Open access • Journal Article • DOI:10.1108/03684921211213043

A systems thinking approach for project vulnerability management

— Source link

Ludovic-Alexandre Vidal, Franck Marle

Institutions: École Centrale Paris

Published on: 02 Mar 2012 - Kybernetes (Emerald Group Publishing Limited)

Topics: Project charter, Project management triangle, Extreme project management, Project management and Risk management plan

A systems thinking approach for project vulnerability management

Ludovic-Alexandre VIDAL[1], Franck MARLE[1]

Ecole Centrale PARIS – Laboratoire Genie Industriel

Grande Voie des Vignes 92290 Chatenay-Malabry France

Abstract

Purpose

This papers aims at developing the concept of project vulnerability in order to focus on the weaknesses of a project system, instead of focusing on risk evaluation only. We then aim at concentrating on a systems thinking based view to highlight the potentially endangered elements of a project, including its outcomes.

Design/methodology/approach

- A broad state of the art in many scientific domains.
- A definition of project vulnerability.
- A description of a project vulnerability management process, including identification, analysis and response plan.
- A test on an industrial case study

Findings

Our project vulnerability management process permits to concentrate directly on the existing weaknesses of a project system which may create potential damages regarding the project values creation. By focusing on this system, response plans may be more adapted to the existing lacks of the project.

Research limitations/implications

Some aspects of the vulnerability definition should be refined, like the concepts of susceptibility or cruciality. Other promising works may focus on the evaluation of the non-resistance and resilience, notably thanks to the introduction of interdependences which exist in complex projects.

Practical implications

A case study was done on a decision support system (called FabACT) developed at Hôpital Européen Georges Pompidou Pharmacy department. The aim of this project was to achieve a better balance between the workload and the efficiency of the compounding unit.

Originality/value

This article presents an innovative way to analyse a project's vulnerability by focusing on its existing weaknesses using a systems thinking-based approach.

Keywords

System, Project, Risk, Vulnerability, Complexity.

Classification

Research Paper

A systems thinking approach for project vulnerability management

1. Introduction

As recent works or communications state it (Zhang 2007), the concept of vulnerability appears to be promising for efficient risk management, notably within the context of project management. Indeed, it enables to have a more systems-oriented vision than the traditional cindynics approach. This one focuses on the evaluation of risks, instead of focusing on the weaknesses of a system facing these risks. Following a systemic approach when coping with project risk management permits to reduce ambiguity by increasing the awareness of the project system. We then aim at:

- Concentrating on a systems-thinking based view in order to highlight the potentially endangered processes and elements of the project system, including its outcomes.
- Focusing therefore on these elements in order to facilitate the identification and analysis of potential negative events and damages on the system.

This paper aims at addressing the concept of project vulnerability by:

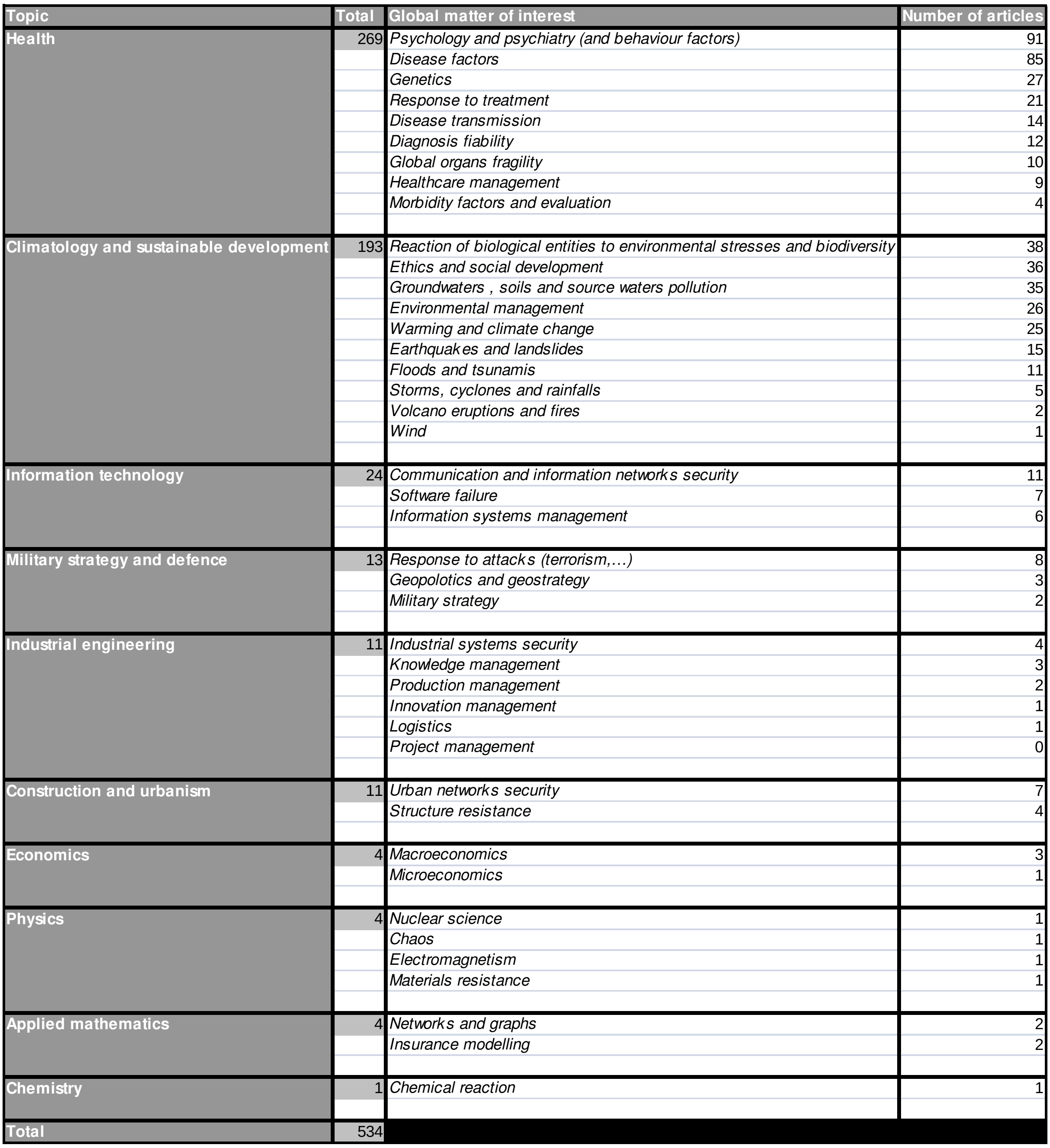
- Carrying out a broad state of the art in many scientific domains, in order to understand the concept of vulnerability and to implement it in the context of project management.
- Defining project vulnerability and its characteristics.
- Describing the steps of a project vulnerability management process in order to permit the industrial application of the concept of vulnerability in projects.
- Permitting the identification and analysis of project vulnerabilities thanks to a systems thinking approach focusing on the potential degradation of the project values creation processes.
- Testing the whole approach on a case study.

2. Background

Etymologically, being vulnerable means either being “capable of being physically or emotionally injured, wounded or hurt”, either being “open to temptation, persuasion, censure, etc.”, or being “liable or exposed to disease, disaster, etc.”. Even though the words vulnerable or invulnerable are thus commonly used in everyday life, little insight has been given to the concept of vulnerability. This paragraph aims at drawing a state of the art on the concept of vulnerability before applying it to project management.

2.1. Quantitative analysis of recent publications in the field of vulnerability and in the web of science database

As an illustration of the interest of the present research community for the notion of vulnerability in different scientific fields, we carried out a review and classification of the up to 2007 Web of Science publications which mentioned the world *vulnerability* in their title. 534 such publications were identified, which underlines the global interest of the scientific community for this concept (see Table I).



Topic	Total	Global matter of interest	Number of articles
Health	269	*Psychology and psychiatry (and behaviour factors)*	91
		Disease factors	85
		Genetics	27
		Response to treatment	21
		Disease transmission	14
		Diagnosis fiability	12
		Global organs fragility	10
		Healthcare management	9
		Morbidity factors and evaluation	4
Climatology and sustainable development	193	*Reaction of biological entities to environmental stresses and biodiversity*	38
		Ethics and social development	36
		Groundwaters , soils and source waters pollution	35
		Environmental management	26
		Warming and climate change	25
		Earthquakes and landslides	15
		Floods and tsunamis	11
		Storms, cyclones and rainfalls	5
		Volcano eruptions and fires	2
		Wind	1
Information technology	24	*Communication and information networks security*	11
		Software failure	7
		Information systems management	6
Military strategy and defence	13	*Response to attacks (terrorism,…)*	8
		Geopolotics and geostrategy	3
		Military strategy	2
Industrial engineering	11	*Industrial systems security*	4
		Knowledge management	3
		Production management	2
		Innovation management	1
		Logistics	1
		Project management	0
Construction and urbanism	11	*Urban networks security*	7
		Structure resistance	4
Economics	4	*Macroeconomics*	3
		Microeconomics	1
Physics	4	*Nuclear science*	1
		Chaos	1
		Electromagnetism	1
		Materials resistance	1
Applied mathematics	4	*Networks and graphs*	2
		Insurance modelling	2
Chemistry	1	*Chemical reaction*	1
Total	534		

Table I. Occurrences of the word *vulnerability* in the Web of Science publications in 2007

It must be noted that vulnerability seems to meet a growing interest in the scientific community as shown on Figure 1 below.

