Skip to main content

WBDG a program of the National Institute of Building Sciences
WHOLE BUILDING DESIGN GUIDE

SECURE / SAFE

the WBDG Secure / Safe Committee
Updated: 01-12-2017

OVERVIEW

WITHIN THIS PAGE

The design and construction of secure and safe buildings (minimal danger or risk of harm) continues to be the primary goal for owners, architects, engineers, project managers, and other stakeholders. In addition to those listed, other stakeholders include: construction managers, developers, facilities managers, code officials, fire marshals, building inspectors, city/county/state officials, emergency managers, law enforcement agencies, lenders, insurers, and product manufacturers. Risk assessment is the activity that estimates potential building and infrastructure losses from earthquakes, riverine and coastal floods, hurricane winds, and other hazards. Realizing this goal is often a challenge due to funding limitations, resistance from the occupants due to impacts on operations, productivity and accessibility, and the impacts on the surrounding environment and building architecture due to perimeter security, hardening, and standoff requirements. Understanding the impact site security has on the overall security of the building is important as well.

A balance between the security and safety goals and the other design objectives and needs of the facility can be attained. The establishment of an integrated design process where all of the design team members understand each other's goals can aid in overcoming these challenges and will lead to the development of a solution which addresses all of the requirements. Understanding the interrelationship with the other WBDG design objectives (i.e., Sustainable, Aesthetics, Cost-Effective, Historic Preservation, Accessible, Functional / Operational and Productive), early in the design process, is an essential step in overcoming the obstacles commonly encountered in the achievement of a secure and safe building.

Consistent with areas of professional responsibility, it is useful to identify four fundamental principles of all-hazard building design:

- Plan for Fire Protection
  Planning for fire protection for a building involves a systems approach that enables the designer to analyze all of the building's components as a total building fire safety system package.
- Protect Occupant Safety and Health
  Some injuries and illnesses are related to unsafe or unhealthy building design and operation. These can usually be prevented by measures that take into account issues such as indoor air quality, electrical safety, fall protection, ergonomics, and accident prevention.
- Natural Hazards Mitigation

Exterior of National Museum of the American Indian—Washington, DC

Each year U.S. taxpayers pay over $35 billion for recovery efforts, including repairing damaged buildings and infrastructure, from the impacts of hurricanes, floods, earthquakes, tornados, blizzards, and other natural disasters. A significant percentage of this amount could be saved if our buildings properly anticipated the risk associated with major natural hazards.

- Provide Security for Building Occupants and Assets
  Effective secure building design involves implementing countermeasures to deter, detect, delay, and respond to attacks from human aggressors. It also provides for mitigating measures to limit hazards to prevent catastrophic damage and provide resiliency should an attack occur.

Designing buildings for security and safety requires a proactive approach that anticipates—and then protects—the building occupants, resources, structure, and continuity of operations from multiple hazards. The first step in this process is to understand the various risks they pose. There are a number of defined assessment types to consider that will lead the project team in making security and safety design decisions. This effort identifies the resources or "assets" to be protected, highlights the possible perils or "threats," and establishes a likely consequence of occurrence or "risk." This assessment is weighed against the vulnerabilities specific to the site or facility. Based on these assessments and analysis, building owners and other invested parties select the appropriate safety and security measures to implement. Their selection will depend on the security requirements, acceptable levels of risk, the cost-effectiveness of the measures proposed for total design efficiency, evaluation of life cycle cost, and the impact these measures have on the design, construction, and use of the building.

