Managing rare and undetectable events in risk assessment: the case of a satellite system launch project

Cristiano Angeletti

Engineering and Innovation Division,
Nuclear Technical Area, Enel S.p.A.,
Viale Regina Margherita, 125-00198, Roma, Italy
E-mail: cristiano.angeletti@enel.com

Andrea Giacchero*

Risk Management, Cassa Depositi e Prestiti S.p.A.,
Via Goito, 4-00185, Roma, Italy
E-mail: Andrea.Giacchero@uniroma2.it
Fax: +39-06-42215194
*Corresponding author

Massimiliano M. Schiraldi

Department of Enterprise Engineering,
Tor Vergata University of Rome,
Operations Management Research Group,
Via del Politecnico 1, 00133, Roma, Italy
E-mail: schiraldi@uniroma2.it

Abstract: Assessing the wide diversity of risk types in large and complex projects using the traditional hyperbolic iso-risks curves may seem a simplistic and reductive approach, and evaluating the risk factor through the multiplication of likelihood and severity parameters results in defining as dangerous those risks that are associated either with rare but devastating consequences or with probable but minor effects. In this work, the authors aimed at focusing on those risks that, despite their low occurrence probability, may significantly compromise a project result. To this extent, a different formula has been used to compute the risk factor, keeping into account risk detectability and evaluating the potential consequences in four different domains (cost, time, performance, reputation). This approach has been validated on the case of a large industrial project related to the launch of an innovative mobile telecommunications system, collecting the experts' opinions in a primary Italian firm in aerospace industry.

Keywords: risk assessment; risk detectability; rare events; satellite communication systems; satellite launchs; undetectable events; project management; iso-risks curves; black swans; risk factor evaluation; financial risks; economic risks; technical risks.

Reference to this paper should be made as follows: Angeletti, C., Giacchero, A. and Schiraldi, M.M. (2014) 'Managing rare and undetectable events in risk assessment: the case of a satellite system launch project', *Int. J. Project Organisation and Management*, Vol. 6, Nos. 1/2, pp.107–120.

Biographical notes: Cristiano Angeletti works as a Project Controller in the Nuclear Technical Division (ATN) at ENEL S.p.A., Italy's largest power company and Europe's second listed utility by installed capacity. He obtained his MSc in Engineering and Management at Tor Vergata University of Rome (Italy). His work mainly focuses on project management and cost controlling (budgeting and accounting) of several of the company's initiatives at a national and international level. He also works as the interface between the procurement division and ATN, managing the day-by-day progress of all the projects related to subcontracting.

Andrea Giacchero is a Risk Analyst at Cassa depositi e prestiti SpA. He holds a degree in Economics at La Sapienza University of Rome (Italy) and attends a PhD in Engineering and Management at Tor Vergata University of Rome (Italy). He is the author of several scientific publications at the national level. He was in charge of operational risk from 2002 to 2011, first in Capitalia and later in Unicredit, developing skills in the main methodologies of risk measurement. His research interests mainly focus on risk management and corporate social responsibility.

Massimiliano M. Schiraldi is an Assistant Professor in Operations Management at the School of Engineering at Tor Vergata University of Rome (Italy) and Visiting Professor at the Guizhou University of Finance and Economics (P.R. China). He holds an MSc and a PhD in Engineering and Management. He is the author of several scientific publications at national and international level and one book on inventory management. He teaches courses of operations management since 2001 and he teaches in several MBA course in Italy. He mainly focuses on university-industrial research collaborations and his research interests are related to production systems design and operations management, logistics, production and inventory planning and project management.