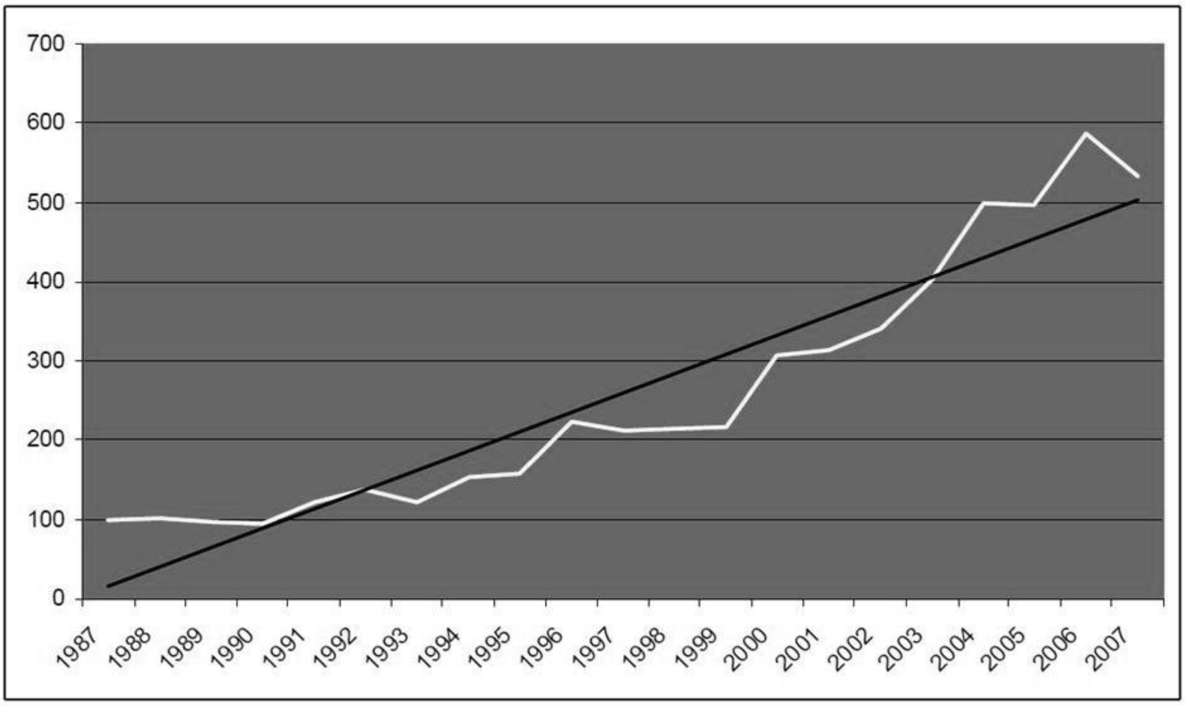


Figure 1. Web of Science publications the title of which contains the word *vulnerability* (1987-2007)

Some conclusions appear to be interesting, even at a first reading of this short survey of the Web of Science. Of these 534 publications, 86% were related to only two scientific topics (health, climatology and sustainable development) (Blaikie, Cameron et al. 2001). Moreover, this survey enlightens the lack of use of the concept of vulnerability in industrial engineering (only 11 publications out of 534; i.e. 2%), which motivates even more to work on this concept in accordance with project management principles.

But following the general trends of this short survey, the following state of the art is firstly carried out separately on the two most contributing topics: "health" and "climatology and sustainable development". Finally, it focuses on some works about vulnerability in the fields of industrial engineering and project management.

2.2. *Focus on the two most contributive fields: "health" and "climatology and sustainable development"*

As suggested by the short survey previously presented, a first literature review was conducted over research works dealing with health or climatology and sustainable development issues. First, it can be observed that some research works relate vulnerability to the presence of weaknesses (Luers, Lobell et al. 2003), (Scoones 1998), (Ellis 2000). These weaknesses can be of different nature, and can for instance impact the activities, assets and outcomes of a system, as shown by Figure 2 (Ellis 2003).

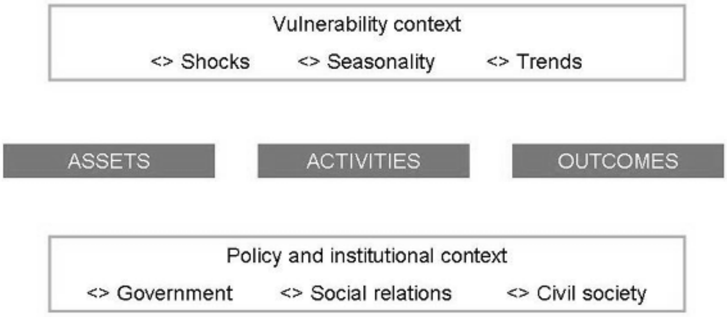


Figure 2. Vulnerability based on assets, activities and outcomes given a specific context (Ellis, 2003)

Second, other papers insist on an aspect of vulnerability, which is the coexistence of conditions of exposures to stresses / dangers and of a state of non-capacity to cope with them. This is notably the case of (Maskrey, 1989) with natural hazards, (Shi 2001) when adressing healthcare systems, or (Ezard, 2001) in the case of drug addiction. Particularly, several works detail the notion of exposure (Watts and Bohle 1993; Blaikie, Cannon et al. 1994), notably in contexts of crisis. This two-side aspect of vulnerability can be synthesized using the definition of Chambers (Chambers, 1983): vulnerability is “the exposure to contingencies and stress, and difficulty coping with them. Vulnerability has thus two sides: an external side of risk, shocks and stress to which an individual or household is subject; and an internal side which is defencelessness, meaning a lack of means to cope without damaging loss”. This expresses that damages (turned out consequences of risks) can be understood as the coincidence between a dangerous event and a vulnerable ground. This coexistence is notably modelled using stressor/receptor models, such as the one in Figure 3.

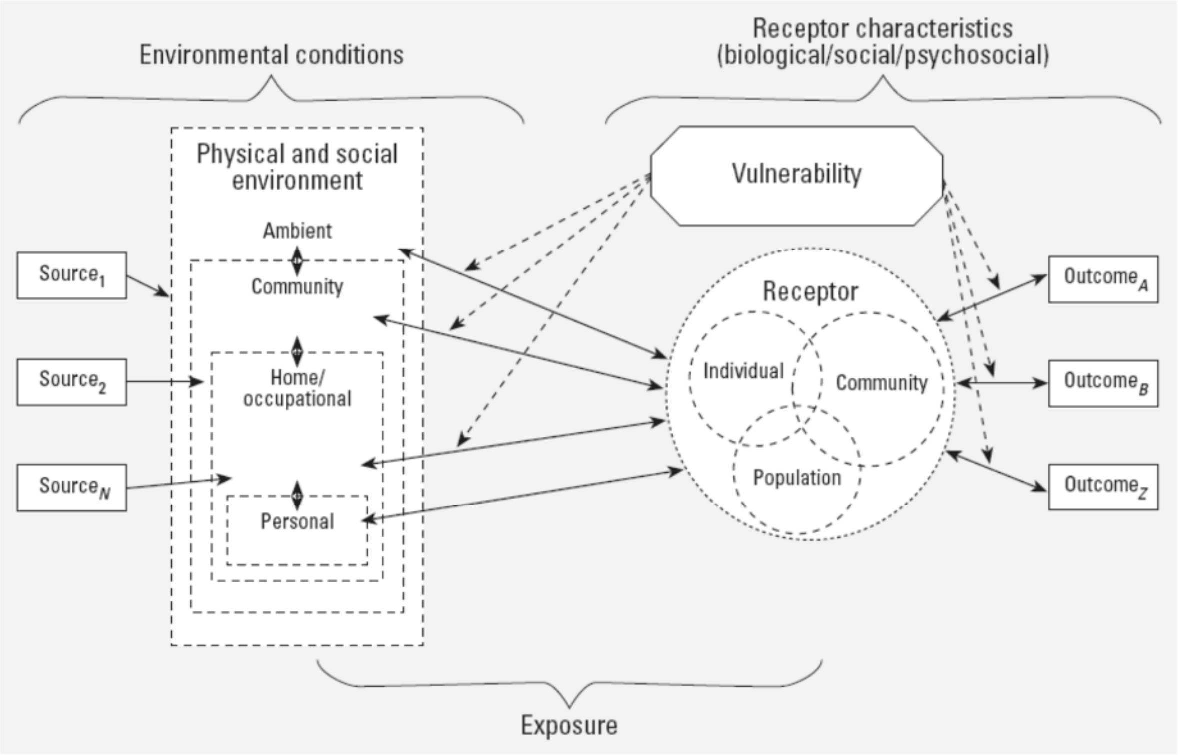


Figure 3. Vulnerability study thanks to a stressor/receptor model (de Fur, Evans et al. 2007)]

Moreover, other works detail the non-capacity to cope with possibly damaging events in terms of resistance and resilience, that is to say how individuals, groups or parts of a system can resist to vulnerability, instantly or when recovering (Perry, Dulio et al. 2006), (Dibben and Chester 1999), (Kelly and Adger 1999). Finally, it can also be oserved in the literature that vulnerability is in essence context-dependent as underlined by (Strauss 1997), (Ellis 2003) who insist on its evolution over time and its people-dependent perception.

2.3. Focus on industrial engineering, including project management

Theys underlines that in the field of industrial engineering and management, “there are still too few languages and tools for analysing vulnerability” (Theys 1987), which motivates to develop them. However, some attempts were already done, like for instance (Bogataj and Bogataj 2007) who place the notion of vulnerability at the centre of the value creation process, which is consistent with (Schneider 2008). In order to understand this possible degradations during the value creation process, systems thinking-based models were developed (Hellström 2007). Particularly, the works of Durand (Durand 2007), which follow a complex systems approach, define vulnerability as the “extent to which an organisation is able or not to cope with the dangers it is exposed to”. This work explains that working on the notion of vulnerability permits to focus on an organisation’s ability to resist to hazards and on the mechanisms that can weaken or strengthen its overall functioning, behaviour and evolution. This also underlines that possibly damaging events should be handled in accordance with their possible impact on the core values of a project (or a system), given its complex structure.

2.4. Synthesis: list of vulnerability characteristics

Before continuing, we propose to list down the main characteristics of vulnerability which can be synthesised after our state of the art:

- Vulnerability is in essence relative to a system which has weaknesses which can alter its trajectory to reach its objectives.
- Vulnerability corresponds to the coexistence of a level of exposure (or a susceptibility to be exposed) to stressors and a non-capacity level to cope with these stressors.
- Two aspects of the system's non-capacity are to be underlined:
  - Static vision: Resistance of the system regarding the apparition of the stressor.
  - Dynamic vision: Resilience of the receptor corresponding to the recovering of the system.
- A system's vulnerability is in essence context-dependent and evolves over time, notably because of the changes over time in the systems' characteristics due to its natural evolution and the apparition of stressors.

Each of these aspects is therefore to be present in the definition of project vulnerability or/and its associated models and tools.

