IMPROVING THE MANAGEMENT OF DESIGN PROJECT RISKS USING THE CONCEPT OF VULNERABILITY : A SYSTEMS APPROACH

Vidal La., Marle F., Bocquet Jc.

ABSTRACT

Since design projects evolve within complex environments, they must face more and more numerous, varied and interrelated risks. Therefore, traditional paradigms of project risk management must be completed by the use of new systems thinking-oriented approaches. After defining the concept of project vulnerability, this paper thus proposes a description of the project vulnerability management process and compares it with the traditional project risk management process in order to highlight the potential benefits of such a new systems-oriented approach. It also proposes a methodology to analyze project vulnerabilities by decomposing them into three levels: values, processes and project elements. A stressor/receptor analogy-based model is the basis to identify and evaluate project vulnerabilities. A simple index then aggregates the concepts of resistance, resilience and contribution to value creation. This enables to rank project vulnerabilities in order to assist decision-making. Finally, a case study is presented: it explains the benefits of the vulnerability approach in the case of a project in the context of the pharmaceutical industry, the aim of which was to design a decision support system and its corresponding work organization.

Keywords: Project management, risk management, vulnerability, systems thinking, complexity.

1 INTRODUCTION

As any projects, design projects must be managed to achieve their objectives [1] but project risks are likely to prevent them from doing so. Design projects are in essence complex [2]. The product is complex, the supply chain that will manufacture and deliver it is complex, the project organization that will design this product is complex and is part of a more complex system, which may be composed of one or several companies. Even if the relation between risks and complexity is still to be clarified, project complexity is defined “as the property of a project which makes it difficult to understand, foresee and keep under control its overall behavior, even when given reasonably complete information about the project system” [3]. This complexity implies that it is even more difficult to manage design projects since it is a major source of ambiguity and unawareness.

That is why, as recent works or communications state it [4], the concept of vulnerability appears to be promising for efficient risk management, notably within the context of project management. This one permits to focus on the current weaknesses of a system instead of focusing on the evaluation of risks, which are in essence potential. However, this concept needs strong clarification before it can be used in the contexts of design and industrial engineering, both for academic and industrial practitioners. This paper thus aims at proposing a project vulnerability process with the following methodology:

1. Carrying out a broad state of the art on vulnerability.
2. Defining project vulnerability and its characteristics.
3. Describing the steps of a project vulnerability management process in order to permit the industrial application of the concept of vulnerability in projects.
4. Permitting the identification and analysis of project vulnerabilities using a systems thinking approach which focuses on the potential degradation of the project values creation processes.
5. Testing the whole approach on a case study.

The advantage of considering the new concept of vulnerability is that it permits to reduce ambiguity and bridge the gaps on the different visions which are likely to exist within project teams, since it permits to focus more on the existing weaknesses of a project system and its present state of exposure to dangerous events, instead of dealing with potential events.

This also facilitates communication on action plans since they are drawn by the improvement of an existing state of the project system instead of focusing on potential events and their potential impacts. Our research approach is then undoubtedly constructivist in order to model project systems (and their vulnerability) with the objective of strengthening them with proper action plans.

2 STATE OF THE ART: THE CONCEPT OF VULNERABILITY

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 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.
As underlined by Zhang [4], dealing with vulnerability management is a paradigm shift from risk management since it notably permits to focus on existing situations and elements rather than on potential events. This article wants to promote this shift since we believe it permits to address issues which were formerly underlined in former works [3] such as ambiguity within project teams, low confidence and low involvement in risk management, etc... Indeed, vulnerability management plans are oriented on existing situations when risk management plans are oriented on potential ones.

2.1 Brief quantitative analysis of the state of the art

A broad state of the art focusing on the keyword "vulnerability" was carried out in the most famous scientific databases (Web Of Science, Scopus, etc.). Publications over the 20 last years (1990-2010) were addressed in this research process. As a whole, 731 different articles were identified, and they were classified according to 10 scientific / application fields : applied mathematics, construction and urbanism, economics, environment, health, industrial and design engineering, information technology, military strategy, physics and chemistry, safety engineering. Of these 731 publications, 78% were related to two scientific / application fields: health and environment (almost a classical 80/20 Pareto distribution). Moreover, this survey enlightens the lack of use of the concept of vulnerability in industrial and design engineering (arriving 7th topic in this state of the art, only 12 publications out of 731; i.e. 1,64%), 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 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 and design engineering.

