UPGRADE is the European Journal for the Informatics Professional, published bimonthly at <http://www.upgrade-cepis.org/>

Publisher
UPGRADE is published on behalf of CEPIS (Council of European Professional Informatics Societies, <http://www.cepis.org/>) by **Novática** <http://www.ati.es/novatica/>, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática,* <http://www.ati.es/>)

UPGRADE monographs are also published in Spanish (full version printed; summary, abstracts and some articles online) by **Novática**

UPGRADE was created in October 2000 by CEPIS and was first published by **Novática** and **INFORMATIK/INFORMATIQUE**, bimonthly journal of SVI/FSI (Swiss Federation of Professional Informatics Societies, <http://www.svifsi.ch/>)

UPGRADE is the anchor point for UPENET (UPGRADE European NETwork), the network of CEPIS member societies' publications, that currently includes the following ones:

- **Informatik-Spektrum**, journal published by Springer Verlag on behalf of the CEPIS societies GI, Germany, and SI, Switzerland
- **ITNOW**, magazine published by Oxford University Press on behalf of the British CEPIS society BCS
- **Mondo Digitale**, digital journal from the Italian CEPIS society AICA
- **Novática**, journal from the Spanish CEPIS society ATI
- **OCG Journal**, journal from the Austrian CEPIS society OCG
- **Pliroforiki**, journal from the Cyprus CEPIS society CCS
- **Pro Dialog**, journal from the Polish CEPIS society PTI-PIPS

Cover page designed by Concha Arias Pérez
"Non-Fragmented Minds" / © ATI 2007
Layout Design: François Louis Nicolet
Composition: Jorge Llácer-Gil de Ramales

Editorial correspondence: Llorenç Pagés-Casas <pages@ati.es>
Advertising correspondence: <novatica@ati.es>

UPGRADE Newslist available at
<http://www.upgrade-cepis.org/pages/editinfo.html#newslist>

ISSN 1684-5285

Monograph of next issue (December 2007)

" Free Software: Scientific and Technological Innovation "

(The full schedule of **UP**GRADE is available at our website)

CEPIS **UP**GRADE

The European Journal for the Informatics Professional
http://www.upgrade-cepis.org

Vol. VIII, issue No. 5, October 2007

Monograph: Advanced Information Systems Project Management (published jointly with Novática*)

Guest Editor: *Julián Marcelo-Cocho, Antonio Teti, and José-María Torralba-Martínez*

UPENET (UPGRADE European NETwork)

CEPIS NEWS

---

* This monograph will be also published in Spanish (full version printed; summary, abstracts, and some articles online) by **Novática**, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*) at <http://www.ati.es/novatica/>.

Risks and Project Management

Julián Marcelo-Cocho and Marta Fernández-Diego

The management of risk in projects (including failure to reach objective) is always dependent on the complexity of the project and the uncertainty of the objective. These are the two main factors that explain the development of a project, and it is here that adequate countermeasures for risk-reducing preventive countermeasures can be found, as well as palliative countermeasures for use when leading a project in the planning, and increasingly, in the monitoring stage.

Keywords: Complexity, Effectiveness, Efficiency, Risk, Success, Uncertainty.

1 Background to Risk Management in Projects

The generic acceptance of the concept of "risk" refers to **business risk**, and the word carries some psychological dualism that is more positive than negative. It is generally hoped that risk will evolve towards **opportunity**; however it should evolve towards the **insecurity** which permeates the concept of **system risk** (including information risks). In a project, risk consists in developing an ***"attained final state"*** (AFS) that differs from the ***"desired final state"*** (DFS) – which is the "objective" (outside the project itself). A project is seen as a dynamic system "adapting" that objective (see Figure 1).

Project Risk Management PRM is a technique that manages the resources available to a project in order to limit the difference between AFS to DFS. If the difference exceeds an established limit, then a risk of not meeting the objective arises. To assure a satisfactory result, decisions are usually required regarding new actions to reduce that difference. The negative aspect of the concept of risk, defined as the "likelihood of loss", underlies current developments in research, science, engineering, economy, society, and everyday life.