3. Preliminary step: Defining the concept of project vulnerability and linking it with the concept of risk

Even though a lack of consensus can be observed around the notion of vulnerability (Luers, Lobell et al. 2003), the state of the art which was conducted led us to propose the following definition for project vulnerability. We claim that this concept permits to analyse a project system and focus on its existing weaknesses thanks to a systems thinking-based approach (Le Moigne 1990). Project vulnerability is then "the characteristic of a project which makes it susceptible to be subject to negative events and, if occurring, which makes it non capable to cope with them, which may in the end allow them to degrade the project values". Project non capability to cope with negative events when occurring includes non-resistance (instantaneous damages) and resilience (recovery over time). Moreover, project vulnerability exists if and only if project susceptibility to be subject to negative events and project non capability to cope with them coexist, i.e. if and only if they simultaneously exist at a given time.

As shown on Figure 4, project vulnerability is then linked with the traditional concept of project risk due to this coexistence possibility (linked to risk probability) and the damages which can occur (linked to risk impact).

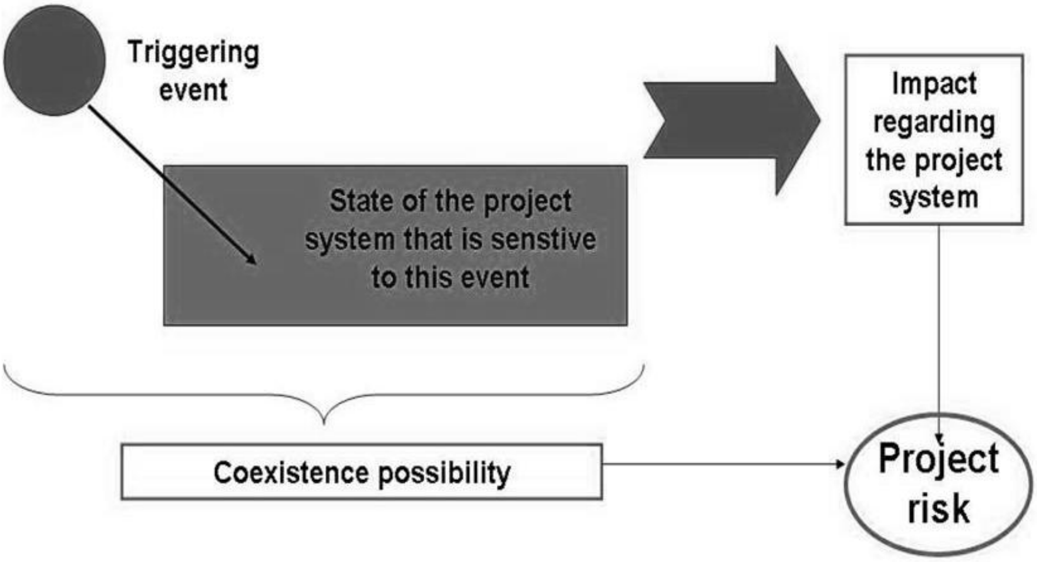

Triggering event
State of the project system that is senstive to this event
Impact regarding the project system
Coexistence possibility
Project risk

Figure 4. Project risk as an impact due to coexistence

As a whole, project performance degradation is the consequence of two coexistences. The first one conditions the apparition of vulnerability: coexistence of susceptibility to be subject to negative events and incapacity to cope with them if occurring. The second one is the temporal coincidence of a triggering event and a vulnerable ground for a risk to occur and to degrade the processes of values creation during the project.

Now that these coexistences are cleared, the aim of this work is to propose a systems thinking-based model of vulnerability to assist complex project risk management. The aspect of susceptibility is neglected in the following section since susceptibility is closely linked to probabilistic aspects of possible negative triggering events, which we do not aim at addressing here. The aim of the next section is to focus on the project system weaknesses and thus on the identification, evaluation and management of non-capabilities in terms of resistance and resilience. As a whole, this section thus proposes a paradigm shift since it focuses on the project system existing elements instead of focusing on possible events.

4. A methodology to model and manage project vulnerability

Our methodology to handle project vulnerability is the following:

- Project vulnerability identification
  - Identifying the objectives of the project in terms of values creation.
  - Identifying elementary vulnerable processes and elements of the project systems (vulnerable tasks, actors, resources, etc…).
- Project vulnerability analysis
  - Assigning a contribution rate of any of these elements to each value creation process.
  - Identifying possible triggering events which can damage a given project vulnerable element and analysing its resistance and resilience through a stressor/receptor model.
- Project vulnerability response plan to cure the weaknesses of the project system and prevent it from possible damages.
- Project vulnerability monitoring and control activity to watch over the project evolution.

As a whole, these four steps are to constitute the project vulnerability management process (Figure 5), which appears to be similar to the existing project risk management processes as defined in (IEC 1995; APM 1996; IEEE 2001; BSI 2002; AFNOR 2003; ISO 2003; PMI 2004; IPMA 2006). Each of them is developed in the following paragraphs.

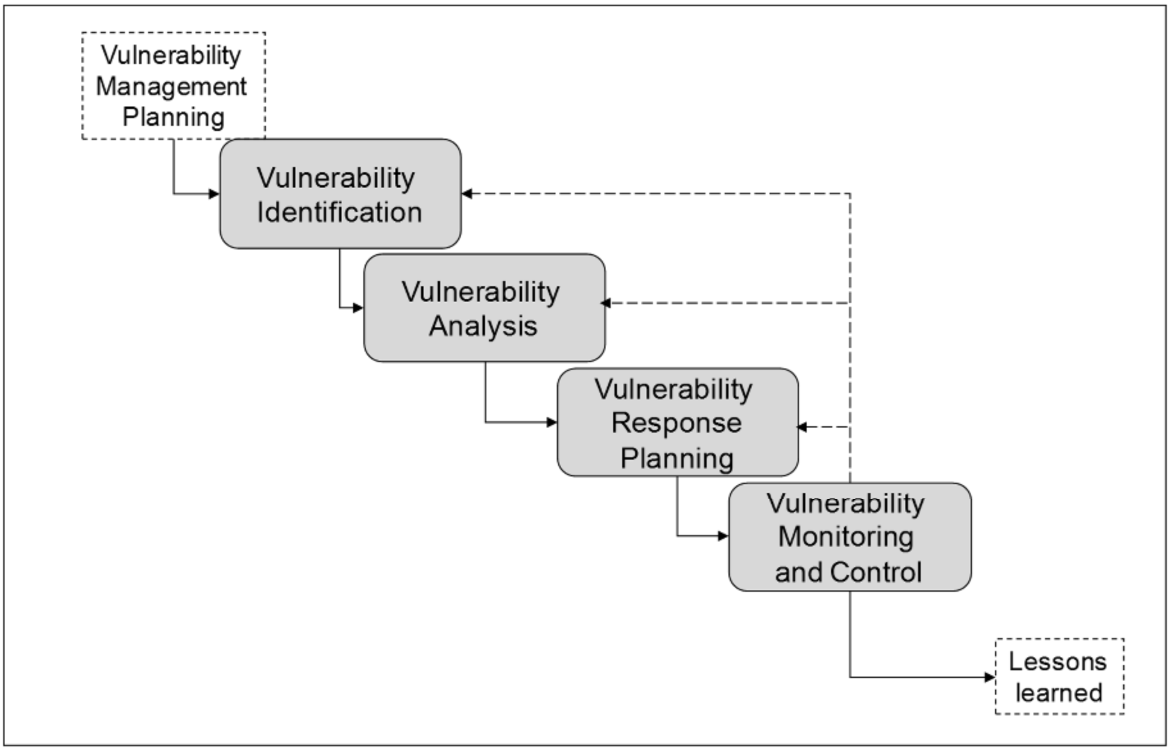

Vulnerability Management Planning
Vulnerability Identification
Vulnerability Analysis
Vulnerability Response Planning
Vulnerability Monitoring and Control
Lessons learned

Figure 5. The project vulnerability management process

4.1. The project vulnerability identification step

In order to identify properly project vulnerabilities, the use of systems thinking is proposed. It must be underlined that vulnerability permits to focus on the project system (its processes, elements, structure,…) which makes project vulnerability a more tangible concept than project risk. For all practical purposes, identifying project vulnerabilities means identifying the weaknesses of a project system which make its values creation vulnerable. In order to do so, a four step processes bases on the systems thinking (Le Moigne 1990; Genelot 2001; Vidal and Marle 2007; Vidal and Marle 2008) approach is proposed. Vulnerability is identified at three levels

- The teleological pole of the project system, which permits to identify the vulnerable stakes of the project (targeted created values).
- The functional pole of the project system, which permits to identify the vulnerable processes / tasks of the project system.
- The ontological pole of the project system, which permits to identify the vulnerable elements (actors, resources, inputs of processes, …) of the project system.

Then follows a reflexion on a stressor / receptor model to identify project process vulnerabilities which are defined as triplets (value, process, event) and project elementary vulnerabilities which are defined as triples (value, element, event).

This means that the genetic aspect (evolution of the project system) is also to be considered. Indeed, whenever the project phase changes, or whenever considerable changes in the project system occur during a project phase, the vulnerability identification process is to be performed again, or at least refined / updated. As a whole, this approach helps to reduce ambiguity and doubts on usefulness since everything is drawn by the final objectives of the project, that is to say values creation.

4.1.1. Identification of vulnerable values, processes and elements through systems thinking

A project is vulnerable if and only if one of its objective values may not reach its target. That is why we argue that project vulnerability should be addressed regarding each value of a given project, in order to underline the different possible kinds of damages within the project. In the end, the first deliverable of the project vulnerability identification step is a three-level hierarchical structure composed of (see Figure 6):

- The project values which are likely to be damaged and make thus the project vulnerable regarding them.

- For each value V_i, the project processes/tasks which contribute to V_i creation. These processes are likely to be altered (and thus to be vulnerable) by negative events, which makes as a consequence the project vulnerable regarding $V_{i.}$
- For each process P_{ij}, the project elements which permit to perform P_{ij} (actors, resources, other inputs). These elements are likely to be altered (and thus to be vulnerable) by negative events, which alters P_{ij}, which makes as a consequence the project vulnerable regarding $V_{i.}$

An arborescence is thus built to classify project vulnerable values, processes and elements as shown hereunder on Figure 6. One should note that this decomposition is analogous to the one mentioned in 2.2 and proposed in (Ellis 2003) in terms of outcomes (values), activities (processes) and assets (project elements).