2.2 Conclusions of health and environment-oriented publications about vulnerability

First, it can be observed that some research works relate vulnerability to the presence of weaknesses [5], [6]. These weaknesses can be of different nature, and can for instance impact the activities, assets and outcomes of a system, as shown hereunder in Figure 1 [7].

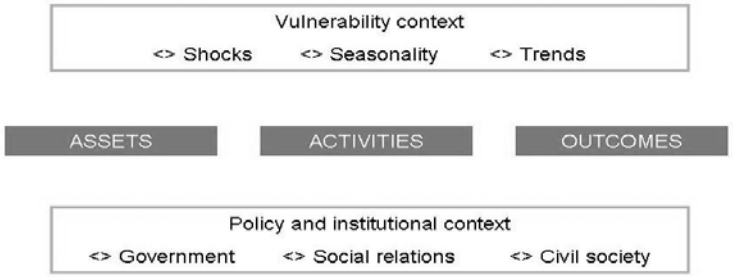

Figure 1. Vulnerability based on assets, activities and outcomes given a context

Second, other papers insist on one particular 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 Shi [8] with healthcare systems. Particularly, several works detail the notion of exposure [9], notably in contexts of crisis [10]. 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 defenselessness, 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 modeled using stressor/receptor models [11].
Finally, 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 [12], [13].

2.3 Conclusions of industrial and design engineering publications about vulnerability

Theys underlines that in the field of industrial engineering and management, "there are still too few languages and tools for analyzing vulnerability" [14]. However, some attempts were already done, like for instance [15] who place the notion of vulnerability at the center of the value creation process, which is consistent with Schneider [16]. In order to understand this possible value degradation, systems thinking-based models were developed [17]. Particularly, the works of Durand [18], which follow a complex systems approach, define vulnerability as the "extent to which an organization 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 organization's ability to resist to hazards and on the mechanisms that can weaken or strengthen its overall functioning, behavior 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. Finally, other recent works in the field of industrial engineering address the vulnerability of supply chain networks, considering them as complex systems and modeling them using graph-based approaches [19].

3. DEFINING THE CONCEPT OF PROJECT VULNERABILITY

Even though a lack of consensus can be observed around the notion of vulnerability [5], the previous state of the art led us to propose the following definition for project vulnerability. We claim that this concept permits to analyze a project system and focus on its existing weaknesses thanks to a systems thinking-based approach [20]. 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 the project susceptibility to be subject to negative events and the project non capability to cope with them coexist, i.e. if and only if they simultaneously exist at a given time. As shown in Figure 2, 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).

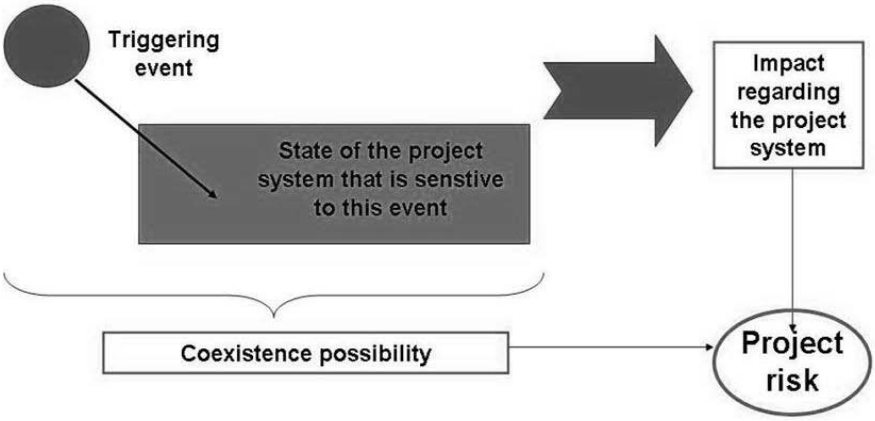

Figure 2. Project risk as an impact due to a coexistence possibility

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.
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. The evaluation of these parameters will permit to analyze and rank existing weaknesses of design projects. As a whole, this section thus proposes a paradigm shift since it focuses on the project system existing elements instead of focusing on potential events.

4. MODELING AND MANAGING THE VULNERABILITY OF DESIGN PROJECTS

The project vulnerability management process (Figure 3) is a four step approach, which appears to be similar to the existing project risk management processes as defined in ([21], [22], [23], [24], [25], [26], [27]). Each of these four steps is developed in the following paragraphs.

