

PAPER • OPEN ACCESS

Assessment and Design of Critical Infrastructures against Intentional Attacks Based on Degraded States Vulnerability Methodology

To cite this article: Hao Geng *et al* 2019 *IOP Conf. Ser.: Earth Environ. Sci.* **295** 032039

View the [article online](#) for updates and enhancements.



IOP | ebooks™

Bringing you innovative digital publishing with leading voices to create your essential collection of books in STEM research.

Start exploring the **collection** - download the first chapter of every title for free.

Assessment and Design of Critical Infrastructures against Intentional Attacks Based on Degraded States Vulnerability Methodology

Hao Geng¹, Hao Lu^{1,a}, Mu Huang¹ and Shanzheng Sun¹

¹State Key Laboratory of Disaster Prevention and Mitigation of Explosion and Impact, Army Engineering University of PLA, 210007 Nanjing Jiangsu Province, China

^aCorresponding author: lh829829@163.com

Abstract. A crucial issue in today's counterterrorism environment is how to assess critical infrastructure damage and develop a more appropriate design rapidly against intentional attacks, since it has become unacceptable to ignore the high impact of disruptions caused by these attacks. Degraded states vulnerability methodology (DSVM) is used to explore the vulnerability analysis and design method of critical infrastructures. After the terrorist attack, the damage status of the components at all levels of the target is quickly determined, and the probability of component level damage is simulated. Using this method to judge the functional damage condition and improve the planning and design under multi-hit. Respond quickly to the damage effect of each hit, and put forward multi-hit's degraded states transition tables and state-effect tables. It provides the basis for rapid assessment, planning and design of critical infrastructure in modern local wars where terrorists are more intensive and frequent.

1. Introduction

Critical infrastructures are vital to maintaining the national or regional economic lifeblood. They occupy an important position in the national economy. It mainly includes: urban lifeline projects, important industrial and mining enterprises, scientific research bases, energy bases, transportation hubs, communication hubs, Bridges, reservoirs, warehouses, power stations, etc.

Many governments have identified critical infrastructures that are, by default, potential targets of terrorist attacks.[1] Today, with the growing power of terror, critical infrastructures' vulnerability analysis and design options are more important. If you want to optimize the design of critical infrastructure under intentional attacks, the extent of damage must be assessed before the planning strategy is designed more accurate. So a crucial issue is how to quickly assess the damage state of target.

There are many mature literatures on facility design and damage assessment with probabilistic failure of components. To some extent, these methods that are adopted to analyze and evaluate infrastructures have solved the demonstration of damage assessment after intentional attack. However, due to the complexity of infrastructures' structure and functions, the analysis and evaluation of our infrastructures are still difficult and complex.

Degraded states vulnerability methodology is used in this paper to research critical infrastructures' evaluation and vulnerability analysis. As an important method of weapon equipment analysis, it plays an important role in the vulnerability analysis of missiles, tanks, aircraft carriers and other large-scale weaponry. The main advantage of this method is that it has distinct layers, and the state of various parts



inside the facility can be understood more intuitively. In the case of clear damage status, relevant design and planning are quickly developed and implemented, such as consulting superiors, engineering repair, personnel dispatch and transfer.

2. Degraded states vulnerability methodology

In recent years, equipment research institutions of various countries have carried out researches on the improvement of vulnerability analysis methods and measurement indexes of weapon equipment. In 1988, degraded states vulnerability methodology (DSVM), which was mainly characterized by classification of target functional damage, was proposed by the Ballistic search Laboratory (BRL) in the United States.[2-3] As time goes by, DSVM has become one of the most important methods of component level vulnerability analysis.

There are many mature literatures in the field of weapons and equipment research by using DSVM. In the pioneering work, the author of [4] started from the overall architecture of DSVM and studied its implementation. Starting from the research overview of damage efficiency evaluation, Huang[5] used DSVM and damage tree method in the engineering mapping process of component failure state for typical targets. Kang[6] analyzed the breaking effect of the ballistic missile against the aircraft carrier system by analyzing the carrier catapult and introducing the DSVM.

