# A Hierarchical Decision Making Framework for Vulnerability Analysis

Tai-Ran Wang, Vincent Mousseau, Enrico Zio

# A Hierarchical Decision Making Framework for Vulnerability Analysis

T. WANG
*Chair on Systems Science and the Energetic challenge, European Foundation for New Energy-Electricité de France, Ecole Centrale Paris and Supelec, Grande Voie des Vignes, F92-295, Chatenay Malabry Cedex*

V. MOUSSEAU
*Laboratory of Industrial Engineering, Ecole Centrale Paris, Grande Voie des Vignes, F92-295, Chatenay Malabry Cedex*

E. ZIO
*Politecnico di Milano, Energy Department, Nuclear Section, c/o Cesnef, via Ponzio 33/A , 20133, Milan, Italy*
*Chair on Systems Science and the Energetic challenge, European Foundation for New Energy-Electricité de France, Ecole Centrale Paris and Supelec, Grande Voie des Vignes, F92-295, Chatenay Malabry Cedex*

ABSTRACT: Embracing an all-hazard view to deal with random failures, natural disasters, accidents and malevolent intentional acts, a framework for the vulnerability analysis of safety-critical systems and infrastructures is set up. A hierarchical structure is used to organise the information on the hazards, which is then manipulated through a decision-making process for vulnerability evaluation. We present the framework and its hierarchical model by way of assessing the susceptibility of a safety-critical system to intentional hazards, considering criteria of diverse nature, such as physical characteristics, social criticality characteristics, exposition to cascading failures, resilience. We use a ranking method to compare systems of different characteristics. The systematic process of analysis is presented with reference to the exemplary case of nuclear power plants.

## 1 INTRODUCTION

The vulnerability of safety-critical systems and infrastructures is of great concern, given the multiple and diverse hazards that they are exposed to and the potential large-scale consequences.

We conceptualise vulnerability as a global system property related to the system susceptibility to all hazards, intentional, random internal and natural, and to resilience. Notably, resilience should not be considered separately but for its effects on the susceptibility to the three different kinds of hazards.

The susceptibility associated with random internal hazards and natural hazards is classically treated within a probabilistic framework to handle both the aleatory uncertainty in the occurrence of the accident events and their consequences (Kröger & Zio 2011) and the epistemic uncertainty on the hypotheses and parameters of the models used. Intentional hazards relate to malevolent acts and lack of a well-established methodology for accounting for uncertainty due to behaviours of different rationality (Depoy & Phelan 2005).

In this paper, we illustrate a decision-making framework intended to guide analysts, managers and stakeholders in the systematic identification of sources of vulnerability. Guided by the framework, effective management can be performed in an all-hazard perspective addressing questions like: what is the level of vulnerability of a site comparing with others? Which one should be protected and ameliorated? How to proceed and how much will it cost?
The evaluation through the framework is shown by way of analysing the susceptibility to intentional hazards of a safety-critical system, namely a Nuclear Power Plant (NPP), considering the vulnerability sources and the related features, the system technical and physical features, and the dependencies and interdependencies on other systems. The paper is organised as follows. In Section 2, the framework is presented with the focus on intentional hazards and by way of the reference example of NPPs. In Section 3, the decision-making methodology for assessing susceptibility is explained. In Section 4, an application is shown to exemplify the process. Conclusions are drawn in Section 5.

Table 1: Criteria, subcriteria and preference directions

| Criterion | Physical characteristics | Social criticality | Possibility of cascading failures |
|---|---|---|---|
| Subcriteria | Number of workers<br>Nominal power production<br>Number of production units | Percentage of contribution to the welfare<br>Size of served cities | Connection distance |
| Preference direction | Min | Min | Min |

| Criterion | Recovery means | Human preparedness | Level of protection |
|---|---|---|---|
| Subcriteria | Number of installed backup components<br>Duration of backup component<br>Duration of repair and recovery actions<br>External emergency measures | Training<br>Safety management | Physical size of the system<br>Number of accesses<br>Entrance control<br>Surveillance |
| Preference direction | Max | Max | Max |

## 2 FRAMEWORK OF ANALYSIS

Vulnerability is defined in different ways depending on the domains of application, e.g.: vulnerability is a measure of possible future harm due to exposure to a hazard (Kröger & Zio 2011); the identification of weaknesses in security, focusing on defined threats that could compromise a system ability to provide a service (NWRA 2002); the set of conditions and processes resulting from physical, social, economic, and environmental factors, which increase the susceptibility of a community to the impact of hazards (Hofmann, Kjølle, & Gjerde 2012).

