INTERNATIONAL CODE COUNCIL®

BUILDING SAFETY AND SECURITY REPORT



December 2022

COPYRIGHT © 2022

BY

INTERNATIONAL CODE COUNCIL, INC.

All RIGHTS RESERVED. This Report is a copyrighted work owned by the International Code Council, Inc. ("ICC"). Without advance written permission from the ICC, not part of this publication may be reproduced, distributed or transmitted in any form or by any means, including, without limitation, electronic, optical or mechanical means (by way of example and not limitation, photocopying, or recording by or in an information storage and retrieval system). For information on use rights and permissions, please contact: ICC Publications, 4051 Flossmoor Road, Country Club Hills, Il 60478, phone 888-ICC-SAFE (422-7233).

The information contained in this document is believed to be accurate; however, it is being provided for information purposes only and is intended for use only as a guide. Publication of this document by the ICC should not be construed as the ICC engaging in or rendering engineering, legal or other professional services. Use of the information contained in this work should not be considered by the user as a substitute for the advice of a building safety and security assessment professional, registered professional engineer, licensed architect, attorney or other professional. If such advice is required, it should be sought through the services of the professionals noted.

Trademarks: "International Code Council," the "International Code Council" logo, "ICC," the "ICC" logo and other names and trademarks appearing in this guide are registered trademarks of the International Code Council, Inc.

ICC FAMILY OF SOLUTIONS

ICC INTERNATIONAL CODE COUNCIL®

PREFACE

Purpose

Building safety and security is an issue of utmost importance. The design, layout and building features in new and existing buildings can have an impact on both safety and security. Safety and security impact a myriad of code regulations as well as considerations which go beyond code compliance. Many states and local jurisdictions are developing legislation and policies in response to a variety of emergency acts including those surrounding this topic. Due to the complex and unpredictable nature of such acts, it is imperative that all aspects of the built environment be thoroughly analyzed in order to develop a comprehensive response.

Goal

The goal is to provide comprehensive, sound and valuable tools for local and state authorities to guide them in keeping occupants of facilities, including schools, safe from intruders and other life-safety hazards in the built environment. See the Scope and Objectives in Appendix A.

Development

The International Code Council Board of Directors established the Ad Hoc Committee on Building Safety and Security (AHC-BSS) to comprehensively explore and assess building safety and security. Building safety impacts our families, first responders and communities as we are confronted with outdated facilities, fire safety concerns, active shooters and other emergency situations. “Safety and security in buildings is of the utmost importance to our children, our coworkers and our communities,” stated ICC Board Director and Committee Chair Angie Wiese, PE, CBO. “I look forward to working closely with the design community, building managers, school districts, and local and state leaders to develop the tools we need to keep us safe in emergency situations.”

The committee consists of a broad cross section of experts from the building industry, building owners and facility managers, the education sector and security fields, code officials, engineers, architects, standards developing organizations such as ICC, NFPA, and UL and the federal government. The committee make-up is on the next page.

Report organization

The report contains information on the following key considerations in achieving building safety and security:

- Risk Assessment
- Administration/Planning
- Facility Hardening
- Access Control
- Video Surveillance
- Appendices are included at the end of this report with additional history, checklists, resource materials and documentation

The considerations are organized by chapter which typically includes the following:

- Overview
- Approach
- Findings
- Discussion
- Recommendations
- References

ICC INTERNATIONAL CODE COUNCIL®

Ad Hoc Committee on Building Safety and Security

Angie Wiese, PE., CHAIR
Fire Safety Manager
City of Saint Paul
Saint Paul, MN

Lou Chavez
Principal Engineer, Security and Life Safety
UL LLC
Northbrook, IL

Ronald W. Clements, Jr., CBO
Assistant Building Official/Assistant Director
Chesterfield County Building Inspection Department
Chesterfield, VA

Benjamin Comm, CPM
Rep: Building Owners and Managers Association
Senior Managing Director
Cushman & Wakefield
Washington, DC

Charles G. Darnell, MBA
Retired: Previously Associate Vice President for Facilities
Utah State University
Logan, UT

Connie Forster
MN Safe School Assessment Coordinator
MN Department of Public Safety/Homeland Security & Emergency Management/MN School Safety Center
St. Paul, MN

Dave Frable
Senior Fire Protection Engineer
U.S. General Services Administration
Geneva, IL

Lew Galante
Chief Financial Officer
Perry Local Schools
Perry, OH

Henry L. Green, Hon. AIA
Retired: Previously President of the
National Institute of Building Sciences
Washington, DC

Jason Ziph
Fire Inspector
City of Ames
Ames, IA

Judith Hoskens, Assoc. AIA, Fellow-A4LE, REFP, LEED AP (AIA)
Chair, AIA Commitee on Architecture for Education
Minneapolis, MN

Scott McCormick
Fire Official
Hamilton Fire Division
Hamilton, NJ

Randall Metz
Battalion Chief – Fire Marshall
Carlsbad Fire Department
Carlsbad, CA

Seth Model
Police Officer
Austin Police Department
Austin, TX

Coy D. Porter
Rep: ICC Fire Service Membership Council
Retired Utah State Fire Marshal
State Fire Marshal's Office
Sandy, UT

Kurt Roeper
Director
ASSA ABLOY Americas
New Haven, CT

B. Karina Ruiz, AIA
Rep: American Institute of Architects
Principal
BRIC Architecture, Inc.
Portland, OR

Robert Solomon, PE
SLS Consulting LLC
Previously Director of Building/Life Safety Codes and Fire Protection Systems
National Fire Protection Association
Boston, MA

John Woestman
Rep: Builders Hardware Manufacturers Association
Director of Codes & Standards
Kellen Company
New York, NY

Staff Secretariat
Mike Pfeiffer, PE
Senior Vice President, Technical Services
International Code Council

AHC-BSS WORK GROUPS

The AHC-BSS relied heavily on the contributions of individual work groups created to study specific topics, typically by chapter as organized in this document. Each chapter starts with an "Overview" which is scope of the respective work group. The following is a list of work groups and participants. Each work group was chaired by a member of the AHC-BSS. AHC-BSS committee members are noted by asterisk (*).

Chapter 2: Risk Assessment
Charles Darnell*, Chair
Tom Czyz, Armoured One
Dennis Elledge, The Upchurch Group
Connie Forster*
Dale Gigandet, Security Entry Consultants
Henry Green*

Chapter 3: Administration/Planning
Robert Solomon*, Chair
Kris Bridges, City of Martinsville, VA
Dennis Elledge, Compsecure
Connie Forster*
William Funk, Cecil County, MD
Henry Green*
Judith Hoskens*
Joseph Lavelle, Architect
Jerry Loghry, American Property Casualty Insurance Association
Kerri Brady (Ranney), Huckabee & Associates, Inc.
Gary Sigrist, Safeguard Risk Solutions

Chapter 4: Facility Hardening
Ron Clements*, Chair
Kerri Brady (Ranney), Huckabee & Associates, Inc.
Thomas Czyz, Armoured One
Daniel Dain, Huckabee & Associates, Inc.
Charles Darnell*
William Funk, Cecil County Maryland Permits and Inspections
Joe Guarrera Jr., Optimus Consulting
Joseph Lavalle, Architect
Scott McCormick*
Craig Miller, Craig Miller Group, LP
Nicholas Resetar, Glazing Industry Code Committee
Kurt Roeper*
Karina Ruiz*
Steven Saffell, American Architectural Manufacturers Association
Kristen Walton, Utah State University
Dan Willham, Fairfax County Virginia Building Inspection Department
Steve Zaferakis, Armoured One
Thom Zaremba, National Glass Association

Chapter 5: Access Control/Hardware
John Woestman*, Chair
Desmond Burke, City of New York City
Micah Chappell, City of Seattle
Lou Chavez*
Ron Clements*
Ben Comm*
Dave Frable*
Dale Gigandet, Security Energy Consultants
Jennifer Gilliland, City of Seattle
Jeff Grove, Jensen Hughes
Joe Guarrera, Optimus Sales, LLC
Kathy Krafka Harkema, FGIA
Scott McCormick*
Coy Porter*
Kim Powers, Jensen Hughes
Nicholas Resetar, Glazing Industry Code Committee
Kurt Roeper*
Dan Willham, Fairfax County Virginia Building Inspection Department
Thom Zaremba, National Glass Association

Chapter 6: Surveillance
Lou Chavez*, Chair
Dale Gigandet, Security Energy Consultants
Bruce Johnson, UL
Jerry Loghry, American Property Casualty Insurance Association

Appendix D Response
Seth Model*, Chair
Randall Metz*
Angie Wiese*

INTERNATIONAL CODE COUNCIL®

TABLE OF CONTENTS

PREFACE 3

CHAPTER 1—INTRODUCTION 9

CHAPTER 2—RISK ASSESSMENT 10

CHAPTER 3—ADMINISTRATION/PLANNING 17

CHAPTER 4—FACILITY HARDENING 24

CHAPTER 5—ACCESS CONTROL 28

CHAPTER 6—SURVEILLANCE 41

APPENDIX A—BUILDING SAFETY AND SECURITY SCOPE AND OBJECTIVES 45

APPENDIX B—ACRONYMS AND DEFINITIONS 46

APPENDIX C—PLANNING CHECKLIST 49

APPENDIX D—FIRST RESPONDER RESPONSE CHECKLIST 52

APPENDIX E—NGA: SECURITY GLAZING SUMMARY 55

APPENDIX F—ACCESS CONTROL FOR BUSINESS OCCUPANCIES 56

APPENDIX G—RESOURCE MATERIAL 59

CHAPTER 1—INTRODUCTION

Since the 1966 slayings of 11 people and the wounding of 31 others on the University of Texas campus, there have been many targeted acts of violence in buildings including the grounds of public schools, university campuses, churches and other high occupancy facilities. These acts of violence have resulted in hundreds of deaths and injuries as well as traumatic stress among survivors that will likely endure over their lifetimes. In 2018, the FBI designated 27 separate shooting acts in 16 US states as active shooter incidents. These incidents resulted in 213 casualties, including 85 killed and 128 wounded (https://www.fbi.gov/file-repository/active-shooter-incidents-in-the-us-2018-041019.pdf/view). Mass shootings involving four or more victims, as defined by the Gun Violence Archive, numbered 611 in 2020 and 693 in 2021. These targeted violent acts resulted in 31 and 21 mass murders for both years, respectively, according to the Gun Violence Archive. In 2019 there were 28 incidents in 16 states, 247 casualties (97 killed and 150 wounded) (https://www.gunviolencearchive.org).

As societal awareness and concerns continue to increase in response to targeted violent acts, the role of building, life safety, and fire codes to help address these acts is now at the forefront of the discussion. Although the codes currently, and previously looked at isolated elements related to security type issues such as delayed egress locks, access control doors, there continues to be ongoing debate and deliberation about developing expanded security content and resources for mainstream audiences and stakeholders.

Because human-initiated, targeted acts of violence in the built environment have increased in number and severity, the International Code Council established an ad hoc committee to comprehensively explore and assess the current status of building safety and security measures being employed during design and construction of facilities. The charge of the multidiscipline Ad Hoc Committee on Building Safety and Security (AHC-BSS) includes a review and evaluation of existing codes and other available resources. The Committee was also tasked with making recommendations to stakeholders who have an obligation to provide reasonable levels of safety and security to building occupants. Many of these stakeholders were represented on the Committee, including a broad cross-section of design professionals, code officials, architects, engineers, first-responders, facilities managers, building product manufacturers, security professionals, and law enforcement personnel.

The premise of this report is that in order to enhance building safety and security in response to targeted violent acts in the built environment, all stakeholders should be focused on: design elements, devices, and protocols that hinder those who intend to commit violent acts; provide some measure of safety and security to building occupants; and facilitate quicker and more effective response from emergency personnel. The report does not focus on cyber security or building security to the extent such issues are addressed in current fire and building codes, or security measures related to safeguarding physical assets in a building.

Based on the recent history of such violent acts, it is clear that this unfortunately is an evolving situation with many different variables such that each act is different . As such, the primary objective of this report is to stimulate thought, communication, and future research on the topic of safety and security assessment among the multiple stakeholders - with the realization that there is much work left to be accomplished.

ICC INTERNATIONAL CODE COUNCIL®

CHAPTER 2—RISK ASSESSMENT

Overview

This chapter highlights the importance of identifying risks to a facility before selecting options for coordinated solutions to safety and security. It also provides a best practices framework for conducting a risk assessment for a facility. Emphasis is placed on the ease of use to support a wide range of users.

Critical components of risk assessment also include privacy documents/process, surveillance and first responder response. Surveillance includes both virtual (cameras/sensors) and physical surveillance at a facility, including best practices and resources available.

The information contained in this chapter is intended to be generic to all occupancies but also includes examples using specific occupancies, where appropriate. It should be noted that this document is intended to be specific to the facility itself and not overall community risk assessment. For community risk assessment, consult NFPA 1300 Standard for an Active Shooter/Hostile Event Response (ASHER) Program.

Approach

The AHC-BSS reviewed reference material from multiple sources, including, but not limited to: NFPA, ASIS, FEMA, ASHRAE, CPTED, and BOMA as listed in Appendices B and G. The AHC-BSS does not believe any single document, or set of cohesive documents from multiple sources, currently exists that fully address the subject of occupant safety and security for targeted violent acts. On one end of the spectrum, the Crime Prevention Through Environmental Design (CPTED) provides very practical guidelines for designing safer facility environments that can help deter criminal activity such as petty crime, simple assaults, or property related crimes. While, CPTED does not appear to have been developed to address targeted violent acts as defined in this document, some of its design principles involving surveillance and occupant/vehicle movement control, could also serve as countermeasures identified in a safety and security assessment. Conversely, FEMA offers design standards for hardening sensitive government facilities, which often requires a significant cost component. What appears to be absent among many existing design and code resources, are practical safety and security design considerations that are specific to varying building functions, address multiple risks, and occupancy types that provide a balance approach to mitigation strategies via an “all-hazard” assessment. These considerations can be objectively assessed early in the design phase.

Findings

Most of the provisions in existing building, fire and live safety codes and related resources are associated with occupant life-safety as opposed to safety and security during targeted violent acts. Design security resources typically focus on limiting petty crimes in the built environment, while active shooter resources focus mostly on planning, as well as command-and-control around the possibility of a violent acts, such as an active shooting incident.

While this document primarily focuses on design of new facilities, it is the position of the AHC-BSS, that with the increasing number of targeted violent acts occurring within the built environment, building owners need to be more proactive regarding building safety and security. Additionally, the AHC-BSS has considered that building owners may need to provide reasonable measures of safety and security to occupants of their facilities. For these reasons, the committee believes that to provide requisite levels of safety and security to building occupants across a broader spectrum of the built environment, the need to perform a Building Safety and Security Assessment (BSSA) should be expanded to include existing facilities deemed to be at high risk for targeted violent acts affecting multiple occupants.

Discussion

Current state of Building Safety and Security Assessments (BSSA) with AHJ's

Currently, safety and security assessments during building design are not required by most state or local authorities having jurisdiction. The State of Virginia, is one example where under state law, Section 22.1-140 (iii) (amended and approved March 15, 2019), there is a requirement that plans and specifications for a public-school building *"be reviewed by an individual or entity with professional expertise in building security and crime prevention through building design."*

However, the Virginia law as written, does not define the standard of review, the credentials for those having professional expertise to perform a review, or which of the available resources should be used as criteria in a review. Even though this information and resources have not been identified at the time of compiling this report, Virginia should be commended for being the first State to conclude that a security and crime prevention review during design of a specific type of building occupancy is necessary.

Within North America, building safety and security measures appear to be primarily driven by product end-users, building owners, facility managers, security officers, and insurance authorities. There are few codes or published best practices that mandate compliance or recommend building safety measures which impact building occupants during targeted violent events. Enforcement of security applications will require oversight by a dedicated authority having jurisdiction (AHJ), who has specific knowledge of building safety and security. Therefore it is important that a certified security design professional is involved in each phase of design and construction of high occupancy and high-risk buildings. (see definitions in Appendix B).

There are many disparate resources currently available to building designers, owners, and facilities managers, which can assist them with building design features that may inhibit targeted violent acts while enhancing occupant safety and first response. However, there also appears to be a void between the most basic and pragmatic design features that most facility designs would automatically include, and those which would add considerable cost for building owners to implement. As noted in Chapter 1 there are three areas of concern that the AHC-BSS have identified from its research which pose challenges to current BSSA practices and procedures: design elements, devices, and protocols that hinder those who intend to commit violent acts; providing some measure of safety and security to building occupants; and facilitating quicker and more effective response from emergency personnel

Recommendation: Local jurisdictions should implement a requirement that all new planned construction of public or private high occupancy or high-risk facilities require a BSSA be performed during planning and design development. The BSSA should be presented in written format, and/or as markups in a plan review presented to the principal in charge of the design team and to the primary owner of the proposed facility. Additionally, the BSSA should be performed by individuals who have received standardized training through an accredited program (where available – see Chapter 3) offering a certificate that acknowledges competence and experience of an assessor to develop a BSSA.