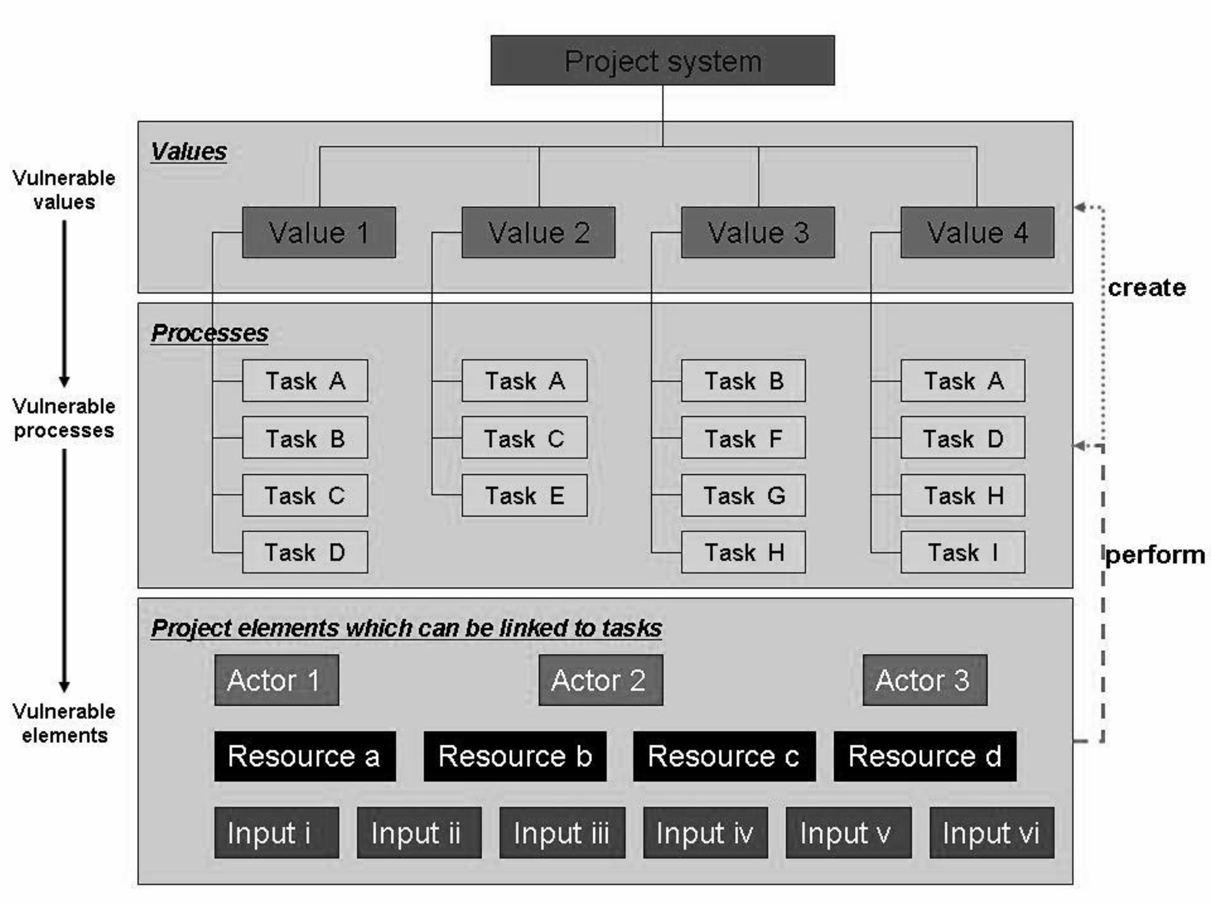


Figure 6. Levels in the project vulnerability identification step

However, some work is still to be done to identify project vulnerabilities as one can talk of vulnerability only if mentioning the event something is vulnerable to.

4.1.2. Identification of process and elementary vulnerabilities

Let (V_1, V_2, …, V_n) be the set of values created by the project. For each V_i, we have identified the corresponding vulnerable project processes and elements. Each value V_i can be weighted by a coefficient α_i which permits to set priorities in the values creation processes (the sum of all these coefficients is equal to 1). If $\alpha_i > \alpha_j$, then project vulnerability regarding value V_i is all the more important to control than project vulnerability regarding value V_j since the creation of V_i is preferred to the one of V_j. Such weights are notably to be set by project stakeholders, by the project management office or by the firm, notably thanks to the consideration of strategic or tactical aspects.

Given a value V_i, as mentioned before, there are several project processes/tasks (P_{i1}, P_{i2}, …, P_{ip}) which contribute to V_i creation. In the same manner, the project manager, the project team or external experts can permit to determine weights β_{ij} which permit to determine the importance of each task regarding V_i creation (for each i, the sum of all β_{ij} is equal to 1). At this stage, one should particularly notice that tasks can contribute to several values creation processes.

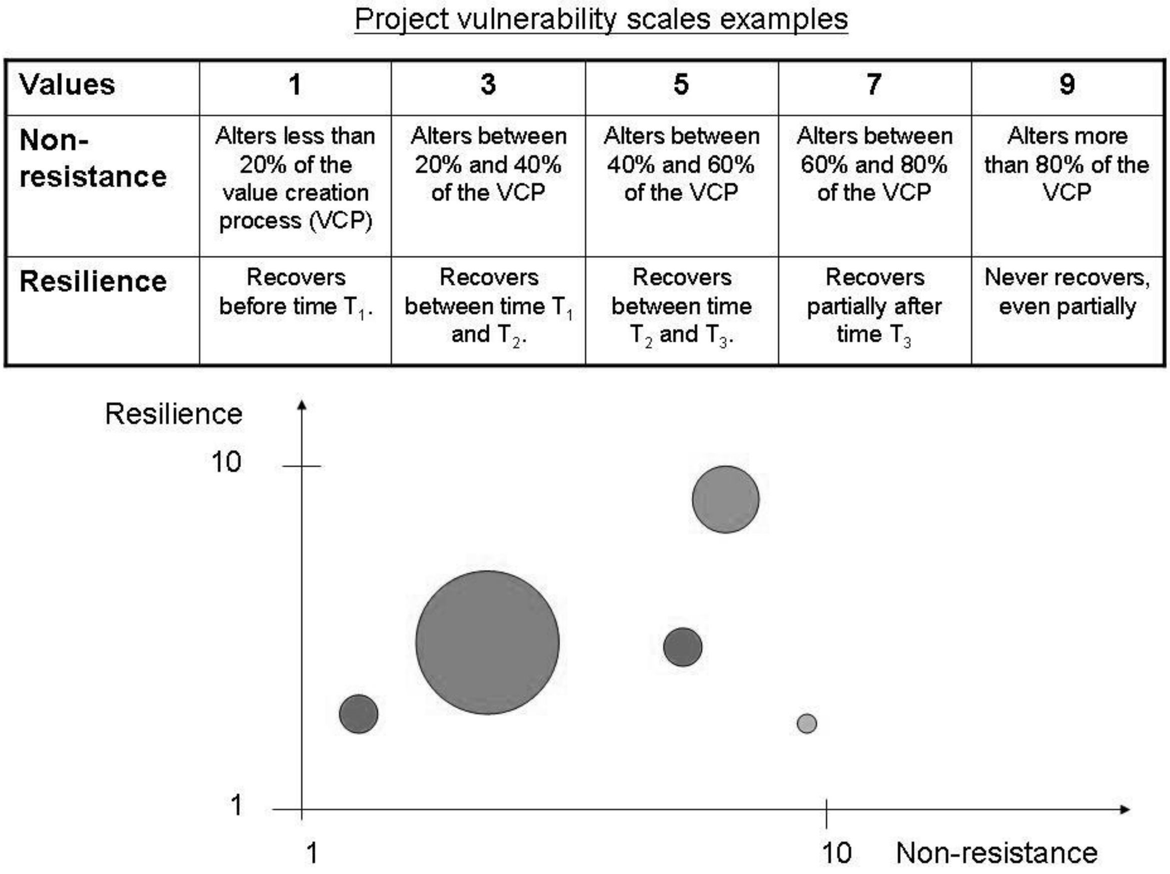
The same work can be done on every category of project elements. In the end, determining all the weights in the hierarchical structure (by expertise or experience) permits to determine the maximum possible degradation linked to a project element/process if it is altered. This first analysis thus permits to neglect aspects which can be neglected due to their low implications in possible damages regarding values creation. This is all the more important to perform since the combinatorial aspects of project vulnerability identification are likely to be very important.

Once refined, we claim for the use of a stressor / receptor model to identify key project vulnerabilities, that is to say key project process vulnerabilities which are triplets (value, process, event) and key project elementary vulnerabilities which are triplets (value, element, event). The first steps of the identification process permitted to identify project values, processes and elements and to refine their lists thanks to issues about contribution rates to values creation. This work now proposes that, given a process or element, one focuses on this process / element as a receptor and tries to list down as exhaustively as possible the possible negative events it may be exposed to (that is to say its potential stressors). This aspect is to be performed thanks to the conjoint use of expertise and experience. We may recommend here the use of some creativity methods such as brainstorming, dissociation or inversion. As a whole, an initial list of project process and elementary vulnerabilities is done. Identifying project vulnerabilities is in itself a first result. However, one should be able to evaluate/analyse them in order to manage them better.

4.2. The project vulnerability analysis step

Once the set of project process or elementary vulnerabilities is identified, theses ones are to be analysed regarding the two principal aspects of vulnerability in terms of non-capability, that is to say resistance and resilience. In order to do so, objective scales should be built up.

A first tool is proposed: objective 1 to 10 Likert scales should be built by experts, like in the risk analysis process when performing the evaluation of probability and impact (see examples in Figure 7). This figure also shows how synthetic diagrams (non-resistance and resilience on axes, contribution rate to the project value V as the diameter of the circle) can be built to highlight principal project vulnerabilities. We recommend that in a diagram, there should be only the project vulnerabilities which correspond to a same value possible degradation, so that the analysis of this diagram is of interest for management use.