With the focus on the susceptibility to intentional hazards, a four-layers hierarchical model is shown in Figure 1. The susceptibility to intentional hazards is characterised in terms of attractiveness and accessibility. These are hierarchically broken down into factors which influence them, including resilience seen as pre-attack protection (which influences on accessibility) and post-attack recovery (which influences on attractiveness). The decomposition is made in 6 criteria which are further decomposed in a layer of basic subcriteria, for which data and information can be collected to make their evaluation. The criteria and subcriteria considered serve as examples and are not to be considered exhaustive.

In the following subSections, the criteria of the layers are defined and assigned preference directions for treatment in the decision-making process. The preference direction of a criterion indicates towards which state it is desirable to lead it to reduce susceptibility, i.e., it is assigned from the point of view of the defender of an attack who is concerned with protecting the system. Although only the 6 criteria in the third level of the hierarchy will be considered in the exemplary demonstration on the NPPs evaluation, examples of scales of evaluation also of the basic subcriteria of the last layer are proposed, in relation to the characteristics of NPPs for exemplification purposes.

### 2.1 *Attractiveness*

This second-layer criterion is intended to capture the interest that terrorists may have to attack the system. Such interest is considered to be driven mainly by the effects that the attack can cause, which include damages to the assets and environment, injured people, deaths. These depend on the physical characteristics of the system, its social criticality, the possibility of cascading effects and the system resilience. In a general sense, resilience represents the ability to avoid the occurrence of accidents despite the persistence of poor circumstances or to recover from some unexpected events (Furniss, Back, & Blandfod 2011). It is the ability of a system to anticipate, cope with/absorb, resist and recover from the impact of a hazard (technical) or a disaster (social). Resilience reflects a dynamic confluence of factors that promotes positive adaptation despite exposure to adverse life experiences. In our model, it is presented in terms of capacity of recovery, human preparedness and level of protection.

The preference direction characterising this factor is such that the more attractive the system is, the more it should be protected.

### 2.2 *Accessibility*

Accessibility is introduced as a criterion in the second layer of the hierarchy to describe the degree to which it is easy or difficult to arrive at a system in order to intentionally damage it. It is a function of resilience through the level of protection present to defend against malevolent attacks.

### 2.3 *Examples of subcriteria*

Each third-layer criterion is constituted by several subcriteria (Table 1). The value of the subcriteria can be crisp numbers or language terms according to the contents. Each of the subcriterion is analysed in giv-

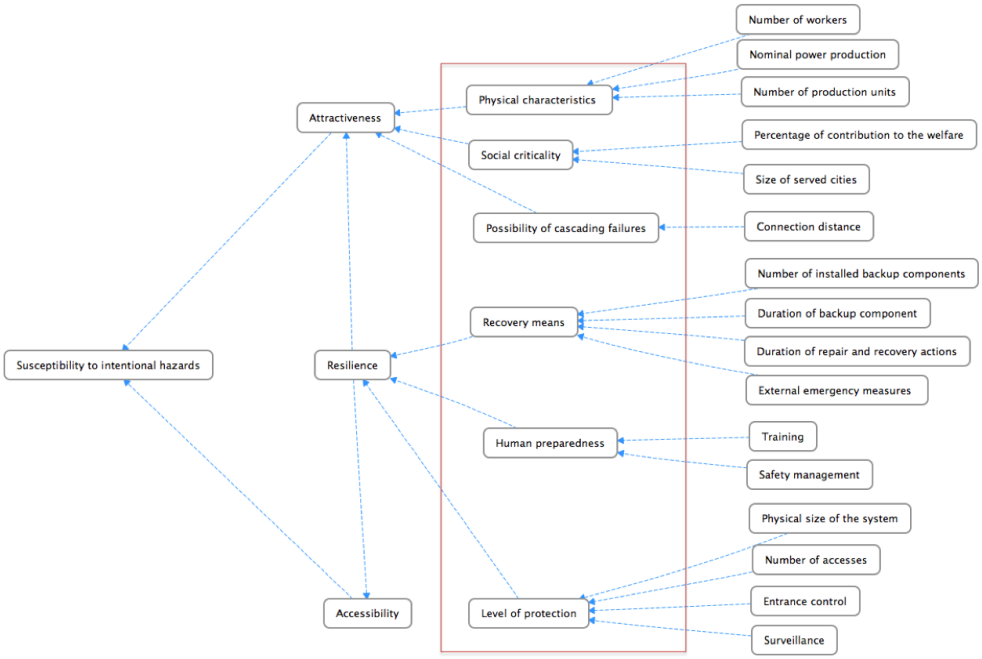


Figure 1: Hierarchical modelSusceptibility to intentional hazards

Table 2: Number of workers

| Level | Number of workers |
|---|---|
| 1 | 500 |
| 2 | 1000 |
| 3 | 1500 |
| 4 | 2000 |
| 5 | 2500 |

Table 3: Entrance control

| Level | Type of entrance control |
|---|---|
| 1 | Completely open, no control, no barriers |
| 2 | Unlocked, non-complex barriers |
| 3 | Complex barriers, security patrols |
| 4 | Secure area |
| 5 | Guarded, secure area, alarmed |
| 6 | Completely secure |

ing an explanation of the contribution on the corresponding third-layer criterion.