The above research results describe in detail the process and steps of DSVM acting on various weapon systems, but they do not take into account the reduction calculation of the state after the target is hit again. In this paper, the degraded states process is introduced, the subsystem transition table and subsystem state-effect table are established, and the DSVM implementation result of tactical strategy transformation is established for degraded states value, so as to improve the damage evaluation process and result of the target.

3. Degraded states modeling

3.1. Defining degraded states

Defining DS value, namely degraded states state value of function damage, is the key step of applying DSVM to evaluate the vulnerability effectiveness of critical infrastructure. The DS value is defined according to the task of each subsystem, which can represent the functional damage of each subsystem after the attack in detail, and reflect the functional damage state of the whole system through the combination of some DS value.

First, according to the principle of mission-related, the target facility is divided into several functional systems, each of which has the ability to independently complete a specific task. In this paper, civil airport which is one type of important transportation hubs is used to illustrate as an example. Table 1 shows the classification of civil airports according to critical infrastructure functions.

Let us divide each subsystem DS values for several basic state values, with subsystem rear facilities $G_i (i = 0, 1, 2, \dots, k)$ as an example. G is the subsystem capability name code, the variable i is DS form of any kind of functional damage, and k is the total number of the basic functional damage forms of the subsystem capability. The initial damage state is defined as G_0 , indicating that the system is not damaged.

In each subsystem, in addition to the individually defined DS values, there are also possible DS combinations among them. Therefore, not only can a set of detailed functional damage levels be established by defining DS values, but there is only one corresponding DS value in each subsystem when the target suffers any degree of functional damage. It indicates that all possible damage states after intentional attack can be described by the corresponding DS combination in the subsystem, such as $F_3 G_2 C_3 M_1 P_0$, etc. Table 2 is the DS definition of civil airport.

Table 1. Infrastructure function classification of civil airports.

Subsystem	Capability name code
Flight	F

Ground Service	G
Command	C
Communication	M
Passenger Service	p

3.2 Constructing subsystem damage trees

Subsystem damage tree contains the DS combination logic relation of each subsystem of critical infrastructure. Using the deductive method, the damage of subsystem is regarded as the highest level event, and the damage of sub-facilities is regarded as the basic event. From top to bottom, damage tree is constructed according to certain logical relation.

In the construction of damage tree, first of all, the structure and functional characteristics of critical infrastructure should be analyzed. The internal structure and completion tasks of each type of critical infrastructure are different. Some functional subfacilities of the airport system are numbered in the form of X_j ($j = 1, 2, \dots, m$) as shown in table 3.

Table 2. DS definition of civil airports.

Subsystem Flight	Subsystem Command	Subsystem Passenger Service
F_0 No flight damage F_1 Aircraft damage F_2 Flight crews damage F_3 F_1 and F_2	C_0 No Command damage C_1 Command equipment damage C_2 Command building damage C_3 Command casualties C_4 C_1 and C_2 C_5 C_1 and C_3 C_6 C_2 and C_3 C_7 C_1 and C_2 and C_3	P_0 No passenger service damage P_1 Service casualties P_2 Airport terminal damage P_3 Passengers casualties P_4 Service equipment damage P_5 P_1 and P_2 P_6 P_1 and P_3 P_7 P_1 and P_4 P_8 P_2 and P_3 P_9 P_2 and P_4 P_{10} P_3 and P_4 P_{11} P_1 and P_2 and P_3 P_{12} P_1 and P_2 and P_4 P_{13} P_1 and P_3 and P_4 P_{14} P_2 and P_3 and P_4 P_{15} P_1 and P_2 and P_3 and P_4
Subsystem Ground Service	Subsystem Communication	
G_0 No Ground service damage G_1 Landing function damage G_2 Maintenance function damage G_3 Air supplies damage G_4 G_1 and G_2 G_5 G_1 and G_3 G_6 G_2 and G_3 G_7 G_1 and G_2 and G_3	M_0 No communication damage M_1 Communication equipment damage M_2 Communication building damage M_3 M_1 and M_2	

Table 3. Partial list of key subfacilities.

