2012 Ninth International Conference on Information Technology - New Generations

A Formal Control Model for Risks Management within Software Projects

Felipe Rafael Motta Cardoso, Paulo Marcelo Tasinaffo, Denis Ávila Montini, Danilo Douradinho Fernandes, Adilson Marques da Cunha, Luiz Alberto Vieira Dias.

Brazilian Aeronautics Institute of Technology *(Instituto Tecnologico de Aeronatica – ITA)*
Sao Jose dos Campos, Brazil

felipemc@ita.br , tasinafo@ita.br , denisavilamontini@yahoo.com.br , danilodf@gmail.com , cunha@ita.br , vdias@ita.br

***Abstract* - This paper presents a proposed Formal Control Model (FCM) using a Colored Petri Net (CPN) and an inspection form for risks management within a software project. The basis for this model was the risk areas of the Capability Maturity Model Integration for Software Development (CMMI-DEV). The integration of risk elements from a formally defined quality model using a graphical and mathematical modeling tool has provided risks management. On the context of a Management Information System (MIS), a FCM prototype was developed to reduce human inference dependences, supporting organizational goals to track critical points for decision makers. The major contribution of this paper was the FCM conceptualization and application. The proposed model was applied to a project within the financial department of an enterprise CMMI level 5. It was able to identify, control, and manage risks of software development using a SG concept of CMMI risk applied to certain other CMMI PAs. At the end, a successful case study was performed involving the two experiments of Project Planning (PP) and Risk Management (RSKM). Their assessments have shown that after the proposed FCM execution, PENDING activities were completely fixed.**

Keywords: Software Project Risks Management, Petri Nets, Capability Maturity Model Integration for Development - CMMI-DEV, Formal Methods, Management Information System.

I. INTRODUCTION

Enterprises are increasingly using information systems to do businesses. Security incidents can direct and negatively impact on enterprises' images and also on their trust relationships with customers, networks and suppliers [1].

Information analysis has been one of the main key factors for conquering new markets and keeping existing ones. It has required mechanisms involved in information handling to be confidential, fair, available, and free from ambiguity.

In spite of security incident occurrences, organizations continuously have been operating and creating values to its stakeholders. Information security has been including broader concepts, not only related to technologies and protection tools. The concept of security has been added as one of the pillars that supports the business strategy for decision makers.

A safe development of information systems requires the use of methods, techniques, and tools that provide a semantic and systemic analysis of project risks throughout its software life cycle.

The utilization of continuous improvement concepts based on evolutionary models (or maturity processes) supports the software development. In this research, risk elements which impact on project objectives are addressed.

The main concern with processes improvements has been leading large organizations to develop and maintain the best practices models, showing which guidelines reflect success or failure. One of the models used and accepted by the world community is the Capability Maturity Model Integration (CMMI) [2], developed by the Software Engineering Institute (SEI).

The CMMI assesses the quality of the organizations processes and provides guidance for what should be done or changed in order to attain more advanced maturity levels. The extraction of the CMMI risk areas and the use of a mathematical formalism to develop a model for risks management provide an important element as part of a Management Information System (MIS) [3] to assist an organization.

Software systems may have two types of complexity: essential and accidental. The essential complexity of software systems increases as computer applications deal with growing number of requirements and critical variables [4]. Ambiguous requirements raise the accidental complexity on risks management for a software project development.

A solution that can help in managing the accidental complexity is the use of a Formal Control Model (FCM). A FCM supports a MIS [3], to verify if the key points of a project solve the proposed problem, through a formal approach.

In a context of quality control, backed by security in the development of software projects, this research paper presents a prototype of a FCM that is able to verify the behavior of a generated product, considering its specification.

It describes a fragment of an ongoing research taking place at the Computer Science Department of the Brazilian Aeronautics Institute of Technology (ITA). It presents a prototype of a Formal Control Model for the Risk Management of a Software Project.

978-0-7695-4654-4/12 $26.00 © 2012 IEEE
DOI 10.1109/ITNG.2012.105

This FCM application provides better inspections within project information systems and dependences reductions on human inferences. To this end, it is proposed the Colored Petri Nets modeling.