Project vulnerability scales examples

Values	1	3	5	7	9
Non-resistance	Alters less than 20% of the value creation process (VCP)	Alters between 20% and 40% of the VCP	Alters between 40% and 60% of the VCP	Alters between 60% and 80% of the VCP	Alters more than 80% of the VCP
Resilience	Recovers before time T_1.	Recovers between time T_1 and T_2.	Recovers between time T_2 and T_3.	Recovers partially after time T_3	Never recovers, even partially

Figure 7. Project vulnerability analysis

In the end, a global index can be calculated in order to give a simple indicator to rank project vulnerabilities regarding a project value V. Let CR(V) be the contribution rate (percentage of the project value) of the vulnerable element/process which is addressed. Let NR be the evaluation of its non resistance. Let R be the evaluation of its resilience. Then, a synthetic aggregated measure (which can help to underline higher priority vulnerabilities), which we name the Crucial Index Γ(V), is given by the following equation (Γ(V) varies between 0 and 100).

$$\Gamma(V) = NR \times R \times CR(V)$$

As during any aggregation operation, part of information is lost. Indeed, several different triplets can have the same value when multiplying the values of its elements. As a consequence, when ranking according to the Γ(V) index, one may rank at the same level several triplets which could not be handled the same way (for example high non-resistance and low resilience versus low resilience and high non-resistance with the same value of Γ(V)). In the end, this classification according to Γ(V) should always be considered with the initial evaluation of NR, R and CR(V) in order to make more relevant decisions during the project vulnerability response plan step.

4.3. The project vulnerability response plan step

The project vulnerability response plan step permits to decide on the actions which are needed to reduce the threat of the existence of project process or elementary vulnerabilities. The project vulnerability response is to determine the overall strategy for strengthening a project. As in the risk management process (PMI 2004), even though slightly different, there are five basic strategies to cope with project vulnerabilities.

4.3.1. Mitigation

Mitigation is the strategy which consists in making decisions in order to improve the resistance of the project processes / elements and / or to lessen their resilience regarding negative triggering events. Another strategy would be to diminish the contribution rate of the process / element to the value creation but whenever possible, this strategy is to be classified under the name of transfer since contributions are transferred to other entities.

4.3.2. Avoidance

Avoidance is the strategy which consists in making decisions in order to eliminate totally project vulnerabilities. The reader should note that for project risk management, there are two ways to avoid risks (reducing to 0 probability or impact) but there is only one way to avoid vulnerability (reducing to 0 non-resistance). Indeed, resilience has no direct impact on avoidance since resilience underlines a dynamical aspect (evolution over time).

4.3.3. Transfer

Transfer is a strategy which consists in making decisions in order to transfer project vulnerabilities to other project processes/elements which have less influence in the values creation processes. This strategy is really different than the transfer strategy in the project risk management process which consists in the transfer of the risk responsibility to a third party.

Here, vulnerabilities exist within the project system and there is no reason to transfer them to third parties which would be external to the system (however, one should note that decisions can still be made to transfer the final risk responsibility to any of the project stakeholders). However, transfer strategies can be defined within the project. For instance, if an actor appears to be vulnerable, then one can choose, whenever possible, to transfer this actor to other processes which have less impact on the creation of project values. The transfer strategy is thus the strategy which proposes to handle contribution rates (to the corresponding value creation) as potential levers for vulnerability reduction.

4.3.4. Acceptance

Acceptance is a strategy which is notably designated for low resilience and high resistance project vulnerabilities. It consists in saying that little or nothing can be done expect letting things run their course, knowing that these low Crucial Index vulnerabilities however exist.

4.3.5. Contingence

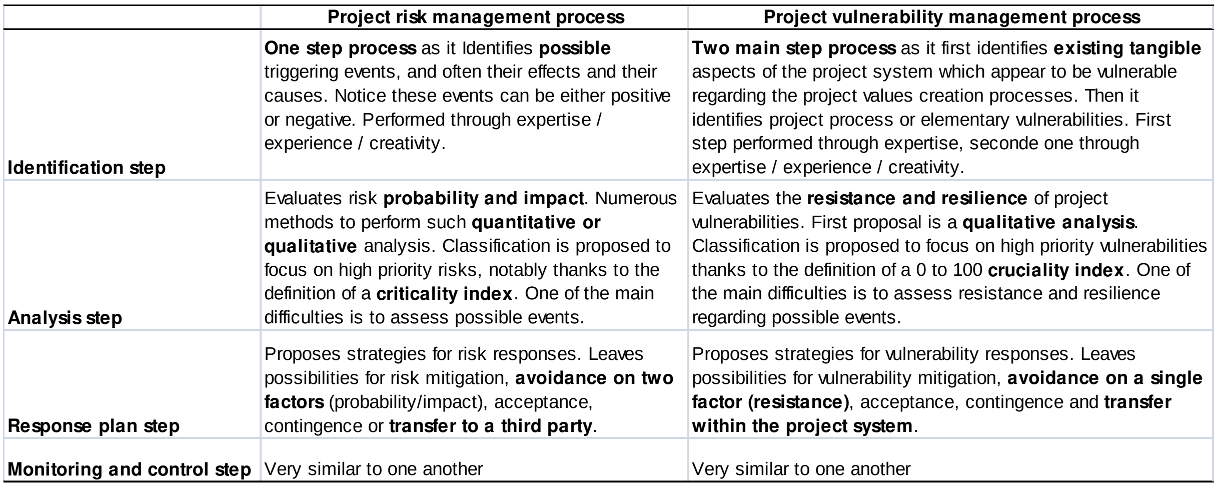
Contingence response is an intermediary manner to cope with vulnerabilities. It is associated with the one of the other strategies (especially mitigation) and determines the actions which should be done if the chosen vulnerability response should fail.

4.4. The project vulnerability monitoring and control step

In essence, a project system is evolving, which means that project vulnerabilities do not remain static. New vulnerabilities may pop up, the characteristics of project vulnerabilities may change or vulnerability responses may not have the effects which were planned. Vulnerabilities are then to be re-identified and re-assessed during the project, since they refer to a project system which is in essence in constant evolution.

4.5. Synthesis : comparison with the project risk management process

Table II. proposes a critical comparison of the project risk management process and the project vulnerability management process.



	Project risk management process	Project vulnerability management process
Identification step	**One step process** as it Identifies **possible** triggering events, and often their effects and their causes. Notice these events can be either positive or negative. Performed through expertise / experience / creativity.	**Two main step process** as it first identifies **existing tangible** aspects of the project system which appear to be vulnerable regarding the project values creation processes. Then it identifies project process or elementary vulnerabilities. First step performed through expertise, seconde one through expertise / experience / creativity.
Analysis step	Evaluates risk **probability and impact**. Numerous methods to perform such **quantitative or qualitative** analysis. Classification is proposed to focus on high priority risks, notably thanks to the definition of a **criticality index**. One of the main difficulties is to assess possible events.	Evaluates the **resistance and resilience** of project vulnerabilities. First proposal is a **qualitative analysis**. Classification is proposed to focus on high priority vulnerabilities thanks to the definition of a 0 to 100 **cruciality index**. One of the main difficulties is to assess resistance and resilience regarding possible events.
Response plan step	Proposes strategies for risk responses. Leaves possibilities for risk mitigation, **avoidance on two factors** (probability/impact), acceptance, contingence or **transfer to a third party**.	Proposes strategies for vulnerability responses. Leaves possibilities for vulnerability mitigation, **avoidance on a single factor (resistance)**, acceptance, contingence and **transfer within the project system**.
Monitoring and control step	Very similar to one another	Very similar to one another

Table II. Comparison between project risk and vulnerability management processes

As a whole, this approach may diminish the observed (in fieldwork) reluctance to risk management processes as vulnerability management processes focus on existing tangible aspects of the project. When possible risks were underlined before, existing weaknesses of the project are stressed thanks to this approach. In the end, the vulnerability response plan may thus appear more relevant as the responses directly focus on the project system instead of dealing with probabilistic events. The required efforts (notably in terms of time and money) for these responses may thus appear more necessary, for existing project weaknesses are underlined.

5. Case study

A case study is performed during the FabACT project (Vidal, Sahin et al. 2009), a software development project within the context of the pharmaceutical industry. This project was executed in collaboration with the Georges Pompidou European Hospital.

5.1. Introduction

The French health system faces ever growing demands under very pressuring conditions as it is much constrained in a complex environment. In our case, production volumes at the chemotherapy compounding unit (UPIO) have drastically increased (5% in a two years time). To support this increasing workload without extra staff, pharmacists wanted to evaluate how anticipating the production of certain drugs may help them in improving the organisation of the production process.Within this context, the FabACT project (Figure 8) has been launched at HEGP Pharmacy department in 2006. The aim was to achieve a better balance between the workload and the ability to hold the admixture compounding burden while respecting constraints such as drug stability and quality of service. The deliverable of the FabACT project was a decision support tool in order to assist pharmacists while choosing the anti-cancer drugs that can be produced in advance. Due to the sensitivity of this project, its vulnerabilities were studied.

