Risk Assessment in Open Innovation Networks

João Rosas, Patrícia Macedo, Alexandra Tenera, António Abreu, Paula Urze

Risk Assessment in Open Innovation Networks

João Rosas[1,2], Patrícia Macedo[2,3], Alexandra Tenera[1,4], António Abreu[2,5] and Paula Urze[1,6],

[1] FCT/UNL, Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa, Portugal
[2] Uninova Institute, Centre of Technology and Systems, Portugal
[3] School of Technology of Setubal, Polytechnic Institute of Setubal, Portugal
[4] UNIDEMI/FCT/UNL, Mechanical and Industrial Engineering Department, Portugal
[5] ISEL/IPL – Instituto Superior de Engenharia de Lisboa do Instituto Politécnico de Lisboa, Portugal
[6] CIUHCT – Centro Interuniversitário de História das Ciências e da Tecnologia
jrosas@uninova.pt, patricia.macedo@estsetubal.ips.pt, {abt, pcu}@fct.unl.pt, ajfa@dem.isel.ipl.pt

Abstract. Innovation is considered crucial for enterprises survival and current economic environment demands the best ways of achieving it. However, the development of complex products and services require the utilization of diverse know-how and technology, which enterprises may not hold. An effective strategy for achieving them is to rely in open innovation. Still, open innovation projects may fail for many causes, e.g. due to the dynamics of collaboration between partners. To effectively benefit from open innovation, it is recommended the utilization of adequate risk models. For achieving such models, a preliminary conceptualization of open innovation and risk is necessary, which includes modeling experiments with existing risk models, such as the FMEA,

Keywords: Open Innovation, Risk Assessment, Collaborative Networks, and FMEA.

1 Introduction

Nowadays, Innovation is crucial for the enterprises survival and current economic environment demands the best ways of achieving it. Open innovation is a useful strategy enterprises adopt to seek knowledge and value from outside of their boundaries. In such way, enterprises share technology and knowledge with their suppliers and customers to develop innovative and improved products, and leveraging value creation. Assuming this strategy, enterprises may even disclose secrete technology or free intellectual property, for the sake of obtaining such benefits. But this is not done without risks, as open innovation projects might fail for diverse reasons. For instance, the appropriation of others' know-how or trying to take

unmerited benefits from a technology are considered disruptive behaviors in open innovation projects.

To effectively benefit from open innovation, it is recommended the utilization of adequate risk models. Open innovation is essentially a collaborative strategy. There is a significant number of risk-like assessment approaches for collaborative networks already, but few specifically addressing risk in open innovation.

Our aim is to develop research work towards developing a risk assessment approach for open innovation. As explained in section 3, this problem has had little attention by the research community. Given this scarcity, we considered a research question, which can be stated as: *How to model open innovation risk assessment*? Our effort is, therefore, devoted to contribute to provide an answer to this question.

Our research method starts by problem formulation. It is followed by the conceptualization of open innovation and risk and by the related research analysis. The next phase is devoted to work on risk modeling in open innovation. In this regard, our risk assessment approach is based on a widely used risk model, namely, FMEA. The obtained approach is illustrated through an application example, followed by result analysis.

In the next section, we provide the relevant concepts regarding open innovation and risk. We briefly describe a few existing risk assessment models. A research on the state of the art related to risk in open innovation is presented in section 3, aiming at identify and characterize risk assessment models in open innovation. In section 4, we illustrate how we could model risk assessment using the FMEA model. We also provide an illustrative application example. We finish the results analysis, conclusions and future work.

2 Base Concepts

2.1 Open Innovation

The concept of open innovation, coined by Chesbrough in 2003 [1], has become relevant in practice and in academia. Open innovation is now a mainstream research focus in innovation literature [2]. One of the reasons for the advance of the open innovation paradigm is based on the principle that today´s problems are often complex and require a wide range of expertise. To create and implement solutions it is required that collaboration occurs among different areas and people with a variety of experience and knowledge. It is very difficult for organizations to build solutions and create knowledge by themselves. The basic assumption of open innovation is opening up the innovation process. This means to treat research and development as an open system. Open innovation is usually put in contrast to closed innovation, supposedly its precursor, where companies generate their own innovation ideas, and then develop, build, market, distribute, service, finance, and support them on their own [1].