A Petri Net (PN) provides a mathematical representation and has analysis mechanisms that, given a finite state model of a system and a formal property, the specified behavior of the system can be checked [5]. In process modeling, it provides traceability in each operation stage.

Some properties of Petri Net (PN) have been studied and shown to be comprehensive and applicable to many areas of knowledge such as: chemical engineering and business administration. Petri Nets have been also widely exploited in computer science and electronic engineering, particularly in software/hardware project, fault diagnosis, among others [5] [6] [7] [8] [9] [10].

The FCM structure is comprised of risks Process Areas (PA) of the Capability Maturity Model Integration for Development (CMMI-DEV) [2].

The PAs that have been used are: the Project Planning (PP), focusing on a Specific Practice (SP), identifying and analyzing project risks and its related sub-practices; the Project Monitoring and Control (PMC), focusing on a SP, which risks previously identified and its related sub-practices are monitored; and the Risk Management (RSKM) aimed at identifying potential problems before they occur.

The development of models (that integrates elements facilitating the identification, monitoring, and managing of risks, from a quality model formally defined by a Petri Net) facilitates the monitoring of critical projects by decision makers. Organizational objectives can be achieved by using prototype models.

This paper is organized into six sections. Besides this introduction, the second section describes the main concepts of the CMMI-DEV, focusing on PAs related to the FCM. The third section tackles the basic characteristics of PNs, its use in the conceptual model of software development, and some techniques to analyze the model. The fourth section presents a prototype of the proposed FCM architecture with the PAs used in CMMI-DEV. The fifth section describes a case study. Finally, some conclusions and perspectives are presented in the sixth section.

II. FOUNDATIONS USED OF THE CMMI

The proposed FCM was composed of the CMMI PAs to derive an instrument for manual inspection in order to support semantically using a Petri Net manual modeling.

The Capability Maturity Model Integration - CMMI is a quality model for the evaluation and improvement of an organization process maturity. It represents the integration and evolution of: the Capability Maturity Model for Software (SW-CMM); the System Engineering Capability Model (SECM); and the Integrated Product Development CMM (IPD-CMM) [11].

The CMMI provides organizations with a guide on how to control their processes to develop and maintain systems, and how to evolve toward the culture of excellence management. It is designed to guide Information Technology (IT) organizations into selection strategies. This is done for process improvement, by determining their current maturity processes and identifying their most critical issues on quality and process improvement. The CMMI supports two approaches: one "per stage", such as SW-CMM; and other "continuous", similar to ISO/IEC 15504 [12].

In the "per stage" approach, the organization should achieve a set of pre-defined objectives for all PAs prescribed by the model to reach the next level.

In the "continuous" approach, a Process Area (PA) may be selected for implementing quality and maturity goals, allowing only the fulfillment of general and specific objectives for each defined PA of maturity level. The CMMI-DEV PAs can be grouped into four categories as shown in Table 1 [2].

TABLE I. THE CMMI-DEV PROCESS AREAS (PAS) CATEGORIES [2]

The CMMI-DEV Process Areas (PAs) Categories	
Categories	**Process Areas (PAs)**
Process Management	Organizational Process Definition (OPD)
	Organizational Process Focus (OPF)
	Organizational Training (OT)
	Organizational Process Performance (OPP)
	Organizational Performance Management (OPM)
Project Management	Quantitative Project Management (QPM)
	Project Planning (PP)
	Integrated Project Management (IPM)
	Supplier Agreement Management (SAM)
	Project Monitoring and Control (PMC)
	Risk Management (RSKM)
	Requirements Management (REQM)
Engineering	Product Integration (PI)
	Requirements Development (RD)
	Technical Solution (TS)
	Validation (VAL)
	Verification (VER)
Support	Causal Analysis and Resolution (CAR)
	Configuration Management (CM)
	Decision Analysis and Resolution (DAR)
	Measurement and Analysis (MA)
	Process and Product Quality Assurance (PPQA)

2.1 Process Areas used in the proposed model

On this paper the research scope was reduced into the Project Management category, in which the PAs of: Project Planning (PP); Project Monitoring and Control (PMC); Risk Management (RSKM) are inserted and implemented by manual

CPN modeling. All these PAs, highlighted on Table I, will be used in a proposed prototype. Each one of them is described as follows.