Some functional relations underlie the risks of a **computing project** related to an **information sub-system** (and its risks) of some **business system** (and its risks), given that:

- The business system functionality requires information sub-systems built with these type of computing projects
- A software construction project carries "project" type risks that imply the existence of "system" risks in the information sub-system.
- These project risks also imply "business" risks in the business system supporting the information sub-system under construction.

After a **first generation** of **Project Risks Management PRM1** based on questionnaires and expert advice, the **second generation PRM2** began the risks analysis at the launching of a project and plans safeguards or countermeasures to reduce risk, with a wide range of models available such as the Boehm [1], Hall[1] [2], Jones[2] [3] or SERIM [4] models**.** This preventive vision of planning is usually seen

Authors

Julián Marcelo-Cocho is a Doctor of Engineering in Computer Science and holds a Master in Industrial Enterprise Management. He currently heads research in the Department of Enterprise Organization of the Universidad Politécnica de Valencia and lectures in IT Project Management at a graduate and postgraduate level. In his more than 40 years' professional experience in the IT and related sectors he has held a great many different positions in national and multinational enterprises, and public, local, regional, and international organizations (such as the UN's Intergovernmental Bureau for Informatics). He was founder and former Chief Editor of Novática and other publications in the IT sector. <jmarcelo@doe.upv.es>.

Marta Fernández-Diego holds a European Doctorate in Electronic and Telecommunications Engineering. After periods of research and work in universities and multinational companies in France and Great Britain, she is currently lecturing on IT Risk and other computer-related subjects at the *Universidad Politécnica de Valencia*. <marferdi@doe.upv.es>.

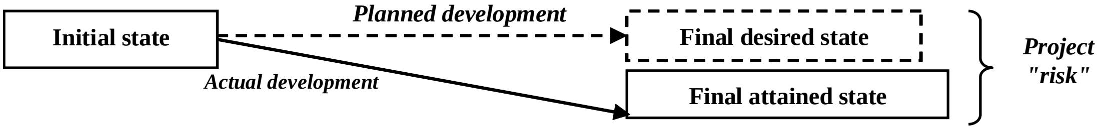


Figure 1: Project Risk seen as a Result deviating from the Objective (source: own development).

---

[1] Hall is president of the INCOSE (*International Council on Systems Engineering*) working group on risk management, and leads a project risk management working group at the Software Engineering Institute of Carnegie Mellon University.

[2] Casper Jones is the president of SPR Inc.

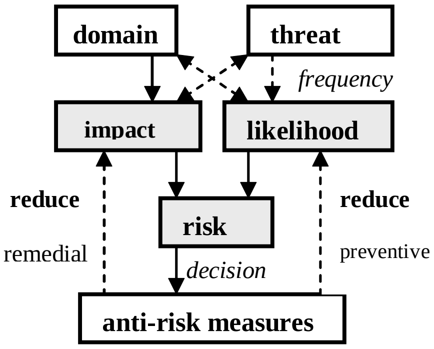


Figure 2: General Model of Risk Management (source: MAGERIT and own development).

as "theoretical" by many project managers, trained in incorporating practical "palliative" countermeasures for offsetting risks as they arise. The "tactical gap" between planners and managers has widened, and this is particularly relevant in the case of software mega-projects which are considered high risk[3]. This introduces a **third generation PRM3** of risks project management that tends to analyse, recover, and incorporate if needed, all other forms of project management – especially the practical type experiences taken from European methodological frameworks such as Euromethod and ISPL [5] or RiskMan-DriveSPI-RiskDriver[4]; as well as guided trajectories such as PMBoK [6]. In PRM3, the quasi-causality given, for example, in Euromethod and ISPL, prepares the way for **project management "by" its risks management**. This is a line that is being researched by various teams such as Moynihan [7][8][9], Barki [10], Schmidt [11][12] or INSEAD [13]**.** Their empirical work is considered promising, but to date, insufficient.