Number	Key functional subfacilities	Number	Key functional subfacilities
X_1	aircraft	X_8	landing equipment
X_2	runway	X_9	control tower
X_3	taxiway	X_{10}	navigation station
X_4	apron	X_{11}	hangar
X_5	oil depot	X_{12}	airport terminal

X_6	air supplies depot	X_{13}	flight crews
X_7	repair station	X_{14}	maintenance staff

The connection between basic events and intermediate events includes two cases, logical "and" and logical "or". The logical "and" operation indicates that all subordinate events must occur before the corresponding superior events can happen. The logical "or" operation means that whenever one or more of the subordinate events occur, the corresponding superior events will occur. If there is a damage path from the basic event to the top event in damage tree, the subsystem has a functional damage event under this terrorist attack.

The damage tree building the "Landing function damage (G_1)" event is shown in figure 1. Where $M_i (i = 1, 2)$ is the intermediate events, M_1 is the entire runway damage and M_2 is the entire aircraft parking facility damage. In the figure, the symbol "+" is the logical "or" operation, and the symbol "•" is the logical "and" operation.

The calculation of G_1 is as follows:

$$G_1 = M_1 + M_2 + X_8 = X_2 + X_3 + X_4 X_{11} + X_8$$

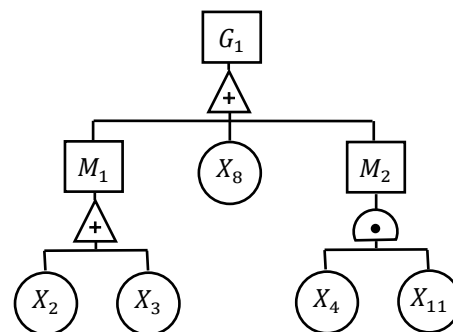


Figure 1. The damage tree of "Landing function damage (G_1)".

3.3 CDS vector simulation and damage probability analysis

The state of the DS damage tree is determined by the Boolean calculation. In general, component damage states (CDS) are defined as 0, 1 and [0, 1]. when the CDS value is equal to 0, it means that the subsystem completely loses its original function; when it is equal to 1, it means that the subsystem maintains its original function; and when it is between [0, 1], it is applicable to some functional structures or facilities that do not obey Bernoulli distribution law. The Boolean logic operation relationships for CDS are listed in table 4.

Table 4. Boolean logical operation relation for CDS values.

logical "and" operation			logical "or" operation		
CDS value 1	CDS value 2	Final CDS value	CDS value 1	CDS value 2	Final CDS value
0	0	0	0	0	0
0	1	0	0	1	1
1	0	0	1	0	1
1	1	1	1	1	1

[0,1]	0	0	[0,1]	0	[0,1]
0	[0,1]	0	0	[0,1]	[0,1]
[0,1]	1	[0,1]	[0,1]	1	1
1	[0,1]	[0,1]	1	[0,1]	1
[0,1]	[0,1]	[0,1]	[0,1]	[0,1]	[0,1]

Damage tree and CDS vector distribution are used as tools by degraded states vulnerability methodology, and the CDS vector is determined by Monte Carlo simulation. The CDS vector is described as follows:

$$S_{CD} = (S_{CD1}, S_{CD2}, \dots, S_{CDn}) \quad (1)$$

Where S_{CD} is a n-dimensional CDS vector. S_{CDi} is the CDS value of the subfacility. The CDS vector is input into the damage tree of each subsystem for logical calculation, and then the degraded states of this critical infrastructure can be evaluated.