Countermeasures

Countermeasures need to be comprehensive and vetted by the project team. In all likelihood, there will be a mixture of high emotion and a sense of urgency which may result in building owners, facilities managers, and occupants sometimes taking matters into their own hands. No matter how well-meaning these actions may be, these stakeholders can inadvertently increase the risk of making emergency situations worse for building occupants and first-responders. In fact, some countermeasures employed for the sake of increasing safety during a targeted violent event are not code compliant and can actually hinder occupant safety during non-violent emergencies, which are also much more common.

Examples include non-fire code compliant locking hardware that has been installed in meeting rooms and classrooms, with the intent to lock out suspected committers of a targeted violent event. In another example, after attending a run-hide-fight training program, an instructor tried to obtain roof access keys for the purpose of having a place of refuge for his students during an active shooting event. The AHC-BSS also learned of non-code compliant building modifications, including the removal of audible fire alarms and other actions which were being initiated by occupants and building owners in an attempt to cope with the possibility of a targeted violent event. By encouraging or inadvertently eliciting human reactions that are contrary to those which should occur during a fire or seismic event, occupant risks can be exacerbated with countermeasures that are non-code compliant.

Certain design and operational countermeasures that are intended to provide occupant safety, and to enhance first response, may also have unintended consequences in practice. Whether a safety proposal is to increase the use of glass for visibility in buildings, implementing lock-down strategies, the use of silent alarms, or enhancing occupant notification procedures, design teams face a myriad of safety and security choices that can inadvertently provide advantages to the committers of violent acts. However, all proposed design countermeasures should be thoroughly evaluated during design development, incorporating whenever possible, the input of the BSSA assessor as well as first-responders. See Chapters 4 and 5 for a discussion on possible safety and security solutions.

> **Recommendation:** A uniform list of potential safety and security countermeasures, concepts, construction materials or products and operational protocols should be developed that can be utilized as the basis of design best practices and assessment during planning and design. Such a list should be transparent, readily available and capable of being updated as countermeasures may change over time. Such an effort should be coordinated among the key stakeholders such as ICC, NFPA, ASIS, AIA, ASHRAE, BOMA, FEMA, and others in the development of standardized BSSA criteria.

The stakeholders should work together to produce a single uniform document, or set of cohesive documents, of BSSA best practices to be considered in the design of all high occupancy or high-risk buildings, public or private. The reference materials listed in Appendix G can be used to further develop and expand the concepts found in this report. For example, NFPA, ASIS, and FEMA have developed security design criteria that could be used as part of a BSSA.

Surveillance

Surveillance is a countermeasure which includes both virtual (cameras/sensors) and physical surveillance at a facility. As with any piece of operational equipment, acceptance testing of security systems is important as well as routine testing and monitoring.

Surveillance must include: an emphasis on digital data captured by network or Internet Protocol (IP) cameras (network camera and IP camera are two names for the same thing) connected via a Wide Area Network (WAN); background material regarding trends and analytics; topical use-cases reflecting newsworthy events shaping the use of video; and an implementation plan.

> **Recommendation:** Surveillance should be incorporated as a countermeasure when implemented based on reliable guidance such as that found in the Department of Homeland Security's "Digital Video quality Handbook Appendix" listed under the "resources" at the end of this chapter.

See Chapter 6 for a complete discussion on surveillance.

First Responders

As a building owner or facility manager, safety and security are paramount to the occupants of your facilities. Owners and managers are part of the local community. When there is an emergency, time is of the essence for first responders. As building and life safety codes strive to keep occupants safe, reaching out to local responders (law enforcement, fire, EMS) helps bring those design features to fruition. Relationships with local responders before an emergency is important as it assists in the effectiveness of an emergency response, such as maps, diagrams and other essential information on the facility and the surrounding area. Training is also beneficial whether using a tabletop or full-scale exercise.

While there exists a minute-by-minute written forensic account of nearly every contemporary targeted violent act in the built environment from a law enforcement perspective, there is minimal information available to inform designers of the perceptions and interactions of first-responders to the built environment during such acts. As noted by a state fire marshal, first-responders are trained to accept the built environment as-is, and to expect that job success, and likely their own survival, hinge on being adaptable in every situation. The AHC-BSS notes that the importance of adaptability of first-responders would not be lessened through their more intensive involvement in the facility planning process. However, the committee concludes that there exists untapped potential to enhance building safety and security best practices, as well as to secure alternate perspectives during design development of high occupancy and high-risk facilities, should first-responders be more integrally involved.

It is important to note that the AHC-BSS is not proposing that first-responders represent an additional code official or other type of authority having jurisdiction outside of established enforceable codes. First-responders, however, are stakeholders who appear to be rarely included in design development meetings of high occupancy or high-risk buildings. The committee suggests that first-responders are an important constituent in their jurisdictions, and that they should be extended similar input authority as other stakeholders involved in facility planning. First-responders should be considered a resource to building owners, designers, and to BSSA assessors.

Recommendation: The AHC-BSS strongly advocates for involvement of law enforcement and fire service personnel, EMS and other first-responders in the development of a uniform set of building safety and security best practices that are tied to a BSSA, as well as involvement of first-responders during design development, as it pertains to building safety and security for high occupancy or high-risk facilities within their jurisdictions. See Appendix D for a first responder checklist.

Building safety and security stakeholder training

Many organizations offer training and education in areas that address building safety and security, including but not limited to ICC, NFPA, ASIS, AIA, ASHRAE, FEMA, BOMA, NGA, etc. As an example, ASIS provides training and professional certification for security practitioners such as the Certified Protection Professional (CPP) and Physical Security Professional (PSP).

The AHC-BSS recommends the following training requirements for each stakeholder group involved in design, ownership, and operation of high occupancy or high-risk facilities:

Assessor training

A certification, if offered by multiple agencies, including private or not for profit organizations, should require a minimum standardized set of learning outcomes, prerequisite professional experience, requirements for on-the-job experience, and a minimum required time investment by a prospective trainee. While a nationally recognized training regimen should be able to be duplicated by multiple qualified agencies, an independent agency should provide oversite of the BSSA accreditation process to ensure standardization and equivalency of training programs leading to a BSSA certification.

Recommendation: A standardized training regimen be identified and developed for certifying a BSSA accessor. Such an effort should be coordinated among the key stakeholders including ICC, NFPA, ASIS, AIA, ASHRAE, BOMA, FEMA and others in the identification or development of standardized and accredited training programs that offer professional BSSA Assessor certifications.

Designers and building owner training

Minimal knowledge is defined as consisting of an implicit understanding that new buildings intended for high occupant loads, or those considered to be high risk, should incorporate a BSSA during planning and design by a certified assessor, and that the process of risk evaluation to occupants also involve first-responders.

Recommendation: Architects, engineers, consultants, and building owners should become at least minimally knowledgeable of occupant safety and security issues impacting building design and operations.

Facility manager training

Training should ensure an understanding of the purpose of a BSSA, as well as knowledge of the physical safety and security assets in the building that will fall under the maintenance and operational supervision of the facility manager. With such knowledge, facility managers can ensure that maintenance staff and occupants do not inadvertently defeat safety measures. Similarly, the facility managers can direct staff to properly maintain safety and security countermeasures implemented in their facilities.

Equipment and devices may include but are not limited to locking and access control hardware, firmware, and software; alarm systems including, fire, panic and blue-light systems; surveillance cameras and other IT systems related to safety and security. Operational protocols may include but are not limited to ASHER planning, personal alert systems, occupant egress, or refuge plans.

Facility managers should utilize periodic onsite visits with first-responders to provide an overview of security devices; equipment and operational protocols, including access control sequencing, alarm locations and types of alarms; way-finding signage and room numbering schemes; mechanical, electrical, communications, and IT systems; types and time-of-day occupancies; standard and non-typical building functions; as well as unique facility characteristics or changes in floorplan and building layout. An example of a robust certificate program for Fire Safety Directors/Emergency Action Managers is a program in Chicago (https://www.chicago.gov/city/en/depts/cfd/provdrs/prevent/svcs/emergency_preparednesscertificateapplication.html)

Recommendation: Facility managers should receive condensed training similar to that received by a certified BSSA accessor. Such managers have a responsibility to ensure proper maintenance of safety and security devices and equipment as well as compliance with safety and security operational protocols. Further, facility managers and their staff have a responsibility to provide periodic site-specific orientation for first responders of high occupancy or high-risk facilities under their purview.

First responder training

A better understanding of construction documents will assist first-responders by providing them with the basic knowledge of the order in which construction documents are organized; how to locate specific rooms by function or room number; location and basic operations of utility infrastructure systems such as power, water, communications, and IT; and, building occupant conveyance systems such as elevators, escalators, and moving walkways, foyers, atriums, and stairs.

An onsite review should include security devices and equipment, as well as operational protocols that include but are not limited to: automated access control; locations and types of alarms; way-finding signage and room numbering schemes; mechanical, electrical, communications, and IT systems; time-of-day occupancy patterns; standard and special building functions as well as unique facility characteristics or changes in floorplan and building layout.

On-site orientation will improve first-responders' understanding of building layouts, mechanical operations, occupancy patterns, as well as safety and security devices, equipment, and protocols. First-responder facility orientation will also assist in their ability to participate in design reviews as well as active first-response by equipping them with basic facilities knowledge and improved ability to speak the language of design and facility management professionals.

Recommendation: First responders, including fire, police, and other emergency personnel who would be required to respond to targeted violent acts in high occupancy or high-risk facilities receive condensed training, similar to that received by a certified BSSA assessor. First-responders must become more proactively involved in safety and security assessment during planning and design development of high occupancy or high-risk buildings in their jurisdictions. First-responders should periodically conduct onsite visits with appropriate facility management staff in high occupancy or high-risk facilities within their jurisdiction. First-responders should attend training to assist them in understanding how building designs are communicated though construction documents..

Recommendations

The following is a compiled list of risk assessment recommendations found in this chapter.

1. Local jurisdictions should require a BSSA for new and existing high occupancy and other high-risk buildings. A BSSA should evaluate and identify occupant risks during a targeted violent event and recommend design countermeasures and operational protocols aimed at mitigating those risks.
2. Building owners should consider providing a reasonable level of safety and security to their building occupants against a targeted violent event.
3. If a BSSA is not required by law or code for existing high occupancy or high-risk buildings within a jurisdiction, owners and facility managers should consider the benefits of conducting a BSSA for their existing facilities.
4. Those who perform a BSSA should be professionally trained and certified to perform this work. An independent agency should take responsibility for establishing uniform certification requirements for assessors and act to convey accreditation to agencies or organizations wishing to offer an official BSSA assessor certification.
5. A single definitive document should be developed to provide best-practices for providing building safety and security, as well as objective and qualitative evaluations of countermeasures that might be employed to increase building safety and security during a targeted violent event. Such an initiative should involve a comprehensive group of industry stakeholders including ICC, NFPA, ASTM, ASIS, AIA, ASHRAE, BOMA, FEMA, NGA, and other experts in construction materials being used to provide building safety and security.

6. Countermeasures involving surveillance must be implemented based on a reliable known source such as the Department of Homeland Security.
7. Building owners, facility managers, and members of design teams should receive condensed training regarding BSSA objectives and countermeasures implemented as a part of a building system or as an operational protocol. Training on these systems should be treated with the same level of importance as the proper function, operation, and maintenance of any other major building system.
8. First-responders should receive condensed training on BSSA objectives and countermeasures that are implemented as a building system or as an operational protocol for high occupancy or high-risk buildings within their jurisdictions.
9. First-responders should be integrated within the planning and design teams for their input regarding high occupancy or high-risk buildings in their jurisdictions.
10. First-responders should receive remedial training in understanding design and construction documents used by the industry to communicate building design and construction criteria, and with specific attention to an ability to review and comprehend floorplans, site plans, mechanical, electrical and IT systems drawings.
11. First-responders and facility managers should meet periodically, but not less than annually, on site of high occupancy or high-risk facilities within their jurisdictions to orient themselves with building specifics, including safety and security systems and countermeasures, as well as general building layout, wayfinding signage, and locations of critical facility infrastructure.

References (See Appendix G)

- First responder response checklist (See Appendix D)
- NFPA 3000 Standard for an Active Shooter/Hostile Event Response (ASHER) Program
- US Department of Homeland Security (DHS) Digital Video Quality Handbook Appendix

ICC INTERNATIONAL CODE COUNCIL®

CHAPTER 3—ADMINISTRATION/PLANNING

Overview

This chapter highlights the stakeholders involved, the importance of coordinated planning for each facility, and the best practices surrounding privacy of documents and communication of the plan. It also encompasses best practices in preparing and performing drills for both safety and security. Communication plays a crucial role in planning - both internally for building occupants and externally with first responders.

The information contained in this chapter is intended to be generic to all occupancies but also includes examples using specific occupancies, where appropriate.

Approach

Seven topical areas are addressed. These include:

- Identification of Stakeholders
- Importance of Planning Scenarios and Concepts
- Document Privacy
- Developing and Reviewing Appropriate Plans and Drills
- Library of Resources
- Generate Work Product for All Occupancy Types
- Identification of existing, or future development of a security professional category

During each review or analysis of these seven areas, it is important to understand that integration of security into the building project is not a one-size-fits-all proposition. Design, planning, drilling, and occupant characteristics will vary between types of occupancies. Systems and features that may be appropriate for an educational occupancy (K-12) would not be appropriate for the health care environment nor a business occupancy. Thus, finding the right mix of attributes will vary between occupancies.

As mentioned previously, the expertise of the design team should include security professionals and first responders. With few exceptions, such expertise is generally not part of the design team early in the project — and in some cases, never really considered. When considering security designs or enhancements, they must be done at the beginning of the project.

Otherwise, security features would be left to being considered once the certificate of occupancy is issued which presents challenges as the features would need to be incorporated into an existing building versus the original design. Such a retro-fit could be costly when compared to initial design features.

Findings

While code provisions and regulations, as well as administrative and operational provisions have been established over many decades, and in some cases centuries, integrating discussions related to security issues for the occupants and the buildings themselves is not necessarily an easy task. However, it is not an impossible task. Chapters 4 and 5 address aspects such as the brick-and-mortar design criteria, locking arrangements, and first responder protocols, while this chapter is looking at the operational controls or management side of those challenges. This can range from controlling access to building drawings that may show security system or building construction/configuration layouts, maintaining restrictions on access to building emergency plans, and limiting the publicly available information related to electronic security system features used in the building.

Administrative controls (also referred to as "engineering controls") require a collaborative approach between building owners/managers, the design team of architects and engineers, contractors, and tenants to name just a few. The development and establishment of policies or regulations from legislative bodies (predominantly from the local and state levels) is a key consideration to having a successful and comprehensive plan in place. Participants in the planning, contingency, or response programs will include professions and positions that normally do not interface with either the code aspect or the everyday building design aspect. A specific example of this would include a company's director of human resources.

Related challenges associated with this effort also include the need to look beyond the crossover between building security and targeted violence. For example, as the cannabis industry continues to expand via production and commercial sale to the public, these buildings and facilities oftentimes have enhanced security measures that are atypical for most industrial manufacturing facilities or mercantile occupancies.

As a result, there may be a need to utilize the legislative process at the state or local level to allow for future changes and enhancements to be made to the model codes and standards that are adopted. This may be a lengthy process to have a connected role in resources between building security, relevant code enforcement provisions, and certification/licensing programs that will help to blend these processes into the built environment.

Discussion

Identification of stakeholders

Stakeholders identified as part of this process include the building owner, building operator, facility manager, law enforcement personnel, fire and EMS personnel and the building occupants. Collectively, each of these entities is either paying for, impacted by, or responding to circumstances or situations that might occur in the building. Derivatives or subsets of these groups will also vary by occupancy. For example, essentially every employee in a school building from the school administrators and principals, to teacher aides and janitors would be a part of the stakeholder group as they are part of the first responder team before the traditional first responders arrive.

The roles for code officials and other authorities having jurisdiction (AHJ) are particularly essential when special enhancements such as door locking, installation of interior security systems and features are being considered, or when exterior features such as bollards or gates are being contemplated. The relevant model codes address these features to varying degrees — but it is crucial that building owners, building operators and facility managers utilize the services provided by local municipalities to avoid any unintended consequences or pitfalls. Related government or public servant groups include the legislative bodies that can help shepherd appropriate and meaningful changes through the formal code process at state and local levels as well as help with financing and funding issues to help implement future changes.

The insurance industry has taken on a larger role in this arena by stepping up their efforts to educate their policy owners as well as reviewing security enhancements being considered. They've also had to look at the challenges associated with business interruption costs when the use of buildings and facilities is lost as a result of certain acts such as mass shootings. Supplemental coverages for things like funerals, employee assistance program, and biohazard cleanup are also among the provisions that have an impact on insurance related risks. As these types of claims or acts increase in frequency, policies may be continuously adjusted to address the types of mitigation measures that are in place.