2 A Risk Management Generic Model

Some research teams have separately confirmed that there is just one underlying model in all the studies of project risks in generations PRM2 and PRM3. And the model is also common in studies of risks in computing systems and other sectors. This axiom is receiving a clear verification in the current construction of the forthcoming standard ISO 31000 (previously called ISO 25700) about "*Guidelines on principles and implementation of **risk management***", which is common to all sectors and based on a shared process of action on a model that inter-relates some defined conceptual entities and which are then interpreted according to the sector.

This model of project risk management is similar to the management models of system risks, for example MAGERIT [14] or CRAMM. These models relate six entities: assets (of the considered domain), threats, likelihood, impact, risk, and anti-risk countermeasures (see Figure 2).

2.1 Domain, Sub-domains, and Assets

In the case of project risk management PRM, its **domain** includes some assets and it delimits them from its **environment** (considering the influence of environment on the domain). Those assets that play a role in the non-fulfilment of the "objective" can be organised as a set of sub-domains whose lower levels influence the upper levels (see Figure 3).

In this way, the **success** of a project is an **asset** of the upper domain ("other assets") and accumulates the risks of all of them, acting as a generic asset with two sub-assets: efficiency and effectiveness. The "internal" project efficiency has a pre-established reference of "technical" parameters (duration, novelty, structure, coherence, etc) and "organic" parameters (such as its interest level for the actors). Effectiveness requires some "satisfactory result" providing an external reference to the project[5].

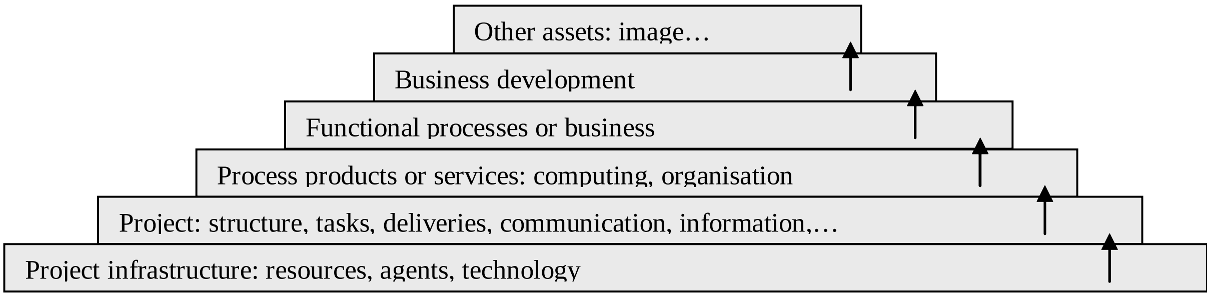


Figure 3: Assets Pyramid in Project Risk Management (source: own development).

---

[3] IEEE Software edited a monograph on Managing Megaprojects (1996) and a monograph on Project Risk Management (1997). Both marked a change of course between the generations PRM2 and PRM3.

[4] Riskman began in 1991 as an EUREKA European project undertaken by a consortium of four participants, for developing an integrated methodology and tool for risk management in all types of projects. The same team launched Drive SPI in 1997 as a risk-driven software process improvement, financed under the fourth European R&D. Drive SPI was prolonged in 1998 under the European RiskDriver initiative, financed by SPIN, as part of an action by the European Commission to promote the dissemination of best practices.

[5] **Efficiency** as global success of a project is formed by partial successes (in the sense of Rockart's critical success factors) achieving final and intermediate states for these factors: as foreseen by Rockart. In any case, the final state includes factors of client satisfaction, for example the 50 user satisfaction factors that Jones (Prentice Hall, 1994) defined qualitatively and slightly ambiguously as "quality".

