CHEMICAL ENGINEERING TRANSACTIONS
VOL. 26, 2012
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at: www.aidic.it/cet
Guest Editors: Valerio Cozzani, Eddy De Rademaeker

ISBN 978-88-95608-17-4; **ISSN** 1974-9791
DOI: 10.3303/CET1226052

A Framework for Ranking the Attack Susceptibility of Components of Critical Infrastructures

Enrico Zio*[a], Roberta Piccinelli[b], Giovanni Sansavini[b]

[a] Chair on Systems Science and the Energetic challenge, European Foundation for New Energy-Electricite' de France Ecole Centrale Paris and Supelec, Grande Voie des Vignes, F92-295, Chatenay Malabry Cedex
[b]Politecnico di Milano, Energy Department, Nuclear Section, c/o Cesnef, via Ponzio 33/A , 20133, Milan, Italy
enrico.zio@ecp.fr

Outages or destruction of Critical Infrastructures (CIs) cause disruption of fundamental services for Society's well being and result in diverse consequences with economical and social implications. An analysis of all the occurrences that can cause such undesired events is necessary. This calls for an *all-hazard approach* capable of dealing with diverse events and conditions such as deterioration and failures, natural disasters, accidents and malevolent acts. In this paper, an *All-HAZard ANalysis* (A-HAZAN) framework is proposed. Starting from the identification of the task of each component in the infrastructure, we use a Table to organize the information on the susceptibility to attacks, and to single and cascading failures. We qualitatively assess the susceptibility to attacks as a function of size, level of demand, level of protection and social criticality. Then, we give a methodology to rank the components with respect to their susceptibility to attacks. The systematic process of analysis is here presented by way of its application to a case study of literature.

1. Introduction

Systems providing energy (electricity, oil & gas supply), transportation (rail, road, air, sea), information and telecommunication (e.g. the internet) are all large-scale, man-made, networked systems, called *infrastructures*. They are named *critical* as any incapacity or destruction can have a debilitating impact on Society's health, safety, security, economics and well being (Kröger and Zio, 2011), so determining their degree of exposure to hazards and intentional attacks has become a topic of great concern.
An *all-hazard approach* is required for identifying the causes of damage or disruption of services in CIs (Waugh, 2004; Pollet and Cummins, 2009). In particular, the approach must handle also malevolent acts, which differ from natural or other man–made hazards and lacks of a well-established methodology for uncertainty assessment.
The all-hazard approach is intended to provide the basis for addressing unexpected events of any nature. The need is to capture the CI vulnerability sources and issues, given technical and physical features of the system, and the dependencies and interdependencies on other systems. This requires an evaluation of the susceptibility to different hazards, including threats of malevolent acts. Whereas the susceptibility to hazards leading to random failures can be quantified in terms of probability, the susceptibility to intentional malevolent acts lacks a well-established framework of evaluation. We propose a framework for an *All-HAZard ANalysis* (A-HAZAN) which relies on tailored tabular procedures to organize the qualitative and quantitative features of the system relevant for revealing and highlighting its vulnerabilities. The A-HAZAN framework is intended as a tool for managers, analysts and stakeholders of CIs to carry out the identification of all the sources of vulnerability in an all-hazard perspective. In particular, a methodology to assess the susceptibility to intentional attacks is

Please cite this article as: Zio E., Piccinelli R. and Sansavini G., 2012, A framework for ranking the attack susceptibility of components of critical infrastructures, Chemical Engineering Transactions, 26, 309-314 DOI: 10.3303/CET1226052

introduced. The paper is organized as follows. In Section 2, a framework of the A-HAZAN analysis is presented. In section 3, a methodology for assessing the susceptibility to attacks is explained. In Section 4, the A-HAZAN methodology is applied to a literature case study. Conclusions are drawn in Section 5.

2. Framework of analysis

The proposed tabular framework for the all-hazard vulnerability analysis is divided into two steps.
A preliminary qualitative step aims at identifying the relevant features, operating conditions and failure modes. This step highlights all the variables and states that impact on the component's role as a possible source of vulnerability and has been introduced in (Zio et al., 2011).
The second step aims at evaluating the components susceptibility to the various hazards: the need is to provide a measure of the likelihood that the specific hazard results in a mishap to the components and the CI. This evaluation requires different treatments and tools suitable to the nature of the specific hazard and the related uncertainties. The uncertainties associated with random failures and natural hazards can be treated within a probabilistic framework, while the uncertainties associated with threats might require an alternative treatment. With the framework, we aim at structuring the identification of the variables and states of the components that affect and contribute to their susceptibility, at pointing out the sources of uncertainties and the most suitable tools to treat them. For the assessment of threats due to malevolent acts, a qualitative evaluation of susceptibility is given.