#### 2.3.1 *Number of workers*

This criterion can be seen to contribute to the attractiveness for an attack from various points of view, for example: 1) the more workers, the more work injuries and deaths from an attack; 2) the more workers, the easier for the attackers to sneak into the system; 3) the more workers, the higher the possibility that one of them can be turned into an attack. Limiting the number of workers can then contribute to the security of the plant and, thus, reduce its attractiveness for an attack. Table 2 reports some reference values, typical of NPPs.

#### 2.3.2 *Entrance control*

This gives due count to the process and technology for entrance control. The more effective the control at the entrance is, the less easy it is to enter the system with bad intentions. Table 3 gives a 6 levels presentation.

## 3 ASSESSMENT METHODOLOGY

The hierarchical model just presented structures the susceptibility of a critical system to intentional attacks in terms of a number of criteria. The 16 basic, bottom-layer subcriteria are organised into 6 main ones: the physical characteristics, the social criticality, the possibility of cascading failures, the recovery means, the human preparedness and the level of protection. For the quantitative assessment, each of the 16 basic subcriteria needs to be assigned a value function in relation to the main criterion to which it contributes. The assignment can be done in relative terms, by comparing different systems with different characteristics. To exemplify how this is done, we consider NPPs as critical systems and perform a decision-making process for the evaluation of their characteristics with respect to susceptibility to intentional attacks. We first build a ranking of fictitious NPPs, through the authors' subjective preferential judgment of indirect data. This serves for constructing the basis for the relative evaluation of the characteristics of real NPPs.

To carry out the decision-making process for the evaluation, we resort to a multiple criteria decision aid (MCDA) technique named ACUTA (Analytic Centre UTilité Additive) based on the computation of the analytic centre of a polyhedron for the selection of additive value functions that are compatible with holistic assessments of the preferences in the criteria (Bous, Fortemps, Glineur, & Pirlot 2010). Being central by definition and uniquely defined, the analytic centre benefits from theoretical advantages over the notion of centrality used in other meta-UTA methods. A brief explanation of the method is given in the subSections

that follow.

For the practical computations, we use an implementation of the method available in the Open Source software Diviz of the Decision Deck Project (http://www.decision deck.org/ ).

### 3.1 *Analytic Center*

The idea of the analytic centre of a polyhedron was first introduced by Huard (1967) and later reintroduced by Sonnevend (1985) in the context of convex optimization techniques. The theoretical framework around this concept lies at the heart of interior-point methods for solving linear programming optimisation problems. In ACUTA, it is suggested to compute a unique, well-defined and central solution for aggregation-disaggregation methods based on additive piecewise linear value function models (Bous, Fortemps, Glineur, & Pirlot 2010).

### 3.2 *ACUTA*

The UTA( UTilité Additive) method consists in building a piecewise linear additive decision model from a preference structure using linear programming. Let $A$ be the set of possible alternatives and $A_L = \{a_j, j = 1, ..., k\}$ the learning set. In $A_L$, alternatives are ranked in order of decreasing preference by the DM (Decision Maker), i.e. $a_j \succsim a_{j+1}, j = 1, ..., k-1$, where $\succsim$ expresses that $a_j$ is either preferred ($\succ$) or indifferent ($\sim$) to $a_{j+1}$. The values of the $n$ criteria, denoted by $x_i (i = 1, ..., n)$ , belong to the interval $[\overline{\chi_i}, \underline{\chi_i}]$ that, for each $i$, corresponds to the range between the worst ($\underline{\chi_i}$) and best $\overline{\chi_i}$ values found for attribute $i$ among the alternatives in $A$. Our purpose is to establish marginal value functions $\nu_i(\chi_i)$ for each criterion in order to model the perceived value of each alternative. Since these values are piecewise linear functions, the range of values on each criterion is divided into subintervals using a predefined number of $a_i$ points such that $\chi_i = \{\underline{\chi_i} = \chi_i^1, \chi_i^2, ..., \chi_i^{a_i} = \overline{\chi_i}\}$ . The subdivision makes it possible to compute value functions by linear interpolation between the values $\nu_i(\chi_i^l)$ that have to be estimated and hence appear as variables in the linear program. Using the degrees of freedom in the definition of a value function, we set $\nu_i(\underline{\chi_i}) = 0$ and