Impact	**EVALUATED RISK**				
Very high	High	Very high	Very high	Very high	Very high
High	Medium	High	Very high	Very high	Very high
Medium	Low	Medium	High	High	Very high
Low	Low	Low	Medium	Medium	High
Very low	Very low	Very low	Low	Low	Medium
Likelihood	***Very low***	***Low***	***Medium***	***High***	***Very high***

Impact	**EVALUATED RISK**				
0.80	0.08	0.24	0.40	0.56	0.72
0.40	0.04	0.12	0.20	0.28	0.36
0.20	0.02	0.06	0.10	0.14	0.18
0.10	0.01	0.03	0.05	0.07	0.09
0.05	0.01	0.15	0.025	0.035	0.045
Likelihood	***0.1***	***0.3***	***0.5***	***0.7***	***0.9***

Figures 4a and 4b: Risk Evaluation in MAGERIT and in PMBoK (sources: MAGERIT and PMBoK).

43	**Factors**	***Dimensions***	***17 X-factors***	***26 Y-factors***
23	**Objective domain**	***Business system:***	1	5
		Process:	2	3
		Information:	2	1
		Agents:	3	3
		Technology:	1	2
20	**Service domain**	Process:	2	6
		Information:	2	1
		Agents:	3	3
		Technology:	1	2

Figure 5: Classification of the 43 Situational Factors (sources: ISPL and own development).

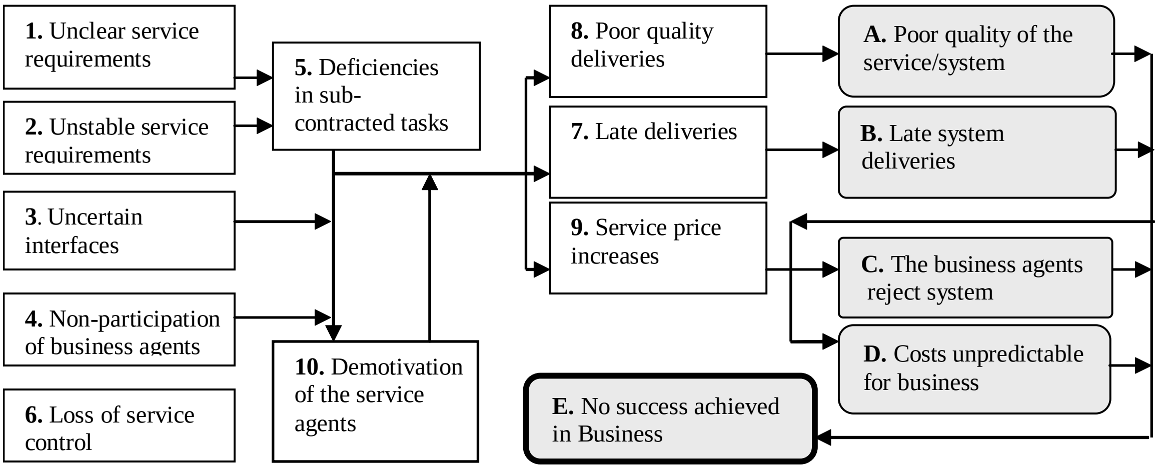


Figure 6: Business and Service Risks (sources: ISPL and own development).