Hazard Mitigation refers to measures that can reduce or eliminate the vulnerability of the built environment to hazards, whether natural or manmade. The fundamental goal of hazard mitigation is to minimize loss of life, property, and function due to disasters. Designing to resist any hazard(s) should always begin with a comprehensive risk assessment. This process includes identification of the hazards present in the location and an assessment of their potential impacts and effects on the built environment based on existing or anticipated vulnerabilities and potential losses. When hazard mitigation is implemented in a risk-informed manner, every dollar spent on mitigation actions results in an average of four dollars' worth of disaster losses being avoided. (*Natural Hazard Mitigation Saves: An Independent Study to Assess the Future Savings from Mitigation Activities*)

Regulations, codes, standards, and best practices will guide the design of buildings to resist natural hazards. For new buildings, code requirements serve to define the minimum mitigation requirements, but compliance with regulations in building design is not always sufficient to guarantee that a facility will perform adequately when impacted by the forces for which it was designed. Indeed, individual evaluation of the costs and benefits of specific hazard mitigation alternatives can lead to effective strategies that will exceed the minimum requirements. Additionally, special mitigation requirements may be imposed on projects in response to locale-specific hazards. When a change in use or occupancy occurs, the designer must determine whether this change triggers other mitigation requirements and must understand how to evaluate alternatives for meeting those requirements.

It is common for different organizations to use varying nomenclature to refer to the components of risk assessment. For example, actual or potential adversary actions such as sabotage and terrorist attacks are referred to as "threats" by the law enforcement and intelligence communities, while natural phenomena such as hurricanes and floods are generally referred to as "hazards" by emergency managers; however, both are simply forces that have the potential to cause damage, casualties, and loss of function in the built environment. Regardless of who is conducting the risk assessment, the fundamental process of identifying what can happen at a given location, how it can affect the built environment, and what the potential losses could be, remains essentially the same from application to application.

INTEGRATING SAFE AND SECURE DESIGN

There are times when design requirements addressing all the various threats will pose conflicts in arriving at acceptable design and construction solutions. Examples include Blast Resistant Glazing, which may impede emergency egress in case of fire; access control measures that prevent intrusion, but may also restrict emergency egress; and Leadership in Energy and Environmental Design (LEED) light pollution reduction and security lighting objectives. Conversely, site design and security can complement each other such as the design of a storm water management requirement that doubles as a vehicle barrier. Good communication between the design team, fire protection and security design team specialists through the entire design process is necessary to achieve the common goal of safe and secure buildings and facilities.

Most security and safety measures involve a balance of *operational, technical, and physical safety methods*. For example, to protect a given facility from unwanted intruders, a primarily operational approach might stress the deployment of guards around the clock; a primarily technical approach might stress camera surveillance and warning sirens; while a primarily physical approach

might stress locked doorways and vehicle barriers. In practice, a combination of approaches is usually employed to some degree and a deficiency in one area may be compensated by a greater emphasis in the other two.

In addition to the operational/technical/physical taxonomy, it is useful to characterize risk reduction strategies as either *structural* or *nonstructural*. Structural mitigation measures focus on those building components that carry gravity, wind, seismic and other loads, such as columns, beams, foundations, and braces. Examples of structural mitigation measures include building material and technique selection (e.g., use of ductile framing and shear walls), building code compliance, and site selection (e.g., soil considerations). In contrast, non-structural strategies focus on risks arising from damage to non-load-bearing building components, including architectural elements such as partitions, decorative ornamentation, and cladding; mechanical, electrical, and plumbing (MEP) components such as HVAC, life safety, and utility systems; and/or furniture, fixtures and equipment (FF&E) such as desks, shelves, and other material contents. Non-structural mitigation actions include efforts to secure these elements to the structure or otherwise keep them in position and to minimize damage and functional disruption. These measures may be prescriptive, engineered, or non-engineered in nature.

It should be noted that in any given building, non-structural components, including general building contents, typically account for over threequarters of the cost of a building; this figure can be even higher for specialized occupancies such as medical facilities. Additionally, structural and non-structural components can potentially interact during an incident, requiring a deliberative approach to implementing a comprehensive agenda of structural and non-structural mitigation actions.

Note: Information in these Secure/Safe pages must be considered together with other design objectives and within a total project context in order to achieve quality, high performance buildings.

RELATED ISSUES

RESILIENCE

Natural and manmade hazardous events can impose a devastating cost to society. As Figure 1.1 shows, the costs of some of these disasters in the US alone can be staggering. Stakeholders of civil infrastructure have a vested interest in reducing these costs by improving and maintaining operational and physical performance.

