designer with more choices for protection. Yet, a building that is resistant from an exterior bomb blast may be in conflict with the threat of an interior bomb blast and having no ability for decompression or blast out walls. Inside the building, zones or layers of security may be established with various types of access control devices reinforcing physical separations. Protected work stations are critical in many occupations, and safe rooms for CEO protection. Building design should also contribute to or ease implementation of operational security policies and procedures.

The site perimeter is the first, not last, line of defense. The State Department seeks setbacks of at least 100 feet for new buildings, and even that distance is difficult to obtain in most urban settings. While most perimeter fences and walls are designed to discourage intruders, they are of little use against a determined person or bomb vehicle. Designs are now available for vehicle-stopping capabilities. However, the bomb of the future may be delivered by a moped or pedestrian, thus rendering truck bombs unnecessary.

4. The GSA Security Standards

The bombing of the Murrah Federal Office Building in Oklahoma City gave birth to a federal effort to develop security standards that would apply to all federal facilities and an Interagency Security Committee has recommended their adoption as a government wide standard. During the testing of the standards, a number of state governments also reviewed the standards and applied them to several new construction projects. Consult local and state authorities for their specific applications.

The process of risk assessment and security design is especially relevant in architecture of schools, hospitals, airports, office buildings, multi-family apartment buildings, etc. Recently, buildings have been targeted for bombing by terrorists because of their "architectural vulnerability". This vulnerability will be addressed by methods described in this section.

The GSA Security Standards encourages a Defensible Space/Crime Prevention Through Environmental Design (CPTED) approach to clearly defining and screening the flow of persons and vehicles through layering from public to private spaces. Edges and boundaries of the properties should clearly define the desired circulation patterns and movements. The screening and funneling of persons through screening techniques is in the effort to screen legitimate users for the building from illegitimate users who might look for opportunities to commit crime, workplace violence, or acts of terrorism.

The result of approximately one year of work by the GSA panel is a set of Criteria covering four levels of protection for every aspect of security addressed by the U.S. Marshals report. The U.S. Marshall's report made a large number of recommendations for both operational and equipment improvements. The GSA Security Standards addresses the functional requirements and desired application of security glazing, bomb resistant design and construction, landscaping and planting designs, site lighting, and natural and mechanical surveillance opportunities (good sight lines, no blind spots, window placement, proper applications of CCTV). These recommendations were further subdivided according to whether they should be implemented for various levels of security (e.g. a level one facility might not require an entry control system while a level four facility would require electronic controls with CCTV assessment). Those requirements of the report which affect facility design and engineering are presented here in four general categories of corrective action used in the report.

The following should be addressed by the architect and engineering team for renovations or new construction on any federal building and is recommended for state and local buildings:

PERIMETER & EXTERIOR SECURITY

- Parking area and parking controls
- CCTV Monitoring
- Lighting to include emergency back up
- Physical Barriers

ENTRY SECURITY

- Intrusion detection system
- Upgrade to current life safety standards
- Screen mail, persons, packages
- Entry control with CCTV and electric door strikes
- High security locks

INTERIOR SECURITY

- Employee ID, Visitor control
- Control access to utilities
- Provide emergency power to critical systems
- Evaluate location of Day Care Centers

SECURITY PLANNING

- Evaluate locations of Tenant Agencies as concerns security needs and risk
- Install Mylar film on exterior windows
- Review/establish blast standards for current projects and new construction
- Develop a design standard for blast resistance and street set-back for new construction

The criteria take a balanced approach to security considering cost effectiveness, acknowledging acceptance of some risk, and recognizing that Federal buildings should be not bunker or fortress-like, but open, accessible, attractive, and representative of the democratic spirit of the country. Prudent, rather than excessive, security measures are appropriate in facilities owned by and serving the public.