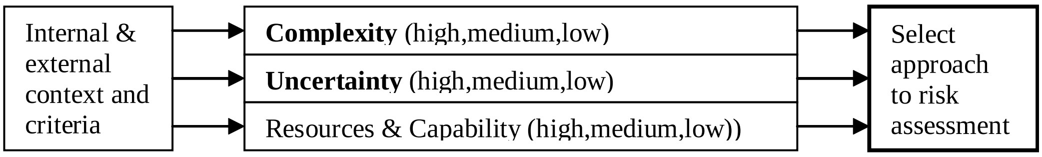
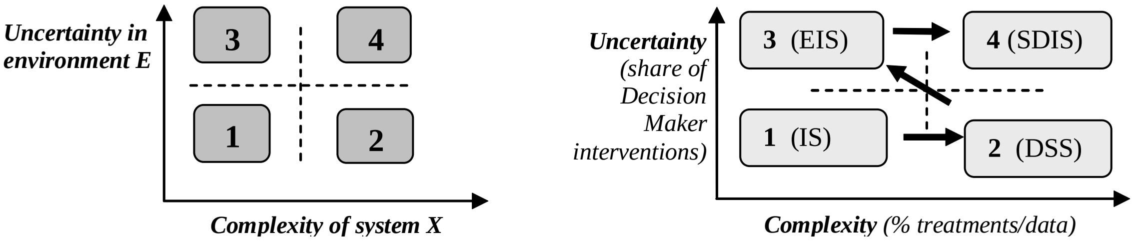


Figure 7: Factors for Selecting a Method of Estimating Risks (source: ISO 31000).



Figures 8 and 9: X and Y Factors in the Selection of Informational and Decisional Systems (source: own development).

Mega-factors		**Project Description stage**		**Construction and Installation stages**		
Complexity	**Uncertainty**	**Cooperative**	**Cognitive**	**One shot**	**Incremental**	**Evolutionary**
Low	***Low***	Expert-driven	Analytical	One shot		
High		Participatory			Incremental	
Low	***High***	Expert-driven	Experimental			Evolutionary
High		Participatory				

Figure 10: X and Y in the Organisation of a Computing Project (source: Euromethod own development).

2.2 Threat (or Risk Factor) Likelihood and Impact

Threats to project success (usually called "risk factors" in PRM) are shown in the pyramid of asset sub-domains and relate to: 1) infrastructure and the project itself (size, technological novelty, structure, agents, presence of subcontractors, relation with other projects); 2) characteristics of the products and services desired as the project "object" (complexity, dispersion, implied change, etc); 3) business processes and the business itself where products and services will be introduced (actors, scope, communication between specialists and users, environmental stability); 4) and "other assets" with subtler relationships.

Risk factors can be classified into two large groups depending on the asset group under threat: firstly, the **project** itself, its **infrastructure** and **environments**, constitute the two lower levels of the pyramid; and secondly, the **project's "referred" assets** (the **business** and its **processes**, the **products and services** obtained).

The **likelihood** of presence of each threat on each vulnerable asset is the degree of possible risk of occurrence associated with each "threatening" factor. The **Impact** measures the direct and indirect consequences of the occurrence of each threat (risk factor) that can be measured in the case of projects by the "distance" between AFS and DFS (attained and desired final states) for each analysed asset (success, satisfaction, duration, cost, structure, quality, etc). Impact may be a simple failure to achieve the objective of an asset, or may be the "degradation" of the objective of the project, in accordance with the "tree" or "chain" of aims achievable by completion of the project. The simple dysfunction of an asset does not usually constitute an impact if there is no change of state, or noticeable deterioration, or damage. A micro-deviation of the project, or the automatic re-launch of some task when the project contains mechanisms for auto-recuperation, cannot be considered an impact (although it may imply transitory forms of operation, more or less degraded, provided these are foreseen).

