A Vulnerability Assessment Methodology for Critical Infrastructure Facilities[1]

George H. Baker III, Ph.D.
James Madison University
Harrisonburg, VA 22807
bakergh@jmu.edu

ABSTRACT

Highly efficient, complex, and interdependent infrastructure systems including electric power, telecommunications, transportation, water utilities, food distribution, housing and shelter, public health, finance and banking are foundations of modern societies. Over the last 3 years, the United States has become acutely aware of the importance of civil infrastructures and their criticality to the nation's economy and quality of life. Our reliance on these systems makes them especially attractive targets for attack. To understand and correct exploitable susceptibilities of critical infrastructure facilities, infrastructure providers and regional planners need a common, repeatable, systematic methodology to understand the comparative risks and vulnerabilities and determine where to invest scarce resources.

This paper proposes and describes a common vulnerability assessment methodology for individual critical infrastructure facilities. It briefly discusses the integration of critical facility results into a regional-scale assessment. The methodology is designed to be comprehensive in terms of accommodating physical and cyber threats against the complete suite of mission-critical systems making up a facility. While the emphasis is on vulnerability assessment, the results provide many of the essential ingredients of a risk assessment. The methodology is applicable for self-assessment by infrastructure service providers or for use by external assessment teams.

INTRODUCTION

In 2003, the Department of Homeland Security issued national strategy documents for the protection of physical and cyber infrastructures that call for vulnerability assessments of critical infrastructure systems.[2,3] Organic to the strategies presented in both documents is the mandate to identify and mitigate system vulnerabilities. As a first step, the strategy document calls on infrastructure service providers to assess the vulnerabilities of their assets.

[1] Effort performed in support of the National Capital Region Critical Infrastructure Vulnerability Assessment Project

[2] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, U.S. Dept of Homeland Security, February 2003.

[3] The National Strategy to Secure Cyberspace, U.S. Dept of Homeland Security, February 2003

This paper outlines a general, repeatable methodology that may be used for such vulnerability assessments. Although the methodology focuses on individual facilities, its results can be used in larger scale regional assessments to rank infrastructure facilities based on their relative resilience, thus providing a basis for priority assignments and resource allocations. The assessment methodology is comprehensive in that it addresses multiple threats, including both physical and cyber, against the complete suite of mission-critical systems comprising a given facility. The methodology is designed to avoid "Achilles' heels."

Metaphorically, if the regional assessment is the Brooklyn Bridge, the present method can be used to assess individual bridge components. The results then provide the basis for a composite (regional) assessment of how the pieces fit together, the locations of weak points, and which pieces are most likely to bring the whole thing down.

The methodology draws on experience the author gained in participating in on-site vulnerability assessments of critical communication facilities during his tenure at the Defense Threat Reduction Agency in addition to local infrastructure assessments performed by the Institute of Infrastructure and Information Assurance at James Madison University. The present methodology focuses on a different problem set, addressing critical private and public sector infrastructure systems and includes guidance on extending the assessment of vulnerability into the assessment of risk. In addition, the methodology is usable by infrastructure service providers themselves as well as "third party" assessment teams. The ability of individual service providers to assess themselves is crucial given the hundreds of thousands of critical infrastructure facilities that need to be assessed.

VULNERABILITY ASSESSMENT IN THE CONTEXT OF RISK ASSESSMENT

Vulnerability assessment is an important subset of the risk assessment process (see figure 1). It can be more prescriptive than risk assessment. Vulnerability assessment involves looking at the system elements and layout and their failure modes based on a given set of threats or "insults." The vulnerability assessment answers the basic question, "what can go wrong should the system be exposed to threats and hazards of concern?" Line managers and technical staff at individual facilities or service provider organizations can perform a vulnerability assessment.

The larger risk assessment process uses the vulnerability assessment results to answer the following additional questions:

(1) Based on the vulnerabilities identified, what is the likelihood that the system will fail?
(2) What are the consequences of such failure (e.g. cost, lives)?
(3) Are these consequences acceptable?

Although risk is often calculated using the likelihood-cost equation, risk assessment ends with the judgment of stakeholders at the executive level of government and private companies. The determination of risk starts with the results of the vulnerability assessment and adds consideration of the likelihood of threats coupled with the economic, political and social consequences of the system failure. The end of the risk assessment process is a decision concerning whether or not to take action based on the acceptability of risks identified.