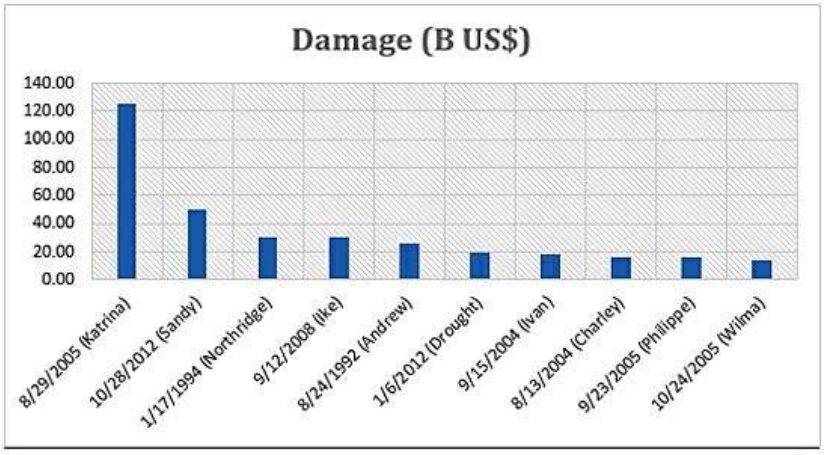

Figure 1.1 - Damages from recent natural disasters in the US. The name of the disaster follows the year of occurrence.
Source EM-DAT (2014)

Throughout history, infrastructure resilience has been defined in numerous ways, the most widely used and most objective is by the National Infrastructure Advisory Council (NIAC*) (2009), which states:

> "Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event."

No city, federal facility, or military installation is immune to challenges, whether natural or manmade, and given the world's growing population, more people than ever are in the potential path of catastrophe. Fortunately, cities can become resilient and

withstand shock and stress. As conditions change over time, cities that are resilient can evolve in the face of disaster and stop failure from rippling through systems; they can reestablish function quickly and avoid long-term disruptions.

This section explores different aspects of resilience management, with increased costs of manmade and natural hazards the primary concern. To reduce these costs and ensure that infrastructure exhibits a high degree of resilience, a definition of resilience was incorporated using four components: robustness, resourcefulness, recovery, and redundancy.

Stakeholders of buildings stand to benefit from resilience management, for which there is a strong business case. Businesses locate where they can rely on critical infrastructure. Communities that become resilient will increasingly attract businesses because executives know they can rely on the services and workforce availability, even in the face of disruptive events.

Natural and manmade hazardous events are unpredictable, but they are still inevitable and impose a devastating cost to civil infrastructure. By improving and maintaining the operational and physical performance of our nation's building stock, strategies for resilience can be developed.

When planning and designing buildings, it is appropriate to try to mitigate the potential of the spiraling cost of operational failures by opting for more resilient performance through well-planned investments in better planning and designs. It no longer makes sense to wait until after a crisis to implement resilience efforts. If strategies for buildings are discussed and implemented now, there is a greater chance of increased efficiency, not only today but for the future, benefiting all buildings stakeholders.

COMPONENTS OF BUILDING RESILIENCE

The NIAC (2009) determined that resilience can be characterized by three key features:

"**Robustness**: the ability to maintain critical operations and functions in the face of crisis. This includes the building itself, the design of the infrastructure (office buildings, power generation, distribution structures, bridges, dams, levees), or in system redundancy and substitution (transportation, power grid, communications networks).

Resourcefulness: the ability to skillfully prepare for, respond to, and manage a crisis or disruption as it unfolds. This includes identifying courses of action and business continuity planning,; training,; supply chain management,; prioritizing actions to control and mitigate damage;, and effectively communicating decisions.

Rapid recovery: the ability to return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption. Components [of rapid recovery] include carefully drafted contingency plans, competent emergency operations, and the means to get the right people and resources to the right places."

It is proposed that resilience has another key feature: **Redundancy**, which means that there are back-up resources to support the originals in case of failure.