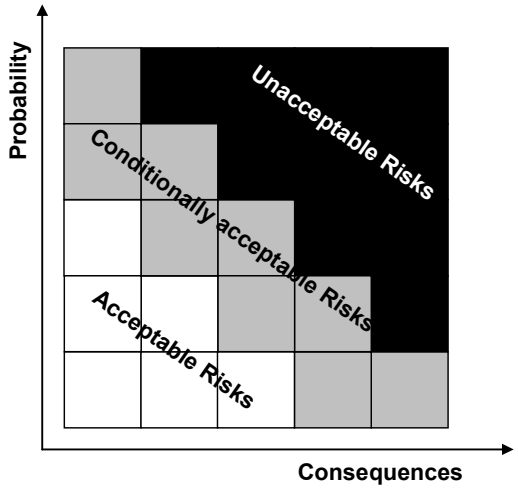
1 Introduction

Large engineering projects are 'high stakes games': characterised by significant permanent commitments, skewed reward structures in case of success and high probabilities of failure, Miller and Lessard (2001) argued that successful projects are not 'selected', but shaped with risk resolution in mind. For this reason, as Van Wyk et al. (2008) remind, risk management plays a major role in the project management of large construction, engineering and technological projects, with the mission of reducing uncertainties, through effective management and efficient risk monitoring, and of achieving project success. Basically, the effectiveness of risk management depends on project management, since the project manager is responsible to achieve project goals (Olsson, 2007): he needs to be able to check and monitor constantly all phases of the project life cycle, because each of them is characterised by different types of risks in the decision-making process (Han et al., 2008). And in this sense, when risks must be identified and analysed, planning becomes the most delicate phase in assessment of project's cost and revenue (Zwikael and Sadeh, 2007): it's important to implement an

effective risk management methodology before the project starts, in order to avoid an excessive and reckless optimism with the perspective of a reduction of the final value of the project (Locatelli and Mancini, 2010).

The International Organization for Standardization (ISO) 31000:2009 standard 'Risk management – principles and guidelines on implementation' states that risk assessment process begins with the description of risks and cause/effect relations (risk identification); then, once risks are identified, proceeds with the risk assessment in terms of occurrence probability and severity (risk analysis), so as to provide a framework for the evaluation of priorities in managing each type of risk (risk evaluation). Despite the ON Rule (ONR) 49001:2008 standard 'Risk management for organisations and systems' points out risk analysis phase complexity, explaining that "the way in which consequences and likelihood are expressed and the way in which they are combined to determine a level of risk will vary according to the type of risk, the information available and the purpose for which the risk assessment output is to be used", the proposed risk matrix is ordinarily shaped with discrete intervals and divided in three linear areas (Figure 1). Moreover, in spite of the fact that the ONR 49002-2 standard indicates as many as 15 different methodologies for risk assessment, the risk factor (R) – which represents the analytical and quantitative translation of a risk measure – is anyway always based on the simple and traditional multiplication of a probability index (P) with a consequence index (C).

Figure 1 Risk evaluation matrix



Source: Netzwerk Risikomanagement, Sicherheitsinstitut (2008) ONR 49001

This well-known approach, based on the intuitive concept of expected value, is clearly sharable under a logical point of view; however, as the latest ONR standard seems to suggests it is reasonable to question if this may result too unsophisticated in assessing operational risks in large and complex projects.

As a matter of fact, if R reflects both the risk probability and the severity of its consequences,

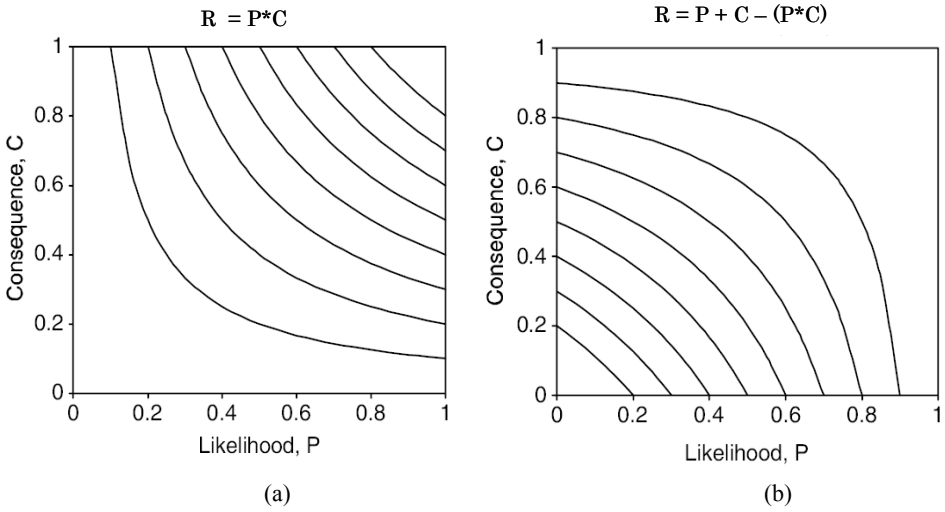
$$R = P * C \tag{1}$$

the resulting hyperbolic iso-risk curves define as tolerable those risks that are associated with devastating consequences, either with low occurrence probability (Figure 2a). Since some years ago, the limits of this approach began however to be recognised: in the popular book *The Black Swan* (Taleb, 2007) the crisis of the banks in the USA since 1970 is cited to suggest the inappropriateness of this method when coping with risks associated to financial operations entailing large amounts of money. A different approach is that suggested by Cooper et al. (2005) defining R as

$$R = P + C - (P * C) \tag{2}$$

According to this approach, those risks associated with catastrophic impact or with high probability are both unacceptable, as it is possible to see through the trend of the iso-risk curves in Figure 2b.