3. Methodology

In the evaluation of the susceptibility to hazards of the system and its components, four categories of possible hazards have been identified: namely, attacks, random single failures, cascading failures induced by initiating failure within the CI, and failures induced by the coupling with other CIs.

- The susceptibility to *attacks* is characterized in terms of *attractivity* and *accessibility*. The term *attractivity* considers the appeal to intentional attacks, while the term *accessibility* considers that components have been designed for efficiency and convenience, yet access must be easy for maintenance staff but difficult for attacks.
- The susceptibility to *random failures* refers to the random failures of the components, i.e., permanent outages and transient outages, the effect of environmental conditions and temperature, or random failures due to maintenance operations.
- The susceptibility to *cascading failures* considers how the components are related in the network, i.e. the connectivity/topology of the network through which an initiating failure may propagate.
- The susceptibility to hazards that originate from *interdependent systems* whose input from external systems is required for the safe operations of the component.

The susceptibility to attacks is influenced by two variables; namely attractivity and accessibility. In turn, attractivity and accessibility are composed by four elements: size, level of demand, level of protection and level of social criticality:

- Size (physical) of the component;
- Level of demand, transmission or supply: the importance of the task of the component is measured both as the consumed, transmitted or supplied power of the component and as the fraction of the overall consumed, transmitted or produced power with respect to the whole system. From the point of view of accessibility, a component can be considered to be relevant in so far as it consumes, transmits or provides to the functioning of the system; for example, if the component is a generating unit and it provides a consistent amount of power to the network, then it should be accessible for maintenance or repairs;
- Level of protection: the logical and physical barriers deployed to prevent or discourage malevolent acts;
- Social criticality: given that the attack will be successfully accomplished, the impact on public opinion is influenced by the (conditional) effects caused by the achieved intentional act. The most relevant consequences here considered are in terms of human lives and geographic extension of the event.

We assume that the more protected a component, because of the security measures, the less accessible it is, but, the most attractive it is perceived, from a malevolent act point of view. This assumption relies on the idea that a malevolent will think that if a component deserves a good level of protection, then its damage would produce a large disruption. For example, nuclear power plants are strongly defended from the point of view of security; in this sense, they could be challenging and "attractive" to attacks. The combination of the above four elements yields different values of susceptibilities that are used in sorting the vulnerabilities of different components. Unfortunately, data and information concerning malevolent acts are incomplete, imprecise, ambiguous. To account for this, one may embrace various uncertainty representation approaches (Marseguerra et al., 2004).
The variables upon which vulnerability depends may be described as follows:

- x_1, size: the generating units are measured by their production of megawatts. They are grouped into small plants (power production ≤ 100 MW), medium plants (100 MW ≤ power production ≤ 300 MW) and large plants (power production ≥ 300 MW). Since the physical dimensions of a power plant are proportional to the produced power, in this frame the size of the power plant and the level of the produced power are joined under the size label;
- x_2, level of protection: as proposed in (Koonce and Apostolakis, 2008), six levels of protection may be considered:

Table 1: Levels of protections of infrastructure elements (Koonce and Apostolakis, 2008)

Level	Description
6 – Extreme (E)	Completely secure
5 – High (H)	Guarded, secure area, alarmed
4 – Moderate (M)	Secure area
3 – Low (L)	Complex barriers, security patrols, video surveillance
2 – Very low (VL)	Unlocked, non-complex barriers
1 – Zero (Z)	Completely open, no control, no barriers

- x_3, social criticality: here, the psychological impact on Society is considered, and attention is focused on human losses and the geographical spread of the event.

Table 2: Levels of social criticality of infrastructure elements

Level	Description
4 – Severe (S)	Many victims, widely spread extension
3 – High (H)	Many victims, contained extension
2 – Moderate (M)	Few victims, widely spread extension
1 – Low (L)	Few victims or no victims, contained extension

The variables x_1 and x_3 influencing accessibility can be described as for attractivity; the variable x_2, level of protection, acts on accessibility in the opposite way as for attractivity. In other words, the level of accessibility of a component is in inverse proportion to the adopted security measures: the weaker the security measures, the more accessible, and therefore more prone to attacks is the component.