A less obvious stakeholder in this category involves those in the human resources (HR) profession. In many circumstances, particularly with smaller companies and organizations, dedicated safety teams and emergency management teams do not exist and the responsibility for developing and carrying out related policies falls to HR. Through the use of employee handbooks, company policies ranging from behavioral type issues to explanation of the emergency plan is often defined and coordinated by HR.

Importance of planning scenarios and concepts

Traditional and historical emergency planning has centered around common and likely emergencies such as fire. Planning scenarios must also account for the need to look beyond just a single, specific type of emergency. Planning contingencies must be comprehensive to address the all-hazards approach, or more accurately, the *likely and expected* hazards approach. Establishment of the team related concept is suggested as one method to make this work. One approach to this would be to look at policy type planning elements and design/construction type planning elements. Knowing the relationship between building performance under different scenarios, the integration of security goals between the building owner, building operator, facility manager should allow the design team elements to come together in a seamless way. Overall building use includes attention to elements such as selection of interior materials, texture, color and layout which can have influence on the occupant comfort level.

It is important to note that building use scenarios can vary quite a bit. For example, while a school is predominantly utilized for educational purposes, they can also be the location for sports activities, concerts and plays among other things that typically bring in a larger and different segment of the general public. It may also be used as a voter location that is purposely set up to allow a freer access into and out of certain parts of the building. In other words, there must be constant vigilance with regard to not only how the building is used on a daily basis but also how it might be used during other time periods.

Document privacy

With an ever-increasing emphasis on "right to know" and open access/open society matters, policy and procedures need to be established that would allow building owners to maintain some level of privacy control over architectural documents and drawings and even emergency planning scenarios from the general public.

Building projects and designs undertaken for private-sector owners typically have no obligation to share every specific detail with the general public beyond fundamental criteria such as overall footprint, height of building or structure, distance between property lines, public rights-of-way and so on. Challenges might come when buildings are constructed or occupied related to public sector or government entities such as schools, courthouses and municipal buildings. It is unclear if there really would be a need to share every level of detail for the public as it relates to obvious, or less than obvious design features that address security. The same holds true for any detailed building emergency operational plans.

There are various ways to manage this part of the challenge such as by maintaining separate files or drawings related to security features. Such drawings would be restricted to certain parties, could utilize encrypted files, or utilize some other type of restricted access and tracking feature. Regardless of the approach taken, developing a robust policy for the jurisdiction would allow for consistent treatment of this item. It should be noted that some state legislative involvement may be required to exempt sensitive building documents from state or federal freedom of information requests for state buildings.

Developing and Reviewing Appropriate Plans and Drills

Hazard and emergency type drills have been in the relevant fire and life safety codes for many, many years. Although the emphasis on these drills has been, and continues to be fire events, in recent years other types of emergency planning scenarios have been implemented. From earthquake drills in California, to tornado drills in Oklahoma, these are among the planning contingencies that these geographic regions need to be aware of — particularly in the K-12 environment. Such natural hazard events will impact large landmass/geographic areas, multiple buildings and structures, and potentially large segments of the population. It is therefore important to look closely at the type, frequency and extent of planning and drills for targeted violent acts that generally impact a single building or a venue. Examples include acts such as the Route 91 Harvest shooting in Las Vegas (2017) or the Garlic Festival in Gilroy (2019).

Crafting the policy or plan for building and occupant emergencies cannot be done in a vacuum. In other words, fire continues to be a common and likely hazard in essentially every building regardless of geographic location. Earthquakes continue to be a common and likely hazard in essentially every building located in an active seismic zone. Hostile/targeted violent acts are possible, but unlikely in essentially every building. This does not mean that planning contingencies and drills should be ignored, but it does mean that such planning contingencies and drills need to be done in addition to, and not in lieu of the other emergency or hazard events that the building is more likely to face.

During the planning phase, as well as the development of any actual emergency drills that are conducted, the AHC-BSS emphasizes the importance of maintaining open channels and lines of communication. Establishing information delivery to building occupants is appropriate, depending on the event. The audible signal portion of the building fire alarm system should exclusively remain as a means to alert occupants of a fire. Public address, text display, text and email messaging, and direct voice announcement or communication are among the mass notification system (MNS) approaches that can be considered for other building emergencies. A protocol should be established to identify the hierarchy or priority of signals and messages when simultaneous events (building fire alarm system activation plus active shooter report) occur.

Building owners, building operators, and facility managers have a range of considerations and programs to review when establishing their plans for hostile acts. Some of those programs, such as Run-Hide-Fight are specifically directed at building occupants. First responder standards such as NFPA 3000 allow for coordinated planning and response by local first responder agencies to such acts. Such owners, operators, and managers are encouraged to be a full participant with local first responders and have a plan in place to avoid confusion and inefficient or less than ideal response to these acts.

A related area involves the utilization of emergency procedures such as lockdown. There are numerous resources, discussions and descriptions of what a lockdown entails. Some considerations include:

- How are building occupants trained and what is the frequency of this training
- Under what conditions is the lockdown or other similar emergency procedure called
- Who is authorized to initiate it
- How is it communicated to building occupants
- Actions and expectations of building occupants and officials
- Who is authorized to cancel it

Identification of Resources for Use by Different Stakeholder Groups.
A centralized list of resources is found in Appendix G. This has been created in order for the user to look through that list and determine what items or elements might have the most application or utility to a given problem or knowledge gap. The AHC-BSS feels that security plans and approaches including emergency planning and the hardware/brick-and-mortar components are currently done on more of a do-it-yourself basis rather than a structured or regulated basis like other building design elements. This same concept was identified in several of the workshops hosted by NFPA dating back to 2014 (see resources at the end of this chapter). The security plan and relevant systems must be able to integrate with other building system and architectural features and blend in as part of any other building design element.

Security professionals becoming an integral part of a design team is much preferred to current methods, which sometimes require one or more of the design team members to assess the issue. In some instances, security enhancements or layers are brought in after the building has been occupied and is up and functioning. It is anticipated that the customers and clients served by architectural, architectural/engineering, and other building consultants will begin to expect to see a professional, credentialed design team member that has unique and specialized expertise in building security.

The resource list or library of available content is quite substantial — and may not have direct application to every circumstance or condition, but rather may apply to select portions of an issue. Combing through those resources and using appropriate criteria can be used to submit code changes through the code development process of organizations such as ICC and NFPA to help individual local government organizations or even private sector organizations develop their own protocols and procedures for their buildings and employees.

Identification of existing, or future development of a security professional category; implementation at the academic level
Chapter 2 on Risk Assessment identified the need for Building Safety and Security Assessments (BSSA). One of the recommendations was the need for those who perform a BSSA to be professionally trained and certified. The AHC-BSS recognizes that specific and established programs, certifications and educational components currently exist with regard to this concept (See Chapter 2). Some of the fundamental criteria for such categories can be found in Section A.5.3 of NFPA 730. At present, the majority of these programs appear to be focused on individuals who may have the responsibility for multiple types of security ranging from personnel protection, building protection, data and IP security, as well as protection of other types of assets and contents (i.e. overall theft protection).

When dealing with building codes, fire codes and life safety codes related to security topics, it is not abundantly clear how well those existing programs can easily be translated into these types of built environment codes — several of which include drilling and planning components for a variety of threats or hazards.

The Physical Security Program (PSP) (Domain Two) from ASIS International (formally the American Society for Industrial Security) does have a module that deals with building codes and related standards but it's not clear from the description if that would satisfy the skill sets that are necessary. It is an understatement to say that authorities having jurisdiction who are responsible for enforcement of building code and fire code provisions may not have the resources to enforce a specialty code governing security. However, the progression of these enforcement responsibilities continues to increase as evidenced by the enforcement of the accessibility provisions found in codes as well as emerging concepts in energy efficiency.

There is a bigger question for the code enforcement community and that is the possible need for highly specialized inspectors or AHJ's for some of these topics. Large jurisdictions may have the inspection resources when compared to small and medium-sized jurisdictions. Regardless of the approach taken, it will be critical to determine how such an enforcement resource could be scalable among the range of jurisdictional populations.

The other credentialing challenge deals prominently with the design professional who must have some level of understanding of the systems, building features and other elements that make up the security layers in the building. This may call for a series of categories such as:

- Level 1: basic security concepts
- Level 2: intermediate security concepts
- Level 3: advanced security concepts which may include a licensing component

While current state licensing models for architects (Registered Architects - RA) and engineers (Professional Engineers – P.E.) could likely be adapted to a formal licensing program, a process that will probably take years. In the interim, the catalog of existing educational and certification programs offers important content and understanding of what is needed. It is imperative these programs: convey fundamental understanding of overall building security elements, including the human component; that the programs remain agile and proactive; and that the programs maintain some form of continuing education. This approach seems to be realistic as a short-term solution.

Security based designs and enhancements that are self-certified without independent third-party review have been a common state of practice in recent years. There is some concern, however that this model is no longer feasible or in the best interest of public safety moving forward. Our regulatory system in the United States minimizes the amount of product or design elements that are self-certified by the designer or the manufacturer — security should be treated no differently.

One model used by an organization in the insurance industry utilizes the concept of a security officer. The role of these individuals is to identify various building hazards during site visits and surveys and develop a report that identifies items requiring mitigation and suggested or recommended remedies and/or actions for follow-up.

There was general agreement among the AHC-BSS that reaching out to ASIS International would be a good way to start the discussion on how their programs might integrate towards a solution as discussed here. At present those programs are:

APP-Associate Protection Professional

PSP®-Physical Security Professional

CPP® -Certified Protection Professional

The APP designation represents the basic or fundamental credentialing while the CPP designation represents the highest. The APP level may have minimal application to the administration and planning components discussed in this report. However, as a starting point, these three categories appear to offer the best way to approach the security challenges in the built environment and make them relatable to the established codes and standards that regulate that environment. The long-term goal however should continue to be how to develop licensure programs related to a security professional that could be part of a design team.

The development of dedicated academic degreed programs on security at the secondary education level is an unlikely concept. However, just like many college and university programs that deal with built environment topics ranging from architecture, architectural-engineering, fire protection engineering, electrical engineering, and structural engineering, that offer some insight to the regulatory world of codes and standards, the ability to develop or offer a courses or that deal with these types of building security issues may be a reasonable goal.

Similar to a building design project, a movement to enhance or engage the other organizations involved in this area including, but not limited to ASIS International must be managed. It is important to note that the other codes and standards development organizations such as ICC, NFPA, UL and others acknowledge the need for security considerations to be integrated into the built environment, design team structure and ultimately into the lexicon of the other types of systems that the various codes and standards regulate and mandate.

Regardless of how these future discussions are resolved, it is not too early to be thinking about development of a certification program that might dovetail with other types of certification programs that authorities having jurisdiction strive to achieve. Any such program would have to integrate and describe the crossover between established building and fire code regulations and the related security measures, systems and features. Development of a job task analysis followed by job performance requirements would be a necessary first step to achieve the desired outcome.

Nestled within these overall discussions is the question dealing with the type of security that the scope and background of this effort can realistically address. The fundamental question is “Are we only talking about physical security?” Companies and organizations are equally concerned with things like data security, cyber security (including physical cyber security), protection of IP, and financial transaction security among other topics. These issues are beyond the scope of this report.

Recommendation
The content of this chapter has been consolidated in the administration/planning checklist found in Appendix C.

References (See Appendix G)

- Administration/planning checklist (See Appendix C)
- ASIS International
- NFPA 3000 Standard for an Active Shooter/Hostile Even Response (ASHER) Program
- NFPA 730 Guide for Premise Security
- NFPA Workshops on School Safety, Codes and Security (2014 & 2018)

ICC INTERNATIONAL CODE COUNCIL®

CHAPTER 4—FACILITY HARDENING

Overview

This chapter addresses the site and exterior envelope of the facility (exterior doors are also addressed in Chapter 5). This includes identification of best practices and resources such as types of designs as well as materials. Procedures under "normal" conditions as well as "incident" conditions are considered.

This chapter considers the many uses of a facility, not just the primary use. The information contained in this chapter is intended to be generic to all occupancies but also includes examples using specific occupancies, where appropriate.

Approach

The AHC-BSS developed a feature/threat mitigation tool to be used by designers, building owners and localities to aide in the evaluation and implementation of threat mitigation measures for threats to the exterior features of a building facility and property. This mitigation tool is intended to address safety and security as an "all-hazards' approach, assessing multiple potential risks with a balance approach to mitigation strategies for a achieving a minimum acceptable level of building occupant safety

Findings

This is a tool to facilitate analysis and is not intended to provide a list of solutions. The reason for this approach is because every situation is different, and the solution needs to be specific to the facility. .

Recommendation

The tool consists of two tables. The first table lists common facility exterior features and potential threats to life associated to each specific feature. Facility features are listed in the rows and associated threats listed in the columns. Threats specific to each facility feature are highlighted in the table.

Following the Feature/Threat table is a second table that lists the following: each feature with the specific threats associated to the feature; a feature cross reference to other related facility features; and mitigation considerations to evaluate and implement. Each of the listed considerations must be individually evaluated for the specific facility feature. Based on the evaluation, if the mitigation method is determined to be valid for the specific facility and feature implementation of the mitigation method should be considered.

See Chapter 5 Access Control for a discussion on the types of protective glazing required.

The shading in the table indicates the following:

- Light grey: Highlights every other row so it is easy to distinguish between rows
- Dark grey: Highlights threats with a higher degree of relation to the specific facility feature. Greater emphasis should be placed on consideration of dark grey threats for a given feature.

References (See Appendix G)

- Crime Prevention Through Environmental Design (CPTED)
- ICC International Green Construction Code (IgCC)
- NFPA 730 Guide for Premise Security
- NFPA 3000 Standard for an Active Shooter/Hostile Event Response (ASHER) Program
- NGA Glass Technical Paper FB71-21

Facility Hardening Feature/Treat Mitigation Tool *(feature=number/threat=letter)*

The tool consists of two tables. The first table lists common facility exterior features and potential threats to life associated to each specific feature. Facility features are listed in the rows and associated threats listed in the columns. Threats specific to each facility feature are highlighted in the table.

Feature/Threat	(A) Shooter	(B) Bomb	(C) Forced Entry	(D) Vehicular Weapon	(E) Suicide	(F) Vandalism	(G) Domestic Violence	(H) Sex Registry
(1) Vehicular Drives/Approaches	1A	1B	1C	1D	1E	1F	1G	1H
(2) Fire (Emergency) Lanes	2A	2B	2C	2D	2E	2F	2G	2H
(3) Parking Lot Layouts	3A	3B	3C	3D	3E	3F	3G	3H
(4) Parking Lot Lighting	4A	4B	4C	4D	4E	4F	4G	4H
(5) Loading Docks	5A	5B	5C	5D	5E	5F	5G	5H
(6) Site & Exterior Bldg. Lighting	6A	6B	6C	6D	6E	6F	6G	6H
(7) Sidewalks	7A	7B	7C	7D	7E	7F	7G	7H
(8) Ped. Approaches/Paths	8A	8B	8C	8D	8E	8F	8G	8H
(9) Glazing	9A	9B	9C	9D	9E	9F	9G	9H
(10) Exterior Doors	10A	10B	10C	10D	10E	10F	10G	10H
(11) Landscaping	11A	11B	11C	11D	11E	11F	11G	11H
(12) Stand-offs (bollards)	12A	12B	12C	12D	12E	12F	12G	12H
(13) Exterior Cameras	13A	13B	13C	13D	13E	13F	13G	13H
(14) Call Boxes and calling aides	14A	14B	14C	14D	14E	14F	14G	14H
(15) Parking Structures	15A	15B	15C	15D	15E	15F	15G	15H
(16) Exterior Walls	16A	16B	16C	16D	16E	16F	16G	16H
(17) Roof Access/Ladders	17A	17B	17C	17D	17E	17F	17G	18H
(18) Outside Assembly Areas	18A	18B	18C	18D	18E	18F	18G	18H

Feature/Threats	Feature Cross-Ref	Mitigation Considerations to Evaluate and Implement
1. Vehicular Drives & Approaches/A, B, C, D, G	2, 7, 8, 12	-Circuitous driveways and approaches for vehicles as opposed to straight on approaches to the building. - The termination of drives and approaches in locations other than directly in front of entrances. -The use of setbacks and standoffs at locations where people stand or gather.
2. Fire Emergency Lanes/A, B, C, D, G	1, 12, 13	-The use of collapsible bollards for fire and emergency access lanes. Coordinate design and layout with the local Authority Having Jurisdiction (AHJ).
3. Parking Lot Layouts/A, B, D, F	4, 7, 8, 11, 12, 13, 14, 15	-The creation of more remote parking areas that do not face main or secondary entries. -The use of circuitous vehicle routing into and out of parking areas with more direct routing and collapsible bollards for emergency vehicles. -The use of card access control to more secure parking areas if possible. -The use of specific accessible parking assignments per person and dedicated secured accessible parking area to a secondary entrance. -Appropriate NFPA 730 and NFPA 3000 recommendations. -Providing signage and lot identification. -A plan for where media, and other interested parties could access the site and park so not to delay response or endanger first responders or building occupants. -The use of dedicated pedestrian aisles or sidewalks to address conflicts between pedestrians and vehicles.