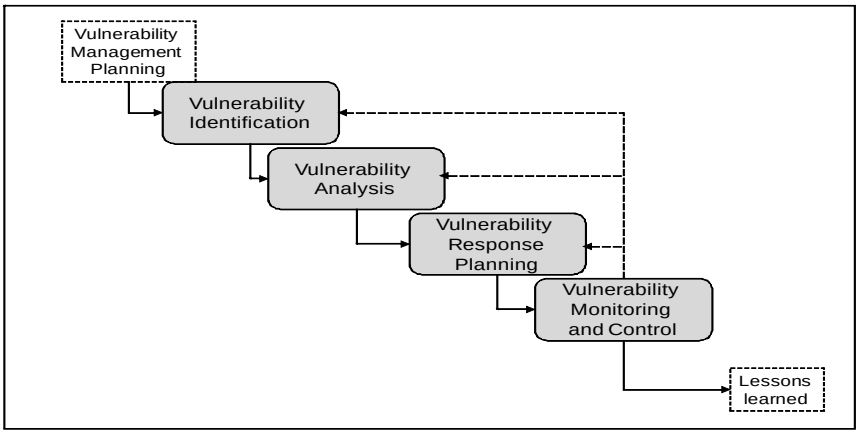

Figure 3. The project vulnerability management process

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, etc.) 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 based on the systems-thinking approach is proposed ([20], [27], [28], [29]). Vulnerability is identified at three levels:

1. The teleological pole of the project system, which permits to identify the vulnerable stakes of the project (targeted created values).
2. The functional pole of the project system, which permits to identify the vulnerable processes and tasks of the project system.
3. The ontological pole of the project system, which permits to identify the vulnerable elements (actors, resources, inputs of processes, etc.) of the project system.

Then follows 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 triplets (value, element, event). 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 4):

1. The project values which are likely to be damaged and make thus the project vulnerable regarding them.
2. For each value Vi, the project processes/tasks which contribute to Vi 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 Vi.
3. For each process Pij, the project elements which permit to perform Pij (actors, resources, other inputs). These elements are likely to be altered (and thus to be vulnerable) by negative events, which alters Pij, which makes as a consequence the project vulnerable regarding Vi.

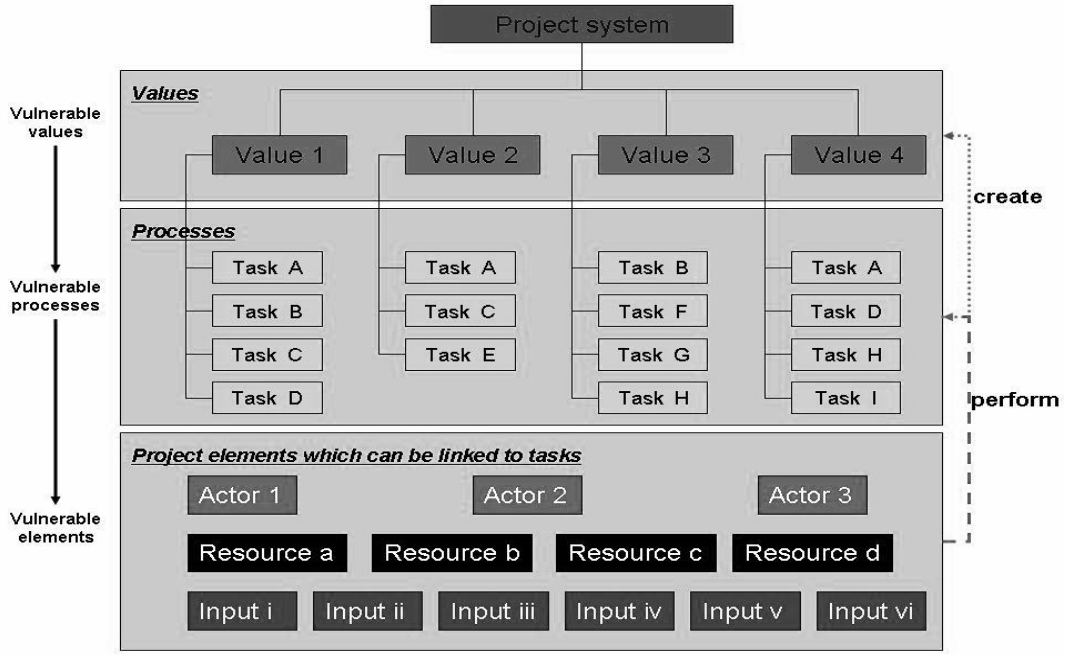

Figure 4. Levels in the project vulnerability identification step

This decomposition is analogous to the one proposed in [7] in terms of outcomes (values), activities (processes) and assets (project elements).