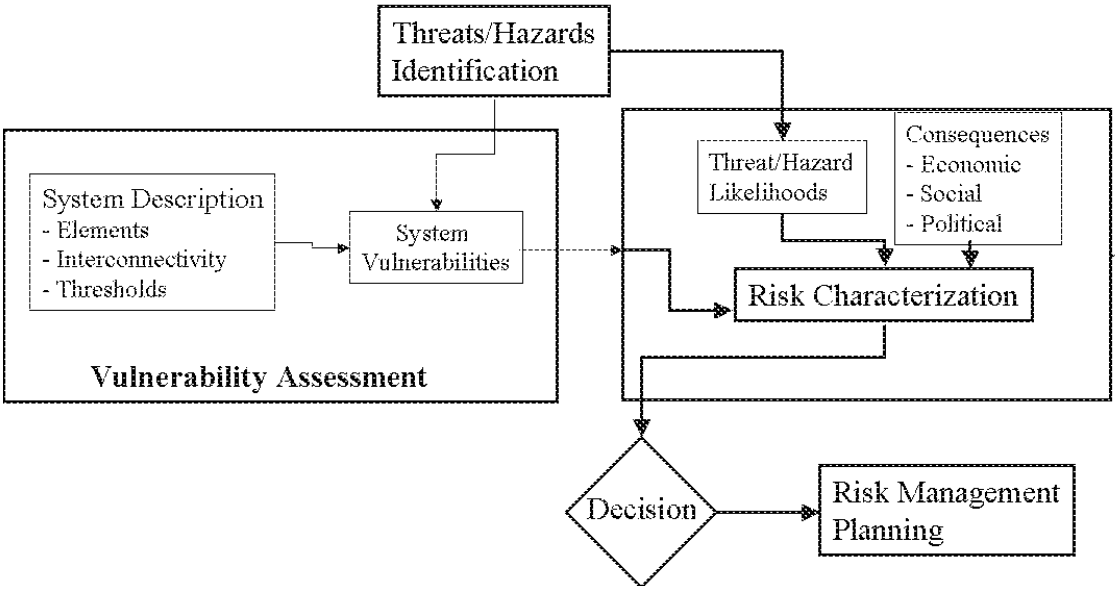


Figure 1. The Risk Assessment Process

THE VULNERABILITY ASSESSMENT PROCESS

The vulnerability assessment methodology has the following objectives:

1. Understand the facility/organization's mission and mission-supporting systems and functions

2. Identify mission-threatening vulnerabilities of critical facility systems

3. Understand system design and operation in order to determine failure modes and likelihoods

4. If possible, identify consequences of system failures in terms of down time, effects on people, and any cascading effects on other systems and organizations. (While failure cost analysis is not an explicit part of a vulnerability assessment, such information may flow from the review of past incidents.)

5. Recommend facility improvements to reduce vulnerability

The vulnerability assessment objectives are achieved by the process outlined below. The order should not be interpreted as strictly consecutive.

1. Threat/Hazard Identification: The vulnerability assessment will be driven by the set of threats and hazards that could affect the facility. Threats refer to malicious insults including both cyber and physical attack or sabotage. Hazards refer to natural disasters or normal accidents that may occur on a random basis. The likelihood and severity of stress should be identified for each type of "insult" deemed worthy of attention. A computer attack might occur on a daily basis (likelihood) and affect 10 computers (severity). Based on similar facilities' experience, arson may occur once every five years (likelihood) and incapacitate the entire facility (severity). Threats and hazards that have occurred in the past should be on the list.

   Local law enforcement and FBI offices can help in identifying activities and hostile organizations that may pose a threat to the infrastructure facility. It is also a useful exercise to consider reasons why your facility might be targeted. Reasons might include unique capabilities, symbolic or high profile operations, controversial operations (animal testing, IRS), high value equipment, systems/equipment that can be used as weapons, and/or a high concentration of experts at the site. A session including managers and employees provides a useful forum for delineating, discussing, and countering possible threats. Employees are very important "intelligence" sources.

   A table of threats and hazards is provided below. Not all threats and hazards listed will pertain to a given facility. For instance, many sites will not be concerned about a nuclear attack since they are not reasonably expected to survive such an event.

Table 1. Threat/Hazard Examples

Threat/Hazard	Typical Elements
	Internal Insults
Accidents	Fire, smoke, HAZMAT contamination, structural failure
Criminal Activity	Arson, personal assault, vandalism
Sabotage/Espionage	Tampering, arson, letter/satchel bombs, data manipulation, theft, malicious insider
	External Insults
Terrorism	Car/truck bob, RPGs, aircraft, incendiaries, duress
Information Warfare (IW)	Viruses, worms, Trojan horses, data alteration
Civil Unrest	Rioting, looting, widespread arson
Natural Disasters/Accidents	Tornados, hurricanes, floods, earthquakes, dam bursts, air crashes
Conventional Weapons	Air drops, missiles, surface-to-surface weapons, air-to-surface weapons, man-portable air defense systems
Weapons of Mass Destruction (WMD)	Nuclear, chemical, radiological, biological

2. <u>Mission Identification</u>: Characterization of the facility starts with the identification of the system mission(s) and the primary functions required to complete the mission(s). As an example, a manufacturing plant mission might be, “to produce and ship a specified number of items per month.” The supporting functions might include an automated production line, the shipping and receiving section, and the computer database and SCADA system required to keep records and control the manufacturing process.