Open innovation suggests that valuable ideas can come from inside or outside the company as well. The mobility of competencies, the increasing presence of venture-capital, the emergence start-ups and the role of university research and its linkages

give rise to a more open approach towards innovation. Collaboration is argued to facilitate the production of new knowledge more than just transferring it. Chesbrough [3] has referred to open innovation not only as being a business model, but also as a way of promoting and sharing knowledge. This means that open innovation can go beyond the idea of knowledge transaction and of in/outsourcing ideas, but promote the creation of new knowledge.

Companies can develop and bring ideas to the market using channels outside of their current businesses, in order to generate value for the organization. A path for accomplishing this can involve new businesses and licensing agreements. These might be financed and staffed with the existing company's personnel. In addition, ideas can also be originated outside the company and be brought inside it, for commercialization [4]. In other words, the connection between a company and its environment is more permeable, enabling innovative ideas to transfer easily where boundaries once existed.

As argued by Felin & Zenger [5], the mechanisms for accessing external knowledge and promoting open innovation encompass a range of alternatives including alliances and joint ventures, corporate venture capital, licensing, open source platforms, and participation in various development communities. Each of the modalities brings distinct benefits, implies distinct levels of openness, and various risks. For instance, they vary in terms of intellectual property ownership, from Joint-ventures, created by formal-agreements, and "open-source models", in which IP is given away to a (large and open) software development community.

An open innovation strategy can generate a positive result, but, it also involves some risks. Therefore, companies should have a policy to secure open innovation within their organization, to create interfaces and make achievements measureable. The way employees manage their external partners is also very important and plays a central role.

2.2 Risk Models in Engineering

Proceeding as specified in our research method, we now address the concept of risk in an engineering context. To overcome global competition and rapid technological advances, in order to predict and positively respond to changes, the development of organizational capability to innovate has become one of the prime strategy in SMEs. This has been done despite the lack on practical models, metrics and tools to assist their risk management efforts [6].

For many years, organizations risk has been seen mainly as a combination of the probability of occurrence of harms and the severity of these harms. Nowadays, such in project management, risk is viewed as related to uncertain events or conditions that, when they occur, pose positive or negative effects on projects objectives. Similarly, as the uncertainty associated with innovative processes is bonded not only to inherent risk of failure, but also to inherent chance of success, these subsequently bring on the necessity of adequate risk management in innovative processes [7]. Thereby, and since the purpose of an integrated risk management is to facilitate innovation rather than stifle it, innovating firms require a strategy not of risk avoidance, but of early

risk diagnosis and management [8,9], which should be spread through organizations and collaborative networks.

Based on general project management practices, several frequently used risk assessment models can be identified, such as the Balanced Scorecard (BSC), Failure Mode Effects Analysis (FMEA), Fault Tree Analysis (FTA), Analytic Hierarchy Process (AHP) and Risk Diagnosing Methodology (RDM).

The BSC model is typically used to facilitate the monitoring of the firm's success factors, which can be viewed as opportunities as well as risks, meaning that the BSC is by nature an instrument close to the risk's grounds function [10].

Another commonly used risk assessment approach is the Failure Mode Effects Analysis (FMEA), which is a systemic approach suited to help identify and reduce critical aspects in early stages of products and processes conception. Due to its role in the context of our research work, this risk assessment technic is explained in more depth in the next section.

The Fault Tree Analysis (FTA) can be both used as a risk identification method or as a risk analysis instrument. In this approach, the probability of negative events can be estimated and their causes deducted from a named Fault Tree, in which the probabilities of alternative situations are assessed. These situations are organized using Boolean logic, in which lower-level events are fed into upper-level ones [10].

Another used risk assessment approach is the Analytic Hierarchy Process (AHP). AHP is considered a multivariate analysis technique that aims to decrease the randomness of subjective assessments, by having in consideration different objectives grounded on distinct criteria [11]. It is predominantly used in scenario selection and evaluation [12].

Another risk assessment approach is Risk Diagnosing Methodology (RDM) which main purpose is to help provide strategies that will support and improve the chance of projects success, by identifying and managing their potential risks [8, 13]. It is used to support the systematic diagnosis of companies, considering issues such as consumer and trade acceptance, commercial viability, competitive responses, external influential responses, product technology and manufacturing technology [8], in which the assessment of project risk is determined not only by risk likelihood and its effects, but also by the companies' ability to influence the course of the risk actions.

2.3 The FMEA Risk Assessment

FMEA is widely used risk assessment approach. It was original developed inside Aeronautic Industry in the 50's to guide the design process. But it has been widely used in a broader sense, not only to assess physical systems but also organizational ones, such as those in the areas of Knowledge Management [14] and supply-chain management [15]. The FMEA can be used as a design tool to systematically analyze postulated component failures and identify the resultant effects on system operations. A failure at a lower level may very well cause a larger failure on the higher level. Therefore, it is essential to find them as fast as possible [16].