$$\sum_{i=1}^{n} \nu_i(\overline{\chi_i}) = 1 \tag{1}$$

This implies that $\nu_i(\overline{\chi_i})$ can be interpreted as the tradeoff associated to criterion $i$. Furthermore, all value functions should be monotonic, that is $\nu_i(\chi_i^{l+1}) - \nu_i(\chi_i^l) \geqslant \lambda (\forall\ i\ and\ l = 1, ..., a_i = 1)$ , with $\lambda \geqslant 0$. According to the additive model, the global value $\nu(a_j)$ of an alternative $a_j$ is given by the sum of its marginal values. In other terms, if the value of the $j^{th}$ alternative on attribute $i$ is denoted by $a_{ij}$ , the global value of $a_j$ is given by

$$\nu(a_j) = \sum_{i=1}^{n} \nu_i(a_{ij}) \tag{2}$$

This analytic expression of an alternative's global value allows for modelling the preferences of the DM, as expressed in the ranking of the learning set, using the following linear constraints, which we call preference constraints:

$$\nu(a_j) - \nu(a_{j+1}) \geqslant \delta \quad if\ a_j \succ a_{j+1}, \tag{3}$$

$$\nu(a_j) - \nu(a_{j+1}) = 0 \quad if\ a_j \sim a_{j+1}. \tag{4}$$

Here, $\lambda$ is a positive number, called preference threshold, which is usually set to a small value. The assessment of the $\nu_i(\chi_i^l)$ variables should be done in such a way that the deviation from the preferences expressed by the DM in the subset $A_L$ is minimal. The adaptation of the linear additive aggregation-disaggregation model to the analytic centre formulation is quite straightforward and gives rise to the ACUTA method; the introduction of slack variables into the objective function leads to the following nonlinear optimisation problem, which can be solved without further modifications:

$$max \sum_{j=1}^{k-1} ln(s_j) = \sum_{i=1}^{n} \sum_{l=1}^{a_i - 1} ln(s_{il}), \tag{5}$$

$$s.t. \quad \nu(a_j) - \nu(a_{j+1}) = 0 \quad if\ a_j \sim a_{j+1}, \tag{6}$$

$$(\nu(a_j) - \nu(a_j + 1)) - \delta = s_j \quad if\ a_j \succ a_{j+1}, \tag{7}$$

$$s_{il} = (\nu(\chi_i^{l+1}) - \nu(\chi_i^l)) - \lambda, \tag{8}$$

$$\sum_{i=1}^{n} \nu_i(\overline{\chi_i}) = 1. \tag{9}$$

Since this approach maximises the sum of slacks, parameters $\delta$ and $\lambda$ can be omitted, and this is considered an advantage. The essential advantage of this method, however, is the centrality and uniqueness of the solutions it produces.

### 3.3 *The Diviz tool*

Diviz is a software for designing, executing and sharing Multicriteria Decision Aid (MCDA) methods, algorithms and experiments. Based on basic algorithmic components, Diviz allows combining these criteria for creating complex MCDA workflows and methods.

Once the workflow is designed, it can be executed on various data sets written according to the XMCDA standard. This execution is performed on distant servers via web services (http://www.decision deck.org/diviz/ ).

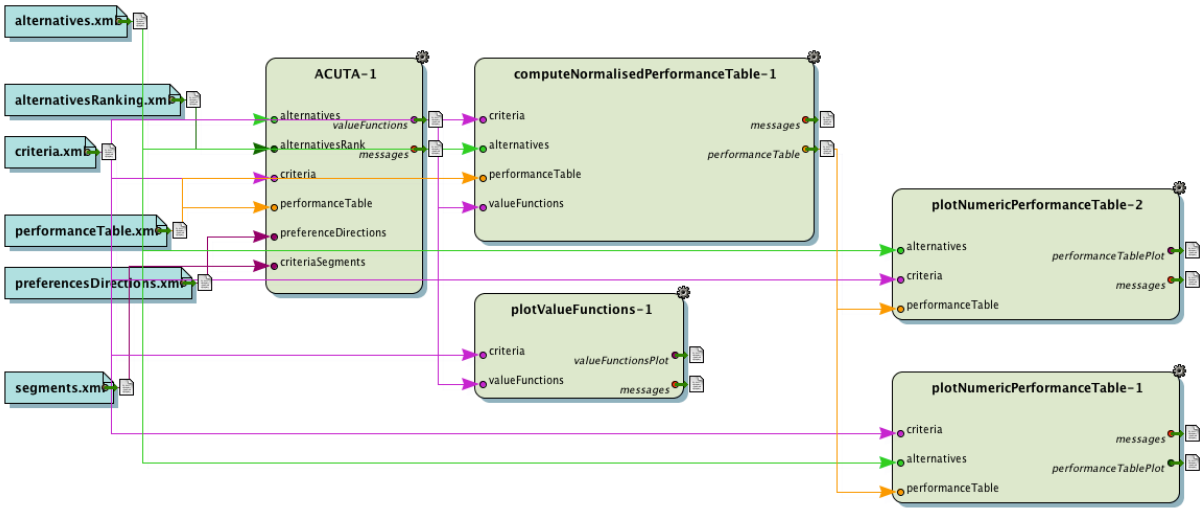


Figure 2: ACUTA analysis workflow for the illustrative example of Section 4

Once the execution is completed, the outputs of the different elementary components are available and can be visualised in Diviz.