3. <u>Supporting System Identification</u>: Based on the primary functions required to perform the facility’s mission, it is necessary to identify the systems that enable these primary functions. Facilities will have specialized “*mission systems*” such as production lines in a manufacturing plant or operating rooms in hospitals. However, equally important from system operation standpoint are the “*support systems*” common to all facilities such as electric power, telecommunications, water supply, computer networks, supervisory control and data acquisition systems (SCADAs), heating-ventilation-air conditioning (HVAC) systems, and security systems. These “support” systems are often more vulnerable than the mission systems due to lack of attention. A taxonomy of systems within facilities is included in figure 2. These are common to many types of facilities. It is useful to involve experts on the identified mission systems and support systems in the vulnerability assessment.

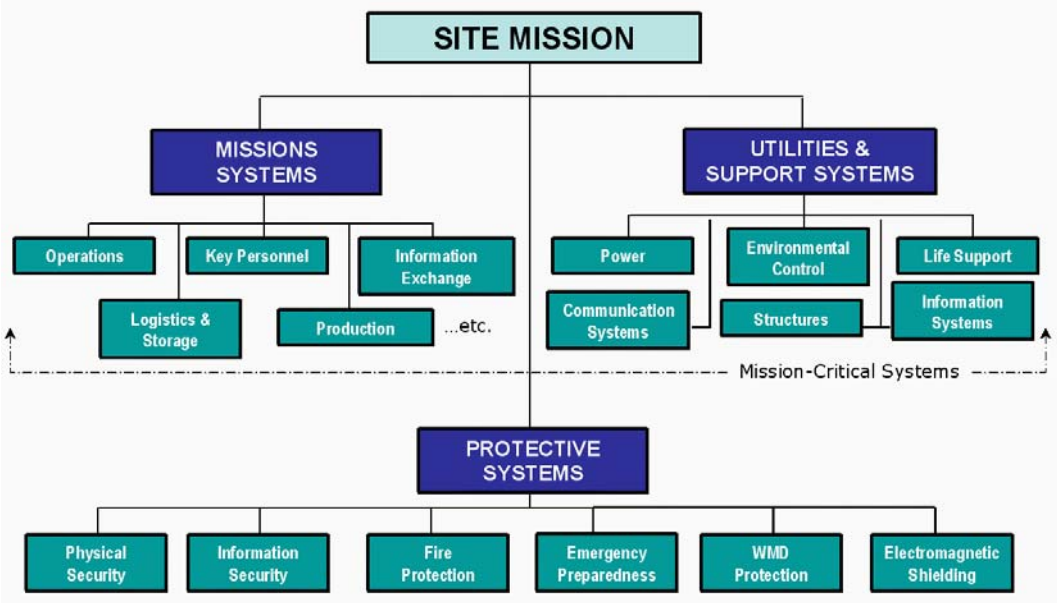


Figure 2. System Taxonomy

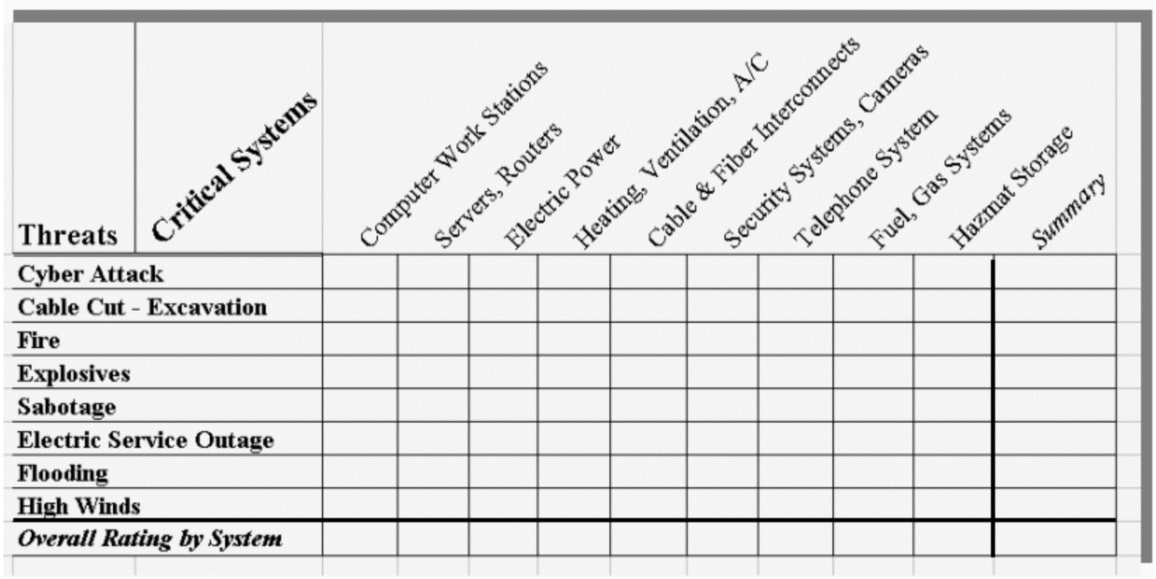
4. Critical System Element Interconnections and Interdependencies: After identifying the systems required to perform the mission, it is important to trace the relationships among critical systems. The result will be a system functional diagram illustrating how the critical systems interconnect. From the system interconnection schematic it is sometimes useful to develop a fault tree representation of the logical dependence of system mission on supporting systems. Understanding system interdependencies enables an evaluation of cascading failures wherein failure of one system can have downstream effects on one or more additional systems. System functional and fault diagrams are the basis for computer analysis of system threat response.[4] An important related consideration is whether critical systems have back-up (or “fail-over”) systems in place, or replacement spares readily available should they fail.