With FMEA, we can quantify the risk level of each identified failure, whether known or potential. Then, an estimate of its likelihood of occurrence, severity, and detectability is made for each one. At this point, an evaluation of the necessary

actions is performed, namely, they can be taken, planned or ignored. The emphasis is to minimize the probability of failures or to minimize their effects. The main constituents of the FMEA model are described as:

Failure - Event/process in which any part of the organizational system does not perform according to the prescribed behavior. Example: absence of knowledge sharing when it was expected.

Failure mode - The specific manner by which a failure occurs in terms of the failure of some part of the organization. It shall at least clearly describe the end state of the item under consideration. It is the result of the failure mechanism (see next). Example: An enterprise owing key knowledge left the project.

Failure cause and/or mechanism - Defects/problems detected in the elements of the organizational system which are the underlying cause or sequence of causes that initiate behaviors leading to a failure mode over a certain time. A failure mode may have several causes. Example: Inadequate organizational rules adoption may cause network weaknesses.

Failure effect: Immediate consequence of a failure. Example: Lack of knowledge sharing decreases the quality of a project and increases its duration.

Likelihood of occurrence (L) – The Likelihood of occurrence is the probability that a specific failure mode, which is the result of a specific cause under current open-innovation network, will happen. Failure Likelihood is a relative ranking within the scope of an individual FMEA. A suggested likelihood scale is given in Table 1.

Severity (S) - Severity is an assessment of the most serious effect for a given failure mode. Example: The severity of problematic partners can be reduced through their exchange. If such an exchange is attainable, the failure can be minimized eliminated. Severity is also a relative ranking within the scope of an individual FMEA.

Detectability (D) - Detectability is an assessment of the ability to identify any potential failure modes, case they occur. Detectability is a relative ranking within the scope of an individual FMEA.

The suggested risk guidelines for severity, occurrence and detection are given in Table 1.

Risk Priority Number (RPN) - The Risk Priority Number defines the priority of each failure. RPNs have no value or meaning by themselves. They are used only to rank (define) the potential open- innovation network deficiencies. The RPN is calculated by multiplying these three ratings:

$$\text{RPN} = \text{Failure Likelihood} \times \text{Severity} \times \text{Detectability}. \quad (1)$$

In this equation, failure Likelihood, Severity and detectability must have a value greater than zero. A suggested RPN ranking is provided in Table 2.

Recommended Action - The recommended action may be specific action(s) or it may correspond to major changes in the operating process of an open innovation project or network. The idea of the recommended actions in FMEA is to reduce the severity, occurrence, detection or them all.

Table 1. Risk guidelines Rank.

Rank	Failure Likelihood	Severity of Effects	Detection Processes
5	Frequent	Maximum Severity - Failure leads to the end of the open-innovation process	Extremely Unlikely - Management processes will almost certainly not detect the potential failure before it occurs.
4	Reasonably Probable	Very High Severity – open innovation network performance severely affected. Members very dissatisfied. Network members will be able to correct the failure/situation with some constraints.	Remote Likelihood – Management process more likely will not detect the existence of a potential failure before it occurs.
3	Occasional	Moderate - Reduced performance with gradual performance degradation. Network members dissatisfied. Network members will be able to correct the failure/situation.	Moderate – Management process may detect the potential failure before it occurs.
2	Remote	Minor – Network members will probably notice the effect, it is considered negligible.	High: Management processes have a good chance of detecting the potential failure before it occurs.
1	Extremely unlikely	Very Slight – Insignificant /negligible effect.	Very high: Management processes almost certainly will detect the potential failure before it occurs.

Table 2. Risk Category guidelines.

Heading level	Risk category
90 – 125	Extreme
60 – 89	Significant
40 – 59	Major
18 – 39	Moderate
1 – 17	Low

3 Depicting Existing Approaches of Risk Assessment in Open Innovation

During our research work, it was relatively difficult to find related research concerning risk assessment in open innovation. This difficulty led us to formulate the hypothesis that such models might be currently scarce. But this is an assumption that is difficult to demonstrate. Frequently in science, we can more easily prove that something exists than proving that it does not [17, 18].

In order to overcome this difficulty, we devised an approach to estimate the amount of research work concerning risk in open innovation. For such, a small content analysis based on the utilization of "Publish or Perish" search engine was performed.