Feature/Threats	Feature Cross-Ref	Mitigation Considerations to Evaluate and Implement
4. Parking Lot Lighting/ A, C, D, F, G	3, 7, 8, 11, 15	- Appropriate Crime Prevention Through Environmental Design (CPTED) recommendations to maximize sight lines from and minimize stealth approach opportunities to buildings or pedestrian areas -The use of appropriate light levels in parking areas and along pedestrian paths.
5. Loading Docks/ A, B, C, D, G	9, 10, 13, 16	-Locating loading docks for receiving and storage in a separate building, 100 feet from the main building if possible. -Locating attached building loading docks at remote areas of the building, away from primary functions and occupants. -Securing the building area served by loading docks, and areas used for receiving and storage from the primary facility through the use of dedicated hallways and secured, monitored access doors. - Use forced impact resistant glazing when loading docks are in remote or moderately monitored areas of the building. -The structural fortifying of intervening walls between loading docks and storage areas and the primary building functions, areas, and occupants. -Constructing interior intervening walls between service and storage areas, and mechanical spaces, from floor or foundation to roof structures. -The use of separate mechanical systems for loading and storage areas and their location separate from the function(s) they serve.
6. Site & Exterior Bldg. Lighting/ A, C, D, F	7, 8, 11, 15	-Appropriate NFPA 730 and CPTED recommendations. -The use of appropriate light levels in parking areas and along pedestrian paths. -The use of "blue light notification systems"
7. Sidewalks/ A, C, D, F	1, 3, 4, 6, 8, 12, 13, 18	- Appropriate CPTED recommendations. -Raised curbs, sidewalk width, setbacks, and standoffs where people stand or gather.
8. Ped. Approaches & Paths/ A, C, D, F	1, 3, 4, 6, 7, 12, 13, 15, 18	-Appropriate CPTED recommendations. -Minimizing places for people to hide or weapons to be hidden. -Raised curbs, sidewalk width, setbacks, and standoffs where people stand or gather.
9. Glazing/ A, B, C, F, G	5, 10, 16	-Appropriate CPTED recommendations. -Minimizing places for people to hide or weapons to be hidden. -Raised curbs, sidewalk width, setbacks, and standoffs where people stand or gather. -The installation of glazing that allows early visual warning facilitates broad observation and advanced reaction time for approaching security threats. -The installation of glazing, or products used in conjunction with glazing, that obstruct vision into the building, at appropriate times and locations. -The fortifying of glass at primary or controlled entrances or other areas identified in the BSSA with glazing appropriate to the risk as described in Appendix E, NGA Glass Technical Paper FB71-21. -Local first responders should be consulted regarding glazing strategies. See Chapter 5 and Appendix E for additional discussion on types of glazing materials.
10. Exterior Doors/ A, B, C, D, E, F, G, H	5, 9, 13	- Appropriate NFPA 730 and NFPA 3000 recommendations. -Designation of one primary building access for entry and egress and limiting other exterior doors to be egress only. -The inclusion of security personnel at main entrance(s). -The inclusion of audible or silent security alarms for remote exterior doors. -The use of electronic access control. -The designation of remote entry and foyer (or roof access) designed specifically for ASHER access for first-responders. -The use of visitor management protocols at primary and other visitor entrances. Local first responders should be consulted regarding door security strategies. -The graphic numbering of building doors so that callers can identify where they are or where an incident is occurring or has occurred. Coordinate door numbering with local first responders.
11. Landscaping/ A, B, C, D, F	3, 4, 6, 13	-The use of trees, groundcover, dwarf shrubs, and xeriscaping (native plants that do not require irrigation) instead of large shrubs and plantings. -Appropriate CPTED recommendations, including sight lines and territorial reinforcement when using landscape and fencing. Evaluate and implement the inclusion of greenspace and open areas near main entrances for clear lines of sight. -Appropriate landscaping recommendations based on the International Green Construction Code (IgCC). -Other measures to minimize stealth approach opportunities to the property and building.
12. Stand-offs (bollards)/ A, B, C, D, E, G	1, 2 ,3, 7, 8	-Controlling access to the site and building. -The inclusion of traffic control devices, permanent and collapsible bollards, and concrete landscape containers to manage traffic and deter use of a vehicle as a weapon. -Providing access methods for emergency response vehicles. -Consult local first responders regarding use of stand-offs.
13. Exterior Cameras/ A, B, C, D, E, F, G, H	2, 3, 5, 7, 8, 10, 11, 14, 15	-The use of live video streaming and recording camera devices to monitor for threats.

Feature/ Threats	Feature Cross-Ref	Mitigation Considerations to Evaluate and Implement
14. Call Boxes & calling aides/ A, F, G	3, 13, 15	-The installation of call boxes in parking lots and structures, sport fields, and other remote facilities. Emergency Call Boxes should be equipped with live video streaming and recording camera devices. -Providing emergency call numbers on signage around the facility. Coordinate emergency call numbers with local first responders.
15. Parking Structures/ A, D, G	3, 4, 6, 8, 13, 14	-Limiting areas that could be used as a sniper's perch oriented toward entrances and glazing on the main structure. Determine sniper site lines to critical or high traffic points and design methods to interrupt identified site lines.
16. Exterior Walls and Windows/ A, B, C, D, F	5, 9	-Building materials and glazing materials resistance to threats, including forced entry, ballistic, bombs, and vehicular. See Chapter 5 and Appendix E for additional discussion on glazing materials. -Locating HVAC outside air intakes away from grade level or in below grade areaways accessible from grade.
17. Roof Access & Ladders/ A, B, C, F, G	none	-Measures to control roof access. -The use of signage alternative to wayfinding signage for roof access points, service and storage areas, and mechanical, electrical and IT rooms. -The inclusion or requiring of active notification and written log to security or administrative personnel when roofs are to be accessed. Make note of reason(s) for access, name of individual(s), as well as date, access and exit times.
18. Outside Assembly Areas/ A, B, D, F	7, 8	The use of planned locations for emergency assembly and how threats to these areas can be mitigated, including sniper lines of sight from the building.

ICC INTERNATIONAL CODE COUNCIL®

CHAPTER 5—ACCESS CONTROL

Overview

This chapter addresses exterior doors and physical security and safety internal to the facility. This includes normally occupied spaces, physical plant spaces, and other accessory areas. This includes access control hardware both in its "normal" use and its "incident" use.

The information contained in this chapter is intended to be generic to all occupancies and includes specific applications for K – 12 educational occupancies. Appendix F also includes considerations for business occupancies.

Approach

A significant challenge of access control systems is designing, developing, and implementing access control (ingress control) with an appropriate balance of safety, security, convenience, and cost. The typical goals of access control systems are controlling access into buildings and controlling access to rooms or spaces within the buildings. Designing and implementing access control systems typically start with a risk and hazard assessment. Access control systems complement hardening of the facility and routinely operate with surveillance systems. Access control:

- May be accomplished by a relatively simple system of appropriately selected and installed key-operated door locks.
- May also be accomplished with wired and/or wireless devices utilizing human machine interfaces such as biometrics, keypads, and/or magnetic cards in combination with electro-mechanical, electro-magnetic, or key-operated door locks.
- May include remote monitoring of activity at doors, and/or remote communications, and may include remote operation of doors and/or door locks.
- May include enhanced materials to deter or prevent entry.

Findings

Design development, implementation, and ongoing interactions with access control systems is likely to be multi-faceted and complex. Effective access control is highly dependent on the design and consideration of routes people may take to gain access to the building and the interior of the building. The human element of access control typically includes plans and procedures for interacting with regular occupants of the building(s), procedures for interacting with visitors, and procedures for responding to threats or detrimental actions. While not easy, it's easier to "design in" access control systems with new construction compared to updating or retrofitting existing buildings.

Cost is always a factor with access control systems. Safety and security are primary objectives with access control systems. An appropriate level of convenience for those that interface with the access control systems must be provided, otherwise ongoing diligent operations of and disciplined interactions with access control systems are at risk.

Long-term effective access control systems are typically designed and implemented using a team approach, with the team including building designers, contractors, building users, and administrators of the access control system and first responders.

For the reasons noted above, the AHC-BSS initially focused on K – 12 schools. Access controls for schools, at a simplistic level, is relatively straight forward. The process entails the identification of the threat and developing the response to the threat by preventing access to the intended victims. This then presents a challenge, since educational facilities function best with an open, inviting and collaborative environment.

Effective access control is accomplished by optimizing solutions which meet the conflicting challenges of a welcoming school environment, safety, security, convenience, and cost. Access control requires well designed and reliable systems complemented by educated, trained and experienced school personnel. This in turn must be supported by an effective response by authorized personnel such as school staff and emergency responders in emergency situations.

Access control systems and personnel actions must mesh with the facilities hardening features, surveillance systems as well as administrative policies, procedures and enforcement. There is no "one size fits all" access control system. Recognizing that security measures can be defeated by human interactions, such as propping a door open, access control systems should include provisions to reduce or prevent occupants intentionally, or not, compromising the security of the building.

Regardless of access control functions at a door, and door locking and unlocking configurations, provisions for egress must be provided as required by the applicable building, fire and life safety codes.

Recommendations
The Access Control Design Matrices, following the references in this section, are intended to assist with the design of access control systems. The matrices focus on K-12 educational occupancies.

On page 32, a matrix entitled "K-12 Situations Motivating People Planning Matrix" identifies possible issues to consider. These are not intended to be design options:

- The three left columns identify the situations and reasons for people movement during the typical school day (curricular), before and/or after school activities (extracurricular), and the use of the building for community-based activities.
- The 4th column identifies movement of people in bulk (i.e. when students typically arrive for school), or non-bulk (i.e. when a parent arrives during the school day)
- The 5th column is the "type" of people who are moving such as known student, teachers with ID's, etc.; people that are not known upon arrival at the school; and people intent on inflicting harm. The latter is the main driver for all this matrix.

On page 33, a second matrix entitled "Access/Ingress Control Planning Options Matrix" identifies possible issues to consider. These are not intended to be design options:

- The 1st column on this page identifies the types and locations of the doors such as the main entry doors, secondary entry doors, interior corridor doors, etc.
- The next four columns identify facility design options at the doors including the layout of the door(s); design options for human interactions at the doors, door status monitoring options, and door unlocking / locking options.
- The next three columns (6th – 8th) columns are options for physical protection at the doors
- The last two columns identify options for expectations and plans for the administrative staff personnel to interact at the door(s).

The following is an example of the steps involved to use these two matrices:

1. Starting with the left side of the first matrix: Assume it's a typical school day (curricular) and it's the time of day the students typically arrive (mass entry) and it's expected the people seeking entry into the building are "known" – but there could be an intermingled "not known" person such as a visitor, and there could be an intermingled person who intends harm.
2. With the situation as described above in mind, move to the second matrix. Assume the situation is at the main entrance door, and that entrance is two-stage (has a vestibule). At this time of the day, there is no physical access control (the doors are unlocked to allow free ingress), and school staff and the school's resource officer (e.g. a sworn police officer) are there in person observing each person as they enter the building. The school staff and the resource officer are keenly observant and scanning the entering people for anyone not known, and are educated, trained, and prepared to respond.

Similar thought processes may be followed for the myriad other situations and doors of a K-12 school. Based on the risk assessment and action plans for when a potential threat shows up, each situation (first matrix) at each door could be thought through (second matrix) as to facility design objectives coupled with administrative / staff plans for actions and response.

Following the investigation of K – 12 schools, the AHC-BSS followed up with an initial investigation of Business Occupancies shown in the matrices in Appendix F.

Glazing

The matrices and sketches which follow include numerous references to special types of glazing including: bullet resistant; ballistic rated; impact; blast resistant; and security glazing. It is important that the risk being designed for is coordinated with the type of glazing.

The different types of risks and glazing fall under the general definition of "Glazing Security Levels" definition in Appendix B and their respective application is found in Appendix E.

The following documents are listed in Appendix G and include important information which matches the type of glazing with the design risk:

- ANSI Z97.1 Safety Glazing Materials Used in Buildings - Safety Performance Specifications and Methods of Test
- ASTM E2395 Standard Specification for Voluntary Security Performance of Window and Door Assemblies with Glazing Impact
- ASTM F1233 Standard Test Method for Security Glazing Materials and Systems
- ASTM F1642 Standard Test Method for Glazing and Glazing Systems Subject to Airblast Loadings
- ASTM F 2912 Standard Specification for Glazing and Glazing Systems Subject to Airblast Loadings
- ASTM F 3006 Standard Specification for Ball Drop Impact Resistance of Laminated Architectural Flat Glazing
- ASTM F3007 Standard Test Method for Ball Drop Impact Resistance of Laminated Architectural Flat Glass
- ASTM F3038 Standard Test Method for Timed Evaluation of Forced-Entry-Resistant Systems
- EN 1063 Glass in building - Security glazing - Testing and classification of resistance against bullet attack (European Standard)
- NGA: FB71 – 21 School Security Glazing, National Glass Association
- NIJ 0108.01 Ballistic Resistant Protective Materials, National Institute of Justice
- UL 752 Standard for Bullet-Resisting Equipment
- UL 972 Standard for Burglary Resisting Glazing Material

References (See Appendix G)

Codes and Standards

- International Building Code (Chapter 10 Means of Egress)
- NFPA 101 Life Safety Code (Chapter 7 Means of Egress)
- NFPA 3000 Standard for an Active Shooter/Hostile Even Response (ASHER) Program

K-12 Schools

- Safety and Security Guidelines, for K-12 Schools, Partner Alliance for Safe Schools, PASS
- K-12 School Security: A Guide for Preventing and Protecting against Gun Violence (2nd ed., 2018), U.S. Department of Homeland Security
- NASFM Classroom Door Security

Glazing

See “Glazing” above

General Information

- Access Control Technologies Handbook, U.S. Department of Homeland Security
- Security Risk Management Series Publications, FEMA, which includes “Primer to Design Safe School Projects in Case of Terrorist Attacks and School Shootings, 2nd Edition (2012)”
- See additional resources under “Educational Facilities” in Appendix G

ICC INTERNATIONAL CODE COUNCIL®

ACCESS CONTROL DESIGN
K-12 SITUATIONS MOTIVATING PEOPLE PLANNING MATRIX

Situations: K-12 Occupancy Drivers/Reasons/Time Period(s) of People Movement				
Curricular School day – typical & non-typical	Extracurricular K-12 student focused activity	Community Not K-12 student focused	People Movement Bulk/Many/Non-bulk/few/single	People "Types"
Student arrival Staff arrival Student departure Staff departure Parent/guardian student pick-up/drop-off Parent-teacher administrator collaboration Vendors/service providers Separating employee departure Emergency/Fire Drills – exiting Emergency/Fire drills – re-entry Emergency drills-shelter in place (weather/violence)	Sports practices or conditioning Fine Arts practices Sports events – indoor Sports events – outdoor Fine arts performances Fine arts events/competitions Unique (i.e. prom-night bash)	Open athletic facilities - indoor Open athletic facilities - outdoor Open trades facilities (i.e. open shop) Community voting location Community classes Community meetings Community fund raising Meals/food distribution	Bulk entry/ingress Bulk exit/egress Bulk entry and exit Non-bulk entry/ingress Non-bulk exit/egress Non-bulk entry and exit	Known, recognized, pre-authorized, preapproved (See Note) Not known, not recognized, not preauthorized, not preapproved (See Note) Person(s) w/intent to inflict harm and/or physical damage
Unplanned/Unscheduled				
Fire issue/emergency Health issue/emergency Law enforcement issue/emergency Violence issue/emergency Weather issue/emergency	Fire issue/emergency Health issue/emergency Law enforcement issue/emergency Violence issue/emergency Weather issue/emergency	Fire issue/emergency Health issue/emergency Law enforcement issue/emergency Violence issue/emergency Weather issue/emergency		

Note: In K-12 incidents, person(s) with intent to harm are more likely to be "known" than "not known," and if known, are as likely to be inside the building as outside when intent to harm is recognized.

How to use this matrix: This matrix is intended to provide multiple scenarios to identify the movement of people. As a matrix it is **not** intended to be read across the row with entries adjacent to the first column entry being applied to the first column entry. See the example on page 29. This matrix is not intended to be all inclusive.