5. System Reconstitution: The physical/logical system interconnections and interdependencies is just one part of the equation. The duration of overall mission outage needs to be evaluated for threats and hazards of concern. This involves understanding time factors associated with individual system vulnerability. Namely, if a system fails, how long will it take to repair or replace it? This time factor includes time delays inherent in failure diagnosis; repair parts requisition, and fix implementation. Repair sequencing is an important factor. For example it is probably necessary to restore electric power before repairing other equipment. The numbers and locations of maintenance personnel have a major effect on reconstitution time. For highly complex systems, resources permitting, it is highly useful to model facility operations including mission and support systems vulnerability, interdependencies and reconstitution times when subjected to threats of concern.[5]

6. Determining Vulnerabilities: The vulnerability assessment process considers threats that have the potential individually or collectively to affect one or more mission critical systems. It is useful to construct a matrix (Figure 3) to correlate threats with systems. Determining which systems will be affected by which threat is obvious in some cases. In other cases it may be necessary to compare the stress levels engendered by the threats/hazards identified with the strengths of exposed system (e.g., blast overpressure stress compared to wall strength). Once a mission critical system is determined to be vulnerable, trace cascading failures by determining if other dependent systems may cease to function as a result of the initial system’s failure.

[4] Modeling is advised for highly complex systems. Commercial software is available for this purpose. James Madison University is developing a Network Security Risk Assessment Model (NSRAM) tool that will be useful for this purpose.

[5] Wolthusen, Stephen D., Modeling Critical Infrastructure Requirements, Proceedings of the 2004 IEEE Workshop on Information Assurance and Security, June 2004.



Critical Systems Threats	Computer Work Stations	Servers, Routers	Electric Power	Heating, Ventilation, A/C	Cable & Fiber Interconnects	Security Systems, Cameras	Telephone System	Fuel, Gas Systems	Hazmat Storage	*Summary*
Cyber Attack										
Cable Cut - Excavation										
Fire										
Explosives										
Sabotage										
Electric Service Outage										
Flooding										
High Winds										
Overall Rating by System										

Figure 3. Threat-System Matrix Example

Single point vulnerabilities are of particular concern. These are places within the facility which collocate more than one critical system or critical system element. Examples are rooms containing main and backup systems, control boards that operate both normal and emergency functions, manholes accessing multiple system cables (communications, electric power) and/or pipes (water, fuel, pressure lines). Every facility will have some of these and they make attractive targets and greatly amplify the effects of otherwise simple accidents. Figure 4 provides examples of common vulnerabilities.

Known vulnerabilities from previous incidents are quite instructional. Past incidents offer lessons not only from the standpoint system vulnerabilities but also real consequences. Consequence data including system down time, costs, other facilities and organizations affected can provide insights into future events of similar and non-similar nature. The following questions are helpful:
(1) what past outages have you experienced and what were their causes? (2) What systems were affected? (3) What types of cascading effects were observed?

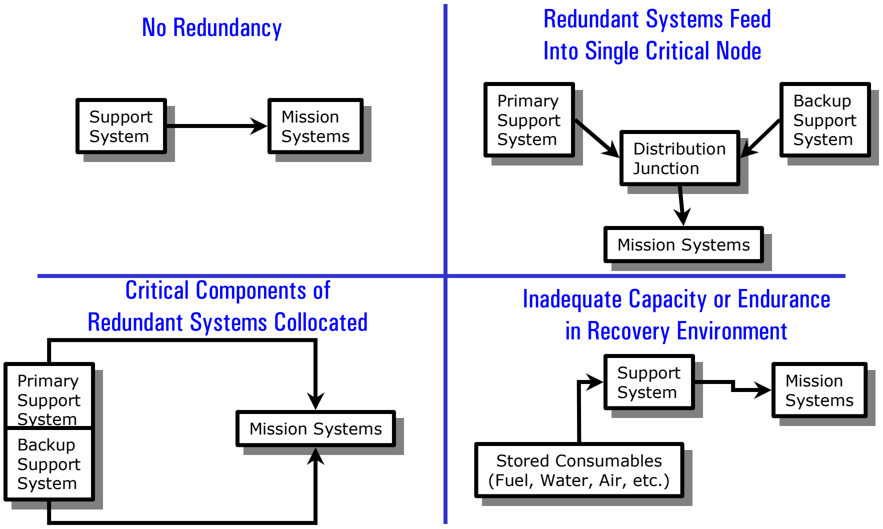


Figure 4. Common Vulnerabilities

7. System Interdependencies. Increasing interdependence among infrastructure service providers intensifies the problem of assuring failure-free operations. Interdependent systems are only as reliable as their least reliable part… risk migrates to the weak links. While it is difficult to know the vulnerabilities of other organizations/facilities both upstream and downstream, it is prudent to consider the effects of outages of both upstream and downstream organizations/facilities. Communication among interdependent organizations can help raise the general robustness of the complex.