"Publish or Perish" allows flexible searches of published research works. In our approach, we looked for papers with certain words in their titles. For instance, when a research intends to publish a paper related to risk modeling or assessment, the word

"risk" or "uncertainty" is likely to appear in its title. Similarly, this is also true for researchers aiming to write papers on innovation. In this case, the word "innovation" or its synonymous would appear in the title.

The search was restricted to publications written since 2004, as the term "open innovation" was coined in 2003. After initial trials, we perceived that many results were unrelated to open innovation, so we tuned the search engine to filter out papers containing the words: "financial", "bank", "credit", "price", "climate" and "drug". We performed similar searches for words in areas that are considered consolidated, to serve as a comparison basis. The obtained results are summarized in Table 3.

Table 3. Publications regarding risk in open innovation, with comparison examples.

Keywords	Papers found	Number of citations
Risk innovation	901	2446
Risk innovation model	48	74
Risk innovation modeling	5	12
Risk innovation assessment	44	93
Risk innovation management	182	461
Open innovation Risk	7	4
Open innovation Risk model	1	0
Open innovation risk management	0	0
Open innovation FMEA	0	0
Virtual organizations risk	6	12
Collaborative networks risk	6	22
Collaborative FMEA	2	0
Collaboration FMEA	2	0
Business risk model	146	361
Risk portfolio selection	280	1672
Failure mode effects analysis	406	2829
FMEA	above 1000	6602 (of these 1000)
Risk management	above 1000	71809 (of these 1000)
Organizational behavior	above 1000	44648 (of these 1000)

The mentioned table is split in three groups of results. The first group indicates there is a significant number of papers addressing risk in either closed and open innovation, and that some of them (could be up to 48) are more specific to risk models. The second group indicates there are few papers which consider risk in open innovation, about 7, and that only one has got the word "model" in title. Concerning risk, such areas of collaborative networks also present similar numbers. The last group of results serves as comparison basis, as it provides figures for areas that are more stabilized. The approach can be repeated and extended with more words. For instance, the number of papers with "uncertainty" and "innovation" in their titles was 308. But if we include the word "open", we only obtain 6 publications. A reader is right stating that the approach may not provide very rigorous figures. But the divergence of values between open innovation and other consolidated areas provides support to our claim, that such models for risk in open innovation might be scarce.

As to establish a theoretical bases for our research in open innovation risk assessment models, we performed an analysis of the more promising publications among the few ones which were obtained during our context analysis:

Research works addressing risks, whiteout risk assessment models: In [19], a risk-based technology management approach was proposed. In this approach, risk is considered as an inherent aspect of the product development. It simultaneously considers both quantitative innovation objectives and quantitative product delivery objectives, such as cost, schedule and performance, enabling to establish formal quantitative technology innovation objectives and to track and monitoring them during a product development cycle. In [20], the external technology dependence, complex process management, difficulty in intellectual property protection, market information leakage, and mismatched resources capacity are identified as situations that pose risks in open innovation projects. In [21], several factors related to intellectual property competition in open innovation are highlighted. The study reveals the likelihood that open and proprietary competitors will clash, according to the industry type, e.g. radio and television, Medical, Electric motors, food and beverages, etc.

Identified risk models in open innovation: The research work in [22] is focused on the risk evaluation of customer integration in new product development. A number of risk factors of customer integration in new product development were identified, namely, organization risk, capacity risk, knowledge risk, and market risk. Their goal was to develop a risk evaluation method. The approach is based on rough set theory to handle vagueness. In [23], a research was conducted towards developing methodologies for managing risks of open-source software adoption in a context of an ecosystem of developers. The approach combined risk monitoring methods in order to provide early warnings of risks and their mitigation. The developed tools also included Bayesian networks and social network analysis. In [24], a risk management approach for crowdsourcing innovation is proposed. It provided overall guidelines to managing risks associated with crowdsourcing strategy, and a risk model suited for small and medium enterprises.

4 Application of FMEA to Open Innovation

4.1 Factors of Risk in Open Innovation

As mentioned in previous section, there are many definitions of risk according to the respective contexts in consideration. For all that matters in this research work, we can assume one of these general descriptions, in which risk can be seen as a probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action [25].

There are several innovation modalities, which as described before, are characterized by several aspects, like degree of openness to external partners. Each of these modalities pose distinct risk types. Envisaging a risk assessment instrument requires the identification of these risk types. Table 4 presents an initial characterization of these risks, which affect enterprises participating in open innovation.