Figure 2 shows the workflow of the analysis of susceptibility to intentional hazards for the illustrative example on NPPs of Section 4. This workflow uses, among other components, the ACUTA component to determine value functions based on the ranking of the NPPs given by the authors. These value functions are then applied to the real plants values and the whole data is then analysed via some graphical representations.

## 4 ILLUSTRATIVE EXAMPLE

For illustration purposes, 9 fictitious plants are considered to obtain the value functions, which are in turn used to evaluate the susceptibility to intentional attacks of 9 real plants. In simple words, the former 9 fictitious plants are evaluated with respect to their susceptibility to intentional hazards, to build the base for comparison of the latter. Best (least vulnerable) and worst (most vulnerable) fictitious plants are defined as bounding references, by taking the best/worst conditions of all subcriteria considered. The details are presented in the following subSections.

### 4.1 *Case study preparation*

In the hierarchical model of susceptibility, we consider 16 basic subcriteria and 6 main criteria.

#### 4.1.1 *Data preparation*

In order to apply the ACUTA method, a data preparation is necessary.

For the 9 fictitious plants (named F1 to F9), the data of the 16 subcriteria are assigned arbitrarily by the authors. The data of one basic subcriterion are assigned to the different fictitious sites in a way to ensure that all possible values of the subcriterion are included.

The worst (named fictitiousWorst) and best (named fictitousBest) fictitious plants are defined by taking the worst/best values of each basic subcriterion. These two fictitious plants bound, in worst and best, the situations that are expected from the other plants.

Then, the descriptive terms and values of the 16 subcriteria are scaled onto the categories.

To illustrate the procedure of comparison of the subcriteria, we refer to the level of the six aggregated main criteria introduced in Section 2 and listed in Table 1. Their preference directions are also presented. They convey the fact that it is preferable to limit the dimension of the plant, minimise social criticality, control the cascading failure, maximise the recovery means, give more training, be better prepared for emergency and take more protection measures.

To get the values of the six aggregated criteria, we apply a simple weighted sum to their constituents subcriteria. For this, the weights for each subcriterion are arbitrarily assigned by the authors. Then, the data of the 9 fictitious NPPs are normalised (that is, rescaled between 0 and 1).

Same steps are applied to the 9 real NPPs (named R1 to R9), whose data have been taken from publicly available documents.

The weights of each basic subcriterion in the group for the main criteria are the same as for the fictitious NPPs.

#### 4.1.2 *Ranking of fictitious NPPs*

As presented in the previous Sections, the analysis using ACUTA method needs a ranking of the fictitious NPPs to begin with. It is usually given by the experts. In our case study, the utility functions are first given by the authors. As presented in Section 3.2, let N be the set of the 9 fictitious plants and $N_L = \{F_j, j = 1, ..., 9\}$ the learning set. The data of fictitiousWorst and fictitiousBest are used to be the limit interval for the given criterion, divided into 5 subintervals. The utility functions are given such that all the data of fictitiousWorst are set to 0 and the data

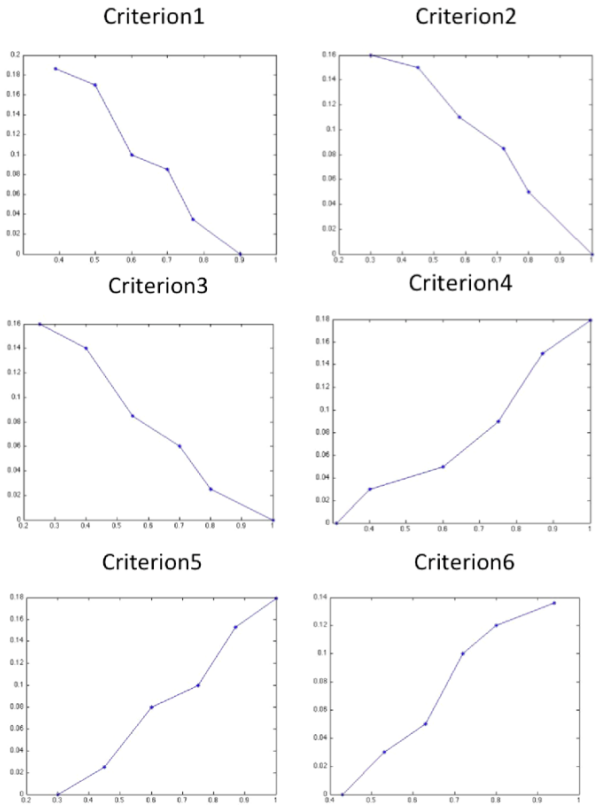


Figure 3: Utility functions given by authors

Table 4: Ranking of the fictitious NPPs based on the utility functions given by the authors

| Rank | Name |
|---|---|
| 1 | fictitiousBest |
| 2 | F1 |
| 3 | F2 |
| 4 | F3 |
| 5 | F4 |
| 6 | F5 |
| 7 | F6 |
| 8 | F7 |
| 9 | F8 |
| 10 | F9 |
| 11 | fictitiousWorst |

sum of the fictitiousBest is set to 1. The value functions can be calculated and visualised in Figure 3.