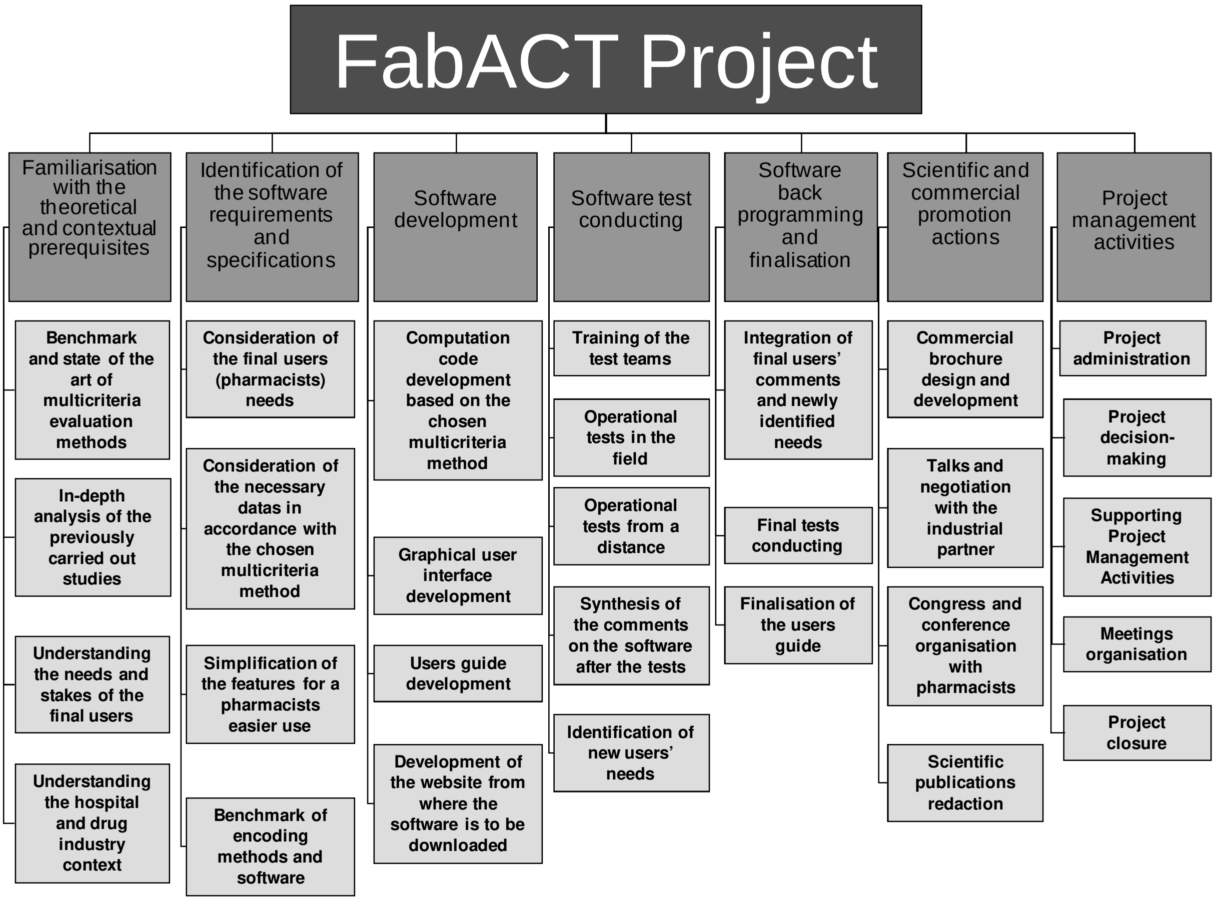

FabACT Project
Familiarisation with the theoretical and contextual prerequisites
Benchmark and state of the art of multicriteria evaluation methods
In-depth analysis of the previously carried out studies
Understanding the needs and stakes of the final users
Understanding the hospital and drug industry context
Identification of the software requirements and specifications
Consideration of the final users (pharmacists) needs
Consideration of the necessary datas in accordance with the chosen multicriteria method
Simplification of the features for a pharmacists easier use
Benchmark of encoding methods and software
Software development
Computation code development based on the chosen multicriteria method
Graphical user interface development
Users guide development
Development of the website from where the software is to be downloaded
Software test conducting
Training of the test teams
Operational tests in the field
Operational tests from a distance
Synthesis of the comments on the software after the tests
Identification of new users' needs
Software back programming and finalisation
Integration of final users' comments and newly identified needs
Final tests conducting
Finalisation of the users guide
Scientific and commercial promotion actions
Commercial brochure design and development
Talks and negotiation with the industrial partner
Congress and conference organisation with pharmacists
Scientific publications redaction
Project management activities
Project administration
Project decision-making
Supporting Project Management Activities
Meetings organisation
Project closure

Figure 8. Work Breakdown Structure of the FabACT project

5.2. *Results and discussion*

5.2.1. Identification of project vulnerabilities

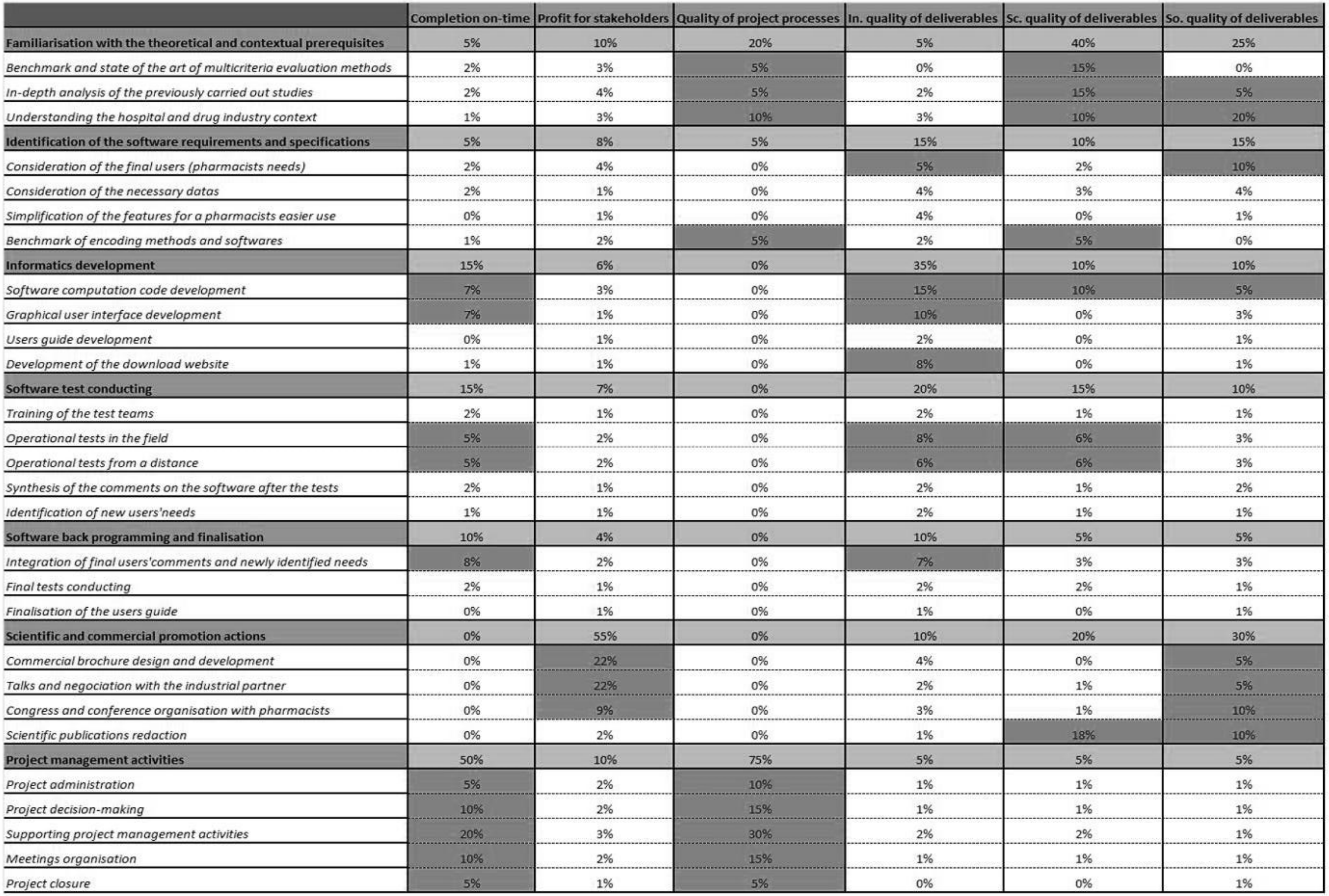
The project values were listed as the following ones:

- Completion of the project on time
- Profit due to the project
- Quality of project processes
- Industrial, scientific and societal quality of project deliverables, which are mainly influenced by
  - ❖ Rigor of the scientific approach. (Sc)
  - ❖ Reliability of the result. (In) (Sc) (So)

- Adjustement of the software to the hospital and drug production context. (In) (So)
- Friendliness and easiness of understanding and use of the software. (In)
- Compatibility with existing computer equipments in hospital pharmacies. (In)
- Number and quality of scientific publications, congresses and conferences. (Sc) (So)
- Number of conference and congresses organised for industrials. (In) (So)

By going back to processes and tasks, it is possible to build up a table which synthesises the contribution of any task to any of theses values creation (Table III). This table permits, as suggested, to refine the analysis of fewer tasks / processes and project elements (corresponding to theses tasks and processes) when performing the project vulnerability analysis.

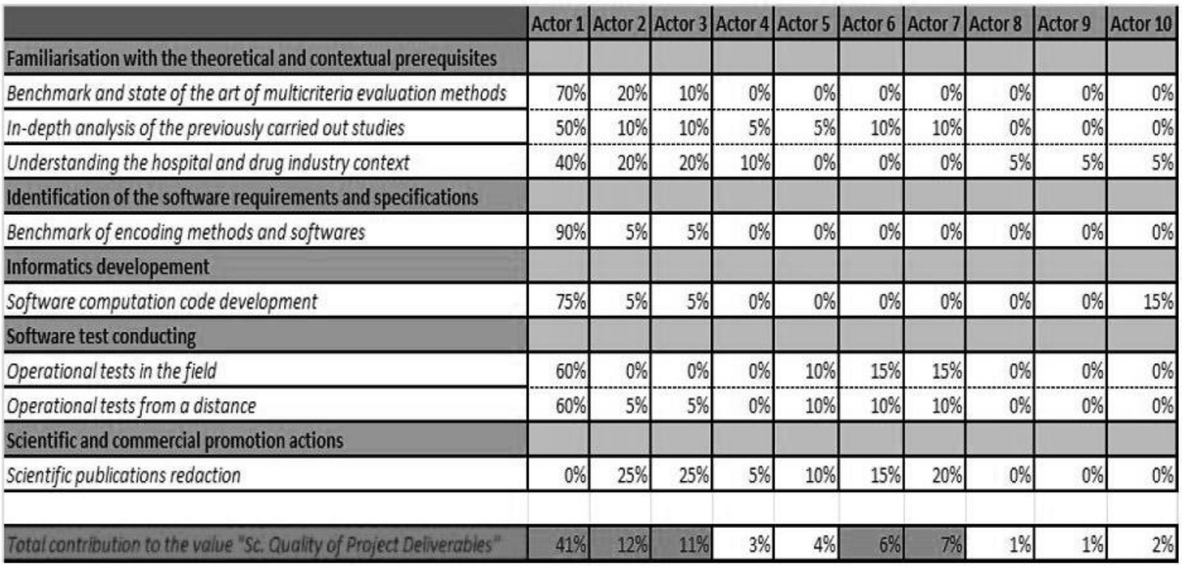
Table III. Identifying project tasks contribution to project values creation