Sometimes, these four resilience features are simply called the 4Rs. Resilience is multidisciplinary and needs the cooperation of different disciplines for successful outcome. Without multidisciplinary cooperation and contributions, there cannot be successful or efficient resilient infrastructure.

For more on this topic see A Regional Resilience/Security Analysis Process for the Nation's Critical Infrastructure Systems and Architectural Graphic Standards - Building Resiliency.

OCCUPANT EMERGENCY PLAN

Occupant emergency plans are an integral part of an emergency management program. Properly developed plans can reduce the risk to personnel, property, and other assets while minimizing work disruption during and immediately following an emergency. See U.S. Department of Energy Model Occupant Emergency Plan.

INFORMATION SENSITIVITY

As a result of the heightened level of interest in homeland security following the attacks of 11 September 2001, the public is even more interested in efforts to protect people, buildings, and operations from disasters. This interest presents both benefits and challenges, because much of the same information that can be used to gather support for mitigation can also be used by potential

terrorists, saboteurs, or others with malevolent intent. For that reason, project delivery teams must carefully maintain the security of any information that pertains to vulnerabilities or facility infrastructure particularly when the building is part of a critical infrastructure or system. Per Department of Homeland Security (DHS), critical infrastructure is defined as "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof." The Department of Homeland Security Protected Critical Infrastructure Information Program (PCII) was developed as an information-protection program that enhances information sharing between the private sector and the government. PCII is used by DHS and other federal, state and local organizations to analyze and secure critical infrastructure and protected systems, identify vulnerabilities and develop risk assessments, and enhance recovery preparedness measures. Legal counsel should be obtained on how best to protect such sensitive information from unauthorized use within the provisions of applicable local, state, and federal laws.

By December 2017, all vendors/contractors will need to have an Information Systems Security Plan per DFARS-CUI Guide. This plan will cover a company's business systems, CAD/BIM, data and processes.

Occupant Emergency Plans should be developed for building Operations staff and occupants to be able to respond to all forms of attacks and threats. Clearly defined lines of communication, responsibilities, and operational procedures are all important parts of Emergency Plans.
Emergency Plans are an essential element of protecting life and property from attacks and threats by preparing for and carrying out activities to prevent or minimize personal injury and physical damage. This will be accomplished by pre-emergency planning; establishing specific functions for Operational staff and occupants; training Organization personnel in appropriate functions; instructing occupants of appropriate responses to emergency situations and evacuation procedures; and conducting actual drills.

Resilience is a primary metric of risk assessment. In addition to mitigating damage and protecting the lives of building occupants, buildings that are designed for resilience can absorb and rapidly recover from a disruptive event. Continuity of operations is a major focus. Estimates should reflect state-of-the-art scientific and engineering knowledge and can be used to inform decision-making at all levels of government by providing a reasonable basis for developing mitigation, emergency preparedness, and response and recovery plans and policies.

STOREFRONT SAFETY

According to the Storefront Safety Council and the Texas Traffic Institute at Texas A&M University, 60 times a day, nearly 500 deaths and more than 4,000 injuries per year happen when out-of-control vehicles crash into homes and buildings. While we may think these happen only to private sector shops and stores, consider that many federal, state, and local government buildings are located on city streets which make them vulnerable as well.

The value of crash rated bollards, planters and site furnishings in protecting pedestrians, sidewalk café patrons, and shoppers and employees inside stores from out-of-control vehicles cannot be disputed. Incidents where a vehicle is employed by terrorists to inflict mass casualties at large gatherings like parades, marathons, and holiday festivities further reinforce the need for and value of crash rated barriers.

While storeowners may be reluctant to pay the cost of these barriers, they should weigh in the losses they face when their store is closed for reconstruction after an incident and for the personal injury suits for which they will be liable.

For more information on this topic see the Storefront Safety Initiative and Storefront Crashes.com.