Table 4. Situations posing risks in innovation, based on [20].

Situations	Description
External technology dependence	When enterprises rely excessively on their partners for technology and knowledge, they might get in weaker situation if cooperation with these partners fail.
Complex process management	The absence of organizational boundaries and the interaction with autonomous partners increases the difficulty of process control and management. Conflicts and uncooperative behavior might manifest.
Intellectual property protection	When a partner gives away its knowledge to its peers, core knowledge is difficult to protect. Enterprises risk lose control of knowledge ownership, and may not collect the desired benefits.
Market information leakage	When participating in open innovation, enterprises may need to disclosure knowledge and business secrets to peers. They risk product and user information being stolen by its peers.
Resources capacity mismatch	When resources and capacity of several partner are mismatched, it creates obstacles for innovation activity.

For each risk of a failure, we can identify its causes, its effects and corresponding degree of impact, and the likelihood of its occurrence, as illustrated in Table 5.

Table 5. Characterization of open innovation risks

Failure	**Failure mode**	**Effect**	**Failure mechanisms**
Partner needs competency not available within the network	A partner left the project	Loss of core competencies vital for the project	Excessive reliance on external partners; Low technological/competence independence
Cooperation issues	Uncooperative behavior	Project disruption	Conflicting goals and expectations; values misalignment
Intellectual property protection (IP)	Abuse of IP by peers	Loss of trust among network partners; loss of competiveness.	Inadequate IP laws and regulations.
Market information sharing	Insecure disclosure of core market knowledge	Theft of product and customers information	Information leakage occurs during customers and suppliers participation in the innovation process
Resource allocation	Mismatched resource capacity	Costs increment; project delay.	Wrong perception of resources capacity and complementarity.

4.2 Assessing Risk Example

The information regarding the risk factors described in previous section can be used to illustrate how we could assess risks in open innovation using.

Let us suppose the existence of an open innovation project aiming at developing an Internet of Things application for health care. In an initial stage of the project, the set of potential failures where identified and analyzed. The corresponding values for the likelihood of occurrences, severity and detectability of each failure were estimated. The obtained risk assessment results are presented in Table 6. The values in the table were merely chosen for illustrative purposes.

Table 6. Open innovation risk assessment illustration with FMEA method

Failure Mode	**Likelihood of occurrence (L)**	**Severity of consequence (S)**	**Detectability of the failure (D)**	**RPN (L × S × D)**
Partner with key technology left the project	5	3	4	60 (significant)
Uncooperative behavior	2	2	3	12 (low)
Abuse of IP by peers	4	5	5	100 (Extreme)
Insecure disclosure of core knowledge	4	4	2	32 (moderate)
Mismatched resource capacity	2	3	3	18 (moderate)

The obtained risk priority numbers provide indication of which failures must receive more attention. For instance, the RPN for "uncooperative behavior" is low, while the risk of abuse of IP by peers is extreme (see Table 2). Based on this assessment, a project manager can take preventive actions in order to minimize the likelihood of these failures and minimize the effects of their eventual occurrence. For instance, reducing the risk that some peers may abuse of intellectual property during the project implies establishing agreements with effective rules to protect IP, as well as the monitoring processes to ensure the compliance with these rules.

5 Conclusions

We described an approach for risk assessment towards providing an answer to the formulated research question, which is concerned on how to access risk in open innovation. Although existing research works address risk in open Innovation, specific works considering risk assessment models seem scarce.

After an initial conceptualization and related research analysis, we identified illustrative examples of failures in open innovation projects from literature. As a way to illustrate how to assess open innovation risks, we characterized these failures according to one widely used risk model, namely the FMEA. To our knowledge, the FMEA model had never been used in the concrete "open innovation" realm. An application example of FMEA illustrated the approach.

The study and development of our approach led us to conclude that it is necessary further research for an adequate open innovation risk assessment, including a more comprehensive characterization of open innovation risks. In this regards, we should assume a more holistic perspective. Furthermore, open innovation is inherently collaborative. Therefore, one line of research for future work may include the adaptation of existing collaborative risk models, so they could suit in open innovation. In the area of collaborative networks, there is a variety of collaboration-related key performance indicators already, as well as assessment models of more soft nature, such as value systems, benefits sharing methods, and collaboration preparedness. Encompassing these elements into a tailored and holistic approach to risk assessment in open innovation is planned for the next phase of this research work.

Acknowledgments. This work was funded in part by the Center of Technology and Systems and FCT-PEST program UID/EEA/00066/2013 (Impactor project), by DEMI/FCT/UNL and by CIUHCT: Interuniversity Center for the History of Science and Technology.