	Completion on-time	Profit for stakeholders	Quality of project processes	In. quality of deliverables	Sc. quality of deliverables	So. quality of deliverables
Familiarisation with the theoretical and contextual prerequisites	5%	10%	20%	5%	40%	25%
Benchmark and state of the art of multicriteria evaluation methods	2%	3%	5%	0%	15%	0%
In-depth analysis of the previously carried out studies	2%	4%	5%	2%	15%	5%
Understanding the hospital and drug industry context	1%	3%	10%	3%	10%	20%
Identification of the software requirements and specifications	5%	8%	5%	15%	10%	15%
Consideration of the final users (pharmacists needs)	2%	4%	0%	5%	2%	10%
Consideration of the necessary datas	2%	1%	0%	4%	3%	4%
Simplification of the features for a pharmacists easier use	0%	1%	0%	4%	0%	1%
Benchmark of encoding methods and softwares	1%	2%	5%	2%	5%	0%
Informatics development	15%	6%	0%	35%	10%	10%
Software computation code development	7%	3%	0%	15%	10%	5%
Graphical user interface development	7%	1%	0%	10%	0%	3%
Users guide development	0%	1%	0%	2%	0%	1%
Development of the download website	1%	1%	0%	8%	0%	1%
Software test conducting	15%	7%	0%	20%	15%	10%
Training of the test teams	2%	1%	0%	2%	1%	1%
Operational tests in the field	5%	2%	0%	8%	6%	3%
Operational tests from a distance	5%	2%	0%	6%	6%	3%
Synthesis of the comments on the software after the tests	2%	1%	0%	2%	1%	2%
Identification of new users'needs	1%	1%	0%	2%	1%	1%
Software back programming and finalisation	10%	4%	0%	10%	5%	5%
Integration of final users'comments and newly identified needs	8%	2%	0%	7%	3%	3%
Final tests conducting	2%	1%	0%	2%	2%	1%
Finalisation of the users guide	0%	1%	0%	1%	0%	1%
Scientific and commercial promotion actions	0%	55%	0%	10%	20%	30%
Commercial brochure design and development	0%	22%	0%	4%	0%	5%
Talks and negociation with the industrial partner	0%	22%	0%	2%	1%	5%
Congress and conference organisation with pharmacists	0%	9%	0%	3%	1%	10%
Scientific publications redaction	0%	2%	0%	1%	18%	10%
Project management activities	50%	10%	75%	5%	5%	5%
Project administration	5%	2%	10%	1%	1%	1%
Project decision-making	10%	2%	15%	1%	1%	1%
Supporting project management activities	20%	3%	30%	2%	2%	1%
Meetings organisation	10%	2%	15%	1%	1%	1%
Project closure	5%	1%	5%	0%	0%	1%

We identify the tasks which have significant contribution rates regarding the creation of this value (over 10% in orange, over 5% in yellow). Only the vulnerability of these tasks is then to be analysed further as a first result since if other tasks are altered because of their vulnerability, they can in the worst case alter less than 5% of the scientific quality of the project deliverables. This step is absolutely necessary in order to lessen the combinatorial aspects of a project vulnerability study.

In order to close the vulnerability identification steps, we then identify the project elements which contribute to the identified tasks. In the same manner, contribution rates tables can be built. The reader will find an example of such a table of elementary vulnerabilities in Table IV (for the creation of high scientific quality deliverables). In the end, a list of vulnerable tasks and associated project elements (here actors) is built. This list is to be analysed in the following step as an illustration on how to perform project vulnerability analysis.



	Actor 1	Actor 2	Actor 3	Actor 4	Actor 5	Actor 6	Actor 7	Actor 8	Actor 9	Actor 10
Familiarisation with the theoretical and contextual prerequisites										
Benchmark and state of the art of multicriteria evaluation methods	70%	20%	10%	0%	0%	0%	0%	0%	0%	0%
In-depth analysis of the previously carried out studies	50%	10%	10%	5%	5%	10%	10%	0%	0%	0%
Understanding the hospital and drug industry context	40%	20%	20%	10%	0%	0%	0%	5%	5%	5%
Identification of the software requirements and specifications										
Benchmark of encoding methods and softwares	90%	5%	5%	0%	0%	0%	0%	0%	0%	0%
Informatics developement										
Software computation code development	75%	5%	5%	0%	0%	0%	0%	0%	0%	15%
Software test conducting										
Operational tests in the field	60%	0%	0%	0%	10%	15%	15%	0%	0%	0%
Operational tests from a distance	60%	5%	5%	0%	10%	10%	10%	0%	0%	0%
Scientific and commercial promotion actions										
Scientific publications redaction	0%	25%	25%	5%	10%	15%	20%	0%	0%	0%
Total contribution to the value "Sc. Quality of Project Deliverables"	41%	12%	11%	3%	4%	6%	7%	1%	1%	2%

Table IV. Identifying the actors which contribute more to the tasks which make the project vulnerable regarding scientific quality creation

5.2.2. Analysis of project vulnerabilities

We now study resilience and resistance in order to quantify their weakness regarding possible negative events.

For instance, one can perform it here on the identified project actors which make the project potentially vulnerable regarding the creation of high scientific quality deliverables. We obtained a list of five actors which contribute significantly to this value creation: ACTOR 1, ACTOR 2, ACTOR 3, ACTOR 6, ACTOR 7. These actors are the ones to be watched over because of their potential impact on the targeted value creation if their usual behaviour during the project is altered. One is to find hereunder an excerpt of the FabACT project actor vulnerability analysis (Table V). The project actor vulnerabilities are ranked according to their Crucial Index Γ(V).

Value	Element	CR(V)	Event	NR	R	Γ(V)
Scientific Quality	Actor 1	0,41	Unclear software requirements and specifications	8	8	26,24
Scientific Quality	Actor 1	0,41	Error when encoding the software	6	8	19,68
Scientific Quality	Actor 1	0,41	New requirements appearing	8	6	19,68
Scientific Quality	Actor 1	0,41	Bad communication within the project team	6	6	14,76
Scientific Quality	Actor 1	0,41	Misunderstanding of previously carried out studies	6	6	14,76
Scientific Quality	Actor 1	0,41	Lack of information	8	4	13,12
Scientific Quality	Actor 1	0,41	Uncorrect information	7	4	11,48
Scientific Quality	Actor 2	0,12	Unclear software requirements and specifications	8	8	7,68
Scientific Quality	Actor 3	0,11	Unclear software requirements and specifications	7	8	6,16
Scientific Quality	Actor 2	0,12	Illness	7	7	5,88
Scientific Quality	Actor 2	0,12	New requirements appearing	8	6	5,76
Scientific Quality	Actor 7	0,07	Misunderstanding of the publication target requirements	9	9	5,67
Scientific Quality	Actor 7	0,07	Unclear software requirements and specifications	9	8	5,04
Scientific Quality	Actor 1	0,41	Too short test phase	6	2	4,92
Scientific Quality	Actor 6	0,06	Misunderstanding of the publication target requirements	9	9	4,86
Scientific Quality	Actor 3	0,11	New requirements appearing	7	6	4,62
Scientific Quality	Actor 7	0,07	Misunderstanding of previously carried out studies	9	7	4,41
Scientific Quality	Actor 2	0,12	Misunderstanding of the publication target requirements	4	9	4,32
Scientific Quality	Actor 6	0,06	Unclear software requirements and specifications	9	8	4,32

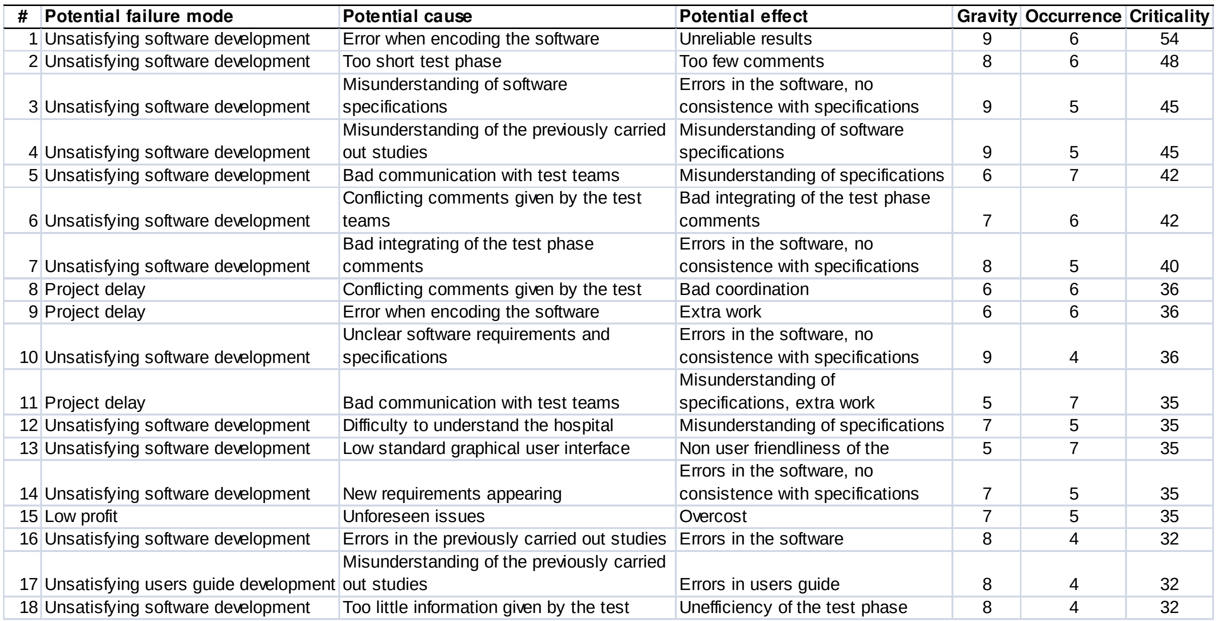
Table V. Excerpt of the FabACT project actor vulnerability analysis

5.2.3. Vulnerability response plan

This analysis underlines here that ACTOR 1 is the most vulnerable one regarding scientific quality creation during the project. The vulnerability response plan should therefore focus on the accompaniment of this actor in order to guarantee its performance regarding value creation or it should propose transfer strategies which transfer some tasks to less vulnerable actors. This analysis permits to underline that ACTOR 1 is particularly vulnerable to problems regarding the requirements of the software (whether they are unclear, changing or potentially misunderstood). As a consequence, this underlines that particular attention should be given to the definition of requirements and specifications as they are likely to condition. Other specific attention should be paid to the event “misunderstanding of the publication target requirements” since it directly impacts several actors in the FabACT project regarding scientific quality creation. This can be understood since the FabACT project is at the meeting point of industrial engineering and pharmacy and that publication targets requirements may not always be clear in the possible integration of articles dealing about this issue in the corresponding journal or revue.