2.3 Risk Evaluation

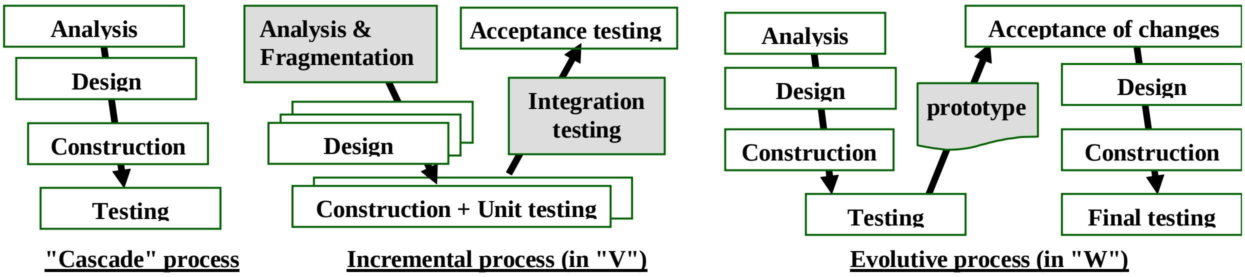
The evaluation of risk combines likelihood and impact as a qualitative matrix (according to Figure 4a taken from MAGERIT), or as a multiplication in simple cases (according to Figure 4b taken from PMBoK). In any case, the matrix is not symmetrical with respect to the diagonal, as greater weight is given to impact than likelihood: risk will be greater with high impact (and low likelihood) than with low impact (and high likelihood).

2.4 Countermeasures against Risks

The risk factors are the immediate causes of risk and play a central role in the search for effective solutions that may prevent, or reduce, these risks. This may be achieved by means of improving the existing countermeasures in the project domain and/or incorporating new countermeasures. Two types of intentional action are proposed:

- ***Preventive measures*** that act on the ***likelihood before*** the occurrence of a specific threat against an asset using awareness-raising actions, training, information, deterrence, prevention, preventive detection, or a simple accumulation of resources for responding.
- ***Palliative and re-establishing measures*** that act on ***impact and after*** it, reducing its seriousness with corrective actions, recuperation, monitoring, and follow-up.

Preventive or palliative countermeasures for projects are classified according to their period of application. Preventive countermeasures are established during the **planning** period before production; palliative countermeasures are established in the **monitoring** period of production. Few project management experts attempt to systemize these countermeasures during the monitoring period. The risk challenge that faces all



"Cascade" process

Incremental process (in "V")

Evolutive process (in "W")

Figure 11: X and Y in the Selection of the Construction and Implementation Method (source: own development).

project management methods is the formal handling of incidences, the choice of countermeasures to resolve them in the monitoring period, and a coherent feedback for risk management in the **re-planning** processes.

3 Complexity and Uncertainty – Sufficient Megafactors

Since 1996 the methodological framework **Euromethod** of the European Union has based project risk analysis and management on two risk mega-factors, **compleXity X** and **uncertaintY Y** (qualified by the limitation of the resource "time" periods). X and Y summarise the other factors causing risk, called **situational factors**. The *Information Services Procurement Library (ISPL)* adds other factors (such as poor quality or imprecision in service/system requirements, non-determination of interfaces, and de-motivation of agents). Some 43 situational factors are classified into two domains (objective and service domains) – their "Dimensions" and both mega-factors of complexity X and uncertainty Y (see Figure 5).

ISPL also uses the value of each situational factor to identify ten "service risks" (from 1 to 10) and five "business risks" (from A to E), related to the situational factors of risk in both domains and the two mega-factors of complexity and uncertainty (see Figure 6).

Euromethod-ISPL only reveals that complexity and uncertainty are mega-factors, characteristics, or ideal dimensions of risk. But it does not show if these are necessary, or even if they are sufficient. However, an increasing number of authors have affirmed their need, and finally, its sufficiency has been theoretically demonstrated. Both mega-factors are enough for dealing with any type of risk[6] [15] .

This demonstration supports a conclusive affirmation of the ISO 31000 standard about "***Guidelines on principles and implementation of risk management*"**, whose Annex B extends complexity and uncertainty to all sectors (completed with the capacity and availability of resources) to select the methodological focus for estimating risk (see Figure 7).

The importance given to complexity X and uncertainty Y does more than just illustrate risk in projects: it becomes a necessary step for a decisive advance in the taxonomy, causality, and prognostic resolution of risk. This opens the possible use of both mega-factors X and Y, as a **necessary condition**, for efficient generalisation of the project concept in many of those sectors that currently study the **theory of complexity**, in the perspective of a **theory of mega-complexity** that is wider and more explicative (in the eco-systematic sense that underlies the combination between the complexity of each system and the uncertainty produced by its environment).