Table 3: Levels of accessibility (y_1) and attractivity (y_2)

Level	Description
Y_5 – Extreme	Extreme degree of attractivity or extreme ease of accessibility
Y_4 – High	Elevated level of attractivity or high ease of accessibility
Y_3 – Moderate	Average degree of attractivity or medium ease of accessibility
Y_2 – Low	Low level of attractivity or low ease of accessibility
Y_1 – Very low	Almost null degree of attractivity or very low ease of accessibility

Then, the six-level scheme of protection of (Koonce and Apostolakis, 2008) is proposed in reverse order, level 0 applying to completely secure and level 6 to completely open, no barriers.
The accessibility and attractivity variables (y_1, y_2) are characterized by five levels, as shown in Table 3. Evaluation can be done by combining in an IF–THEN decision logic the levels of (x_1, x_2, x_3) for attractivity and (x_1, x_2, x_3) for accessibility. For example, the logic rules could be:

IF x_1 is X_{1k} AND IF x_2 is X_{2m} AND IF x_3 is X_{3n} THEN y_i is Y_1, $3 \le k+m+n \le 5$ (1)

IF x_1 is X_{1k} AND IF x_2 is X_{2m} AND IF x_3 is X_{3n} THEN y_i is Y_5, $12 \le k+m+n \le 13$ (2

IF x_1 is X_{1k} AND IF x_2 is X_{2m} AND IF x_3 is X_{3n} THEN y_i is $\begin{cases} Y_2 \text{ if } k+m+n = 6 \text{ or } 7 \\ Y_3 \text{ if } k+m+n = 8 \text{ or } 9 \\ Y_4 \text{ if } k+m+n = 10 \text{ or } 1 \end{cases}$, $6 \le k+m+n \le 11$ (3)

where the index k can vary in the range [1,2,3], m in the range [1,2,3,4,5,6] and n in the range [1,2,3,4]. The rules are set considering all the input variable levels as subsets labeled in linguistic terms as shown in Tables 1, 2 and 3. Each variable x_i is attributed an indexed function X_i representing the corresponding level and the logic rules (1), (2) and (3) are proposed. These rules have been chosen arbitrarily and will change depending on the characterization of the situation under analysis.

Table 4: rules for accessibility variable (y_1) when the size variable x_1 is (a) small, (b) medium and (c) large

	L	M	H	S
Z	Y_3	Y_3	Y_4	Y_4
VL	Y_2	Y_3	Y_3	Y_4
L	Y_2	Y_2	Y_3	Y_3
M	Y_1	Y_2	Y_2	Y_3
H	Y_1	Y_1	Y_2	Y_2
E	Y_1	Y_1	Y_1	Y_2

(a)

	L	M	H	S
Z	Y_3	Y_4	Y_4	Y_5
VL	Y_3	Y_3	Y_4	Y_4
L	Y_2	Y_3	Y_3	Y_4
M	Y_2	Y_2	Y_3	Y_3
H	Y_1	Y_2	Y_2	Y_3
E	Y_1	Y_1	Y_2	Y_2

(b)

	L	M	H	S
Z	Y_4	Y_4	Y_5	Y_5
VL	Y_3	Y_4	Y_4	Y_5
L	Y_3	Y_3	Y_4	Y_4
M	Y_2	Y_3	Y_3	Y_4
H	Y_2	Y_2	Y_3	Y_3
E	Y_1	Y_2	Y_2	Y_3

(c)

Table 5: rules for attractivity variable (y_2) when the size variable x_1 is (a) small, (b) medium and (c) large

	L	M	H	S
Z	Y_1	Y_1	Y_1	Y_2
VL	Y_1	Y_1	Y_2	Y_2
L	Y_1	Y_2	Y_2	Y_3
M	Y_2	Y_2	Y_3	Y_3
H	Y_2	Y_3	Y_3	Y_4
E	Y_3	Y_3	Y_4	Y_4

(a)