   a. Downstream Dependencies. The effects of the debilitation of your facility will cascade to other facilities and organizations. Start by developing a complete list of facilities and organizations dependent on your mission. Understand the extent to which outside organizations depend on your products and services. There are time factors involved here as well. Outages of limited duration may not be noticed. Determine how long it will be before other dependent organizations become aware of your incapacitation. Identify the outage time that will result in dependent organizations becoming unable to perform their missions. Review of past downtime incidents are very instructive in this regard.

   b. Upstream Dependencies. Your facility depends on services from other "*resource*" facilities. Again, it is important to recognize and list these. Identify any single-supplier organizations whose products and/or services are not duplicated by competitors. Consider threats that might affect upstream organizations and try to estimate the duration of their downtime and effects on your operations under possible threat and hazard conditions.

8. Personnel and Responsibilities. A physical plant is useless without its people. Begin by reviewing the complement of people essential to your mission. Determine which mission-critical personnel are needed during normal operations. What are their responsibilities? Then consider how the personnel requirements may change under disaster conditions. Identify functions with no back-up operators. Identify which and how many on-site personnel are trained for repair and work-around procedures in the event of normal and emergency system failures. If you are depending on off-site emergency responders, how far away are they and what is their response time?

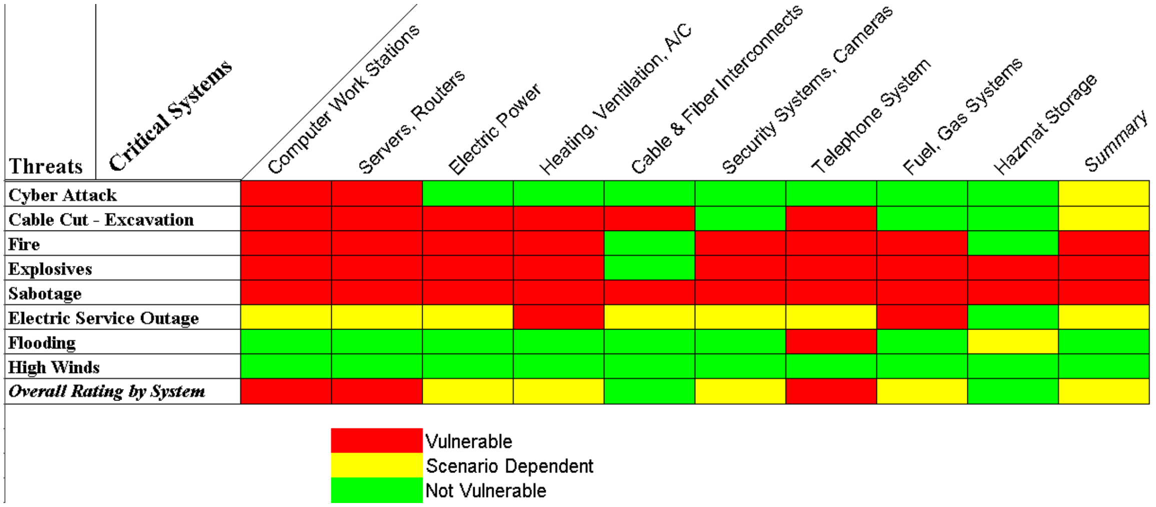
9. Endurability. Endurability is dependent on extant procedures, spares and damage recovery equipment to minimize the effects of and restore operations following accidental, natural or malicious incidents. If they are not in pocket, contingency plans should be developed and kept current that prescribe procedures, protocol, and responsible individuals in the event of a system failures. An important factor is the on-site presence of backup systems and the time required to switch over to these.

10. Planned System Changes. Most facilities are not static. Equipment and configuration changes are a matter of routine and can greatly change the vulnerability status. Take into consideration planned facility upgrades or moves. Also consider major changes in the personnel complement and capabilities. Most facilities replace systems frequently based on maintenance or technology upgrade requirements. An important consideration is the past frequency of system replacement and upgrades.

INFRASTRUCTURE FACILITY VULNERABILITY ASSESSMENT RESULTS

The assessment results provide information on the vulnerability of the facility to threats of concern. It is helpful to provide a written summary of the assessment results for each mission-critical system in the facility. This summary provides a basis for developing an investment strategy to improve system resiliency against identified threats and hazards. The summary also provides a snapshot of system condition as a baseline for future improvements.

The system/threat matrix becomes a useful summary of assessment results. A hypothetical example for a regional telecommunications operations center is provided in figure 5. The matrix is useful for evaluating system behavior when exposed to the various threats. The matrix can also be used as a checklist as system upgrades are completed.