For example, the degraded states that may appear in a civil airport can be given as follows:

$$DS_i = (F_{i=0\sim3} G_{i=0\sim7} C_{i=0\sim7} M_{i=0\sim3} P_{i=0\sim15}) \quad (2)$$

A large number of Monte Carlo simulations can be used to determine the DS value of critical infrastructure each time. When the simulation times are large enough, the approximate probability value of each DS_i can be obtained based on statistics, we have: right-hand side.

$$P(DS_i) \approx \frac{k_i}{n} \quad (3)$$

Where k_i is the number of occurrence of a certain DS_i value during Monte Carlo simulation.

4. Planning and design for critical Infrastructures suffering multiple attack

4.1. DS conversion after multi-hit

This section is used to discuss the assessment process of functional impairment after multi-hit. After the target is subjected to multiple terrorist attacks, the superposition effect of damage caused by the next attack is evaluated, and the improvement plan is designed in advance, so as to win the opportunity in preventing hidden dangers and tactical games. In addition, this process can also be applied to the rapid planning of engineering damage status after the target is re-attacked, to carry out a quick survey of the site, to find new damage subsystems and the superposition operation of pre-subsystem states, to conduct a rapid damage evaluation of the project, and to improve efficiency and win design time.

The state of the critical infrastructure is described by the state values of each subsystems. In the previous example, DS combination in the undamaged state of civil airport is described as:

$$F_0 G_0 C_0 M_0 P_0$$

The undamaged state of each subsystem is 0. After hitting the target, the airport subsystem may reach the following damaged state:

$$F_1 G_4 C_4 M_0 P_2$$

When assessing subsequent attack damage to the critical infrastructure, each subsystem value of the previsual DS as drawn from the distribution is compared to its previous value. Four types of situations may occur as follows:

- If the new subsystem state is more severe than the previous subsystem state, more specifically, the particular capabilities of the subsystem is degraded, the subsystem value will assign the drawn value.

- If the new subsystem state is less severe than the previous subsystem state, more specifically, the particular capabilities of the subsystem has not been degraded, the subsystem value will remain unchanged.

- If the new subsystem state has a different damage type from the previous subsystem state, the new subsystem value is defined as a combination of two damage categories.

- If the new subsystem state is a combination of different damage types, compare it with the previous subsystem state and select the more severe state as the new subsystem value.

For example, a supposed civil airport has the following degraded state:

$$F_1 G_2 C_4 M_0 P_7$$

Next, the target is attacked, and the simulated random DS is:

$$F_2 G_2 C_0 M_2 P_4$$

The damage of subsystem command and subsystem passenger service is not serious compared with the initial state, so the new DS value is still $C_4 P_7$. There is new degraded states in the subsystem flight and subsystem communication, so the new DS value is $F_3 M_2$ after stacking. The target's new degraded state is thus:

$$F_3 G_4 C_0 M_2 P_7$$

In order to realize this process more quickly in damage assessment, a degraded states transition table is introduced. Given a target's current substate (subsystem state value). Then another vulnerability simulation was performed on the target to generate drawn degraded substate. The two are superimposed and expressed in the degraded states transition table. Thus, we can describe the function

$$\text{New Substate} = F(\text{Current Substate}, \text{Drawn Substate}) \quad (4)$$

Table 5 shows the Transition Table for Subsystem Command.

Table 5. Subsystem transition table for command.

Drawn substate	Current substate							
	C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7
C_0	0	1	2	3	4	5	6	7
C_1	1	1	4	5	4	5	7	7
C_2	2	4	2	6	4	7	6	7
C_3	3	5	6	3	7	5	6	7
C_4	4	4	4	7	4	7	7	7
C_5	5	5	7	5	7	5	7	7
C_6	6	7	6	6	7	7	6	7
C_7	7	7	7	7	7	7	7	7

4.2. Critical infrastructure design and planning for substate value

Previously, the process of calculating the target substate value under multiple strikes is analyzed, and the subsequent design and planning of the target is discussed by using the results.