Figure 2 Iso-risk curves



Source: Cooper et al. (2005)

On the other hand, however, this approach is clearly less consistent in logical-mathematical terms; to ensure that P and C are comparable and combinable; an appropriate measurement scale in a 0–1 range must be carefully defined. This could represent a problem in managing a complex project: risks differ in nature (financial and capital, economic, technical) and have an impact on different aspects of the business (cost, time, performance, reputation). This paper aims exactly in this direction: a risk analysis procedure has been developed in order to bring a long list of possible risk factors back to the evaluation criteria expressed in (2); then, borrowing the basic principle of failure mode and effect criticality analysis (FMECA, MIL-STD-1629A standard, US Department of Defence), a specific factor has been introduced to take into account the risk detectability, i.e., the company's sensitivity in promptly detecting a possible adverse event. Then, risks have been sorted on the intervention priority and ranked on a 3D risk matrix, caring to highlight how this mapping can vary according to risk detectability. This procedure can easily feed the implementation of the risk register which may effectively aid the management of project risks (Patterson and Neailey, 2002).

The original approach here described is only the beginning of a much more complex risk management process, based on business strategy analysis, comparison with major competitors' reports and interviews with several process owners, directly or indirectly involved in project. Thus, this article presents the first phase of the risk assessment approach, validated on the case of a large industrial project related to the launch of an innovative mobile telecommunications system, whose references and data are undisclosed due to confidentiality issues.

2 A risk evaluation procedure

Risk identification starts here from the generic risks list proposed by Cooper et al. (2005), revised in accordance to contributions from the specific project internal reports, which have helped in identifying some peculiarities of the analysis. Then, 40 potential risks have been classified (Table 1) and divided among:

- financial and capital risks, that affect company liquidity and assets, including those risks related to long-term debts with credit institutions
- economic risks, which affect the profitability of the project and the relationships of the company with the external environment
- technical risk, related to technology and to the key equipments of the project.

Table 1 Risk mapping

Type	*Risk*
Financial and capital risk	• Failure to pay or delayed refunding
	• Deficiency of funding sources
	• Decrease in shareholder value
	• Equity funding and ownership
	• Impairment of the brand value due to problems of system reliability
	• Legal actions against the company
	• Mismatch with the holding company's goal
	• Funding withdrawn or delayed
Economic risk	• Stability of joint ventures, partnerships
	• Demand management
	• Problems from customers bargaining power
	• Reliability of supplier
	• Reliability of dealers
	• Ability to meet contract commitments
	• Difficulties in installing new gateways
	• Loss of customers for high prices
	• Excessive dependence on niche products
	• Increase of competitors number

Table 1 Risk mapping (continued)

Type	*Risk*
Economic risk	• Negative feedbacks from services sold
	• Operations constraints
	• Increase in direct competition pressure (existing competitors)
	• Increase in indirect competition pressure (existing competitors)
	• Interest rate variation
	• Exchange rate variation
	• Operational problems in penetrating developing countries
Technical risk	• Insufficient service coverage service
	• Loss of broadband services customers
	• Launch failures
	• Reduction of the available frequency spectrum
	• Amendment of security requirements
	• Defects in purchased products
	• Damages to the network gateway
	• Damages to satellites control centres
	• Damages to satellites
	• Emergence of alternative technologies (space side)
	• Emergence of alternative technologies (land side)
	• Postponement of launch
	• Reliability of terminal technology
	• Reliability of space components
	• Reliability of ground components

Then, four domains where evaluating the potential consequences of events have been identified. The choice to define four different domains comes from the need to use homogeneous criteria to compare risks, although these are extremely different. The four domains used to assess the severity of possible consequences, are:

- costs (x): possible cost increases that involve raising of required budget for the project
- time (τ): possible delays of the project over the scheduled timetables
- performance (π): possible deterioration of the service quality and/or service level
- reputation (ρ): related to all other consequences that, even if cannot be brought back to the aforementioned three domains, can damage the company's image.

Five levels, in terms of probability of occurrence (Table 2) and severity (Table 3) have been thus defined for each domain.