ELECTRONIC SECURITY CONSIDERATIONS	THREAT	
	LOW	HIGH
Co-locate the Operational Control Center (OCC), Fire Command Center (FCC), and Security Control Center (SCC)	Not required	Yes
The Backup Control Center (BCC)	Not required	Manager's or Engineer's office consider redundant BCC
Electrical Utility Closets, Mechanical Rooms, and Telephone Closets	Present system of key entry should be maintained, with some method of noting times of entry and departure, such as a watchman's clock system	Access to mechanical, electrical, and telecommunication rooms shall be authorized, programmed, and monitored by the SCC through pre identification of maintenance personnel
Elevator Recall	Yes	Yes
Door Lock	Key-locked Security keying system	High security keying system/ electronic locks
Intrusion Detection	Magnetic reed switches w/optional glass break sensor	Same as LOW w/ balanced magnetic contact switch set and glass break sensor
Monitoring	Commercial Central Station	On-site, proprietary security control center review roof intrusion detection
CCTV	Not required	Yes

Duress Alarms	Key public contact areas, executive offices and garages as needed	Same as LOW

5.**Application of GSA Security Standards to all building types**

Whatever the building or its use, security and crime prevention should be a design criteria similar to fire safety, accessibility, and structural integrity. Any piece of architecture should establish a hierarchy of space that go from open access by the public, to semi-public, to semi-private, to private spaces. Any areas or spaces that are unassigned to a specific purpose or capable guardian should be avoided as it becomes "no man's land" and not claimed, protected, or defended by any individual or group. Traffic patterns of pedestrians and vehicles into sites and buildings should be carefully thought out and controlled for the desired goal. The design of any building should maximize the potential for natural observation by the legitimate building users.

Key defensive architectural site design considerations for bomb resistance:

- Establish a secured perimeter around the building that is as far from the building as is feasible. Setbacks of 100 feet are desired.
- Design artistically pleasing concrete barriers as flower planters or works of art and position them near curbing at a distance from the building with less than four feet of spacing between them to block vehicular passage.
- Build new buildings in a simple geometric rectangular layout to minimize the "defraction effect" when blast waves bounce off U-shaped or L-shaped buildings causing additional damage.
- Drastically reduce or totally eliminate ornamentation on buildings which can easily break away causing further damage to building occupants or pedestrians at street level. All external cladding should be made of light-weight materials that will minimize damage when they become flying objects following an explosion (or hurricane!).
- Eliminate potential hiding places near the facility.
- Provide unobstructed view around the facility.
- Site or place the facility within view of other occupied facilities.
- Locate assets stored on site, but outside of the facility within view of occupied rooms of the facility.
- Minimize the signage or indication of assets on the property.
- Provide a 100 foot minimum facility separation from the facility boundary if possible.
- Eliminate lines of approach perpendicular to the building.

- Minimize the number of vehicle access points.
- Eliminate or strictly control parking beneath facilities.
- Locate parking as far from the building as practical (yet address ADA spaces and proximity) and place parking within view of occupied rooms or facilities.
- Illuminate building exterior or exterior sites where assets are located.
- Secure access to power/heat plants, gas mains, water supplies, electrical and phone service

On a building level the GSA Security Standards recommend:

- Employ the concept of security layering.
- Locate assets in spaces occupied 24 hours a day where possible.
- Locate activities with large visitor populations away from protected assets where possible.
- Locate protected assets in common areas where they are visible to more than one person.
- Place high risk activities, such as the mailroom, on the perimeter of the facility.

On an interior security level the GSA Security Standards recommend:

- Employees and visitor identification systems.
- Secure the utility closets and vulnerable utilities.
- Develop emergency plans, policy, and procedures.
- Have daycare located and protected from unauthorized access.
- Screening points where applicable for weapons, pilferage, or identification.
- Secured and controlled shipping and receiving areas with integrated access control, CCTV, intercoms, data logging, and report capabilities.

6.**Application of security standards to other building types:**

The process can apply to all forms of architecture:

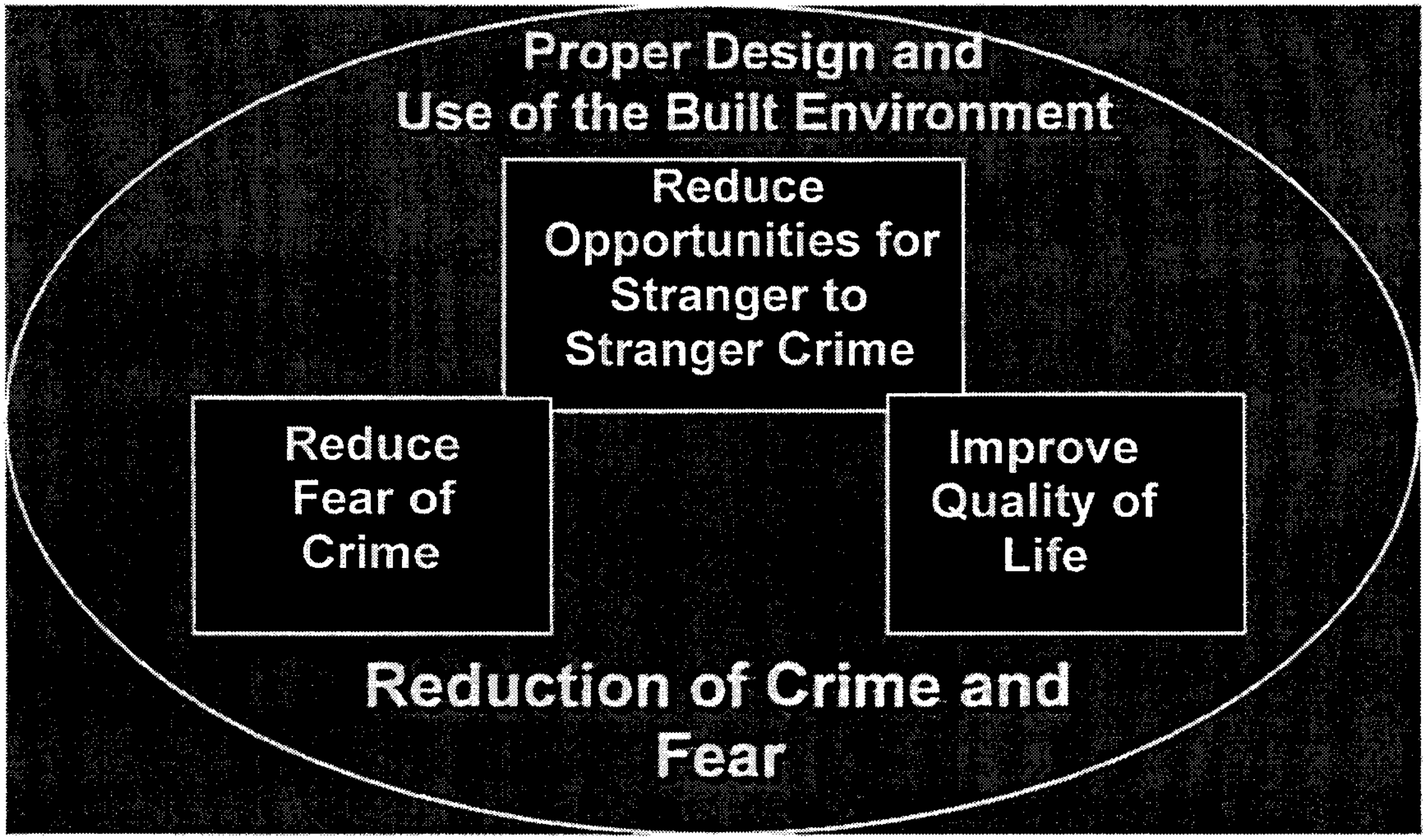
Institutional architecture: Police stations, courthouses, jails and prisons, post offices, schools, hospitals, airports

Commercial architecture: Office buildings, shopping centers, retail stores, restaurants, entertainment facilities

Residential architecture: Single family homes, townhouses, low-mid-high rise multi-family residential facilities, planned urban developments, hotels, rental apartments, public housing.

7.Security and Design: Crime Prevention Through Environmental Design (CPTED)

The definition of CPTED is: Through proper design and use of the built environment you can reduce the opportunities and fear of predatory stranger to stranger crime and improve the quality of life.


Proper Design and
Use of the Built Environment
Reduce Opportunities for Stranger to Stranger Crime
Reduce Fear of Crime
Improve Quality of Life
Reduction of Crime and Fear

CPTED strategies uses natural access control, natural surveillance, territoriality and boundary definition, maintenance and management enforcement, and legitimate activity support.

Any crime prevention strategy must accomplish the following: increasing the effort needed to commit a crime; increasing the risks associated with committing a crime; reducing the rewards of committing crime; and remove the excuses to commit crime. These goals are accomplished with organized methods of using people such as security guards or police or capable guardians or mechanical solutions that use technology systems and barriers together with natural methods that involve design decisions and behavioral psychology to choose and focus how persons and vehicles use our buildings.