In the PA of Project Planning (PP), risks are identified and analyzed. Their identification and analysis involve determining the impact that some risks will bring to the project, as well as their probability of occurrence. These elements provide a holistic view from points that can prevent the occurrence of established objectives. Thus, it is possible to prioritize the above mentioned risks.

In the PA of Project Monitoring and Control (PMC), previously identified risks are monitored. In order to achieve this goal, the periodic documentation of risks is reviewed within the project status context. If any additional information is verified, it is incorporated into the inspection form to be monitored and controlled.

Within the PMC PA, the project risk status also should be reported to stakeholders. In this case, a specific risk after identified and monitored may have its priority altered during the project life cycle.

The PA of Risk Management (RSKM) aims to identify potential problems before they occur. In this case, risk management activities can be planned and carried out when necessary throughout the project life cycle, to mitigate impacts to its objectives.

Within the RSKM PA, the risk management is continuous and proactive. To this end, sources, categories of risk, and parameters surrounding them are determined in advance. With these data, a risk management strategy is established.

Table 2 presents a brief description of concepts used by CMMI-DEV. These concepts guide and determine the specificity level of study.

TABLE II. CONCEPTS DESCRIPTION OF CMMI-DEV: PROCESS AREA (PA), SPECIFIC GOAL (SG), SPECIFIC PRACTICE (SP) AND SUBPRACTICES [2]

Process Area (PA)	A set of related practices in an area that, when performed collectively, satisfy a set of important considered goals for making improvement in that area.
Specific Goal (SG)	A required model component describing the unique characteristics that must be present to satisfy the PA.
Specific Practice (SP)	A component model that is considered important in achieving the associated specific goal. A SP describes expected activities.
Subpractices	An informative model component that provides guidance for interpreting and implementing SP.

Based upon concepts of the CMMI-DEV, Figure 1 shows the strategy of obtaining the FCM, specifically under a performed scope reduction. This scope reduction aimed to extract elements addressing process risks. A mapping function of interest was performed, in order to construct the proposed prototype model, formally defined by a Colored Petri Net (CPN). To facilitate a project systemic visualization, a PN methodology was used. The proposal was to formally represent activities of the selected PA.

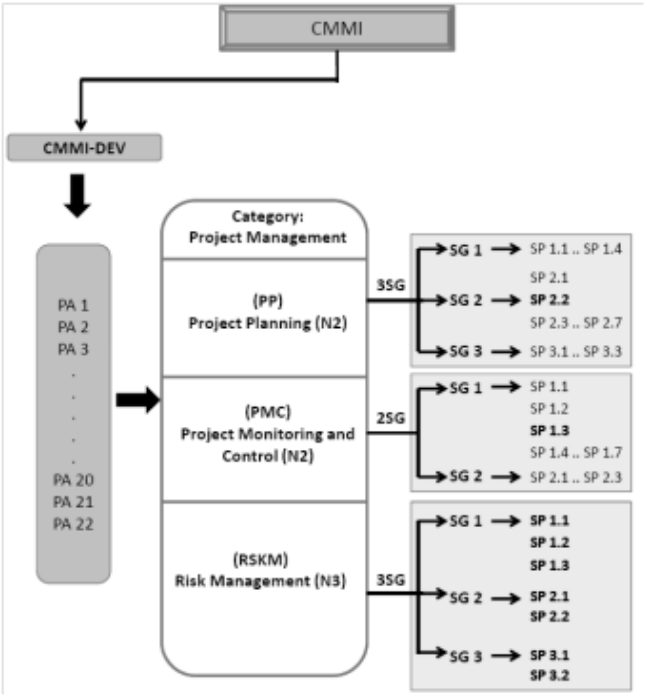

Figure 1. SCOPE REDUCTION OF THE CMMI-DEV REFERENCE MODEL TO THE PROPOSED MODEL

III. FCM IMPLEMENTED BY PETRI NETS (PN)

A Petri Net (PN) is a graphical and mathematical modeling tool applicable to many systems, specifically in the description and study of concurrent, asynchronous, distributed, parallel, non-deterministic or stochastic systems [5]. A PN can be mathematically defined as PN = (P,T,F,w, M_0), where [5]:

$P = \{\text{SetHLD, CCI, PDP, Error, AnReq, GerDemAnd, FinalStatus}\}$ a finite set of places;

$T = \{t_1, t_2 ... t_n\}$ a finite set of transitions;

$F \subseteq (P \times T) \cup (T \times P)$ the set of arcs;

$w : F \rightarrow \{1,2,...\}$ the function that defines the value of the arcs; and

$M_0 : P \rightarrow \{0,1,2...\}$ the initial marking of the network, with

$(P \cap T) = \varnothing$ and $(P \cup T) = \varnothing$

In a PN model, states are associated with places and their markings and events are associated with transitions [13]. The behavior of a system modeled by PN is described in terms of its states and its changes [5]. PNs are graphs. Graphs are classic data structures, using well known representation techniques [14] [15]. A PN is a particular kind of directed graph comprised of four types of elements [16]:

- Places – are represented by ellipses showing states of a system. They are passive components of a PN;

- Marks or Tokens – are represented by dots showing the current system status or in which state the system is. The initial marks report the primitive state of the system
- Transitions – are represented by vertices showing actions (events) of the system symbolized by lines or bars (horizontals or verticals). They are used to model the dynamic behavior of the system; and
- Arcs - connect places to transitions and transitions to places, by means of arrows indicating network execution sequences. Arcs carry marks among vertices of a graph, indicating pre-and post-conditions of a transition. They may also have labels defining the number of marks to carry from one vertex to another.

Figure 2 illustrates the visual representation of a PN basics elements.

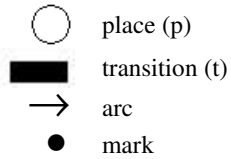

Figure 2. Visual representation of a Petri Net basics elements.

Using PN to model software process risks provides:

- Detailed and unambiguous tracking from each operation step under study;
- Formal mathematical representations and mechanisms for model analysis and verification;
- A communication language among specialists from different areas; and
- Description of static and dynamic aspects of a system.

For this work, it was used a PN extension called CPN, formally defined by Jensen [17]. The CPN aims to reduce the model size, by assigning colors to individual marks. Thus different processes or resources can be represented in a single network [18].

A CPN is described as an intuitive graphical representation to facilitate viewing the basic structure of a complex model, allowing an individual understanding of system behavior processes [17].

Within a CPN, each state can be colored. There are three states that represent the set of each analyst interpretation: red (high risk - not tolerated in projects), yellow (medium risk - needed to be reviewed in projects), and green (low risk - accepted in projects).

IV. PROPOSED MODEL

Figure 3 shows, in a high-level of abstraction, the Formal Control Model (FCM) proposed in this research. It involves the reduced scope of the CMMI Risks Process Areas (PA) aimed to extract elements addressing process risks.

The integration of used PAs allows risks identification, monitoring, and management within software projects. The formal definitions inherent to PNs, facilitates the monitoring of critical projects and occur throughout a process life cycle.

Figure 3. The conceptualization of Formal Control Model (FCM) proposed.

V. CASE STUDY

A case study was conducted in an enterprise at Sao Paulo state, Brazil, during the second semester of 2010.

The target enterprise usually performed several different activities. This case study focused only in a specific department responsible for developing financial software applications. Since this enterprise was certified CMMI level 5, a high quality model was able to be applied in this case study.

After running the Formal Control Model (FCM) proposed in this research (Figure 3), an analysis was performed from the obtained results, by using the CPN model and an inspection form. At this point, the financial department project activities of the enterprise were mapped into this research Formal Control Model (FCM).

The inspected activities of the enterprise financial department were transcribed into the inspection form and received one of the following classifications from an analyst: red (high risk - not tolerated in projects), yellow (medium risk - needed to be reviewed in projects), and green (low risk - accepted in projects).

The main results of the inspection activities provided a data collection for the proposed model. During each inspection, three activities were identified, analyzed, and classified with red indicators (**PENDING**), or high risk. The main results of these analysis and classification activities are presented in Figure 4 and Figure 5.