Threats \ Critical Systems	Computer Work Stations	Servers, Routers	Electric Power	Heating, Ventilation, A/C	Cable & Fiber Interconnects	Security Systems, Cameras	Telephone System	Fuel, Gas Systems	Hazmat Storage	Summary
Cyber Attack	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨
Cable Cut - Excavation	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟩	🟩	🟨
Fire	🟥	🟥	🟥	🟥	🟩	🟥	🟥	🟥	🟩	🟥
Explosives	🟥	🟥	🟥	🟥	🟩	🟥	🟥	🟥	🟥	🟥
Sabotage	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Electric Service Outage	🟨	🟨	🟨	🟥	🟨	🟨	🟨	🟥	🟩	🟨
Flooding	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟩	🟨	🟩
High Winds	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Overall Rating by System	🟥	🟥	🟨	🟨	🟩	🟨	🟥	🟨	🟩	🟨

🟥 Vulnerable
🟨 Scenario Dependent
🟩 Not Vulnerable

Figure 5. Example Vulnerability Assessment: Threat-System Matrix Results

The example matrix indicates that for many critical systems the protection is not balanced; i.e., vulnerability is not uniform across all hazards and threats. A good investment strategy would be to provide protection, spares, and/or specific work-around procedures for those systems with unaddressed threat/hazard vulnerabilities. In this example, the most serious threats across the board are fire, explosives and sabotage. For this infrastructure facility, the computer network and telephone system need the most attention.

Common vulnerabilities include unrestricted access to engineering and utility spaces. In many facilities, critical equipment is concentrated in single locations. Excessive fire loads make facilities vulnerable to a match. Most commercial infrastructure facilities have not considered the possibility of bomb attacks in their design or operations. Buildings are designed using industrial standards that don't compensate for catastrophic failure caused by explosions. Most facilities do not monitor for hazardous material leakage or bio-chemical agents. Most facilities do not have stored consumables for operating in a post-attack environment.

Single point vulnerabilities are quite common. In many cases critical systems do not have backup capability. If they do, often the backup systems or components of the backup systems are most often collocated with the primary systems. In many cases, redundant systems feed into a single critical node shared by the primary systems. A typical example is a single electrical distribution panel that controls the flow of commercial power, diesel backup generators, and uninterruptible power supply (UPS) batteries (refer to figure 6). Another common example is a single manhole housing all communications lines leading to and from the facility.

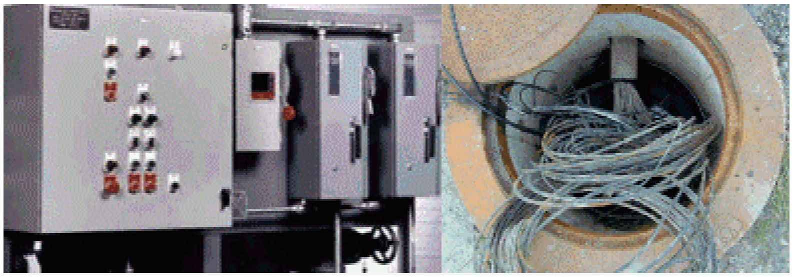


Figure 6. Single Point Failures to Avoid: Commercial/Diesel/UPS in One Electrical Control Panel; Facility Communication Lines Through Single Man Hole

VULNERABILITY MITIGATION

Assessments may identify options for reducing or alleviating vulnerabilities identified. There are two basic approaches to this: equipment upgrades and procedural improvements. Procedural improvements are less costly, and are effective for the majority of identified problems. As one example, simply deleting certain information from your website may reduce terrorist visibility into your operations.

Vulnerability mitigation should involve a careful look at existing protective systems including security procedures and personnel (see figure 2). Consider the facility perimeter and gates and work inward. Look at fencing, inspection and load verification, vehicle barriers, guard posts, lighting, sensors, alarms, parking lots, and communication. Upgrades to access control procedures may be in order. Equipment upgrades might include the addition of security systems such as sensors and access control systems.

As far as mission support systems, equipment upgrades might include firewalls, hardware isolation, and the addition of backup capability for information systems. Electromagnetic shielding could be added for systems subject to electromagnetic interference. Fire protection and suppression systems can be added including fire barricades, smoke detectors, alarms, hose stations, and automatic sprinklers. Care should be taken to position overhead sprinklers so that critical electronic systems are not in the direct path.

A useful, generally applicable procedural improvement is to achieve threat and hazard awareness by instituting regular contact between facility security staff and local law enforcement authorities and the FBI. Development and practice of contingency plans including training and exercises for emergency responders and technical staff is highly beneficial. Reduction of fire load and hazardous materials (hazmat) inventories will greatly reduce consequences of accidents or malicious activity. Configuration control of facilities and networks is often neglected and enables prevention of system failures and diagnosing any problems that do occur. Identification of security-critical items and processes in the facility fosters awareness. Implementation of a follow-on audit of facility security/vulnerability status on a regular basis enables both the identification of any degradation and maintenance of critical systems and procedures. In all cases, security training and exercises are important procedural measures.