Crimes are committed because they are easy to commit. A person sees an easy opportunity and so they do it regardless of the legality or consequences. Casual criminals are eliminated by increasing the effort needed to commit a crime. Target hardening is one method of increasing the effort using techniques such as: improving locks to be dead bolts, upgrading window screens, using break resistant glazing, increased use of fencing, and using magnetic locking doors. Another technique is access control which includes installing barriers, designing paths, walkways, and roads so that unwanted and unauthorized users are prevented from entering vulnerable areas. Barriers may include: limiting entrance to specific individuals, places, or times; security vestibules; parking lot barriers; entry phones; visitor check-in booths; guard stations; vehicle control systems; and bio-metric screening for access control.

The following may also be applicable:

Control access to the facility by pedestrian and vehicular traffic.

Divide interior and exterior spaces into small easily identified areas that are associated within a specific group of individuals or users.

Have detection devices easily visible to increase the perceived risk to the offender and by posting signs advertising the use of such devices.

Minimize the number of entrances to the interior of a building with the function of the remaining entrances clearly identified. Entrances should be secured when not in use.

Provide keyed access to vulnerable areas such as laundry rooms, storage areas, elevators, bathrooms.

Control parking lot access by means of gates and passes.

Restrict emergency stairs and exits to their intended use by equipping them with alarm panic bars with time egress delays and no exterior door handles.

Install barriers on vulnerable openings such as ground floor windows, exterior fire stairs, roof openings, and skylights. Fence off problem areas to prevent unauthorized access and funnel movement along desired paths.

Provide lockable security areas for items which are stored in low surveillance areas or items that are easily portable.

Control access for servicing and deliveries.

Increasing the risks associated with crime contributes to crime prevention by improving the probability that the criminal will be observed, identified, and arrested. Criminals commit crime because they believe they will not get caught. Ways to increase the risk of being detected and caught include entry and exit screening, formal surveillance, increasing surveillance capabilities by employees, and improving natural surveillance.

The following may also be applicable:

Screening devices should be used when appropriate to allow legitimate building users and guests. Employee screening should be separate with use of badges or ID's.

Formal surveillance uses security personnel and hardware such as CCTV and intrusion detection systems.

Informal surveillance by use of the facility employees uses the existing resources of doormen, concierge, maintenance workers, and secretaries to increase site surveillance and crime reporting.

Improving natural surveillance by careful architectural placement of windows, doors, lighting, and controlled landscaping and plantings.

Interior lighting enhances opportunities for casual or formal surveillance in spaces visible through doors and windows. Lighting should be even without deep shadows and fixtures should be vandal proof.

Interior blind spots such as alcoves and dead end corridors create vulnerable entrapment areas and should be eliminated when possible.

Reducing the rewards of crime makes illegal activity not worthwhile or productive to commit. This includes techniques that make targets of crime less valuable to the offender or which remove crime targets that have value to the criminal. To reduce the rewards of crime, the design professional can remove the high risk target from the premises or the architectural program (not to be included as part of the scope of work), identifying or tagging property assets, removing the inducements for crime, and rule and boundary setting. Removing the inducements of crime include removing those targets before they can become an easy opportunity.

- Vacant lots, apartments, offices, spaces should be used or given to legitimate users to protect against vandalism and damage.
- Exterior walls should be painted with graffiti resistant epoxy and/or landscaped with creeping vines to prevent the wall from acting as a mural for graffiti taggers.

Removing the excuses for criminal behavior is accomplished by clearly stating the ground rules against crime and establishing standard procedures to punish those who violate the rules. Clearly defined regulations and signage prevents offenders from excusing their crimes with claims of ignorance or misunderstanding.

The GOAL for architects and design professionals: Minimizing fortress design and target hardening, except where required AFTER thorough analysis and study. The design professional must address the issue of how can architectural design features and approaches be enhanced with security without intruding objectionable on the aesthetics and functionality of the building. How can electronic and automated physical security systems be integrated with the increasingly complex management and monitoring systems for fire protection, building environmental control, transportation and communications, and accessibility?