ICC INTERNATIONAL CODE COUNCIL®

ACCESS CONTROL DESIGN

ACCESS/INGRESS CONTROL PLANNING OPTIONS MATRIX

Type/ Location of Entrance/ Exit	Facility Design Options				Facility Design Physical Protection & Hardening			Facility Design-Expected Administrative/Staff Responsibilities at Door(s) Regarding People Movement	
Intended function	Door(s)/Areas Layout Design	Human interaction & Facilitation Design at Door(s)	Door Status Monitoring Design	Door Unlocking/ Locking Ingress/Access Control(Note 1)	Doors	Glazing	Walls	Ingress/Access Monitoring/ Control	Egress Monitoring/ Control (Note 2)
Main/formal/ front entrance to building Secondary entrance/exit – for students Secondary entrance/ exit for staff/ administration Secondary entrance/exit- for students and staff Doors between classrooms Sports competitions entrance/exit Fine arts performances entrance/exit Playground/ recess exit/ entrance Physical education exit/ entrance Mechanical/ utility/loading dock entrance	None/no door(s)/open to outside (not likely, but possible) Single stage (designed to pass through only one door for ingress) Two stage (designed to pass through two doors in series for ingress) Two-stage – exterior door(s) not ingress controlled Two stage- exterior door(s) ingress controlled Two stage – interior door(s) not ingress controlled Two stage- interior door(s) ingress controlled	None/no human interaction at door(s) Audio & visual - direct w/o physical protection Audio & visual direct w/physical protection Visual only – direct with physical protection Audio only- indirect (assumed with physical protection) Visual only – indirect (assumed with physical protection) Audio & visual – indirect (assumed with physical protection)	None/no monitoring of door(s) open/ close status Visual direct (status of door can be observed directly by a person) Visual – indirect – video Visual – indirect open/closed status (i.e. text or graphic on display screen) Visual – indirect-people activity at door(s) (i.e. text or graphic on display screen) Audio - indirect door open general alarm Audio – indirect-door open specific alarm Audio -indirect-people activity at door(s) (i.e. audible alarm)	None (doors not locked to control ingress) Key or credential-temp unlocking (door locks when closed) Key or credential – unlocked until active re-locking Remote operated – temp unlocking (door locks when closed) Remote operated unlocking – req's active relocking at door Remote operated unlocking – req's active relocking remotely	None Impact Ballistics	None Impact Ballistics	None Impact Ballistics	None/no staff responsibilities at door(s) re: access control Visual monitoring Audio monitoring Visual interaction Audio interaction Physical interaction – locks operated remotely Physical interaction – in person prior to door, passive Physical interaction – in-person prior to door, active Physical interaction – in person after door, passive Physical interaction, in-person after door, active	None/no staff responsibilities at door(s) re: egress control Visual/audio monitoring direct Visual/audio monitoring direct w/ passive physical presence Visual/audio monitoring direct with active physical presence. Visual monitoring remotely - passive Visual monitoring remotely-active Audio monitoring – remote passive Audio monitoring – remote active

ICC INTERNATIONAL CODE COUNCIL®

ACCESS CONTROL DESIGN

ACCESS/INGRESS CONTROL PLANNING OPTIONS MATRIX (CONT'D)

Type/ Location of Entrance/ Exit	Facility Design Options				Facility Design Physical Protection & Hardening			Facility Design-Expected Administrative/Staff Responsibilities at Door(s) Regarding People Movement	
Intended function	Door(s)/Areas Layout Design	Human interaction & Facilitation Design at Door(s)	Door Status Monitoring Design	Door Unlocking/ Locking Ingress/Access Control (Note 1)	Doors	Glazing	Walls	Ingress/Access Monitoring/ Control	Egress Monitoring/ Control(Note 2)
Food service delivery entrance			Audio -indirect-people activity at door(s) (i.e. audible alarm)						
Trades/shop entrance									
Egress-only exit – academic areas									
Egress-only exit sports/ athletic areas									
Egress-only exit-fine arts									
Interior doors – corridors; to/ from individual rooms									

Note 1: Regardless of ingress/access control functions such as door locking and unlocking configurations, provisions for egress shall be provided as required by applicable building, fire and life safety codes.

Note 2: Regardless of egress monitoring or control functions such as door locking and unlocking configurations, provisions for egress shall be provided as required by applicable building, fire, and life safety codes.

How to use this matrix: This matrix is intended to provide scenarios/applications when considering the control of the movement of people in the building. As a matrix it is **not** intended to be read across the row with entries adjacent to the first column entry being applied to the first column entry. See the example on page 29. This matrix is not intended to be all inclusive.

Design Concepts and Examples
Main Entry –
The Access Control Design Matrices are intended to assist with the design of access control systems. The matrices focuses on K-12 educational occupancies.

1. The main entry is the designated primary entry location.
    a. There should only be one main entry per building “Single Point Entry”.
        i. A building could have multiple main entries with different entrances dedicated to Elementary, Intermediate/ Middle and High School.
    b. Identifying which door(s) are considered the main entry – the designated primary entry location – typically the responsibility of the building owner and architect
    c. All other exterior doors should always remain locked.
2. The Main Entry should consist of a secure vestibule with a transaction window in the vestibule.
    a. This will prevent visitors from getting fully into the school until they have been vetted by school staff or security.
3. Options of physically securing the Main Entry are illustrated on the next four pages.

Main Entry: Figure 1	Security level: Minimal
Exterior Doors	During student arrival and dismissal times, doors to be unlocked allowing for free entry.
	At the end of arrival and dismissal times all the doors will be locked to prevent entry except for one exterior door at the main entry. Visitors enter the secure vestibule and proceed to the transaction window where admin staff screens visitors per policies and procedures.
	After school operating hours all the doors shall be locked.
	Include provisions for access for first responders. Consult NFPA 3000
Secure Vestibule interior doors, sidelights and transoms	During student arrival and dismissal times the exit devices will be unlocked or held in the "dogged" position allowing for free entry. Persons entering the building actively monitored by trained and experienced staff.
	At the end of arrival and dismissal times all the secure vestibule doors will be locked to prevent entry.
	One door leaf on the secure vestibule interior doors to have remote release capabilities controlled by the main or security office. After the visitor has been vetted, visitor permitted to enter the building via remote release of locked secure vestibule door.
	Exposed glass below 7' to be security glazing, including in sidelights, appropriate to the risk assessment.
Transaction Window	Provide security glazing in the window assembly.
	Walls protecting staff at the transaction window designed appropriate to the risk assessment.

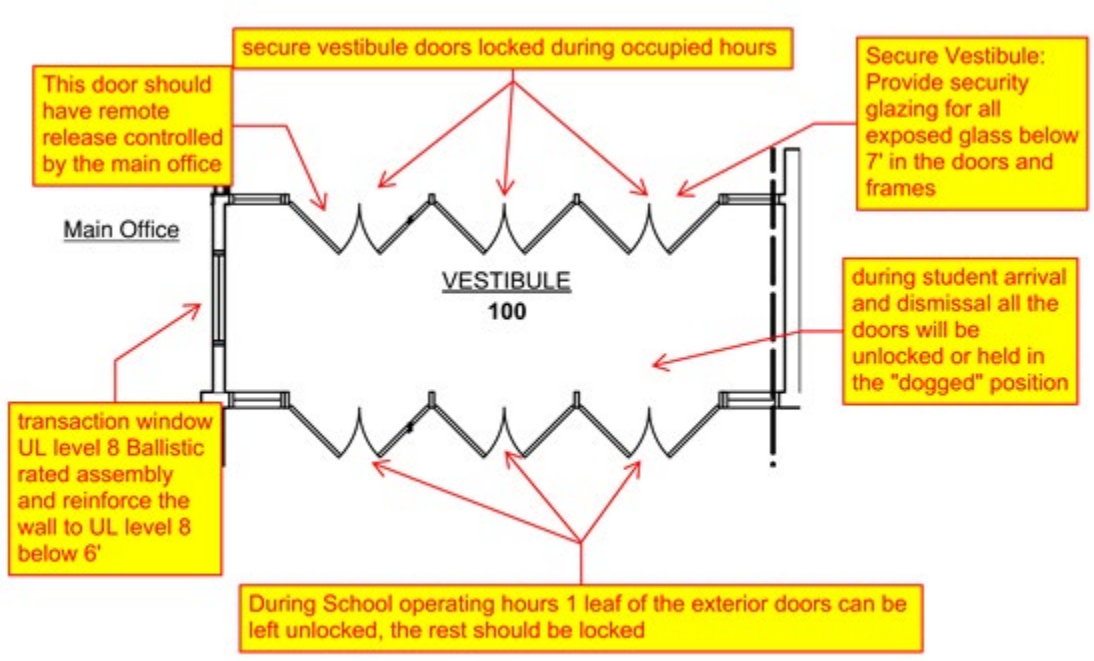


Figure 1

Main Entry: Figure 2	Security Level: Good
Exterior Doors	Added to the "Minimal" level: One door leaf of the exterior doors to have remote release capabilities controlled by the main or security office. Visitors will be required to ring the intercom/video phone to connect to the main/security office. Once vetted they will be allowed to enter the secure vestibule. Security glazing in the exterior doors for all exposed glass below 7', including sidelights.
Secure Vestibule interior doors, sidelights and transoms	For glazing, consider increases resistance compared to "Minimal" level.
Transaction Window	For glazing, consider increases resistance compared to "Minimal" level.
Exterior intercom/video system	Two-way communication system for initial screening of visitors prior to entry into the secure vestibule

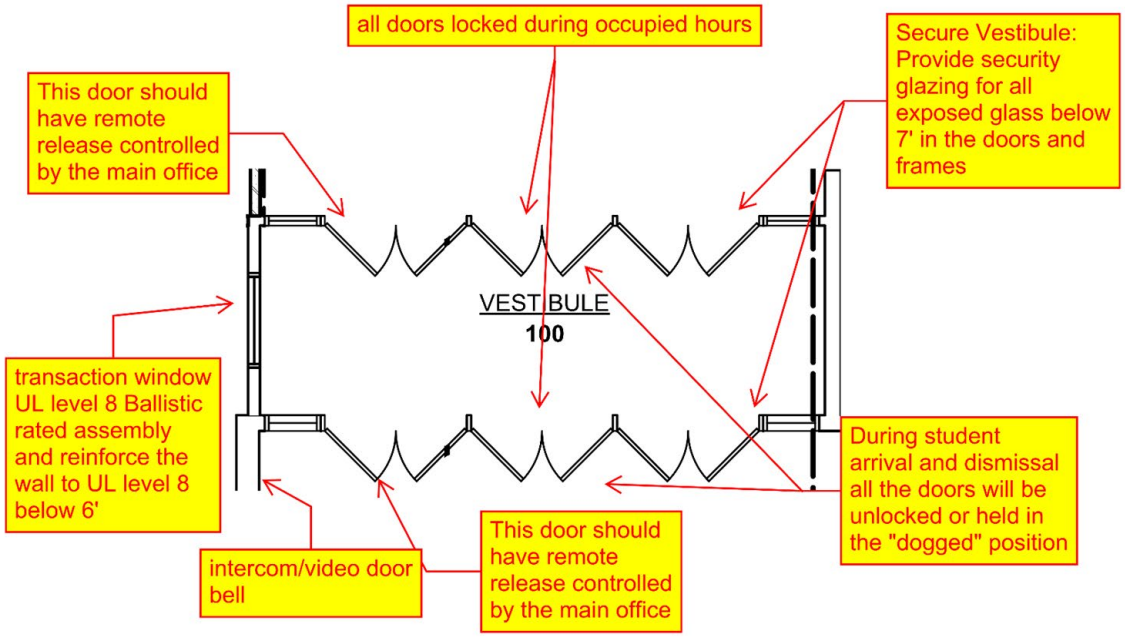


Figure 2

Main Entry: Figure 3	Security Level: Better
Exterior Doors, sidelights and transoms	Added to the "Good" level: All exterior doors of the main entry vestibule provided with electronic locking capability permitting doors to be locked or unlocked via programmed schedule or via remote action. One door leaf with electronic access control to allow for authorized entry. For glazing, consider increased resistance compared to the "Good" level.
Secure Vestibule interior doors, sidelights and transoms	Added to the "Good" level: All interior doors of the main entry secure vestibule provided with electronic locking capability permitting doors to be locked or unlocked via programmed schedule or via remote action. One door leaf with electronic access control to allow for authorized entry.
	For glazing, consider increased resistance compared to the "Good" level.
Transaction Window	For glazing, consider increased resistance compared to the "Good" level.
Exterior intercom/video system	Same as "Good" level.

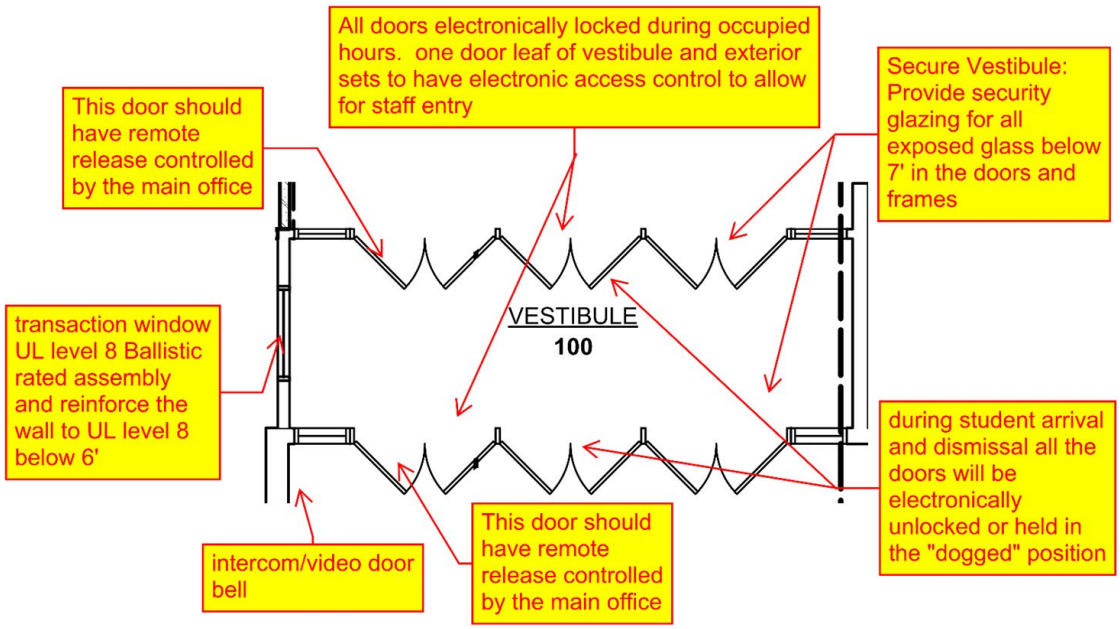


Figure 3

Main Entry: Figure 4	Security Level: Even Better Visitor entry separated from student entry
Exterior Doors (Student Entry), sidelights and transoms	Enhanced from the "Better" level: Exposed glass below 7' to be security glazing, including in sidelights, appropriate to risk assessment.
Vestibule interior doors	No requirements to lock these doors (visitors use separate entry path).
Exterior door (Visitor Entry)	Doors unlocked during operating hours.
Transaction Window and vision windows	Exposed glass below 7' to be security glazing, including in sidelights, appropriate to risk assessment
Secure Vestibule interior door (Visitors Entry)	Door locked at all time unless unlocked via remote release capabilities controlled by the main or security office after the visitor has been vetted. Exposed glass below 7' to be security glazing, including in sidelights, appropriate to risk assessment

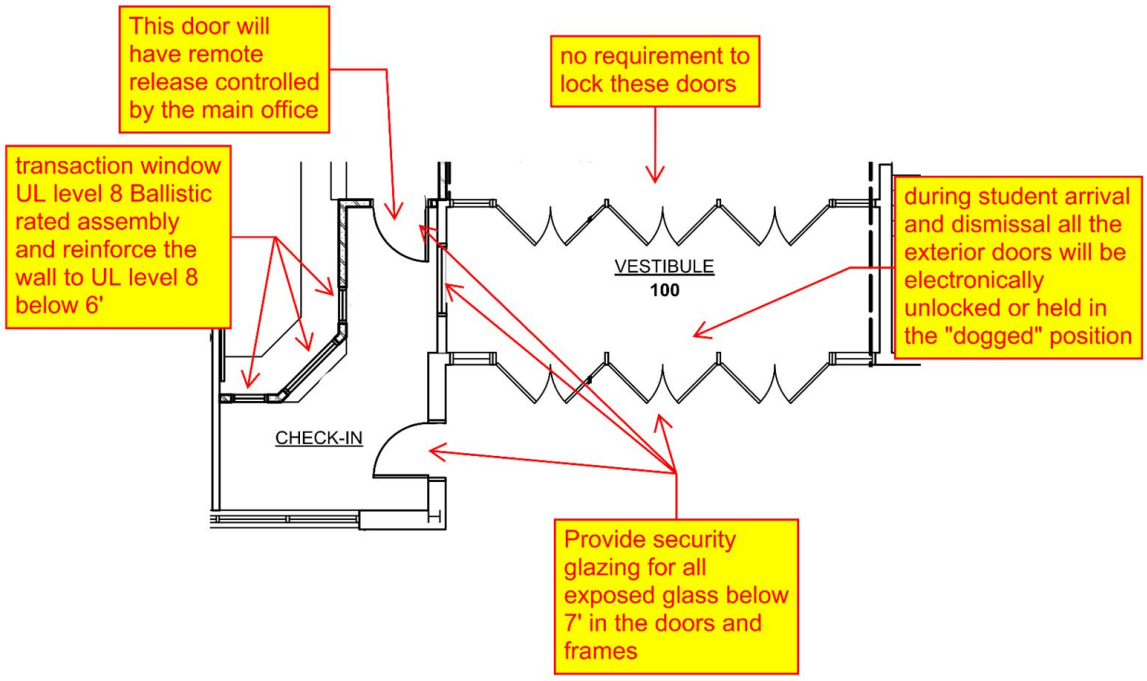


Figure 4

Secondary Entries – Examples

1. Secondary Entries are those entries that will not be handling student arrival and dismissals.
   a. Identifying which door(s) are considered the secondary entries is the responsibility of building owner, architect, building officials, and law enforcement.
2. Recommended methods of physically securing the Secondary Entries:

Secondary Entries	Security Level: Minimal
	Door to be closed and locked to prevent entry. Door to provide for egress as required by fire codes.
	Entry may be allowed by mechanical key.
	Door may be unlocked if required for a school event that requires a large group of people to be entering
	Exposed glass below 7' to be security glazing, including in sidelights, appropriate to risk assessment
	Option electronic monitoring of door open / door closed.