Based on the utility functions of the main criteria and the data, we can obtain the marginal value of the corresponding criterion for each fictitious NPP.

As a characteristic of the additive model, the global values which represent the susceptibility of the NPPs to the intentional hazards are given by the sum of its marginal values. These values are used to rank the NPPs. The ranking obtained is integrated into the decision-making process in the following subSection, to find out the value functions for the 6 criteria through the ACUTA method. The intentional hazards of real plants is then analysed and represented by using Diviz.

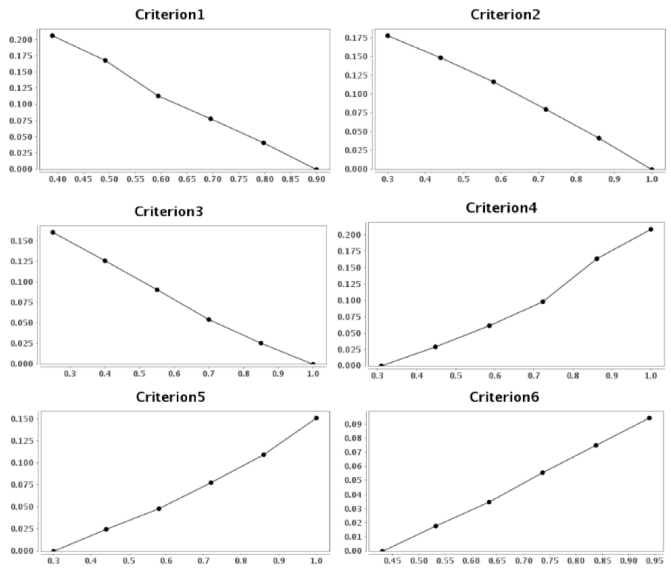


Figure 4: Representation of the Value Functions

## 4.2 *Results*

Applying the ACUTA method on the 9 fictitious plants in Diviz, we can calculate the value functions of the 6 criteria (Figure 4).

First of all, the criteria preference directions can be recognised easily from the trends of the curves. Also, for most part of each curve, it is natural that the vertical axis values are roughly proportional to the abscissa axis ones, because the vulnerability performance is roughly proportional to the value of the related parameters. More importantly, we can figure out the sensitive interval of each criterion. For example, for criterion 4, Recovery means, in the interval from 0.7 to 0.8 of the abscissa axis, there is an obvious change of gradient that is larger than before. This phenomenon also occurs in intervals of the other criteria and is due to the authors' preferences in the judgments. The more recovery means, the less susceptible the NPPs are to intentional hazards. Especially after a certain level (0.7 of the abscissa axis value), the extra-added measure can substantially increase the protection. This can be an indicator to know better the preference of the DMs during the ranking step and can also serve as a guidance during the amelioration of the plants.

In using the value functions, the former data of the 9 real NPPs can then be taken into account. We can compare the NPPs by single criterion. As shown in the 6 histograms (Figure 5), for one criterion, each column represents the corresponding performance of a given NPP. The length of each column is proportional to the marginal values. The longer the column, the better performance it has for the criterion. In the solid line frame there are the representative columns for each criterion of the real plants.

For the 6 criteria, the performances of most of the real NPPs are at least as good as the fictitious ones. Especially for possibility of cascading failure and level of protection, the performances of the real