Phase	Activity	CMMI Acronym	Result
Demand Management in Process	PDP	RSKM	CLOSED
Demand Management in Process	CCI	RSKM	PENDING
Requirements Analysis	Set up the environment for HLD phase	RSKM	PENDING

Figure 4. Risk assessment from the PA RSKM (before corrections).

Phase	Activity	CMMI Acronym	Result
Initiation	SRS Get Preliminary	PP	CLOSED
Initiation	Prepare Project Estimates	PP	CLOSED
Initiation	Get Work Order Part A	PP	CLOSED
Initiation	Prepare WO Part B	PP	CLOSED
PSU	Develop Project Plan	PP	CLOSED
PSU	Develop Induction Manual	PP	CLOSED
PSU	Prepare Capacity Plan	PP	CLOSED
Requirements Analysis	Prepare detailed pan for phase	PP	CLOSED
Requirements Analysis	Generate alternative solutions	PP	PENDING
Requirements Analysis	Upgrade Project Plan (if necessary)	PP	PENDING
High Level Design	Prepare detailed pan for phase	PP	CLOSED

Figure 5. Risk assessment from the PA PP (before corrections).

At this point, the project manager asked the staff to redo identified non-compliance activities from Figures 4 and 5. The

inspection process was repeated to carry out the collection of new data, in order to know if PENDING issues have been fixed.

Within later performed tests, activities that had problems start presenting satisfactory results (CLOSED). Figures 6 and 7 present final results after analyses.

Phase	Activity	CMMI Acronym	Result
Demand Management in Process	PDP	RSKM	CLOSED
Demand Management in Process	CCI	RSKM	CLOSED
Requirements Analysis	Set up the environment for HLD phase	RSKM	CLOSED

Figure 6. Risk assessment of the PA RSKM (after corrections).

APN may represent the project as a whole or just the phase where an assessment is performed. The assessment and traceability processes were not restricted only at the end of the project. The same processes can be run at the end of each phase and provide corrective actions taken to reduce or neutralize risks.

Phase	Activity	CMMI Acronym	Result
Initiation	SRS Get Preliminary	PP	CLOSED
Initiation	Prepare Project Estimates	PP	CLOSED
Initiation	Get Work Order Part A	PP	CLOSED
Initiation	Prepare WO Part B	PP	CLOSED
PSU	Develop Project Plan	PP	CLOSED
PSU	Develop Induction Manual	PP	CLOSED
PSU	Prepare Capacity Plan	PP	CLOSED
Requirements Analysis	Prepare detailed plan for phase	PP	CLOSED
Requirements Analysis	Generate alternative solutions	PP	CLOSED
Requirements Analysis	Upgrade Project Plan (if necessary)	PP	CLOSED
High Level Design	Prepare detailed plan for phase	PP	CLOSED

Figure 7. Risk assessment of the PA PP (after corrections).

Figure 8 illustrates the modeling performed using a PN for activities and phases of the PA RSKM shown in Figure 4. In this experiment, three places are presented: PDP (Project Development Plan), CCI (Component of Internal Control), and SetHLD (Set High Level Design), representing activities. All acronyms and their meanings are inherent of the internal terminology used by the enterprise. It is also possible to visualize, within the modeled PN, four different places: 1) **GerDemAnd** (Demand Management in Process), and 2) **AnReq** (Requirements Analysis), representing phases under consideration; and 3) **Error,** providing an inconsistent view of the system, and 4) **FinalStatus,** indicating test results arising from activities and phases. Arcs connect places to transitions, which in its turn model the dynamic behavior of the system.