Table 2 Occurrence probability (P) levels and values

Level	*Value*	*Likelihood*	*Frequency description*
A	0.9	Very likely	The event may occur several times during the same year
B	0.7	Likely	The event may occur several times during a period of 1–5 years
C	0.5	Possible	The event could occur more than once within 15 years
D	0.3	Unlikely	The event might occur once in 15 years
E	0.1	Rare	The event should not occur before 15 years (life of the project)

Table 3 Consequences severity (C) levels and values

Level	*Value*	*Cost*	*Time*	*Performance*	*Reputation*
A	0.9	Budget increase >25%	Large delays, non-recoverable	Performance and marketing are seriously compromised	Damage to company's image at an international level
B	0.7	Budget increase 10%–25%	Large delays, only partially recoverable	Performance is compromised but partially restorable	Damage to company's image at a national level
C	0.5	Budget increase 5%–10%	Small delays, only partially recoverable	Local and/or transitory inefficiencies. Performance is acceptable but lower than expected	Small claims
D	0.3	Budget increase <5%	Minor delays, almost fully recoverable	Performance slightly worse than expected, reduced quality	Reduced consensus only in small geographical areas or specific market segments
E	0.1	Budget almost unchanged	No significant delays	Performance substantially in line with expectations	No damage to the company's image

To determine the risk level according to Cooper's approach (2) and taking into account four different domains, two different indicators can be computed per each risk:

1 R_P = primary risk level, in which the component C is computed as the average of the severity values in each domain:

$$R_p = P + C_{avg} - \left(P * C_{avg}\right) \tag{3}$$

2 R_s = secondary risk level, in which the component C is the maximum among the severity values in each domain:

$$R_s = P + C_{max} - \left(P * C_{max}\right) \tag{4}$$

Table 4 Risk levels for the analysed project

Risk	*C*				*P*	*R*		*Group*
	χ	τ	π	ρ		R_s	R_p	
Loss of broadband services customers	D	E	E	C	A	0.95	0.93	●
Increase in competitors number	C	E	E	E	A	0.95	0.92	●
Reliability of space components	A	B	A	A	E	0.91	0.87	●
Failure to pay or delayed refunding	A	B	B	A	D	0.93	0.86	●
Insufficient service coverage	D	E	D	D	B	0.79	0.78	●
Increase in direct competition pressure	C	E	E	E	B	0.85	0.76	●
Decrease in shareholder value	C	D	C	B	C	0.85	0.75	●
Funding withdrawn or delayed	A	B	B	C	E	0.91	0.73	●
Damage to satellites	B	B	B	B	E	0.73	0.73	●
Deficiency of funding sources	C	C	C	B	D	0.79	0.69	◍
Reliability of ground components	B	C	B	B	E	0.73	0.69	◍
Ability to meet contract commitments	B	C	D	B	D	0.79	0.69	◍
Mismatch with the holding company's goal	E	C	D	D	C	0.75	0.65	◍
Emergence of alternative technologies (space side)	A	E	C	A	E	0.91	0.64	◍
Reliability of dealers	D	E	E	C	C	0.75	0.63	◍
Reduction of the available frequency spectrum	D	E	C	E	C	0.75	0.63	◍
Excessive dependence on niche products	D	D	E	D	C	0.65	0.63	◍
Reliability of supplier	C	B	D	D	D	0.79	0.62	◍
Demand management	C	E	E	E	C	0.75	0.6	◍
Increase in indirect competition pressure	C	E	E	E	C	0.75	0.6	◍
Operational problems in developing countries	D	C	C	D	D	0.65	0.58	◌
Reliability of terminal technology	C	C	E	D	D	0.65	0.55	◌
Launch failures	C	A	C	E	E	0.91	0.55	◌
Postponement of launch	D	B	D	E	D	0.79	0.55	◌
Damages to satellite control centres	D	C	B	C	E	0.73	0.55	◌
Damages to the network gateway	D	D	C	D	D	0.65	0.55	◌
Impairment of the brand value due to reliability	D	E	E	B	D	0.79	0.51	◌
Defects in purchased products	D	C	C	C	E	0.55	0.51	◌
Loss of customers for high prices	D	E	E	B	D	0.79	0.51	◌
Operations constraints	E	D	D	D	D	0.51	0.48	○
Emergence of alternative technologies (land side)	C	C	E	C	E	0.55	0.46	○
Interest rate variation	C	E	E	E	D	0.65	0.44	○
Legal action against the company	D	E	E	D	D	0.51	0.44	○
Exchange rate variation	C	E	E	E	D	0.65	0.44	○
Stability of joint ventures, partnerships	C	C	E	D	E	0.55	0.42	○
Amendment of security requirements	D	E	E	E	D	0.51	0.41	○
Difficulty in installing new gateways	C	D	D	D	E	0.55	0.42	○
Negative feedbacks from services sold	D	E	E	E	D	0.51	0.41	○
Problems from customers bargaining power	B	E	E	D	E	0.73	0.37	○
Equity funding and ownership	E	D	E	C	E	0.55	0.33	○