Secondary Entries	Security Level: Good
	Enhanced from "Minimal" level with: Electronic access control for authorized personnel entry. For glazing, consider increased resistance compared to "Minimal" level.

Other Exterior Doors – Examples

Secondary Entries	Security Level: Better
	For glazing, consider increased resistance compared to "Good" level.

1. Doors that are not normally used during the school day and are typically for egress only
   a. Identifying these door(s) is the responsibility of building owner, architect, building officials, and law enforcement.
2. At least one door on every side of the building needs to allow for entry.
3. Recommended methods of physically securing the other exterior door:

Other Exterior Doors	Security Level: Minimal
	Door to be closed and locked to prevent entry. Door to provide for egress as required by fire codes
	Entry is allowed by mechanical key on one door leaf only
	For openings with glass, provide security glazing for all exposed glass below 7', including in sidelights
	Options for electronic monitoring of door open / door closed.

Secondary Entries	Security Level: Better
	Door is always to be closed and locked. Free egress always
	Entry is allowed by mechanical key or electronic access control for staff entry.
	For glazing, consider increased resistance compared to "Minimal" level.

CHAPTER 6—SURVEILLANCE

Overview

This chapter focuses on both virtual (cameras/sensors) and physical surveillance at a facility. This will include both best practices and resources available. Best practices in acceptance testing of security systems along with routine testing/monitoring. Cyber security, although it intersects many areas, is not specifically addressed in this chapter. The information contained in this chapter is intended to be generic to all occupancies but also includes examples using specific occupancies, where appropriate.

Situational awareness is invaluable when designing a security solution. In addition to various layers of security protection, video applications provide intelligence and data that can help mitigate security risks and increase response effectiveness.

Common uses of video solutions include surveillance of perimeters of a protected area, observing crowds and behaviors at sporting events, public transportation facilities, campuses, manufacturing facilities, parking lots, vehicular traffic, critical infrastructures, etc.

Video surveillance provides a layer of protection and is commonly recommended in security vulnerability plans. It provides stored or real time images of a protected area and can serve as an early warning or provide information of an observed or recorded event. The application and specifications of an appropriate video surveillance system is dependent on the intended "use case". Use case scenarios considers the design process and equipment needs relative to the application and video image quality. It is important that use case factors, such as lighting, positioning, photographic parameters, environmental conditions, etc., be considered during the design phase of a security vulnerability assessment. Routine maintenance and periodic review of the video application, installations and changing environmental conditions must be conducted to ensure that any dynamic factors that may affect your video surveillance objectives be identified and addressed appropriately.

This chapter provides a high-level overview of key video surveillance concepts and is intended to compliment the more detailed information included in the helpful references included below.

Approach

An organized video solution approach includes consideration of multiple factors that address the application and use case needs. The planning of an effective video surveillance system should include various stages including:

Planning – during this stage the video surveillance design team will work with project stakeholders to determine best fit for the project application. This should include a security specialist who can explain the capabilities of the system as well as technical limitations.

Infrastructure – the technical demands of a system can range from simple to very complex. Internet protocol (IP) cameras will utilize a different infrastructure compared to analog systems. Developing and planning for the appropriate infrastructure is critical to the overall performance of the system. Factors to consider include system and equipment bandwidth requirements, recording equipment, network architecture, cyber security considerations and implementations, new cabling and existing cabling infrastructures, compatibility with existing IT infrastructures, design resiliency requirements, etc. It is recommended that the end user and security specialist complete a security risk assessment to identify critical factors and address system expectations and infrastructure requirements.

Analytic Capabilities – There are two basic dimensions of analytic capabilities that should be considered. The system design should consider the scalability to support analysis of the video content as well the scalability of expanding the video surveillance system components edge devices and infrastructure.

When planning a video surveillance solution, here are some basic infrastructure elements to consider:

IP vs. Analog – There are two basic technologies that are prevalent for security surveillance cameras. Analog cameras are moderately priced and offer a dedicated solution utilizing coax cable connected devices and DVR's with separate power runs for each camera. Compared to IP cameras, they generically offer lower resolution with less range of vision.

IP or Internet Protocol cameras reside on an IT backbone, typically connected to an NVR through a POE switch. IP cameras can offer high resolution images which can be digitally enhanced. IP cameras may take up significant bandwidth from your IT infrastructure to transmit and store digital images. IP cameras can be wireless and communicate through RF networks or wired using CAT5e or CAT6 cable infrastructures. Providing cyber security protection when implementing IP camera solutions is highly advised due to vulnerabilities of network connected devices and Internet of Things (IoT) threats.

Findings

Types of Cameras, Equipment and Systems

PTZ – Pan, Tilt, Zoom cameras (PTZ) allow for interaction from a remote monitoring site. An operator can have control to move the camera in different direction, such as left or right, up or down and remotely zoom in on an object or event.

Dome – Dome cameras are typically used in indoor or outdoor applications. The camera is housed within a dome shaped enclosure. This provides for a degree of vandal resistance since the camera is not easily accessible as its housing is a dome normally mounted out of reach. Another security benefit is that the dome hides the camera, so it is not easy to determine what the camera is focused on when at a distance. Dome cameras allow for mounting or placement of the camera similar to a box and turret construction.

Box and Bullet Cameras – bullet cameras perform well where lighting is minimal. Box cameras are similar to bullet cameras and can commonly be used with different lens' allowing for application versatility. Both cameras can be suitable for indoor or outdoor use based on their design and equipment attributes.

Infrared – Infrared cameras are used when light conditions are low and can provide images with the use of infrared light. Infrared cameras typically include infrared lights near or around the camera lens.

Thermal Imaging – Thermal imaging cameras provide for the ability to detect objects in low light conditions based on thermal differences between objects and background thermal environments.

License Plate – License plate recognition (LPR) cameras are specialized IP cameras that can read numbers associated with license plates. License plate cameras are digital and can accurately distinguish between pixels of an image.

Storage and Integration: Traditional analog surveillance systems utilize magnetic storage media as a fundamental design. Storage needs can vary depending on system architecture and your retention policy for recorded video. There are several options that system integrators can use to create hybrid solutions for existing systems that can convert analogue to digital or integrate separate systems allowing for scalability and flexibility.

DVR – Digital Video Recorders are discrete devices which store images in digital formats. They replaced legacy systems that recorded analog signals to magnet tape. DVR's generally have a storage capacity that is determined by the size of the onboard hard drive of the recorder.

NVR - Network video recorders work similar to DVR's. A main difference is that NVR's are connected to an IT network and are used with IP cameras. The cameras and NVR's are connected through an IT network's infrastructure. Display of images can be through connected monitors, remotely through web browsers or mobile apps.

Cloud Storage: Cloud storage providers offer services to manage and store video files to a remote storage system which is accessed online instead of locally on equipment such as hard drives, DVR, local NVR's or local computers. Cloud storage is a service that is available and allows greater storage capacity than local, traditional storage solutions. Additional advantages to cloud storage are that files are stored remotely, so if your equipment is damages or stolen, the stored videos are still safe. Because cloud storage utilizes internet connections it is important to ensure that good cyber security measures are in place to protect your files, infrastructure and equipment.

Video Analytics: Smart cameras and video systems sometimes offer embedded and specific software that allows the camera (or related equipment) to recognize objects, events, biometrics, facial recognition, or actions and automatically signal / record. Examples of triggering events include packages left behind, reverse flow of vehicles or pedestrians, peculiar crowd actions such as fighting or pushing, bright flashes, etc. Video analytics can be a helpful tool as it affords assistance in automatically monitoring a scene without direct human oversight and can trigger a notice when a known event or action occurs.

Video Latency: It is important to recognize that some video systems may have latency factors that can be intentional delays or may be a factor of system bandwidth. Latency is the time between a frame capture and display. Latency can be introduced by the camera, network or receiver side. Some systems may have buffer, decoder, image processing, encoding, transmission or display latencies. The end user should be aware of latency factors and recognize potential impacts that may affect the desired surveillance application.

Fixed and Mobile Surveillance: Video surveillance solutions can be designed as fixed installations or mobile applications. Video capable drones and temporary video operations can support first responders and security professionals by providing images that can assist in situational awareness. Fixed video equipment is typically hardwired compared to mobile surveillance which generally incorporates wireless technologies and system solutions.

Cyber Protection and Physical Controls: IP based cameras and systems can have inherent security vulnerabilities in Internet of Things (IoT) based systems. Use of IoT based technologies such as cameras and NVR's without good cyber security practices in place can be risky. IP cameras have been exploited through specific attacks that can be disruptive to interconnected equipment, and the system. Most current attacks relied on weak or default passwords, link exploitations, and interception and listening to unsecured or unencrypted communication and video channels. The use of dedicated video channels, dedicated networks, establishing good cyber hygiene practices, physical protections methods, and use of analytic tamper detection are examples of system attributes that can help reduce cyber security vulnerabilities and are essential in planning and maintaining a secured network.

Policy Considerations

When deploying video surveillance, it is important to also have documented policy guidelines that consider the current social and legal environment. Issues such as video retention periods, privacy and chain of custody, and a well-defined governance structure is critical for a video surveillance programs success. Each organization that uses video will need to consider factors that may be sensitive and address the use of video in a logical way.
Other factors that should be considered include but are not limited to:

- Available surveillance tools incorporated into first responder training/pre-planning of tactical operations.
- The location(s) where the video can be viewed should be considered (e.g. a fire command center).
- Any "delay" in the display of the video surveillance must be considered and made known to first responders

Recommendations
In addition to the general overview of key factors mentioned above, more comprehensive and detailed information is available in the documents referenced below. There are many available and valuable guidance documents, codes, recommended practices and standards that should be considered. Video surveillance technologies and designs continues to advance at a rapid pace. The following references are commonly used by security design professionals, specifiers, manufacturers, end users, and Authorities Having Jurisdiction, CIO's, CTO's, Security and Loss Prevention, etc. These resources include relevant information and provide tools to better understand the complexities of a video surveillance system.

References (See Appendix G)
The following references are not intended to be all inclusive and there are many other valuable resources that should be considered when considering video surveillance solutions. The following references provide fundamental guidance and offer more in-depth details of the above topics.

- DHS Science and Technology Directorate – Video Quality in Public Safety:
- Digital Video Quality Handbook, May 2013-2018
- Digital Video Quality Handbook Appendix, January 2018
- Policy Considerations for the Use of Video in Public Safety, June 2016
- NIST Definition of Cloud Computing, Special Publication 800-145, September 2011
- UL White Paper – Video Image Quality Testing
- ASIS Facilities Physical Security Measures Guideline (ASIS GDL FPSM-2009)
- ASIS Physical Asset Protection Standard (Feb. 2021)
- Department of Army, Physical Security, FM3-19.30
- DHS, CCTV Technology Handbook, System Assessment and Validation for Emergency Responders (SAVER)
- Sample Policy for School Use of Video Surveillance and Audio Monitoring

ICC INTERNATIONAL CODE COUNCIL®

APPENDIX A—BUILDING SAFETY AND SECURITY SCOPE AND OBJECTIVES

Building safety and security is an issue of upmost importance. Many states and local jurisdictions are developing legislation and policies in response to recent emergency events. Due to the complex and unpredictable nature of such events, it is imperative that all aspects of the built environment be thoroughly analyzed in order to develop a comprehensive response. Recognizing this critical threat to both new and existing construction, the International Code Council Board of Directors created a new Ad Hoc Committee on Building Safety and Security.

The design and layout in new and existing facilities can have a significant impact on safety and security. Safety and security touch a myriad of code regulations as well as considerations which fall outside the purview of the code. Accordingly, a comprehensive assessment must go beyond minimum code compliance.

Goal: Provide comprehensive, sound and valuable tools for local and state leaders to guide them in keeping occupants of facilities, including schools, safe from intruders and other life-safety hazards in the built environment.

Scope: The scope of this effort is likely to evolve over time in response to the complexity of the issues raised by the committee members. The Code Council anticipates that the outcome of the effort will include:

- A comprehensive review of current code requirements as they relate to developing the necessary balance between facility security and safety considerations. Any suggested revisions to current code requirements based on this assessment will be processed as proposed code changes to the International Codes.
- A comprehensive review of existing guides, white papers, reports and standards (e.g. NFPA 3000 Standard for an Active Shooter/Hostile Event Response (ASHER) Program), as they relate to design standards, event preparedness, emergency response and recovery.
- Identification of best practices and guides to address the design and layout of new and existing facilities.
- A comprehensive package of public information materials.

APPENDIX B—ACRONYMS AND DEFINITIONS

Acronyms

AHC – BSS: Ad Hoc Committee on Building Safety and Security

AHJ: Authority Having Jurisdiction

AIA: American Institute of Architects

ANSI: American National Standards Institute

ASHRAE: American Society of Heating, Refrigeration and Air-Conditioning Engineers

ASIS: American Society for Industrial Security (now ASIS International)

ASTM: American Society for Testing and Materials (now ASTM International)

BOMA: Building Owners and Managers Association

BSSA: Building Safety and Security Assessment

CPTED: Crime Prevention Through Environmental Design

DHS: Department of Homeland Security

FEMA: Federal Emergency Management Agency

IAFC: International Association of Fire Chiefs

ICC: International Code Council

NASFM: National Association of State Fire Marshals

NFPA: National Fire Protection Association

NGA: National Glass Association

NIBS: National Institute of Building Sciences

NIST: National Institute of Standards and Technology

UL: Underwriters Laboratories

Definitions

For the purpose of this report, the following are definitions used by the AHC-BSS. These are not intended to be all encompassing definitions but rather to support this report within the context used.

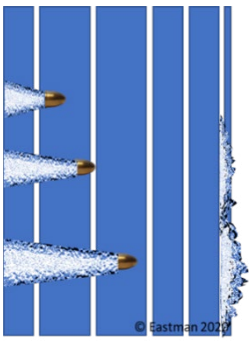
Building Safety and Security Assessment (BSSA) is intended for the purpose of facilitating occupant safety and security, and generally refers to the evaluation and recommendation of countermeasures, including design layout, devices, equipment, and protocols that can inhibit targeted violent acts, while possibly safeguarding occupants from the impacts of these acts and hastening emergency first-response.

Note: In developing this definition, the AHC-BSS understands that there are multiple definitions for safety and security assessment of facilities among design officials, industry practitioners, and code agencies. This definition is offered as a reference for how the AHC-BSS viewed, discussed, and deliberated on the process of BSSA with regard to the scope of the

recommendations found in this report. The terms safety and security used in this paper do not specifically refer to the body of existing fire and building codes, cyber related threats, or mitigation of the destruction of physical property or petty crimes, although it is acknowledged that these problems may also arise during a targeted violent event.

Glazing Security Levels (see Appendix E for application)

- **Basic:** The basic level of safety glazing is based on human impact forces and glass containment upon breakage. Often written into building codes, the intent is to ensure the glass has enough strength to withstand accidental impact with the glass, and also has requirements that glass fragments be contained to avoid injury. The products rated for this category are recommended for situations such as slowing immediate entry through glass and reducing the ability of someone to reach through an opening to release a door handle. Products such as laminated glazing or surface-applied safety films are readily available to meet applicable test standards.
- **Enhanced:** Burglary resistant glazing can be a deterrent to smash-and-grab crimes involving the use of hands, elbows, fists and general burglary tools such as a hammer. Products in this category are intended to deter vandalism such as breaking into a display case or entering the building and fleeing.
- **Ballistic Protection:** Bullet-resistant (BR) glazing is designed to resist penetration from a variety of firearm ammunitions. Several examples of bullet resistant laminated glazing include all-glass laminates, glass clad polycarbonate laminates, glass laminates containing other rigid polymers, laminated polycarbonates, and glass/exposed plastic laminates (exposed polycarbonate or PET). Bullet-resistant glazing provides an improved safety barrier against bullets and related flying glass or plastic fragments (spall or splinters).