4 Complexity, Uncertainty, Organisation, and Decision

An awareness of the explicative and discriminatory importance of complexity X and uncertainty Y in the theory of management is not new. However, the relation with risk is new. The investigative school led by Mélèse and Le Moigne was already classifying information systems according to the X and Y mega-factors, and relating these to the organisational system S and its environment E[7] as shown in Figure 8.

The application of X and Y enables more advanced correlations between organisational, informational, and decisional systems – and the most appropriate computing systems for dealing with them. The decision aided information systems can be organised according to the two axes X and Y[8]. This qualitative "matrix" (X,Y) establishes four types of organisational systems in its quadrants that, when translated into forms of relation or internal communication between system components, also require four types of specific informational, decisional and computing systems– as shown in Figure 9 [16].

1. X low, Y low. The **Organisation** retains the classic hierarchical pyramidal structure. Its traditional ***Information System (IS)*** (high volumes of operational data batch-handled) implies that the types of data are more numerous than their simple and repetitive treatments.

2. X high, Y low. The growing differentiation offered by a hierarchical **Organisation** requires more levels to control it and forms of communication integrated by a common **informational system –** where the implied volumes of data and the heterogeneity of the treatments are balanced; and including ***Decision Support Systems (DSS)***, i.e. expert systems.

3. X low, Y high. Organisation is fragmented into vertical divisions with little interaction to reduce risks and facilitate re-adaptations; but this implies problems of communication that must be resolved with forms of rapid access to a central informational system, culminating in an ***Executive Information System (EIS).*** This EIS implies that a human decision-maker (DM) frequently intervenes with information search systems to reduce the uncertainty of the organisational system.

---

[6] The demonstration is based on an amplification of Shannon's model (which identified types of uncertainty and the entropy related with the system environment) with identification between system complexity and another type of entropy, convergent with the previous one. It concludes that complexity and uncertainty are manifestations of the same entropy that covers the system and environment (or the "universe" of an eco-system). It is therefore sufficient to explain relations between entities inside the same system, and the system with its environment (and even more so, the internal and external relations between the entities of any project, seen as a dynamic system).

[7] "Complexity is a function of the number of elements in the system S, and the number and variety of its relations; every increase in the complexity of the structure and functioning of S gives rise to a more intense exchange of information. The uncertainty of environment E is linked to the acceleration in the evolution of E; the greater is E, greater will be the amount of information to handle". J. Mélèse. *Approches systémiques des organisations, vers l'entreprise à complexité humaine*. *Editions d'Organisation*, 1990.

[8] The horizontal axis captures the X complexity, defined now as "the rate of volume of handling with respect to data....The vertical corresponds to the intervention and role played by the decision-maker... This looks for the resolution to a problem that is a priori unknown*"*. P. Lévine, J. Pomerol. *Systèmes interactifs d'aide à la décision et systèmes experts*, Hermès, 1989)

4. X high, Y high. Organisation adopts a type of matrix structure with horizontal support functions for vertical divisions. To respond in real-time to changes, ***decisions*** are based on a system that enables rapid and specific selection of data (data-mining) from a global information base (data warehouse). This information sub-system combines the search and information treatment systems 2 and 3, in a ***Strategic Decision Information System (SDIS),*** which is formulated with two types of computing programs: the "search motors" such as those that cross the nodes of Internet type networks; and the knowledge motors that access data warehouses through "Intranet" networks and intelligently search for the required information.

Euromethod not only uses X and Y to deduce the anti-risk countermeasures required during the project monitoring stage (e.g. increasing the Production milestones and control frequencies). X and Y help focus the design of organisational, informational, and decisional systems, facilitating the organisation of a computing project in its various stages of Description, Construction, and Installation.