5.2.4. Comparison with a traditional risk management process

Once can find hereunder an excerpt of a traditional FMECA performed for the FabACT project (Table VI) to be a point of comparison in order to underline the potential benefits of a project vulnerability analysis.



#	Potential failure mode	Potential cause	Potential effect	Gravity	Occurrence	Criticality
1	Unsatisfying software development	Error when encoding the software	Unreliable results	9	6	54
2	Unsatisfying software development	Too short test phase	Too few comments	8	6	48
3	Unsatisfying software development	Misunderstanding of software specifications	Errors in the software, no consistence with specifications	9	5	45
4	Unsatisfying software development	Misunderstanding of the previously carried out studies	Misunderstanding of software specifications	9	5	45
5	Unsatisfying software development	Bad communication with test teams	Misunderstanding of specifications	6	7	42
6	Unsatisfying software development	Conflicting comments given by the test teams	Bad integrating of the test phase comments	7	6	42
7	Unsatisfying software development	Bad integrating of the test phase comments	Errors in the software, no consistence with specifications	8	5	40
8	Project delay	Conflicting comments given by the test	Bad coordination	6	6	36
9	Project delay	Error when encoding the software	Extra work	6	6	36
10	Unsatisfying software development	Unclear software requirements and specifications	Errors in the software, no consistence with specifications	9	4	36
11	Project delay	Bad communication with test teams	Misunderstanding of specifications, extra work	5	7	35
12	Unsatisfying software development	Difficulty to understand the hospital	Misunderstanding of specifications	7	5	35
13	Unsatisfying software development	Low standard graphical user interface	Non user friendliness of the	5	7	35
14	Unsatisfying software development	New requirements appearing	Errors in the software, no consistence with specifications	7	5	35
15	Low profit	Unforeseen issues	Overcost	7	5	35
16	Unsatisfying software development	Errors in the previously carried out studies	Errors in the software	8	4	32
17	Unsatisfying users guide development	Misunderstanding of the previously carried out studies	Errors in users guide	8	4	32
18	Unsatisfying software development	Too little information given by the test	Unefficiency of the test phase	8	4	32

Table VI. Excerpt of the FMECA of the FabACT project

First, one should notice that the lack of integration of project values does not permit to understand properly the consequences of the potential failure modes, even though there effects are likely to be mentioned. Vulnerability analysis permits to understand better the possible damage chains which exist within a project. It must be noticed that for instance, no aspect about publication target requirements had been mentioned in the FMECA although it appeared to be a high potential source of vulnerability regarding scientific quality creation. Second, by analysing the project system's weaknesses, one is to make better and more specific decisions when establishing a response plan. Indeed, the FMECA mentions "unclear software requirements and specifications" or "misunderstanding of software specifications" as potential causes of important failure modes. This is consistent with the project vulnerability analysis which was performed. However, the project vulnerability analysis permits to focus on the project elements or processes which are impacted the most by this potential cause / stressor event. For instance, actors did not appear equally vulnerable to these events, which permitted to concentrate on the weakest parts / actors / processes of the project.

6. Conclusions and perspectives

As a whole, this article presents an innovative way to assist project risk management through the integration of the concept of project vulnerability. This concept permits to analyse a project system and focus on its existing weaknesses thanks to a systems thinking-based approach. After proposing a definition and a description of project vulnerability, a proposition to describe the project vulnerability management process into four successive steps is done. The reader should remind them as a first proposal to perform project vulnerability analysis:

This project vulnerability management process permits to concentrate directly on the existing weaknesses of a project system which may create potential damages regarding the project values creation. By focusing on this system, response plans may be more adapted to the existing lacks of the project, as shown by the case study with the FabACT project. Such focus on the system is to be of great interest for project managers and project teams. When before there was ambiguity or lack of confidence in dealing with potential events and potential impacts, vulnerability management permits to point out the weaknesses of a project. Attention should however be paid on vulnerability communication so that it is not seen as a way to underline low performance elements or actors in a project. Vulnerability management must therefore be highlighted as a promising tool for complex project performance management as it permits a more effective and efficient accompaniment of project teams thanks to a better understanding of possible damage creation within complex project systems. Some aspects of this work may however be discussed. We thus identify several research perspectives to consolidate the proposals of this chapter:

- First, the susceptibility aspect of vulnerability is neglected in this first approach of project vulnerability management. Future research work may explore this concept.
- Moreover, the calculation of the Crucial Index $\Gamma(V)$ is to be improved thanks to the integration of multicriteria aspects
- Other promising works may focus on the evaluation of the non-resistance and resilience of project vulnerabilities, notably thanks to the introduction of interdependences which exist in complex project systems.

7. References

AFNOR (2003). FD X 50-117: Management de projet, Gestion du risque, Management des risques d'un projet, AFNOR.

APM (1996). Project Risk Analysis & Management (PRAM) Guide. High Wycombe, ASSOCIATION FOR PROJECT MANAGEMENT.

Blaikie, P., J. Cameron, et al. (2001). Nepal in Crisis: Growth and Stagnation at the Periphery, Adroit Publishers, New Delhi, India.

Blaikie, P., T. Cannon, et al. (1994). At risk, Routledge.

Bogataj, D. and M. Bogataj (2007). "Measuring the supply chain risk

and vulnerability in frequency space." International Journal of Production Economics **108**(1-2): 291-301.

BSI (2002). ISO/IEC Guide 73:2002. Risk Management – Vocabulary – Guidelines for use in standards. London, BRITISH STANDARD INSTITUTE.

de Fur, P. L., G. W. Evans, et al. (2007). "Vulnerability as a Function of Individual and Group Resources in Cumulative Risk Assessment " Environmental Health Perspectives **115**(5).

Dibben, C. and D. K. Chester (1999). "Human vulnerability in volcanic environments: the case of Furnas, Sao Miguel, Azores." Journal of Volcanology and Geothermal Research **92**: 133-150.

Durand, J. (2007). Management des risques dans les organisations industrielles complexes: prépondérance de la dimension managériale dans la genèse des vulnérabilités, Thèse de Doctorat de l'Ecole Centrale de Paris, Paris, France.

Ellis, F. (2000). Rural Livelihoods and Diversity in Developing Countries. Oxford, UK, Oxford University Press.

Ellis, F. (2003). Human Vulnerability and Food Insecurity:Policy Implications

Forum for Food Security in Southern Africa.

Genelot, D. (2001). Manager dans la complexité – Réflexions à l'usage des dirigeants. Paris, INSEP Consulting Editions.

Hellström, T. (2007). "Critical infrastructure and systemic vulnerability :

Towards a planning framework." Safety science **45**(3): 415-430.

IEC (1995). CEI/IEC 300-3-9:1995 Risk Management: part 3 – guide to risk analysis of technological systems. Geneva, INTERNATIONAL ELECTROTECHNICAL COMMISSION.

IEEE (2001). IEEE Standard 1540-2001: standard for software life cycle processes – risk management. New York, INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS.

IPMA (2006). IPMA Competence Baseline (ICB), Version 3.0, March 2006 International Project Management Association.

ISO (2003). ISO 10006 - Quality Management Systems - Guidelines for quality management in projects. Switzerland, International Organization for Standardization.

Kelly, P. M. and W. N. Adger (1999). Assessing vulnerability to climate change and facilitating adaptation, Centre for Social & Economic Research on the Global Environment, School of Environmental Sciences, University of East Anglia, Norwich, U.K.

Le Moigne, J. (1990). La théorie du système général. Théorie de la modélisation, Presses Universitaires de France.

Luers, A., D. Lobell, et al. (2003). "A method for quantifying vulnerability, applied to the Yaqui Valley, Mexico." Global Environmental Change **13**: 255-267.

Luers, A., D. Lobell, et al. (2003). "A method for quantifying vulnerability, applied to the Yaqui Valley, Mexico." Global Environmental
Change **13**: 255-267.

Perry, M., A. Dulio, et al. (2006). Voices of beneficiaries: Medicare Part D insights and observations one year later, Kaiser Family Foundation report.

PMI, S. C. (2004). A guide to the project management body of knowledge (PMBOK) (2004 ed.). Newton Square, PA, USA. , Project Management Institute.

Schneider, C. (2008). "Fences and Competition in Patent Races." International
Journal of Industrial Organization **26**(6): 1348-1364.

Scoones, I. (1998). Sustainable rural livelihoods. A framework for analysis - IDS, Working Paper No. 72. IDS, Brighton.

Shi, L. (2001). "The convergence of vulnerable characteristics and health insurance in the USA. ." Social Science Medicine **53**(5): 519-529.

Strauss, J. S. (1997). Processes of healing and the nature of schizophrenia. Towards a comprehensive therapy for schizophrenia. W. B. R. G. E. D. Brenner. Kirkland, WA, Hogrefe & Huber**:** 252-261.

Theys, J. (1987). La société vulnérable. La société vulnérable. Evaluer et maîtriser les risques, in Jean Louis Fabiani et Jacques Theys (dir.), Presses de l'Ecole Normale Supérieure**:** 3-35.

Vidal, L. and F. Marle (2007). Modeling project complexity. International Conference on Engineering Design, Paris, FRANCE.

Vidal, L. and F. Marle (2008). "Understanding project complexity: implications on project management." Kybernetes, the International Journal of Systems, Cybernetics and Management Science.

Vidal, L. A., E. Sahin, et al. (2009). "Using the AHP to select anticancer drugs to produce by anticipation." Expert
Systems With Applications.

Watts, M. J. and H. G. Bohle (1993). "The space of vulnerability: the causal structure of hunger and famine." Progress in Human Geography **17**(1).

Zhang, H. (2007). "A redefinition of the project risk process: Using vulnerability to open up the event-consequence link." International Journal of Project Management **25**(7): 694-701.