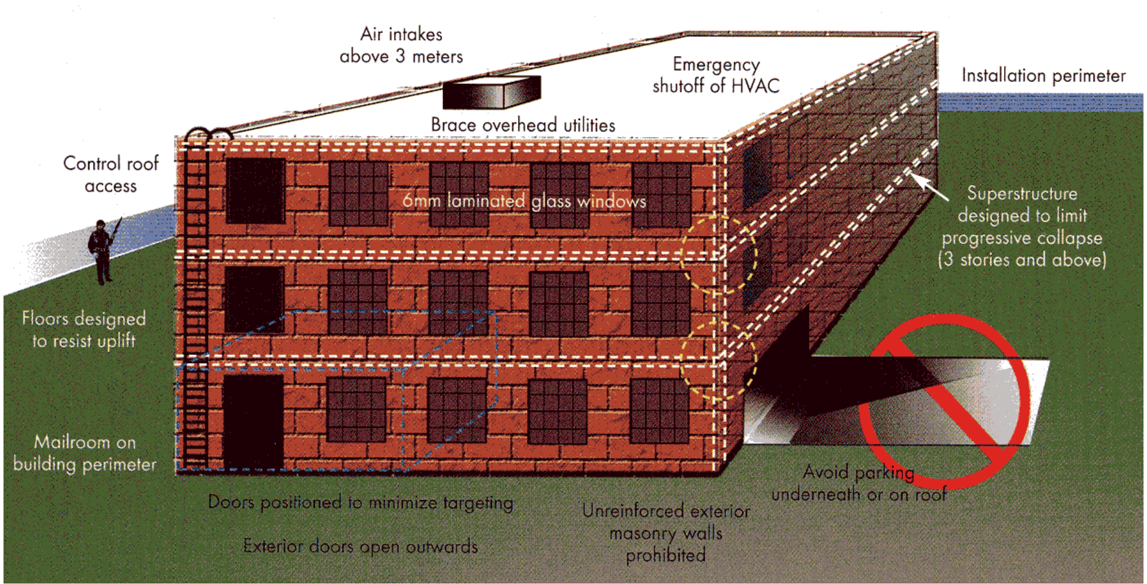

Air intakes above 3 meters
Emergency shutoff of HVAC
Installation perimeter
Brace overhead utilities
Control roof access
6mm laminated glass windows
Superstructure designed to limit progressive collapse (3 stories and above)
Floors designed to resist uplift
Mailroom on building perimeter
Avoid parking underneath or on roof
Doors positioned to minimize targeting
Unreinforced exterior masonry walls prohibited
Exterior doors open outwards

Figure 7. Desired Facility Structural Features[6]

USE OF INDIVIDUAL FACILITY RESULTS IN REGIONAL ASSESSMENTS

The methodology outlined above can be used as a common, repeatable methodology for most critical infrastructure facilities. Much commonality exists with respect to support systems in all facilities, i.e., most facilities have electric power, heating, ventilation, air conditioning, water, and communications systems. Each infrastructure sector facilities will have some unique mission systems that will need special evaluation. But facility support systems are ubiquitous and will have many common vulnerabilities.

The facility-level methodology is the "basis-function" for the more important, larger scale, regional assessments. The objective of regional assessments is to identify impediments on the ability to provide critical services. It is straightforward to identify these services by sector. It is then necessary to determine the facilities necessary to these services and their interdependencies. By collecting information on each facility's *resource* facilities and *dependent* facilities, it is possible to develop a functional diagram of regional interdependencies. A notional schema for integrating individual facility assessments into a regional assessment is depicted in figure 8. Conceptually, in this schema the system interdependencies flow in one direction (horizontal in this illustration)

[6] Protecting People at Risk, Special Issue, Advanced Materials and Processes Technology Information Analysis Center Quarterly, Volume 6, Number 4, Rome NY

and the threat/system effects information in the other orthogonal direction (vertical).