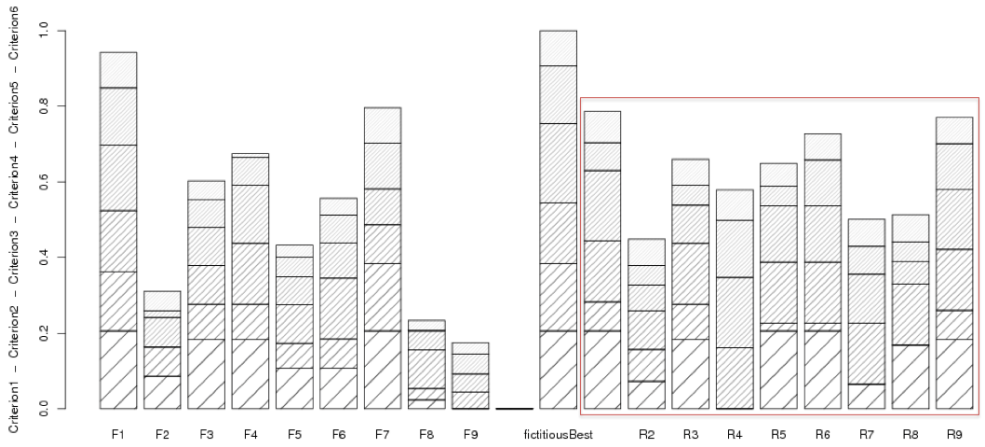


Figure 6: Histogram of susceptibility to intentional hazards of the NPPs

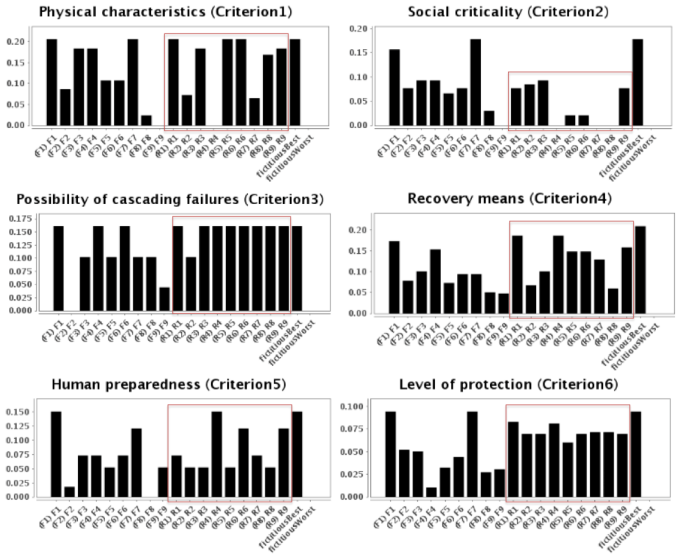


Figure 5: Histograms of subcriteria of the NPPs

ones are nearly the best among all these 20 NPPs. But for the physical characteristics of the system, there are 3 plants that are worse than the others because of their higher production power and bigger size. For human preparedness, because of certain enhanced training and safety management systems, there are 3 plants that present a better result. For recovery means, the differences among the NPPs are not very big. And for the social criticality, they are more vulnerable than the fictitious ones.

As a characteristic of the additive model, the global values which represent the susceptibility of the NPPs to the intentional hazards are given by the sum of the marginal values. An overview of the 20 NPPs is presented graphically in Figure 6. Each column represents the susceptibility performance of one NPP to intentional hazards. Each column is constituted by 6 blocks with different textures that represent the 6 main criteria. As mentioned before, the height of each block of the representative column is proportional to the value of the corresponding criterion data. The smaller the height of the representative column of a plant is, the more susceptible it is in facing an intentional hazard.

Based on the performance values, we put the 20

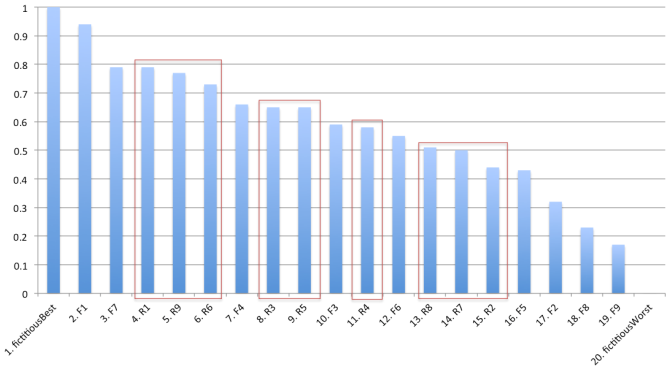


Figure 7: Ranking of the 20 NPPs

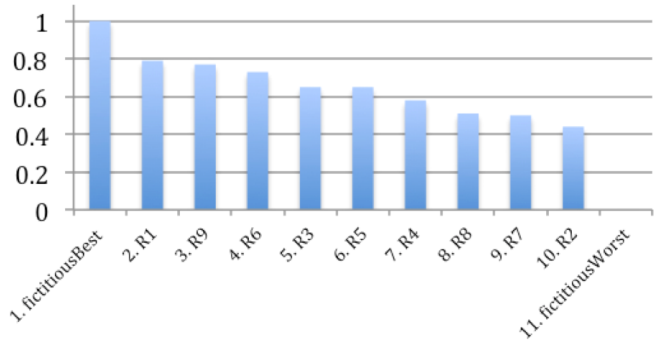


Figure 8: Ranking of the Real NPPs

NPPs in order as shown in Figure 7.

