International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

Vulnerability Assessment Methodology on Critical Infrastructure Facilities

TIMMIRI M NIKITHA[1] & Mrs. M.SRIDEVI[2]

[1]M-Tech Dept of CSE Laqshya Institute of Technology and Science, Khammam.

Mail id: nikithat11@gmail.com

[2]Asst. Professor & HOD, Dept of CSE in Laqshya Institute of Technology and Science, Khammam. Mail Id: - sreetech99@gmail.com

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 nationOs 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.

Keywords: Vulnerability, Assessment Methodology, Critical Infrastructure Facilities.

1. 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.

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 [1]. 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 [AchillesO 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.

2. Related Work

2.1 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

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

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.

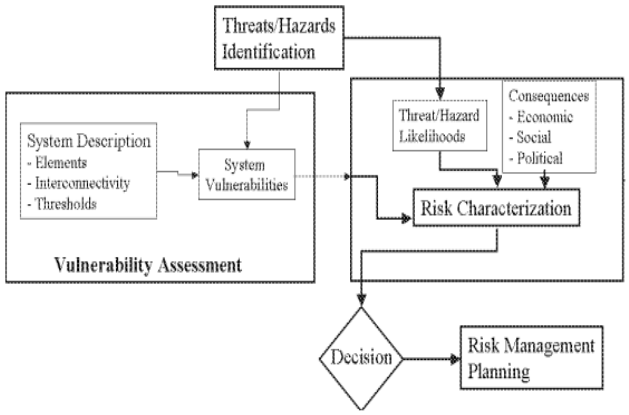


Figure 1. The Risk Assessment Process

3. Implementation

3.1 THE VULNERABILITY ASSESSMENT PROCESS:

The vulnerability assessment methodology has the following objectives:

1. Understand the facility/organizations 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. Mission Identification: Characterization of the facility starts with the identification of the system mission(s) and the primary functions required completing 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. Supporting System Identification: 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

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

mission systems due to lack of attention. 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.

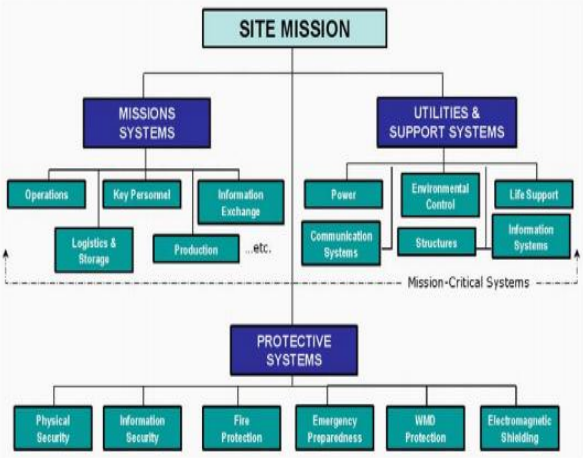


Figure 2. System Taxonomy.