References

1. Chesbrough, Henry (2003) Open Innovation: The New Imperative for Creating and Profiting from Technology. Boston: Harvard Business School Press.
2. Elmquist, Fredberg, Ollila, (2009) "Exploring the field of open innovation", European Journal of Innovation Management, Vol. 12(3), pp.326 – 345.
3. Chesbrough, H. (2010) Open Services Innovation: Rethinking Your Business to Grow and Compete in a New Era, Jossey-Bass.
4. Chesbrough, H., Vanhaverbeke, W., & West, J. (Eds.). (2006). Open innovation: Researching a new paradigm. Oxford university press.
5. Felin, T., & Zenger, T. R. Open or Closed Innovation? Problem Solving and Governance Choice Research Policy, Volume 43, Issue 5, June 2014, Pages 914–925.
6. Aleixo, G. & Tenera, A. (2009). New Product Development Process on High-Tech Innovation Life Cycle. World Academy of Science, Engineering and Technology, 58,794-800.
7. Vargas-hernández, J. G., & García-santillán, A. (2011). Management in the Innovation Project. Journal of Knowledge Management, Economics and Information Technology, 1(7), 1–24.
8. Keizer, J., Halman, J., & Song, M. (2002). From experience: Applying the Risk Diagnosing methodology. Journal of Product Innovation Management, 19(3): 213-232.
9. Pereira, L., Tenera, A., & Wemans, J. (2013). Insights on Individual's Risk Perception for Risk Assessment in Web-based Risk Management Tools. Procedia Technology, 9, 886-892.
10. Henschel, T. (2008). Risk Management Practices of SMEs: Evaluating and Implementing Effective Risk Management Systems. ESV- Erich Schmidt Verlag.(Edwards & Bowen, 2005).

11. Goodwin, P. & Wright, G. (2004). Decision Analysis for Management Judgment (3rd edition). John Wiley & Sons, Ltd.
12. Hulle, J., Kaspar, R., & Möller (2013). Analytic network process - an overview of applications in research and practice. International Journal of Operational Research (IJOR), 16(2), 172 – 213.
13. Pereira L., Tenera A., Bispo J. and Wemans J. (2015). A Risk Diagnosing Methodology Web-based Platform for Micro, Small and Medium Businesses: Remarks and Enhancements. In Communications in Computer and Information Science: Knowledge Discovery, Knowledge Engineering and Knowledge Management, 454, 340-356. Springer-Verlag GmbH.
14. Shih-Hsiung Luoa & Gwo-Guang Leea, (2006), Application of Failure Mode and Effect Analysis (FMEA) for audit of HACCP system.
15. S. Gary Teng, S. Michael Ho, Debra Shumar, Paul C. Liu, (2006). Implementing FMEA in a collaborative supply chain environment. International Journal of Quality & Reliability Management, 23(2), 179 – 196.
16. IEC 60812 Technical Committee (2006). , IEC 60812, Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA)," IEC, 2006.
17. Alderson, P. (2004). Absence of evidence is not evidence of absence: We need to report uncertain results and do it clearly. BMJ: British Medical Journal, 328(7438), 476.
18. Walton, D. (1992). Nonfallacious arguments from ignorance. American Philosophical Quarterly, Vol. 29(4), pp. 381-387.
19. Sleefe, G. E. (2010). Quantification of technology innovation using a risk-based framework. In Proceedings of World Academy of Science, Engineering and Technology, 66, 589-593.
20. Xiaoren, Z., Ling, D., Xiangdong, C. (2014). Interaction of open innovation and business ecosystem. International Journal of u-and e-Service, Science and Technology, 7(1), 51-64.
21. Alexy, O., & Reitzig, M. (2012). Managing the business risks of open innovation. McKinsey Quarterly, 1, 17-21.
22. Song, W., Ming, X., & Xu, Z. (2013). Risk evaluation of customer integration in new product development under uncertainty. Computers & Industrial Engineering, 65(3), 402-412.
23. Rossi, B., Russo, B., & Succi, G. (2012). Adoption of free/libre open source software in public organizations: factors of impact. Information Technology & People, 25(2), 156-187.
24. Souza, L., Ramos, I., & Esteves, J. (2009). Crowdsourcing Innovation: A Risk Management Approach. In MCIS (p. 67).
25. Business dictionary, http://www.businessdictionary.com/definition/risk.html seen in 2015/04/15.