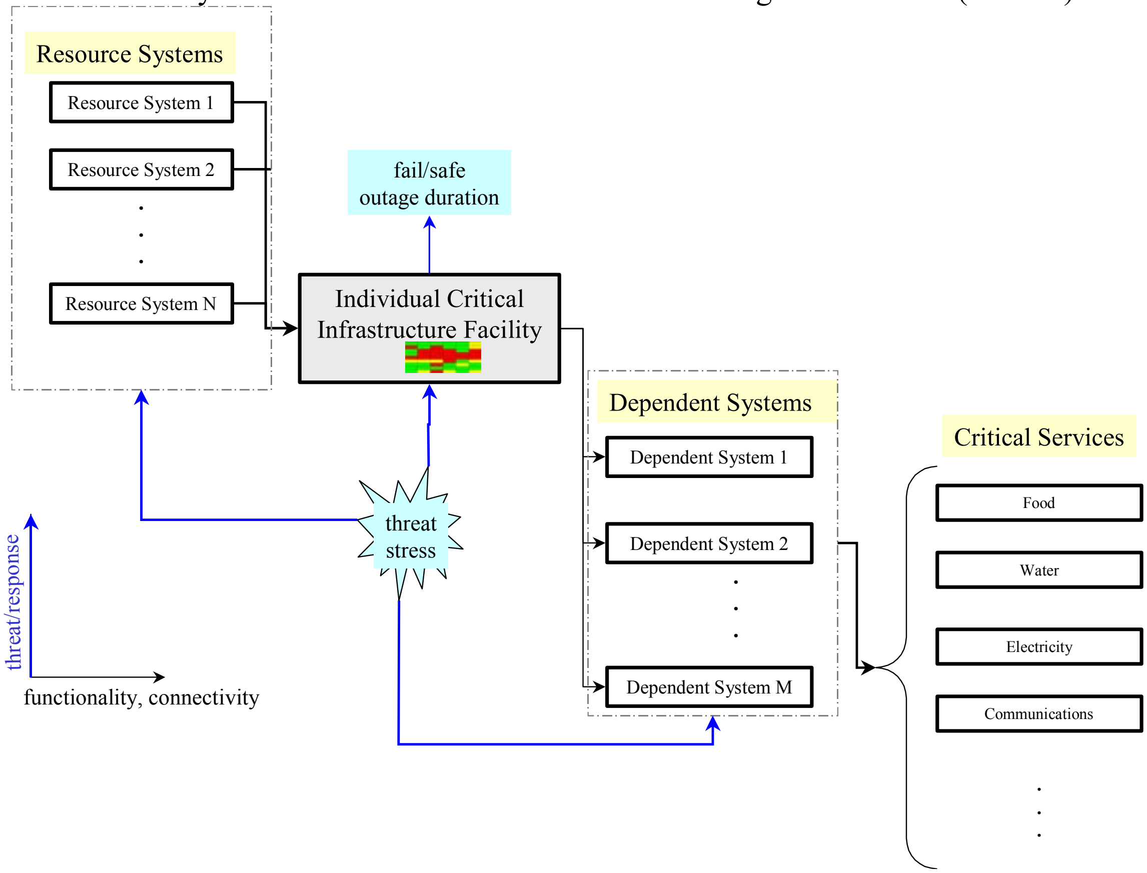


Figure 8. Regional Assessment Schema

Once individual facility vulnerabilities are known, it is possible to understand the composite effect on the ability to provide critical services as shown. It is instructive to look at the problem both from a "service-to-resource" approach (right to left on the schema) and a "resource-to-service" approach (left to right). The first approach gives an appreciation for the top-tier facilities necessary for regional function. The second is helpful in identifying sole-source suppliers of services and commodities necessary for infrastructure operation.

Using this schema, it is possible to evaluate, the weak-link facilities that impede the delivery of critical services. This, of course, can vary somewhat depending on the threat scenario. The schema shows a single channel diagram that might pertain to one infrastructure sector. One approach is to develop a single diagram for each sector before combining them into the complete regional composite. This exercise will very quickly reveal the infrastructure sectors and individual facilities that pose the highest risks and enable regional planners to prioritize resources for remediation.

SUMMARY

This paper describes a vulnerability assessment methodology for individual critical infrastructure facilities and briefly discusses the integration of critical facility results into a regional-scale assessment. The methodology is designed to be comprehensive in terms of accommodating physical and cyber threats against the complete suite of mission-critical systems making up a facility. While the emphasis is on vulnerability assessment, the results provide many of the essential ingredients of an overall risk assessment. The methodology is applicable for self-assessment by infrastructure service providers or for use by external assessment teams.

The methodology incorporates a matrix to identify the most problematic system-threat combinations for individual facilities. A taxonomy of systems within a facility is developed that divides systems into *mission*, support, and *protective* systems. Application of a "common" methodology is aided by the presence of similar *support* systems in most facilities including electric power, telecommunications, computer, water, heating, ventilation, and air conditioning systems. In the author's experience, common systematic vulnerabilities exist in many facilities that are easily identified. Furthermore, similar "single point failure" mechanisms exist in most facilities.

The methodology can be used as the "basis function" for regional assessments to determine weak-link impediments in the ability to provide critical services. The paper provides a schema for integrating facility assessments into a regional composite. The methodology enables regional planners to compare the strength/vulnerability status of multiple infrastructures to develop priorities for planning remediation investment.

Bio: George Baker is a member of the faculty at James Madison University and serves as Associate Director of JMU's Institute for Infrastructure and Information Assurance. He consults with industry and government in the areas of critical infrastructure assurance, high power electromagnetics, nuclear and directed energy effects. He is the former director (1996-99) of the Defense Threat Reduction Agency's Springfield Research Facility, involved in assessing and protecting critical underground, infrastructure and mobile systems. Much of his career was spent at the Defense Nuclear Agency directing RDT&E related to hardening systems to nuclear effects. He is a member of the National Committee of the American Electromagnetic (AMEREM) conference. He chaired the Nonproliferation and Arms Control Technology Working Group (NPAC) focus group on underground facilities and the Underground Site Infrastructure Applications Working Group. He also chaired the international Technical Cooperation Program EMP Group and recently served as an invited member of the Congressional EMP Commission staff. He is a member of IEEE and an EMP Fellow. He holds a Ph.D. from the U.S. Air Force Institute of Technology.