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. And that is where the set of values created by the project needs to be considered (time, cost, quality, environmental values, societal values, etc…). Given each value Vi, there are several project processes/tasks (Pi1, Pi2, …, Pip) which contribute to Vi creation. The project manager, the project team or external experts can permit to determine weights βij which permit to determine the importance of each task regarding Vi creation (for each i, the sum of all βij is equal to 1). These weights will permit to evaluate vulnerability as seen later in the paper.

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 since the combinatorial aspects 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. However, one should be able to evaluate/assess them in order to manage them better. This is the object of the next step, called vulnerability analysis.

4.2 The project vulnerability analysis step

Once the set of project process or elementary vulnerabilities is identified, theses ones are to be analyzed regarding the two main aspects of vulnerability in terms of non-capability, that is to say resistance and resilience. The notion of susceptibility is not addressed yet, and is for the moment comparable to the classical occurrence probability assessment. In order to do so, objective scales should be built by experts (see Table 2), like in the risk analysis process when performing the evaluation of probability and impact. The Figure 5 below 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.

Table 2 : examples of project vulnerability scales

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

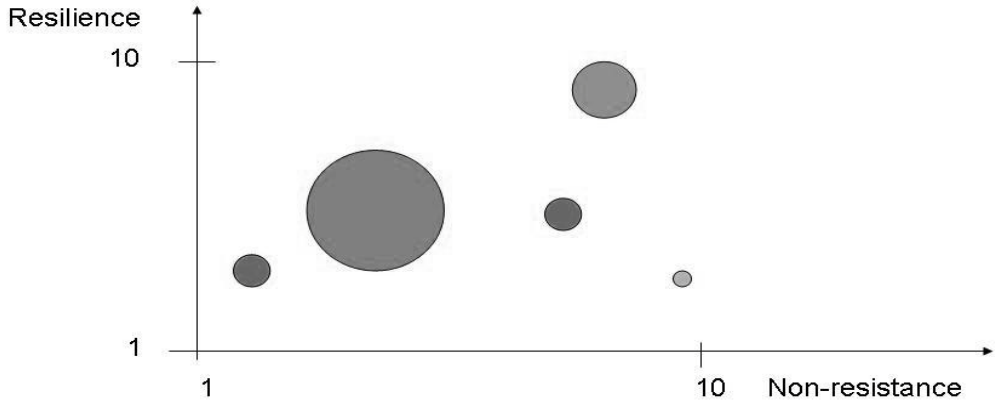

Figure 5. Project vulnerability analysis

In one 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. 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).

$$\Gamma(V) = NR \times R \times CR(V) \quad (1)$$

As during any aggregation operation, part of information is lost. 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 planning 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 [26], even though slightly different, there are five basic strategies to cope with project vulnerabilities: mitigation, avoidance, transfer, acceptance and contingence.

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. 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).

As for it, 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 value creation processes. This strategy is really different than the transfer 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 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 leverage points for vulnerability reduction.

Finally, acceptance is a strategy which is notably adequate 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. Another case is when there is nothing to do, or the action would be too expensive or too risky compared to the initial vulnerability. 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.

5. CASE STUDY: THE FABACT PROJECT

A case study is performed during the FabACT project [30], 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 Context of the study

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 organization of the production process. Within this context, the FabACT project was 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 FabACT project was thus supposed to design a decision support tool and design the corresponding work organization in order to assist pharmacists when choosing the anti-cancer drugs that can be produced in advance. Due to the sensitivity of this project, its vulnerabilities were studied.

5.2 Results of the study

The global project vulnerability management process was performed, though not presented entirely in this paper. For instance, one can perform it here on the identified project actors which make the project potentially vulnerable regarding the creation of the scientific value of deliverables while designing the decisions support tool. We obtained a list of five actors which contribute significantly to this value creation process: 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 behavior during the project is altered.

One is to find hereunder an excerpt of the FabACT project actor vulnerability analysis (Table 2). The project actor vulnerabilities are ranked according to their Crucial Index Γ(V).