When substate values change, the impact of functional failures should be taken into account in the planning and design of critical infrastructure. Based on the actual situation of the project and the specific conditions such as the geographical location and value realization of the important infrastructure, the designer shall make appropriate and reasonable arrangements according to local conditions, rely on the existing design scheme and establish the planning and design plan database comprehensively.

The state-effect table determines how to change the design scheme after the degraded states of the target under attack. Through this table, corresponding effect-flag between the old and new states of the target can be found. Each effect-flag represents the execution of a specific set of planning schemes. By comparing the effect-flags of the previous substates and the new substates, it can be determined whether the planning scheme needs to be changed. If the new substate effect flag is included in the previous substate effect flag, the preset planning scheme does not need to be changed. If the new substate effect flag is different from the previous one, the degraded states planning transition is performed. Thus, we have

$$\text{State Effect} = F(\text{Old Substate}, \text{Flag Type}) \quad (5)$$

Table 6 is flight subsystem's state-effect table of civil airport, and table 7 is flag type of flight subsystem.

Table 6. Flight state-effect table.

Flag type	Current substate			
	F_0	F_1	F_2	F_3
f_1	0	1	0	1
f_2	0	0	1	1

Table 7. Flight flag types.

Flag type	Flight substate
	F_0 - No flight damage
f_1	F_1 - Aircraft damage
f_2	F_2 - Flight crews damage
f_1, f_2	F_3 - F_1 and F_2

When the state changes, the degraded state transition function gives a new substate value, and then the state-effect table is called to change and optimize the design scheme. For example, we assume that the target's initial flight substate value is F_1 . After the simulated restrike process, the new substate value is F_3 . Each type should be checked with the old subsystem state and the new subsystem state. For flight subsystem, there are two flag types, which are calculated as follows:

$$\begin{aligned} F(F_1, f_1) &= \text{TRUE} & F(F_3, f_1) &= \text{TRUE} \\ F(F_1, f_2) &= \text{FALSE} & F(F_3, f_2) &= \text{TRUE} \end{aligned}$$

Only for flag f_2 do we have the (*FALSE*, *TRUE*) combination to signify that the the preset planning scheme changes for flag f_2 take place. Therefore, when the flight substate value changes from F_1 to F_3 , the flag f_2 needs to be referred to, which represents the planning scheme guides relevant personnel to carry out the next planning and design.

5. Conclusion

By applying the degraded states vulnerability methodology (DSVM) to the damage assessment and planning design of critical infrastructure, the target damage status can be judged quickly, and the component-level damage probability of infrastructure can be simulated, so as to realize the rapid planning and design of engineering. The Monte Carlo simulation method based on degraded states vulnerability methodology not only improves the accuracy of vulnerability simulation, but also

significantly improves the application value of simulation results. In the simulation process, the hierarchical modularization step of the method is also beneficial to the realization of object-oriented programming.

At the same time, this method can be used to judge the functional damage status in multiple attacks, and to respond quickly to the damage effect of each intentional attack, and to propose the transformation of the design scheme, so as to gain the fast response time to the greatest extent.

References

- [1] N. Bricha, M. Nourelfath. Reliability Engineering & System Safety. **119**, 1-10 (2013)
- [2] J.M. Abell, M.D. Burdeshaw, B.A. Richter. BRL-TR, **3161** (1990)
- [3] G.R. Comstock. AMSAA-TR, **495** (1991)
- [4] H. Wang, X. Lu, S. Feng. Transactions of Beijing Institute of Technology. **22(2)**, 214-216 (2002)
- [5] H. Huang, Z. Wang. Journal of Astronautics. **30(03)**, 827-836 (2009)
- [6] P. Kang, M. Bi, L. Zhai. Journal of Ordnance Equipment Engineering. **34(01)**, 53-57 (2013)