Design elements:

- Bollards/planters
- Curbs
- Vehicle barriers
- Security lighting
- Signage and groundrules
- Gates

Security Systems Elements:

- Consider space for placement of hardware and servicing
- Plan for generous wiring
- Plan for backup power
- Plan for intrusion detection devices
- Plan for site intrusion detection
- Plan for boundary penetration sensors
- Plan for Motion detection systems
- Plan for access control systems
- Plan for contraband and weapons detection
- Plan for explosive detectors
- Plan for credential readers and positive personnel identification systems
- Plan for security control and information display systems

Key defensive architectural design considerations for bomb resistance:

- Establish a secured perimeter around the building that is as far from the building as is feasible. Setbacks of 100 feet are desired.
- Use poured in place reinforced concrete for all framing including slabs, alls, columns, and roofs. Roof and base slabs should be at least 8 inches thick, exterior walls 12 inches thick, and columns spaced no more than 30 feet apart.
- Use "seismic detailing" at connection points (i.e., interconnect rebar in slabs with rebar in columns and beams so framing within a building becomes and integrated whole). Reinforce floor slabs and roofs using a two-way reinforcing scheme (i.e., place rebar in a criss-cross pattern with concrete).
- Design windows that comprise no more than 15 % of the wall area between supporting columns.
- Reduce flying glass hazard using a plastic mylar coating placed on the inside face of the windows.
- Install specially designed blast curtains inside windows that can catch pieces of glass while permitting airblast pressure to pass through the curtain.
- Design artistically pleasing concrete barriers as flower planters or works of art and position them near curbing at a distance from the building with less than four feet of spacing between them to block vehicular passage.
- Build new buildings in a simple geometric rectangular layout to minimize the "defraction effect" when blast waves bounce off U-shaped or L-shaped buildings causing additional damage.
- Drastically reduce or totally eliminate ornamentation on buildings which can easily break away causing further damage to building occupants or pedestrians at street level. All external cladding should be made of light-weight materials that will minimize damage when they become flying objects following an explosion (or hurricane!).

8.**CONCLUSION**

The GOAL for architects, design, and security professionals are: Minimizing fortress design and target hardening, except where required AFTER thorough analysis and study. The design professional must address the issue of how can architectural design features and approaches enhance security without intruding objectionably on the aesthetics and functionality of the building.

Site Security Design elements can include:

- Bollards/planters
- Curbs
- Vehicle barriers
- Security lighting

- Signage and groundrules
- Gates

Site Security Systems Elements:

Consider space for placement of hardware and servicing .

Plan for generous wiring.

Plan for backup power.

Plan for intrusion detection devices.

Plan for site intrusion detection.

Plan for boundary penetration sensors.

Plan for Motion detection systems.

Plan for access control systems.

Plan for contraband and weapons detection.

Plan for explosive detectors.

Plan for credential readers and positive personnel identification systems.

Plan for security control and information display systems.

Conduct the need assessment and include it as part of the architectural programming.

Determine the level of criticality and threats to the building assets.

Change how people use the building for legitimate authorized uses.

Use security technology last, once the circulation patterns are clear and the architecture of form reflects the function of facility.

Use the national standards as a starting point to establishing a standard of care in order to improve efficiency, safety, and security and to reduce premises liability from negligent security design and practices.

In conclusion, the design and security professional should:

Conduct the need assessment and include it as part of the architectural programming.

Determine the level of criticality and threats to the building assets.

Change how people use the building for legitimate authorized uses.

Use security technology last, once the circulation patterns are clear and the architecture of form reflects the function of facility.

Use the national standards as a starting point to establishing a standard of care, in order to improve efficiency, safety, and security and to reduce premises liability from negligent security design and practices.

9. Where to get more information:

ASIS - American Society for Industrial Security- www.Asisonline.org

CPTED: Web: www.CPTED-security.com

www.spartacc.com

www.ncjrs.org

BOMBCAD - Everett Brown Co. 950 N Meridian ST. Indianapolis, In. 46204, 317-237-7043
SECURITY LIGHTING - Illumination Engineering Society of North America

Written by Dr. Randall I. Atlas, AIA, CPP of Atlas Safety & Security Design Inc. Miami, Florida. and Anthony DiGreggario, Applied Research Associates, Washington DC.,