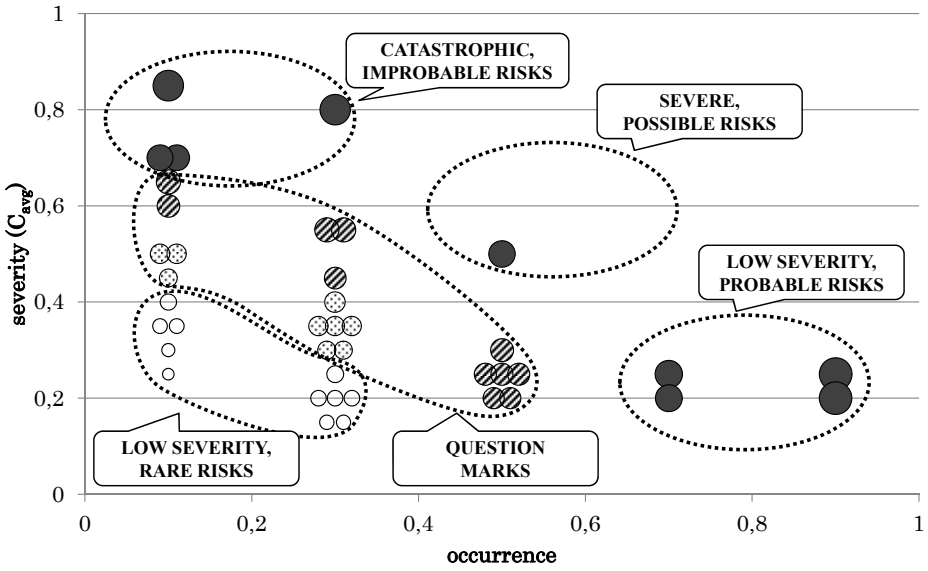
The second indicator obviously returns a higher risk level, but, dealing with risks that could entail very heterogeneous consequences among the four domains, may provide an over pessimistic score. Thus, for each risk, R_p value will be mainly used in the analysis while, however, both indicators are reported in Table 4.

In Table 4, risks are ordered by decreasing values of primary risk (R_p) and, in order to define priorities for mitigation actions, the potential impacts have been divided into four groups, in according to the guidelines of the ISO/DIS 31000 standard:

- Critical risks (black spots): risk with $R_p \geq 0.7$. A prudent risk reduction and timely mitigation measures are needed.
- High risks (striped spots): risk with $0.6 \leq R_p < 0.7$. A more thorough check to assess the opportunity of appropriate interventions needs to be performed.
- Average risks (dotted spots): risk with $0.5 < R_p \leq 0.6$. Risks with acceptable consequences, that should be addressed with lower priority.
- Low risks (white spots): risk with $R_p < 0.5$. No urgent actions are needed.

As already mentioned, the evaluations shown in Table 4 come from the advices of experts and of technical personnel working on the specific project. Plotting the risks on a diagram in which C_{avg} is the indicator of the consequences severity, P that of probability and using R_p as a third dimension (the size of each spot) we get the graph in Figure 3.

Figure 3 Occurrence, severity and risk levels



On top of being divided into four groups based on the primary risk levels, risk can be further classified according to their position on the graph in Figure 3. This leads back to the traditional consideration: the critical risks – which need urgent and un-deferrable countermeasures – can be either "low severity and probable" (where the high value of R_p mainly comes from the high probability of occurrence) or "catastrophic and improbable"

(where the criticality mainly originates from the severity of consequences). For example, the risk associated with "loss of broadband services customers" (i.e., the risk that the primary market for the new TLC system gets reduced only to voice communication users, while the more profitable heavy-users market share would prefer the competitors' technologies) is critical because of its reasonable likelihood; on the contrary, the risk associated with "reliability of space components" is critical due to the devastating consequences, despite its low occurrence probability thanks to the traditional space components design approach with multiple redundant apparatus. Obviously, the elements in these different classes should be treated differently.