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

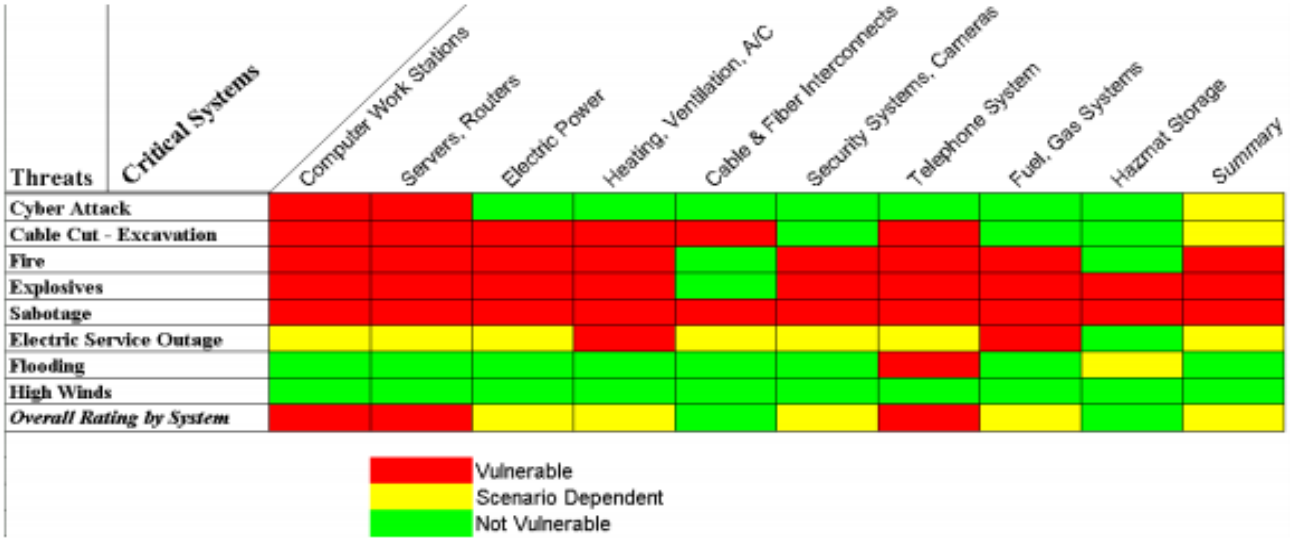
International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

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 systems failure.

4. Experimental Work

4.1 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.



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 donor 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.

5. Conclusion

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. 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.

6. References

[1] Olivarez-Miranda, E., Candia-Velar, A., Carrizozo, E., & Pérez-Galarce, F. (2014). Vulnerability Assessment of Spatial Networks: Models and Solutions. In Combinatorial Optimization (pp. 433-444). Springer International Publishing. DOI: 10.1007/978-3-319-09174-7_37

[2] Handbook of International Electrical Safety Practices

[3] US Department of Energy. (2002). Vulnerability Assessment Methodology, Electric Power Infrastructure. [1]

[4] ^ Jump up to: a b Turner, B. L.; Kasperson, R. E.; Matson, P. A.; McCarthy, J. J.; Corell, R. W.; Christensen, L.; Eckley, N.; Kasperson, J. X.; Luers, A.; Martello, M. L.; Polsky, C.; Pulsipher, A.; Schiller, A. (5 June 2003). "Science and Technology for Sustainable Development Special Feature: A framework for vulnerability analysis in sustainability science". Proceedings of the National Academy of Sciences. 100 (14): 8074–8079. doi:10.1073/pnas.1231335100.

[5] Jump up ^ Ford, James D.; Barry Smit (Dec 2004). "A Framework for Assessing the Vulnerability of Communities in the Canadian Arctic to Risks Associated with Climate Change". Arctic. 57 (4): 389–400. doi:10.14430/arctic516.

[6] Jump up ^ Adger, W. Neil (August 2006). "Vulnerability". Global Environmental Change. 16 (3): 268–281. doi:10.1016/j.gloenvcha.2006.02.006.

[7] Jump up ^ Fraser, Evan D. G. (August 2008). "Travelling in antique lands: using past famines to develop an adaptability/resilience framework to identify food systems vulnerable

to climate change". Climatic Change. 83 (4): 495–514. doi:10.1007/s10584-007-9240-9.

[8] Jump up ^ Patt, Anthony; Dagmar Schröter, Richard Klein, Anne Cristina de la, Vega-Leinert (2010). Assessing vulnerability to global environmental change : making research useful for adaptation decision making and policy (Paperback ed. 1. publ. ed.). London: Earthscan. ISBN 9781849711548. Cite uses deprecated parameter |coauthors= (help)

Authors Profile

TIMMIRI M NIKITHA

B-Tech in Laqshya Institute of Technology And Science, Khammam, M-Tech Computer Science and Engineering **College:** Laqshya Institute of Technology and Science, Khammam,

Mail id: nikithat11@gmail.com

Phone number: 9550379199

M.SRI DEVI

Working as Asst. Professor and HOD, Department of CSE in Laqshya Institute of Technology and Sciences since 2008 July to till date. Working as IEEE student branch councellor, Deputy Representative for ISO certification work.

Email id: - sridevi279.gunti@gmail.com