BUILDING INFORMATION MODELING

Building Information Modeling (BIM) can be a useful tool for building security. For example, intelligent objects in 3D provide better understanding of vulnerabilities and better correlation with other design aspects like building and site access, location and types of doors and windows, and structural design characteristics for seismic versus blast design. BIM will further the integration between project team members, design disciplines, and the various stages of a project to achieve the goal of a high performance building. Properly maintained, BIM can provide complete, up-to-date information on the building and its' systems throughout the building service life.

RELEVANT CODES AND STANDARDS

- ASIS SPC.1 *Organizational Resilience: Security Preparedness, and Continuity Management Systems—Requirements with*
- *Guidance for Use Standard*
- ASIS GDL BC 01 *Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and*
- *Disaster Recovery*
- ASIS/BSI BCM.01 *Business Continuity Management Systems: Requirements with Guidance for Use*
- *ASIS Chief Security Officer—An Organizational Model*

NFPA 1600 *Standard on Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs*, 2016 edition NFPA 72 *National Fire Alarm and Signaling Code*, 2013 edition

MAJOR RESOURCES

WBDG

DESIGN OBJECTIVES

Historic Preservation—Accommodate Life Safety and Security Needs

PUBLICATIONS

- ASIS SPC.1-2009 *Organizational Resilience: Security, Preparedness, and Continuity Management Systems—Requirements with Guidance for Use*, by ASIS International
- Buildings and Infrastructure Protection Series by the Department of Homeland Security:
  - BIPS 01 Aging Infrastructure: Issues, Research, and Technology/li>
  - BIPS 02 Integrated Rapid Visual Screening of Mass Transit Stations
  - BIPS 03 Integrated Rapid Visual Screening of Tunnels
  - BIPS 04 Integrated Rapid Visual Screening of Buildings
  - BIPS 05 Preventing Structures from Collapsing
  - BIPS 06 / FEMA 426 Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings
  - BIPS 07 / FEMA 428 Primer to Design Safe School Projects in Case of Terrorist Attacks and School Shootings
  - BIPS 08 Field Guide for Building Stabilization and Shoring Techniques
  - BIPS 09 Blast Load Effects in Urban Canyons: A New York City
  - Study (FOUO) BIPS 10 High Performance Based Design for the Building Enclosure
- Department of Homeland Security *Federal Continuity Directive 1*
- FEMA 386 Series, *Mitigation Planning How-To Guide Series*

FEMA 386-2 *Understanding Your Risks: Identifying Hazards and Estimating Losses*

- FEMA 452 *Risk Assessment—A How-To Guide to Mitigate Potential Terrorist*
- *Attacks Against Buildings* ICC IBC *International Building Code*
- *The National Strategy for "The Physical Protection of Critical Infrastructure and Key Assets"*, The White House. February
- 2003.
- National Institute of Standards and Technology (NIST) Publications
- PBS-P100 *Facilities Standards for the Public Buildings Service* by the General Services Administration (GSA).

A Regional Resilience/Security Analysis Process for the Nation's Critical Infrastructure Systems by UT-Battelle, LLC,

- operator of Oak Ridge National Laboratories, and ASME Innovative Technologies Institute, LLC. December 2011.

Uses of Risk Analysis to Achieve Balanced Safety in Building Design and Operations by Bruce D. McDowell and Andrew C. Lemer, Editors;
Committee on Risk Appraisal in the Development of Facilities Design Criteria, National Research Council. Washington, DC: National Academy Press, 1991.

WEBSITES

- Department of Homeland Security—Science & Technology—Resilient Systems Division
- Department of Veterans Affairs (VA) Office of Construction & Facilities Management
- Interagency Security Committee (ISC)
- The Integrated Resilient Design Program by the National Institute of Building Sciences
- National Institute of Standards and Technology
- National Fire Protection Association
- Unified Facilities Criteria (UFC)

OTHERS

- Building Research Information Knowledgebase (BRIK)—an interactive portal offering online access to peer-reviewed research projects and case studies in all facets of building, from predesign, design, and construction through occupancy and reuse.

TOOLS

- Information Systems Security Plan

TRAINING COURSES

WBDG10 Seismic Design Basics