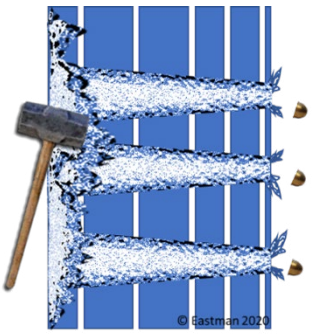
Example of Ballistics

- **Forced Entry:** Forced entry (FE) resistant glazing is designed to increase the amount of time required to gain entry. This additional time is intended to allow for the enactment of lock-down protocols. These products may be used in areas with high risk of prolonged attack or in critical areas such as entry vestibules. Forced entry resistant glazing should meet the criteria above and also resist penetration from hand-held or hand-thrown objects such as hammers, crowbars, bats, knives, bricks, and rocks.



Example of Forced Entry

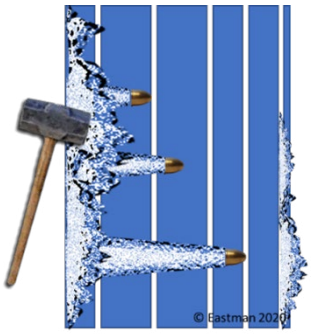
- **Enhanced Forced Entry** : Products in this category are intended to meet the requirements for forced entry resistant glazing after being weakened by ballistic assault. They are not designed for ballistic classification; thus, the bullets may penetrate the glazing. Enhanced forced entry testing can include shooting through the glass to weaken it followed by physical impact with various weapons. The glazing classification would carry an indication of the type of ballistic assault used along with a forced entry classification. The goal is to resist entry for an adequate amount of time to allow for the arrival emergency response personnel.



Example of Enhanced Forced Entry

- **Multiple Forced Entry Assault (Ballistics + Forced Entry):** Products in this category are designed to combine the resistance of ballistics classified laminates with additional resistance to forced entry. Testing for these glazing systems involves weakening the sample by ballistic assault but not allowing the bullets to penetrate. The glazing is then tested to withstand physical impact and attack with various weapons. This glazing would carry a ballistic and forced entry classification and would be used in very high-risk areas, where intruders may be armed with guns.

Example of Multiple Forced Entry Assault (Ballistic + Forced Entry):



- **Blast Resistance:** Blast-resistant glazing can substantially reduce injury from flying glass resulting from direct blast shock waves (over-pressures). When properly designed, framed, and anchored, blast-resistant glazing is capable of maintaining the integrity of the building envelope following an explosion and reducing interior damage. Blast-resistant glazing may offer some level of burglary or forced entry resistance but without testing to burglary or forced entry standards, how much resistance is not quantifiable. Also, this glazing is not typically bullet-resistant without being tested to a ballistic threat level.

First-responder includes all emergency personnel who as part of their profession, are required to respond to targeted violent acts, including but not limited to, local fire departments, local or regional police, FBI, SWAT, Homeland Security, the National Guard, military, ATF, EMTs, and private security personnel.

High occupancy or high-risk buildings may be used interchangeably in this report. High occupancy buildings generally refer to all or portions of the ICC International Building Code Occupancy Classification Groups A1, A2, A3, A4, A5 (Assembly), B (Business), E (Educational), I-2 (Institutional), (F) Factory and M (Mercantile), R-1 and R-2 to include Hotels, Resorts, Dormitories and Fraternity/Sorority Housing. These occupancies represent a majority of the locations where targeted violent acts have occurred, and which have resulted in multiple deaths and injuries. Reference to a high occupancy building within this document does not presume that all buildings with an elevated risk for a targeted violent event are included within the occupancies listed. As such, the work group believes that building owners, designers, and code officials should review each facility based on its own safety and security risks in order to make an informed decision whether to conduct a building safety and security assessment.

Process of Building Safety and Security Assessment is the professional evaluation of safety and security risks, and identification of possible design countermeasures of those risks to occupants during a targeted violent event. This process is defined in this report to distinguish it from a safety and security assessment which may be performed by others using different parameters than those envisioned in this report, or without requisite training and certification as being recommended in this report.

Targeted violent acts are human caused and committed with the intent to harm any or all occupants within a high occupancy or high-risk facility or within its property boundaries. Such acts might include, but are not limited to, an active shooter, workplace violence, hate crimes, or terroristic activities, armed violence, bomb, chemical, or biological threats.

ICC INTERNATIONAL CODE COUNCIL®

APPENDIX C—PLANNING CHECKLIST

1. Identification of stakeholders:
    a. Client
    b. Law enforcement
    c. Occupants
    d. First Responders
    e. Administrators in the K-12 environment including teachers, aides, janitors, students, school board members, legal counsel, PTA/PTO, and school resource officer. In essence everybody who attends, participates, is involved, or works at the school.
    f. Code officials including building, fire, planning and zoning officials who would likely be involved at various levels and to various degrees.
    g. Lawmakers/legislative bodies who may be at the state or local levels. These bodies may promote funding ideas and grant applications for security upgrades.
    h. Design and engineering team members who can stress the overall importance of building design but can also serve in a role to influence and empower clients to take a proactive approach in building security.
    i. Insurance carriers
    j. Facility managers
    k. Human resource team members
    l. Association of Threat Assessment Managers
    m. National Association of School Psychologists
2. The importance of planning and the resultant:
    a. Comprehensive plan and assessment
    b. Established team
    c. Identification of certified security professionals
    d. Identification of certified processes
    e. Identification of certified products which should be directed at specific product standards and product evaluation.
    f. Planning elements which include general administrative planning (policy related) and project administrative planning (design/construction related).
    g. Functional performance which identifies how buildings should either perform or be expected to perform under different hazard scenarios.
    h. Assessment of how building functional performance related to design accounts for culture. For example, personal space, sense of belonging, sense of wanting to be there.
    i. Insurance efforts in this area which become more crucial related to reimbursable costs for building cleanup and repair, biohazard remediation, employee assistance program, employee funeral expenses and memorials and business interruption costs due to loss of the building.
    j. Management of the insurance risk through formalized programs and plans and their impact on future premium costs.
    k. Hardware or architectural features.

3. Identification of best practices surrounding the privacy of documents:
    a. Separate set of documents related to security features and systems should have restricted access.
    b. A required watermark stamp
    c. A required confidential privacy warning
    d. Identification of the stakeholders who should be part of a limited distribution and the need for tracking/recording the stakeholders. Considerations should include whether the project is taxpayer funded.
    e. Establishment of a policy to define what buildings should have restricted access to plans and drawings. Establish boundaries for the information that should be available to the general public or the building occupants and their expectations of access. Certain buildings such as schools and court houses are examples where restricting access to certain types of building information should be a priority.
    f. Encryption of files
    g. Entrusted/bonded recipients
    h. Identification of established procedures
    i. Identification of insurance carriers
    j. Assessment of the extent of information involving emergency procedures and protocols that should be given to the public when visiting the building and how the information should be made available.

It is important to note that the identification of best practices or policies needs to be flexible and capable of being continuously reviewed and updated as technology and circumstances change.

4. The identification of fire drill best practices for preparation and performing the drills for both safety and security considerations. At present, these provisions are best covered and regulated in legally adopted codes including but not limited to the IFC, NFPA 1, and NFPA 101. The following are typical events and drill requirements to consider:
    a. Fire
    b. Intruder
    c. Storm
    d. Earthquake
    e. Tornado
    f. Hurricane
    g. Event that occurs external to the building (armed bank robbery near an occupied office building). The required building lockdown procedure must account for this situation.
    h. Schedule-semi-annually
    i. Evaluations
    j. Testing Record
    k. Determine how alarm systems or other notification means are utilized based on the event.
    l. Develop a plan for multiple simultaneous events and the resulting priority of notification to the occupants and the mechanism for notification.
    m. Develop a plan for the use of mass notification systems (MNS) designed to deliver warning as well as provide direction to the occupants.
    n. Develop a robust training and emergency planning goal to deal with response to targeted violent acts — in particular by occupants or employees. Such short fuse acts do not allow the luxury of time to make life-saving decisions as opposed to other types of building hazards that the occupant may encounter.

Regardless of approaches taken or hazards to be considered, the policies must be proactive and utilize over-the-top communication on drills. Recent violent acts have identified that occupants may not realize they were in the midst of an active shooter and injuries have occurred.

Active violence/targeted violence programs and drills come in many forms from tabletop to all out exercises or drills. Some of these training programs are risky and should be avoided — in particular those that may use a soft projectile or masked actors serving as the intruder.

Although there is no single national training program on prevention and response, certain federal programs such as those from the Secret Service or Department of Homeland Security (four phases of emergency management) or the run hide fight program are often referenced for this purpose.

5. Develop a library of resources for stakeholders.
    a. Focus on certified processes whenever possible.
    b. Integrate security planning (related to building design and policy/planning) into the upfront basis of design concepts. Security systems and approaches are more complex and must work seamlessly with other building design systems, features and operating plans.
    c. Look at measures to have a certified security professional as part of the design team rather than relying on other team member who lacks the specific expertise. See Chapter 2 Risk Assessment for a discussion on Building Safety and Security Assessment (BSSA).
    d. Building owners should come to expect a certified security professional as part of the design team.
    e. Facility managers need to be able to maintain and manage the internal policy and planning components for their employees.
    f. Resources and relevant knowledge and information must be tailored to specific types of occupancies and events. There is not a one-size-fits-all solution (see item 6).
    g. Catalog/cross reference information to make sure that correct decisions are being made with regard to building security based upon the identified security risks and factors.
6. Building safety and security should be generic to all occupancies but at the same time may require customization for specific projects/occupancies and threats, where appropriate. Sources of information on risks/occupancies include:
    a. I-Codes and Standards
    b. NFPA Codes and Standards
    c. Compiled data and statistic information and trends (See Appendix G).
    d. Certified security professionals
7. Identification of existing or new security professional certifications I-Codes and Standards
    a. See Chapter 1 discussion on Building Safety and Security Assessment.
    b. Establish baseline of existing programs
    c. Determine which programs are most appropriate or applicable depending on the professional category being considered — architect, engineer, authority having jurisdiction, or security professional.
    d. Identification of scalability of a certification program for AHJ's based upon size of jurisdiction or size of the project.
    e. Identify the justification for such a program such as the legal and moral responsibility related to public safety and the good of society.

ICC INTERNATIONAL CODE COUNCIL®

APPENDIX D—FIRST RESPONDER RESPONSE CHECKLIST

Overview

This appendix identifies key considerations and practices for response to targeted/active violence acts. This information is intended to inform facility managers so they are prepared for what responders will do when arriving to their facility as well as what the responders expect from facility operations.

Approach

This checklist is designed for use as a preliminary assessment of emergency preparedness for first responders. The intent is to promote a discussion about what is needed in the event of an emergency. It is also meant as a starting point for a conversation with local responders. An effective response to an emergency is contingent of coordination of all affected personnel.

First responders have internal standards and practices. When responding to an emergency, the response varies based on the situation - but it is fair to say the primary goal is to have injured people receive medical attention as soon as possible. In some cases, the active threat must be isolated before medical attention can be administered. Each situation is different so there it is not practical to develop a single uniform response protocol. However, opening a dialog with local responders will result in improvements in how responders establish their scene and the decisions they make.

Materials and information needed

As a starting point, gather all the emergency preparedness plans. These plans may be formal plans or informal plans.

- Emergency planning and preparedness documents.
  - This helps responders know how the facility intends to handle certain emergencies.
  - Use similar routines and roles that coincide with daily activities.
  - This doesn't have to be complicated. Overthinking the plan is not productive.
- Materials used to train employees and volunteers who perform emergency management and safety functions.
  - This helps responders know what the facility team has been trained to do.
- Policies and procedures for distribution of such materials (see Chapter 3 for a discussion on privacy of documents)
  - Responders will need to know which documents have been distributed/shared.
- Current contracts or other documents reflecting the facility's relationship with other public entities and/or private organizations who provide security or other response to the premise.
  - This gives responders a full picture of who their partners will be during an emergency response.
- A list of the facilities and locations designated as "emergency shelters" and "shelter in place." This is likely within the emergency preparedness plan. Other locations within the plan might include rally/muster points and family reunification locations.
  - This gives responders an idea where occupants will be gathering during an emergency.
- A site plan showing the extent of the property. A site plan may be accessible from an internet mapping system.
  - This gives responders an awareness of the accessibility and constraints of the site which informs staging and response locations.
- Are employees charged with the responsibility to act as a liaison with first responders?
  - It is a generally good idea to have a designated employee who has primary or additional duties which are part of the emergency management of the facility.

Facility managers and first responders
Typically, the facility manager will reach out to their local responders to initiate a relationship. Hiring an expert security consultant to participate in the discussion may prove to be beneficial. See discussion in Chapter 2 about the BSSA.

- Introduce key personnel including any point of contacts for critical incidents.
- Share key issues of concern from a building operation perspective, including sensitive, secure, and hazardous areas of the facility.
- Ensure that each party understands facility access protocol requirements involving key control or specialized security access procedures when appropriate in order to expedite access by first responders in concert with planned occupant movements during emergency operations
- After providing an overview of the plan, fill in any knowledge gaps in the responder's preplan.
- Fill in any knowledge gaps in the responder's plan. This is an opportunity to confirm a mutual understanding of processes.
- Set up future tours, trainings, etc., if desired. A tabletop exercise can highlight areas of improvement in the plan.
- Make a plan for future engagement. A routine check-in will keep information fresh as both sides experience attrition.

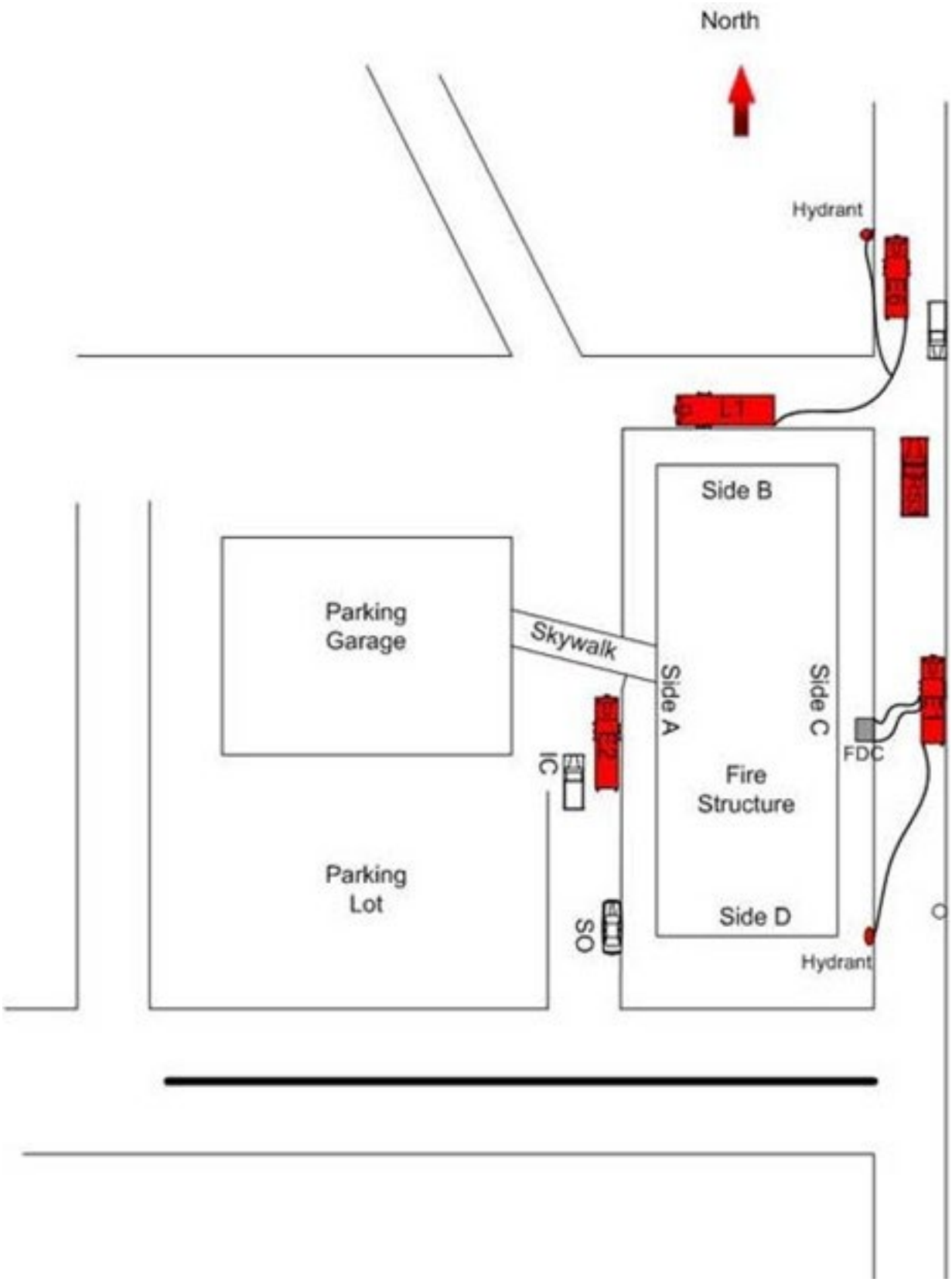
Emergency responders are trained to take in very little information and quickly develop an action plan. They will adapt to what is happening in a given situation. Following your plan gives responders the space they need to isolate and resolve the incident quickly utilizing their own training and procedures.