For the 9 real NPPs, according to the ranking, there are 5 that are among the first 10; all of them are among the first 15. Most of their performances are better than the fictitious ones. This is reasonable because for certain basic subcriteria, we have given some abnormally low values to the fictitious NPPs (e.g. for the basic subcriterion Type of entrance control, we have set certain fictitious plants to have unlocked barriers which is impossible for a real NPP). For the real NPPs, in view of production safety and international standards, certain criteria are already forced to be in limited intervals, that leads to improved situations than for the fictitious ones. We then concentrate only on the real NPPs, whose ranking result is given in Figure 8.

In order to find out the weaknesses of the real NPPs, we have done first the comparison between the

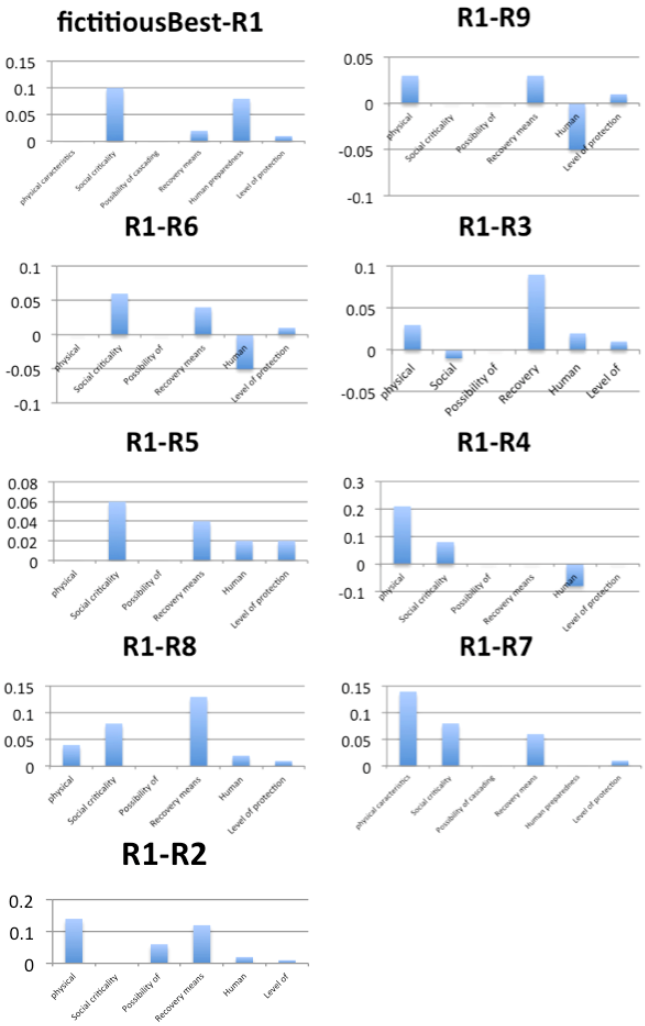


Figure 9: Performance comparison of the Real NPPs

fictitiousBest and R1 (which is the best among all the Real NPPs) and then between R1 and the rest of the Real NPPs, separately. The difference of the marginal value of each criterion is shown in Figure 9.

R1 is as good as the fictitiousBest for two criteria. In comparing with the rest of the Real NPPs, for R2, R5, R7 and R8, R1 is at least as good as them for each of the criteria. But for R3, R4, R6 and R9, R1 has an advantage only on the sum of the differences. There are criteria for which R1 is not as good as the others.

## 5 CONCLUSIONS

This paper proposes a decision making framework for analysing the vulnerability of critical infrastructures. A hierarchical model of susceptibility to intentional attacks has been taken as reference example. A case study of NPPs has been analysed by using the ACUTA method and the results calculated with the software Diviz.

The main contributions of this paper are the establishment of the hierarchical modelling framework for system vulnerability analysis and the decision making setting for its evaluation.

## REFERENCES

Bous, G., P. Fortemps, F. Glineur, & M. Pirlot (2010). ACUTA: A novel method for eliciting additive value functions on the basis of holistic preference statements. *European Journal of Operational Research 206*(2), 435–444.

Depoy, J. & J. Phelan (2005). Risk assessment for physical and cyber attacks on critical infrastructures. Volume 3.

Furniss, D., J. Back, & A. Blandfod (2011). A resilience markers framework for small teams. *Reliability Engineering & System Safety 96*.

Hofmann, M., G. Kjølle, & O. Gjerde (2012). Development of indicators to monitor vulnerabilities in power systems.

http://www.decision deck.org/.

http://www.decision deck.org/diviz/.

Huard, P. (1967). Resolution of mathematical programming with nonlinear constraints by the method of centers. *Nonlinear Programming*, 209–219.

Kröger, W. & E. Zio (2011). *Vulnerable Systems*. UK: Springer.

NWRA, N. W. R. A. (2002). Risk assessment methods for water infrastructure systems.

Sonnevend, G. (1985). An analytical centre for polyhedrons and new classes of global algorithms for linear (smooth, convex) programming. *Lecture Notes in Control and Information Sciences*, 866–876.