	L	M	H	S
Z	Y_1	Y_1	Y_2	Y_2
VL	Y_1	Y_2	Y_2	Y_3
L	Y_2	Y_2	Y_3	Y_3
M	Y_2	Y_3	Y_3	Y_4
H	Y_3	Y_3	Y_4	Y_4
E	Y_3	Y_4	Y_4	Y_5

(b)

	L	M	H	S
Z	Y_1	Y_2	Y_2	Y_3
VL	Y_2	Y_2	Y_3	Y_3
L	Y_2	Y_3	Y_3	Y_4
M	Y_3	Y_3	Y_4	Y_4
H	Y_3	Y_4	Y_4	Y_5
E	Y_4	Y_4	Y_5	Y_5

(c)

In Tables 4 and 5, the model rules are represented: they are shown with reference to input x_2 (level of protection) and x_3 (social criticality) and are parameterized with respect to the three different linguistic terms of variable x_1 (size). Then, accessibility (y_1) and attractivity (y_2) are combined to yield the susceptibility to attacks, y. The logic approach deployed to combine x_1, x_2 and x_3 into y_1 and y_2, is applied to y_1 and y_2 to yield the susceptibility, y. The logic rules that yield the values of y are described in the following. Again, the IF – THEN logic rule is proposed.
Five Threat Conditions are identified by means of Roman numerals. From lowest to highest, the levels are:
Low = **I**. This condition refers to a low susceptibility of terrorist attacks.
Guarded = **II**. This condition is declared when there is a general susceptibility of terrorist attacks.
Elevated = **III**. An elevated condition is declared when the susceptibility of attack is significant.

High = **IV**. A high condition is declared when there is a high susceptibility of malevolent attacks.
Severe = **V**. A severe condition reflects a severe susceptibility of terrorist attacks.

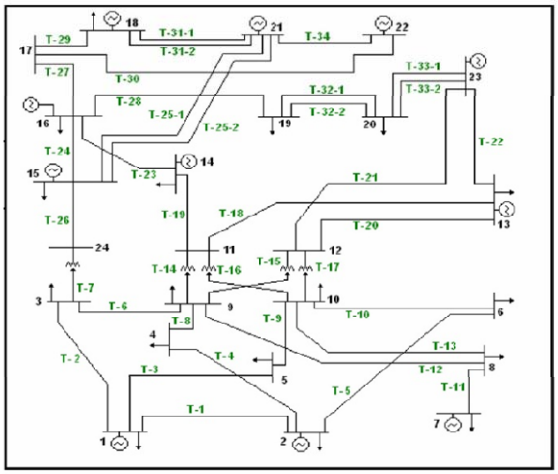
The higher the threat condition, the greater is the susceptibility of an intentional attack, going from **I**, low susceptibility to attacks, to **V**, severe condition of malevolent acts. To evaluate susceptibility to attacks, the set of rules that relate the two input variables, attractivity, y_1 and accessibility, y_2, to the output, susceptibility, y, are assigned in Table 6.
Table 6 shows how the levels of attractivity and accessibility yield the different levels of susceptibility to attacks. The numeral numbers distribute along east-west diagonal lines. The susceptibility to attack increases from the upper left corner where the susceptibility to intentional attacks is low, **I** level, to the lower right corner where the threat of attacks is severe, **V** level.

Table 6: Rules linking the linguistic variables attractivity (y_1) and accessibility (y_2) to the linguistic variable susceptibility y. The Roman numerals refer to the five levels: I, II, III, IV and V

y_1 \ y_2	Y_{21}=I	Y_{22}=II	Y_{23}=III	Y_{24}=IV	Y_{25}=V
Y_{11}=I	**I**	**I**	**I**	**II**	**III**
Y_{12}=II	**I**	**I**	**II**	**III**	**IV**
Y_{13}=III	**I**	**II**	**III**	**IV**	**V**
Y_{14}=IV	**II**	**III**	**IV**	**V**	**V**
Y_{15}=V	**III**	**IV**	**V**	**V**	**V**

4. Application

For illustration purposes, the rules have been applied to a study case of literature: the IEEE RTS-96 (IEEE RTS-96, 1999) power grid showed in Figure 1.