3 Coping with detectability issues

At least once in the life, each risk manager had thought that a two-parameter classification (probability and severity) is a too simplistic and reductive approach to take into account the wide diversity of risk types. For this reason, similarly to the FMECA methodology, in this approach an additional parameter – detectability, V – has been introduced in order to discriminate between risks can be mitigated by a prompt intervention and risks that, in contrast, cannot be anticipated in any way. Even though an increase in the probability of occurrence results, in many cases, in an increase of the detectability and vice versa, it is however important to keep separate the two aspects: by way of example, dealing with electronic components reliability, it is common to manage with risks associated to high occurrence probability that, however, cannot be detected in advance; this usually results in expensive countermeasures, i.e., components redundancy.

Table 5 Detectability and correction factor

Level	*Detectability*	*$\Delta(R_p; R_s)$*	*Description*	*R_p increase*
A	Not detectable	≥0.20	The event occurs rapidly and the consequences can be identified only after the occurrence or within a time windows which is not sufficient to implement any appropriate countermeasure – the difference between primary and secondary level of risk is at least equal to 0.20	+0.10
B	Not detectable	<0.20	The event occurs rapidly and the consequences can be identified only after the occurrence or within a time windows which is not sufficient to implement the appropriate strategy – the difference between primary and secondary level of risk is lower at 0.20	+0.05
C	Detectable	≥0.20	The event is anticipated by detectable signs sufficiently in advance for the preparation of countermeasures – the difference between primary and secondary level of risk is at least equal to 0.20	0
D	Detectable	<0.20	The event is anticipated by detectable signs sufficiently in advance for the preparation of countermeasures – the difference between primary and secondary level of risk is less than 0.20	–0.05

Different empirical approaches have been proposed by experts in order to cope with detectability issues in risk management, and neither a focused literature review helped in selecting a unique methodology. The heuristic method presented in this work does not pretend to represent a universal solution but propose a practical approach that has clearly demonstrated its effectiveness inside the selected application: per each risk, two detectability levels are estimated (detectable/not detectable) and a correction factor is computed in accordance to the difference between the values of primary (R_p) and secondary (R_s) risk level, as it is outlined in Table 5.

As far as the choice of the increase value magnitude is concerned, the ±0.05 value has been fixed in order to forbid an element placed at the bottom list of a group (in example, average risks) to raise to the higher group (in example, high risks). In most cases, this will not happen even though the difference between primary and secondary level of risk is equal or greater than 0.20. With these corrections, primary risk values are recomputed and shown in Table 6 under the column R^*_p (Table 6).

Table 6 Risk levels corrected through the detectability factor

Risk	*P*	*D*	*R*		R_s–R_p	ΔR_p	R^*_p	*Group*
			R_s	R_p				
Loss of broadband services customers	A	D	0.95	0.93	0.025	–0.050	0.875	●
Increase in competitors number	A	D	0.95	0.92	0.030	–0.050	0.870	●
Reliability of space components	E	B	0.91	0.87	0.045	0.050	0.915	●
Failure to pay or delayed refunding	D	D	0.93	0.86	0.070	–0.050	0.810	●
Insufficient service coverage	B	D	0.79	0.78	0.015	–0.050	0.725	●
Increase in direct competition pressure	B	D	0.85	0.76	0.090	–0.050	0.710	●
Decrease in shareholder value	C	B	0.85	0.75	0.100	0.050	0.800	●
Funding withdrawn or delayed	E	B	0.91	0.73	0.180	0.050	0.780	●
Damage to satellites	E	B	0.73	0.73	0.000	0.050	0.780	●
Deficiency of funding sources	D	D	0.79	0.69	0.105	–0.050	0.635	▨
Reliability of ground components	E	B	0.73	0.69	0.045	0.050	0.735	●
Ability to meet contract commitments	D	D	0.79	0.69	0.105	–0.050	0.635	▨
Mismatch with the holding company's goal	C	D	0.75	0.65	0.100	–0.050	0.600	▨
Emergence of alternative technologies (space side)	E	A	0.91	0.64	0.270	0.100	0.740	●
Reliability of dealers	C	D	0.75	0.63	0.125	–0.050	0.575	⊙
Reduction of the available frequency spectrum	C	D	0.75	0.63	0.125	–0.050	0.575	⊙
Excessive dependence on niche products	C	D	0.65	0.63	0.025	–0.050	0.575	⊙
Reliability of supplier	D	D	0.79	0.62	0.175	–0.050	0.565	⊙
Demand management	C	D	0.75	0.6	0.150	–0.050	0.550	⊙
Increase in indirect competition pressure	C	D	0.75	0.6	0.150	–0.050	0.550	⊙