The Description of the result combines *the social or agent cooperative approach* (expert-driven or participatory) and the *cognitive approach* (analytical or experimental) for low or high X and Y (Figure 10). It enables also the selection of the best method and process in the Construction and Installation of the result (see Figures 10 and 11):

- "One shot" method (and the "cascade" process), only if uncertainty Y and complexity X are low
- Incremental method (and the process of fragmentation and reintegration), only if X increases
- Evolutionary method (and the prototype process), if uncertainty Y increases.

In a computing project that supports **strategic decisions**, uncertainty Y tends to prevail over complexity X. It is possible to resolve this with a DSS for routine problems and situations, but its complexity means a choice must be made between an EIS and a SDIS. ***Obtaining*** the necessary strategic information is linked to the structure of the jobs and this represents a problem of complexity, linked to the synthesis of the strategic information from disintegrated basic information.

Its ***treatment*** is not related to the size and characteristics of the primitive database, but with the level of technological maturity relative to implementing an application architecture with standardised interfaces: whether they originate from the user, the communication with other systems, the operational programming, etc.

Acknowledgements

We would like to thank the R&D&I Linguistic Assistance Office at the *Universidad Politécnica de Valencia* for their help in translating this paper.

References

[1] B. Boehm. Software Risk Management. IEEE Computer Society Press, 1989. ISBN: 0818689064.

[2] E. Hall. Managing Risk. Methods for Software Systems Development. Addison-Wesley Longman Inc., 1998. ISBN: 0201255928.

[3] C. Jones. Assessment and Control of Software Risks. Prentice Hall, 1994. ISBN: 0137414064.

[4] D. Karolak. SERIM, Software Engineering Risk Management. Ed. IEEE, 1996. ISBN: 081671947.

[5] ISPL. Information Systems Procurement Library, can be seen as the version 2 of Euromethod. <http://projekte.fast.de/Euromethod/>.

[6] PMI Standards Committee. A guide to the Project Management Body of Knowledge (PMBoK Guide). Co-edited with the American National Standards Institute as a joint norm ANSI/PMI 99-001-2000) and recognised as the IEEE Standard 1490: 2003.

[7] T. Moynihan. An Inventory of Personal Constructs for Risk Researchers. Journal of Information Technology, Vol. 11, Dec.1996.

[8] T. Moynihan. How experienced Projects Managers assess RISK. Monografía "Software Risk Management". IEEE Software, May-June 1997.

[9] T. Moynihan. Coping with IS/IT Risk Management. Springer-Verlag, 2002. ISBN: 1852335556.

[10] H. Barki, S. Rivard, J. Talbot. An Integrative Contingency Model of Software Project Development Risk. Journal of Management Information Systems, Vol. 17, Nº. 4, 2001).

[11] R. Schmidt, K. Lyytinen, M. Keil, P. Cule. A framework for identifying software project risks. Comms of the ACM, 41, 11, 1998.

[12] R. Schmidt, K. Lyytinen, M. Keil, P. Cule. Identifying software project risks: An International Delphi Study. Journal of Management Information Systems, vol.17, nº 4. 2001.

[13] A. De Meyer, C. Loch, M. Pich. On Uncertainty, Ambiguity and Complexity in Project Management. INSEAD, April 2002.

[14] A. De Meyer, C. Loch, M. Pich. Managing Project Uncertainty: From Variation to Chaos. MIT Sloan Management Review, Winter 2002.

[15] MAGERIT. The Spanish government IT Risks Analysis and Management Method <http://www.csi.map.es/csi/pg5m20.htm>. Comparable to the UK government CRAMM <http://www.insight.co.uk/products/cramm.htm>.

[16] J. Marcelo. Risks in Systems and Projects with high Complexity and/or Uncertainty. Doctoral thesis, 2004.

[17] J.L. Le Moigne. *Les systèmes de décision dans les Organisations. Presses Universitaires de France*, 1974. EAN-13: 9782130327394.