References (See Appendix G)

- NFPA 3000 Standard for an Active Shooter/Hostile Even Response (ASHER) Program

Examples of Parking Lot Staging Areas
The following are simplified examples of how staging in a parking lot for evacuations and staging of responders may occur. In most cases, such staging is specific to the type of event and as such, each staging plan may differ significantly. All staging plans should be discussed pro-actively as part of the plan to be prepared to respond to such acts.




North
Hydrant
L1
Side B
Parking Garage
Skywalk
Side A
Side C
FDC
IC
Fire Structure
Parking Lot
SO
Side D
Hydrant

APPENDIX E—NGA: SECURITY GLAZING SUMMARY

National Glass Association: Security Selection Quick Reference Summary

		Security Level of the Selection*		
Security Selection	**Test Standard**	**Low**	**Medium**	**High**
Basic Safety Glazing	ANSI Z97.1	Class B		Class A
	CPSC	Cat I		Cat II
	CAN CGSB	Class B		Class A
	ASTM F3006/F3007	0.75 m Cat 2	3.66 m Cat 3	3.66 m Cat 2
Enhanced	UL 972	Std – 10 ft	Ind/Outdoor	High Energy (40 ft)
	ASTM E2395	L1	L3	L5
	ASTM F1233	1.0	1.1	1.2
Forced Entry	ASTM F1233	1.4	2.3	5.0
	ASTM F3038 – mob with hand tools	5 min	15 min	30 min
Enhanced Forced Entry	ASTM F1233 Annex A2	3 shots with 9 mm handgun; Class 1.4	3 shots with .357 Magnum; Class 2.3	3 shots with .44 Magnum; Class 5.0
Ballistic Protection (Hand-guns)	UL 752	1 (9 mm handgun)	2 (.357 Magnum)	3 (.44 Magnum)
	ASTM F1233	HG3 (9 mm handgun)	HG2 (.357 Magnum)	HG4 (.44 Magnum)
Multiple Forced Entry Assault (Ballistics + Forced Entry)	ASTM F1233	HG1/R1-1.4	HG2/R2-2.3	HG4/R3-5.0
Blast Resistance	ASTM F1642/F2912	H3	H2	H1

** This is not meant to be all-inclusive; there are levels existing outside of this table.*

ICC INTERNATIONAL CODE COUNCIL®

APPENDIX F—ACCESS CONTROL FOR BUSINESS OCCUPANCIES

Overview

As noted in Chapter 5, the primary focus of the AHC-BSS was access control for K-12 schools. This appendix includes access control considerations for business occupancies.

ACCESS CONTROL OPTIONS MATRIX FOR BUSINESS OCCUPANCIES: PERSONNEL AND ACTIVITIES

<table>
<tr><th colspan="4">Situations: Business Occupancy
Drivers/Reasons/Time Period(s) of People Movement</th></tr>
<tr><th>Typical business day/ time frame</th><th>Outside of typical business day/time frame</th><th>People Movement Bulk/Many</th><th>People “Types”</th></tr>
<tr><td>Employee/staff arrival
Customer/client/visitor arrival
Service/delivery personnel arrival
Employee/staff departure
Customer/client/visitor departure
Service/delivery personnel departure
Separating employee departure
Emergency/fire drills-exiting
Emergency/Fire drills-re-entry</td><td>Employee/staff arrival
Customer/client/visitor arrival
Service/delivery personnel arrival
Employee/staff departure
Customer/client/visitor/ departure
Service/delivery personal departure</td><td rowspan="4">Bulk entry/ingress
Bulk exit/egress
Bulk entry and exit
Non-bulk exit/egress
Non-bulk entry and exit</td><td rowspan="4">Known, recognized, pre-authorized, preapproved
Not known, not recognized, not preauthorized, not preapproved
Person(s) w/intent to inflict harm and/or physical damage</td></tr>
<tr><td colspan="2">Unplanned/unscheduled</td></tr>
<tr><td>Fire issue/Emergency
Health issue/emergency
Violence issue/ emergency
Weather issue/emergency
Law enforcement issue/ emergency</td><td>Fire issue/emergency
Health issue/emergency
Violence issue/ emergency
Weather issue/emergency
Law enforcement issue/ emergency</td></tr>
</table>

How to use this matrix: This matrix is intended to provide multiple scenarios to identify the movement of people. As a matrix it is **not** intended to be read across the row with entries adjacent to the first column entry being applied to the first column entry. See the example on page 29. This matrix is not intended to be all inclusive.

ICC INTERNATIONAL CODE COUNCIL®

ACCESS CONTROL OPTIONS MATRIX FOR BUSINESS OCCUPANCIES: ACCESS-INGRESS CONTROL PLANNING OPTIONS

Type/Location of Entrance/ Exit	Facility Design Options				Facility Design Physical Protection & Hardening (Note 1)			Facility Design-Expected Administrative/Staff Responsibilities at Door(s) Regarding People Movement	
Intended function	Door(s)/Areas Layout Design	Human interaction & Facilitation Design at Door(s)	Door Status Monitoring Design	Door Unlocking/ Locking Ingress/Access Control	Doors	Glazing	Walls	Ingress/Access Monitoring/ Control	Egress Monitoring/ Control (Note 2)
Main/formal/ front entrance to building Secondary entrance/ exit – for employees/ staff. Secondary entrance/exit for customers/ clients/visitors Secondary entrance/exit-for service/ delivery Emergency ops/control room	None/no door(s)/open to outside Single stage (designed to pass only one door for ingress) Two stage (designed to pass through two doors in series for ingress Two stage-exterior door(s) not ingress controlled Two stage-exterior door(s) ingress controlled	None/ no human interaction at door(s) Audio & visual – direct w/o physical protection Audio & visual – direct with physical protection Visual only-direct with physical protection Audio only – indirect (assumed w/physical protection)	None/no monitoring of door(s) open/ close status Visual-direct (status of door can be observed directly by a person) Visual-indirect – video Visual-indirect-open/closed status (i.e. text or graphic on display screen) Visual – indirect-people activity at door(s) (i.e. text graphic on display screen).	None (doors not locked to control ingress) Key or credential-temp unlocking (door locks when closed) Key or credential – unlocked until active re-locking Remote operated-temp unlocking (door locks when closed) Remote operated-unlocking – req's active relocking at door.	None Impact Ballistics Blast Protection	None Impact Ballistics Blast Protection	None Impact Ballistics Blast Protection	None/no staff responsibilities at door(s) re: access control Visual Monitoring Audio Monitoring Visual Interaction Audio Interaction	None/no staff responsibilities at door(s) re: egress control Visual/audio monitoring direct Visual/audio monitoring direct with passive physical presence Visual monitoring remotely - passive presence

ICC INTERNATIONAL CODE COUNCIL®

ACCESS CONTROL OPTIONS MATRIX FOR BUSINESS OCCUPANCIES: ACCESS-INGRESS CONTROL PLANNING OPTIONS (CONT'D)

Type/Location of Entrance/ Exit	Facility Design Options				Facility Design Physical Protection & Hardening (Note 1)			Facility Design-Expected Administrative/Staff Responsibilities at Door(s) Regarding People Movement	
Intended function	Door(s)/Areas Layout Design	Human interaction & Facilitation Design at Door(s)	Door Status Monitoring Design	Door Unlocking/ Locking Ingress/Access Control	Doors	Glazing	Walls	Ingress/Access Monitoring/ Control	Egress Monitoring/ Control (Note 2)
Emergency exit/egress (only)	Two stage-Interior door(s) not ingress controlled Two stage-Interior door(s) ingress controlled	Visual only -indirect (assumed with physical protection) Audio & Visual – indirect (assumed with physical protection)	Audio-indirect-door open general alarm Audio-indirect-door open specific alarm Audio-indirect-people activity at door(s) (i.e. audible alarm)	Remote operated unlocking-reqs active/ relocking remotely. Regardless of ingress/ access control functions such as door locking and unlocking configurations, provision for egress shall provided as required by applicable building, fire and life safety codes				Physical interaction-locks operated remotely Physical interaction-in-person prior to door, passive Physical interaction-in person prior to door, active Physical interaction – in person after door, passive Physical interaction – in person after door, active	Visual monitoring remotely - active Audio monitoring – remote passive Audio monitoring – remoting active

Note 1: See Appendix E for physical protection of hardening security selections.

Note 2: Regardless of egress monitoring or control functions such as door locking and unlocking configurations, provisions for egress shall be provided as required by applicable building, fire and the life safety codes.

How to use this matrix: This matrix is intended to provide scenarios/applications when considering the control of the movement of people in the building. As a matrix it is **not** intended to be read across the row with entries adjacent to the first column entry being applied to the first column entry. See the example on page 29. This matrix is not intended to be all inclusive.

ICC INTERNATIONAL CODE COUNCIL®

APPENDIX G—RESOURCE MATERIAL

This appendix includes the identification of resources referenced in this document as well as other resource material on the subject of building security and safety. This appendix includes links to publicly available documents as underlined. This list also includes pdf's "[see pdf]" of publicly available documents which are posted under "Literature Review" on ICC's AHC-BSS site linked below. In order to access those documents not publicly available in this appendix, please contact the promulgator.

ICC's AHC-BSS webpage: https://www.iccsafe.org/products-and-services/i-codes/code-development/cs/ad-hoc-committee-on-building-safety-and-security-bss/

Federal

- US Dept. of Homeland Security: Active Shooter How to Respond
- US Secret Service Threat Assessment
- US General Services Administration Site Security Design Guide
- DHS Active Shooter Preparedness
- Access Control Technologies Handbook, U.S. Department of Homeland Security https://www.dhs.gov/sites/default/files/publications/ACT-HB_0915-508.pdf
- Security Risk Management Series Publications, FEMA https://www.fema.gov/security-risk-management-series-publications
- NIBS: Security for Building Occupants and Assets

State and Local

See "Educational Facilities" below for numerous state and local educational parameters

Educational Facilities

- AIA Where do we stand: School design and student safety
- Partner Alliance for Safer Schools (PASS)
- AIA Committee on Architecture for Education [see pdf]
- DHS: K-12 School Security: A Guide for Preventing & Protecting Against Gun Violence
- NIBS: Integrated Rapid Visual Screening of Schools: A How-to Guide to Mitigate Multihazard Effects Against School Facilities
- Safety and Security Guidelines, for K-12 Schools, Partner Alliance for Safe Schools, PASS https://passk12.org/guidelines-resources/pass-school-security-guidelines/
- K-12 School Security Guide Product Suite: https://www.cisa.gov/publication/k-12-school-security-guide
- "FEMA 428/BIPS 07 - Primer to Design Safe School Projects in Case of Terrorist Attacks and School Shootings, 2nd Edition (2012)"
- NFPA School Safety and Security Update
- FEMA P-1000: Safer, Stronger Smarter: A Guide to Improving School Natural Hazard Safety
- Final report of the Federal Commission on School Safety
- Massachusetts: Emergency Planning and Preparedness in Schools [see pdf]
- Utah 2018 General Session: School Security Locks [see pdf]

- New Jersey 218th Legislature [see pdf]
- Marjory Stoneman Douglas High School Public Safety Commission Initial Report
- Emergency Preparedness & Classroom Security in CA [see pdf]
- Virginia State Law for School Design
- National Clearing House for School Safety https://www/schoolsafety.gov (I Love U Guys Foundation): https://iloveuguys.org/

Building Materials and Systems

Glazing

- ANSI Z97.1 Safety Glazing Materials Used in Buildings - Safety Performance Specifications and Methods of Test
- ASTM E2395 Standard Specification for Voluntary Security Performance of Window and Door Assemblies with Glazing Impact
- ASTM F1233 Standard Test Method for Security Glazing Materials and Systems
- ASTM F1642 *Standard Test Method for Glazing and Glazing Systems Subject to Airblast Loadings*
- ASTM F 2912 Standard Specification for Glazing and Glazing Systems Subject to Airblast Loadings
- ASTM F 3006 Standard Specification for Ball Drop Impact Resistance of Laminated Architectural Flat Glazing
- ASTM F3007 Standard Test Method for Ball Drop Impact Resistance of Laminated Architectural Flat Glass
- ASTM F3038 Standard Test Method for Timed Evaluation of Forced-Entry-Resistant Systems
- EN 1063 *Glass in building - Security glazing - Testing and classification of resistance against bullet attack* (European Standard)
- NGA FB71 – 21 School Security Glazing, National Glass Association
- NIJ 0108.01 Ballistic Resistant Protective Materials, National Institute of Justice
- UL 752 *Standard for Bullet-Resisting Equipment*
- UL 972 *Standard for Burglary Resisting Glazing Material*

Surveillance

- DHS Science and Technology Directorate – Video Quality in Public Safety https://www.dhs.gov/sites/default/files/publications/VQIPS_Video-Quality-in-Public-Safety_Fact-Sheet-170301_v2-508.pdf
- Digital Video Quality Handbook, May 2013-2018 https://www.dhs.gov/sites/default/files/publications/VQiPS_Digital-Video-Quality-HB_UPDATED-180117-508.pdf
- Digital Video Quality Handbook Appendix, January 2018 https://www.dhs.gov/sites/default/files/publications/VQiPS_Digital-Video-Quality-HB-Appendix_180117-508.pdf
- Policy Considerations for the Use of Video in Public Safety, June 2016 https://www.dhs.gov/sites/default/files/publications/Policy_Considerations_for_the_Use_of_Video_in_Public_Safety_Final_v5.pdf
- NIST Definition of Cloud Computing, Special Publication 800-145, September 2011 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
- UL White Paper – Video Image Quality Testing
- ASIS Facilities Physical Security Measures Guideline (ASIS GDL FPSM-2009) https://store.asisonline.org/
- ASIS Physical Asset Protection Standard (Feb. 2021) https://store.asisonline.org/

- Department of Army, Physical Security, FM3-19.30 https://www.wbdg.org/FFC/ARMYCOE/FIELDMAN/fm31930.pdf
- DHS, CCTV Technology Handbook, System Assessment and Validation for Emergency Responders (SAVER) https://www.dhs.gov/sites/default/files/publications/CCTV-Tech-HBK_0713-508.pdf
- Sample Policy for School Use of Video Surveillance and Audio Monitoring Sample Policy for School Use of Video Surveillance and Audio Monitoring | Security Industry Association
- CISA – Cybersecurity and Infrastructure Agency https://www.cisa.gov/

I- Codes
The following I-Codes can be accessed from ICC's Public Access site https://codes.iccsafe.org/

- 2021 International Building Code (IBC)
- 2021 International Fire Code (IFC)
- 2021 International Green Construction Code (IgCC)

Standards
- NFPA 1, Fire Code
- NFPA 101 Life Safety Code
- NFPA 730 Guide for Premises Security
- NFPA 731 Standard for the Installation of Electronic Premises Security Systems
- NFPA 3000: Standard for an Active Shooter/Hostile Event Response (ASHER) Program
- UL 294 Access Control System Units
- UL 2802 Performance Testing of Camera Image Quality
- Proper Application of UL Standards for Controlled or Delayed Egress Locking Devices – UL 294 & 1034 | UL Solutions

Fire Service
- IAFC Position Paper: Maintaining Building and Fire Safety During Active Assailant Events
- IAFC Position Paper: Active Violence and Mass Casualty Terrorist Incidents
- NASFM School Safety Position Statement
- NASFM Classroom Door Security https://www.firemarshals.org/resources/Documents/NASFM%20Classroom%20Door%20Security%2020210217.pdf

Reports, Summits, Workshops and Symposiums
- NFPA Workshop on School Safety, Codes and Security Final Report (December 3 – 4, 2014)
- NFPA Building Safety and Security Workshop (May 2018)
- 1 October After Action Review: Las Vegas Mandalay Bay [pdf]

Data/Statistics
- Global Terrorism Database
- Indicators of School Crime and Safety: 2017

Magazine/News Articles

- EMS World: Parkland: Lessons Learned
- NPR: The Shootings that Weren't
- NFPA Journal September/October 2018; Campus Safety in the age of active Shooters
- Run Hide Fight
- NFPA Journal Exiting Smarter

You Tube Videos

- School training
- Alice training institute

Other Resources

- Certified Protection Professional ASIS International
- iDigHardware: https://idighardware.com/schools/
- Crime Prevention through Environmental Design https://www.cpted.net