Table 6 Risk levels corrected through the detectability factor (continued)

Risk	*P*	*D*	*R*		R_s–R_p	ΔR_p	R^*_p	*Group*
			R_s	R_p				
Operational problems in developing countries	D	D	0.65	0.58	0.070	–0.050	0.530	
Reliability of terminal technology	D	B	0.65	0.55	0.105	0.050	0.595	
Launch failures	E	A	0.91	0.55	0.360	0.100	0.650	
Postponement of launch	D	A	0.79	0.55	0.245	0.100	0.645	
Damages to satellite control centres	E	B	0.73	0.55	0.180	0.050	0.600	
Damages to the network gateway	D	B	0.65	0.55	0.105	0.050	0.595	
Impairment of the brand value due to reliability	D	C	0.79	0.51	0.280	0.000	0.510	
Defects in purchased products	E	D	0.55	0.51	0.045	–0.050	0.455	
Loss of customers for high prices	D	C	0.79	0.51	0.280	0.000	0.510	
Operations constraints	D	D	0.51	0.48	0.035	–0.050	0.425	
Emergence of alternative technologies (land side)	E	B	0.55	0.46	0.090	0.050	0.510	
Interest rate variation	D	A	0.65	0.44	0.210	0.100	0.540	
Legal action against the company	D	B	0.51	0.44	0.070	0.050	0.490	
Exchange rate variation	D	A	0.65	0.44	0.210	0.100	0.540	
Stability of joint ventures, partnerships	E	D	0.55	0.42	0.135	–0.050	0.365	
Amendment of security requirements	D	D	0.51	0.41	0.105	–0.050	0.355	
Difficulty in installing new gateways	E	D	0.55	0.42	0.135	–0.050	0.365	
Negative feedbacks from services sold	D	D	0.51	0.41	0.105	–0.050	0.355	
Problems from customers bargaining power	E	C	0.73	0.37	0.360	0.000	0.370	
Equity funding and ownership	E	C	0.55	0.33	0.225	0.000	0.325	

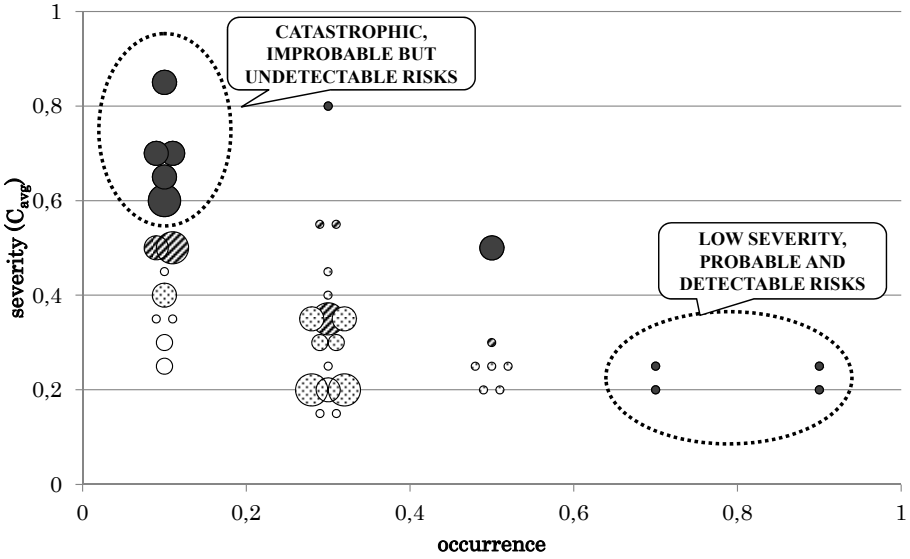
In Table 6, risks are sorted as in Table 2: last column shows that several risks changed group: the introduction of the corrective factor has resulted in raising the attention to some specific risks that, as to the previous step, may have been underestimated. For example, risks associated with launch failures or postponement, with the emergence of alternative technologies, with the reliability of ground components, with potential damages to satellite control centres and with interest rate variation and exchange rate variation seems to need more attention. At the top of the list, also risks associated with the possible decrease in shareholder value, with funding withdrawn or delayed, with potential damage to satellites and with reliability of space components raise in importance, even if they do not change class because were already labelled as critical risks in the previous step. Despite the reader may not be familiar with the technical issues related to satellite communications systems projects, relying on the public knowledge of the international financial situation and of the technology renewal pace on top of common sense, these considerations seem reasonable.