Table 2. Excerpt of the FabACT project actor vulnerability analysis

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

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. Comparison was finally made with a traditional FMECA performed for the FabACT project (Table 3) to be a point of comparison in order to underline the potential benefits of a project vulnerability analysis.

Table 3. Excerpt of the FMECA of the FabACT project

#	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

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. In order to be fully validated, our research needs to be confronted to other case studies and experts' opinions. However, we do believe that, by following a methodology based on a systems thinking approach, we are likely to encompass all the aspects of project systems, their complexity and their vulnerability. We identify several research perspectives to consolidate the proposals of this paper:

1. First, the susceptibility aspect of vulnerability is neglected in this first approach of project vulnerability management. Future research work may explore this concept.
2. Moreover, the calculation of the Crucial Index $\Gamma(V)$ is to be improved thanks to the integration of multi-criteria aspects
3. 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.
4. Improving this systems thinking approach by exploring graph-based approaches to understand better the vulnerability of complex networks such as design project networks [31], [32].

REFERENCES

[1] Turner, W.S., R.P. Langerhorst, et al., SDM: system development methodology, 1988 (North-Holland).

[2] Duffy, A.H.B., Designing design, *Proceedings of the Third International Seminar and Workshop on Engineering Design in Integrated Product Development*, 2002, pp.37-46.

[3] Vidal, L.A., Thinking project management in the age of complexity : implications on project risk management, *Ph.D. thesis*, 2009 (EcoleCentrale Paris, France).

[4] Zhang, H., 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, 2007.

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

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

[7] Ellis, F., *Human Vulnerability and Food Insecurity:Policy Implications Forum for Food Security in Southern Africa*, 2003.

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

[9] Blaikie, P., T. Cannon, et al.,*At risk*, 1994 (Routledge).

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

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

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

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

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

[15] Bogataj, D. and M. Bogataj, Measuring the supply chain risk and vulnerability in frequency space, *International Journal of Production Economics* 108(1-2): 291-301, 2007.

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

[17] Hellström, T., Critical infrastructure and systemic vulnerability : Towards a planning framework, *Safety science* 45(3): 415-430, 2007.

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

[19] Wagner, S.M. and N., Neshat, Assessing the vulnerability of supply chains using graph theory,

International Journal of Production Economics, Volume 126, Issue 1, Pages 121-129, 2010.
[20] Le Moigne, J.L., *La théorie du système général. Théorie de la modélisation*, 1990 (Presses Universitaires de France).
[21] APM, *Project Risk Analysis & Management (PRAM) Guide*, 1996 (High Wycombe – APM).
[22] IEC, *CEI/IEC 300-3-9:1995 Risk Management: part 3 – guide to risk analysis of technological systems*, 1995. (Geneva, INTERNATIONAL ELECTROTECHNICAL COMMISSION).
[23] IEEE,*IEEE Standard 1540-2001: standard for software life cycle processes – risk management*, 2001 (New York, INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS).
[24] IPMA,*IPMA Competence Baseline (ICB), Version 3.0*, 2006 (IPMA)
[25] ISO,*ISO 10006 - Quality Management Systems - Guidelines for quality management in projects*, 2003 (Switzerland, International Organization for Standardization).
[26] PMI, S. C., *A guide to the project management body of knowledge (PMBOK)*, 2004 (Newton Square, PA, USA. , Project Management Institute).
[27] Genelot, D., Manager dans la complexité – Réflexions à l'usage des dirigeants, 2001. (Paris, INSEP Consulting Editions).
[28] Vidal, L. and F. Marle, Modeling project complexity. *International Conference on Engineering Design*, Paris, FRANCE, 2007.
[29] Vidal, L. and F. Marle, Understanding project complexity: implications on project management, *Kybernetes, the International Journal of Systems, Cybernetics and Management Science*, 2008.
[30] Vidal, L. A., E. Sahin, et al., Using the AHP to select anticancer drugs to produce by anticipation. *Expert Systems With Applications*, 2009.
[31] Minciardi, R., R. Sacile et al., Modeling the vulnerability of complex territorial systems: An application to hydrological risk, *Environmental Modelling& Software*, 21(7), 2006.
[32] Mishkovski, I., M. Biey, and L. Kocarev, Vulnerability of complex networks, *Communications in Nonlinear Science and Numerical Simulation*, 16(1), 2001.