Provider ID	Attractivity	Accessibility	Susceptibility to attacks
1	4	2	III
2	4	2	III
7	4	2	III
13	4	3	IV
14	3	2	II
15	4	2	III
16	4	2	III
18	5	3	V
21	5	3	V
22	4	3	IV
23	4	3	IV

Figure 1: Single area IEEE RTS-96 grid (IEEE RTS-96, 1999) and list of the Susceptibility levels of the providers of IEEE RTS-96 grid

It consists of 24 load buses (users), 11 of these are generating units (providers), and 38 transmission lines (transmitters). In order to calculate the susceptibility of the elements of the network, each element has been assigned a level of protection and a level of social criticality.
Concerning the users, the level of protection is taken into account depending on the type of load bus. For example, a transmission grid load bus is typically located far from densely-populated areas and it is

usually locked, surrounded by fences but no other complex barriers (level 3, Table 1). The impact of the component role is assumed moderate (level 2, Table 2) since it is expected that if a load bus cannot receive power, the generation of power can be modulated, the power excess eliminated, and the overall infrastructure put in conditions to still provide its service. On the other hand, a provider is assumed to have a high level of criticality (level 4, Table 2), because in general its lost power supply may not be readily replaced by alternative generation. From the level of protection point of view, it can be assumed that the plant is isolated from the urbanized areas and it is usually guarded with security patrols, video surveillance of the entire power plant and alarms (level 5 or 6, Table 1). Finally, transmission towers are usually located in isolated sites, e.g., open country and they are not provided with any particular fence or barriers, nor are they watched by patrol (level 1 or 2, Table 1). The impact of their role may be assumed as low (level 1, Table 2). By these considerations, all the components of the network have been assigned attractivity and accessibility levels. The susceptibility to attacks can then be derived by the rules in Section 3 and the levels of susceptibility for providers are reported in Figure 1. The Tables of the levels of susceptibility for users and transmitters are here not reported, due to limitation of space. However, the salient aspects are described in the following. As can be seen from Figure 1, the susceptibility to attacks turns out to be strongest for generators sited in the upper part of the grid where the highest percentage of the generation is provided. The levels of susceptibility to attacks are low both for users and transmitters: however it is worthwhile noting that the transmission lines that have the highest susceptibility to attacks are placed in the central part of the network (for example, lines connecting bus 11 to bus 13 and bus 12 to bus 23). In the performed analysis the components of the network with the highest level of susceptibility turn out to be the providers: an attack to them will cause a strong effect in terms of disruption, hence the highest success from a terroristic perspective.

5. Conclusions

An approach for identifying the vulnerabilities of critical infrastructures has been presented within an all-hazard analysis framework which allows merging two different perspectives on vulnerability: on the one hand, there is the demand to encompass the vulnerabilities due to random failures and to natural hazards; on the other hand, there is the need to include vulnerabilities due to malevolent acts.
A structured organization of the relevant information on the system components is made on the basis of their tasks and of the features that influence them in the potential role as source of vulnerability. Then, an evaluation is made of the degree of exposure, i.e., the susceptibility of the components to malevolent acts. The future step of the analysis will be the development of a quantitative decision logic method for evaluating the susceptibility encompassing the whole set of hazards, i.e., random failures unintentional acts and natural hazards, but also malevolent acts, while accounting for the related uncertainties.

References

IEEE RTS-96, 1999, Reliability test system task force of the application of probability methods subcommittee. The IEEE reliability test system – 1996. IEEE Trans Power Syst; 14, 1010 – 20.

Koonce A.M., Apostolakis G.E., 2008, Bulk power risk analysis: ranking infrastruture elements according to their risk significance, Electrical Power and Energy Systems, 30, 169-183.

Kroeger W., Zio E., 2011, Vulnerable Systems, Springer, London, UK. ISBN 978-0-85729-654-2.

Marseguerra M., Zio E., Bianchi M., 2004, A fuzzy modeling approach to road transport with application to a case of spent nuclear fuel transport, Nuclear Technology, 146 (3), 290-302.

Pollet J., Cummins, J., 2009, All-Hazard approach for Assessing Readiness of Critical Infrastructure, HST'09 IEEE Conference on Technologies for Homeland Security, 366-372.

Waugh, W. L., 2005, Terrorism and the All-Hazard Model, J. of Emergency Management, 3(2), 8-10.

Zio E., Piccinelli R., Sansavini G., 2011, An All-Hazard Approach for the Vulnerability Analysis of Critical Infrastructures, Proceedings of the Annual Conference ESREL, 18-22 september 2011, Troyes, France, 2451-2458.