Meanwhile, risks associated with reliability of dealers, reduction of the available frequency spectrum, excessive dependence on niche products, reliability of supplier,

demand management and the increase in indirect competition shifted to the lower group. These, indeed, represent potential problems that may be treated more evenly and without that urgency. Also these reflections sound realistic. This last step had thus succeeded in defining each risk priority more accurately.

Figure 4 shows the new risk map after the update of R^*_p value. Comparing Figure 3 and Figure 4, it is possible to check that several spots had changed pattern (and thus, group).

Figure 4 Occurrence, severity and detectability



Differently from Figure 3, the size of the point now indicates the value associated with the detectability factor, reported in Table 5. Among the critical risks group (black spots), two main set can be further identified: detectable risks associate with low severity consequence and high probability (loss of broadband services customers, increase in competitors number, failure to pay or delayed refunding. insufficient service coverage, increase in direct competition) and undetectable risks associated with catastrophic, though improbable, consequences (those that Taleb would call 'black swans': reliability of space components, funding withdrawn or delayed, decrease in shareholder value, damage to satellites, reliability of ground components, emergence of alternative technologies on space side). All of these risks in Figure 4 were classified at the same importance. However, once more the reader should agree that the element belonging to these two sets should be clearly approached in different ways.

4 Concluding remarks

One should always remember that a perfect and precise procedure of risk assessment does not save from risk occurrence neither helps in mitigating the consequences. Risk identification, analysis and evaluation are only the first steps in the risk management

procedure, where the organisation of countermeasures represents the most effective phase. However, a great care should be given to the risk assessment procedure, even because it is deeply affected by the analyst skills and competences. Even a clever analyst will inevitably be influenced by his experience: he may concentrate on risks that recall past situations and accidents he have been involved in, or he have been informed of; while ignoring dangerous threats only because are perceived to be extremely improbable and, thus, far from his perception. This work aimed at stressing the importance of those undetectable risks associated to rare but disastrous consequences.

The different approach in computing the risk factor – leaving behind the traditional multiplication of severity and probability – together with the introduction of a corrective factor to keep into account detectability, may help the risk manager not to underestimate hidden threats which can really compromise the development of the project, instead of approaching uniquely those risks linked to probable but manageable consequences.

On top of this, in this work a classification of the main domain where to assess the severity of possible impacts has been introduced (time, cost, performance and/or reputation). This came from the need of using homogeneous criteria to compare risks. On the other hand, however, it is clearly necessary to define different mitigation strategies depending on which domains are affected by the possible consequences. In this sense, computing factor C as an average (C_{avg}) or as a maximum (C_{max}) within the levels of primary and secondary risk it is an evident limit that may be removed with further research.

References

Cooper, D.F., Grey, S., Raymond, G. and Walker, P. (2005) *Project Risk Management Guidelines: Managing Risk in Large Projects and Complex Procurements*, John Wiley & Sons, Chichester.

Han, S.H., Kim, D.Y., Kim, H. and Jang, W-S. (2008) 'A web-based integrated system for international project risk management', *Automation in Construction*, Vol. 17, No. 3, pp.342–356.

Locatelli, G. and Mancini, M. (2010) 'Risk management in a mega-project: the universal EXPO 2015 case', *International Journal Project Organisation and Management*, Vol. 2, No. 3, pp.236–253.

Miller, R. and Lessard, D. (2001) 'Understanding and managing risks in large engineering projects', *International Journal of Project Management*, Vol. 19, No. 8, pp.437–443.

Olsson, R. (2007) 'In search of opportunity management: is the risk management process enough?', *International Journal of Project Management*, Vol. 25, No. 8, pp.745–752.

Patterson, F.D. and Neailey, K. (2002) 'A risk register database system to aid the management of project risk', *International Journal of Project Management*, Vol. 20, No. 5, pp.365–374.

Taleb, N.N. (2007) *The Black Swan: The Impact of the Highly Improbable*, Random House, London.

Van Wyk, R., Bowen, P. and Akintoye, A. (2008) 'Project risk management practice: the case of a South African utility company', *International Journal of Project Management*, Vol. 26, No. 2, pp.149–163.

Zwikael, O. and Sadeh, A. (2007) 'Planning effort as an effective risk management tool', *Journal of Operations Management*, Vol. 25, No. 4, pp.755–767.