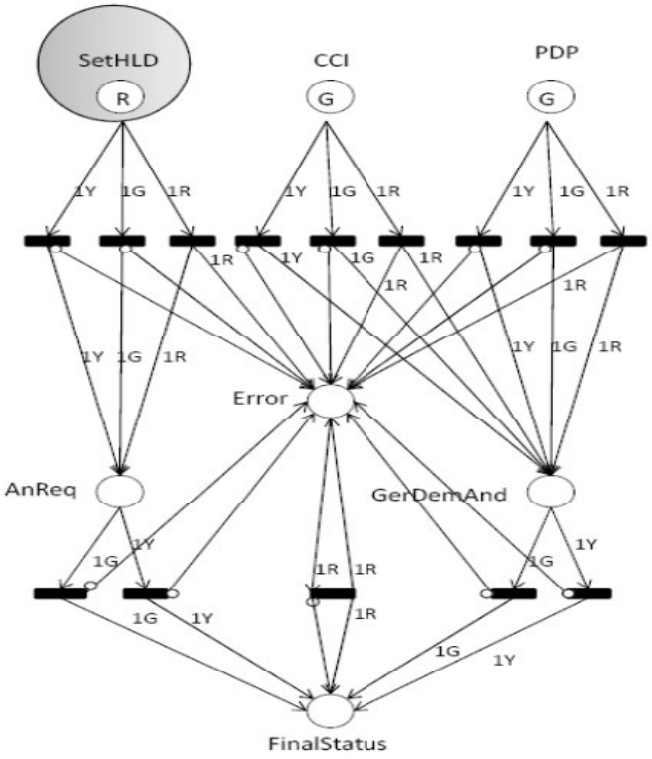

Figure 8. An FCM implementation modeling through a manual for the CPN using three activities and phases from the PA RSKM (before executions).1R=Red; 1Y=Yellow; and 1G=Green.

Figure 8 provides the CPN visualization before its execution. It shows CPN initial marks, as primitive system states. After running the CPN shown in Figure 9, an error scenario can be viewed. Arcs carried out marks from **SetHLD** into **Error**, **AnReq,** and **FinalStatus**, indicating post-conditions of transitions.

In this experiment, it was found out that both tools, the CPN and the inspection form, had the property to register non-compliances. However, it is noticed that each tool is able to complement each other. The inspection form has provided a better semantic understanding of the problem. The CPN facilitated the systemic visualization of the problem. The simultaneous use of these tools, has advised the project manager to take appropriate actions to redesigning and refactoring activities, in order to correct deviations were adopted using the CPN property generated in an automated colored on a specific problemstate.

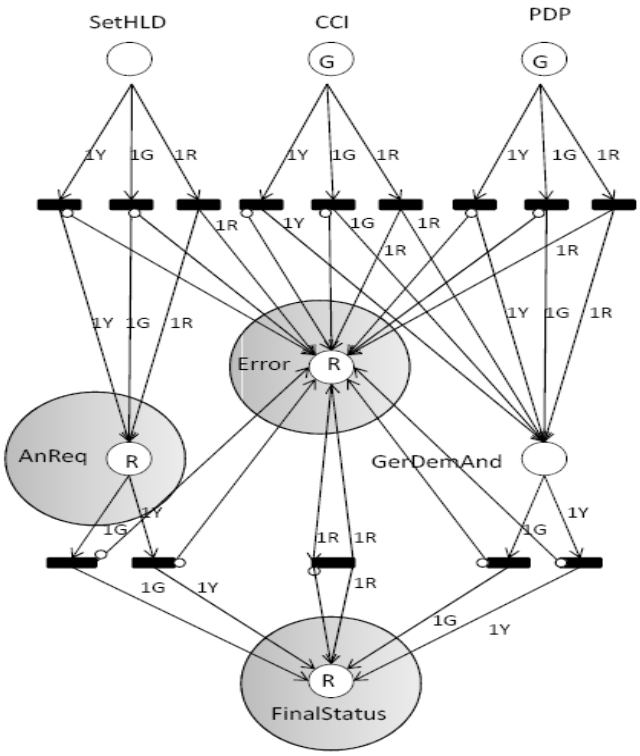

Figure 9. The modeled CPN assessing three activities and phases from the PA RSKM (after executions). 1R=Red; 1Y=Yellow; 1G=Green.

VI. CONCLUSION

This paper described a fragment of an ongoing research taking place at the Computer Science Department of the Brazilian Aeronautics Institute of Technology (ITA). It presented a prototype of a Formal Control Model (FCM) for Risks Management of a Software Project.

Some Process Areas (PA) of risk were extracted from the Capability Maturity Model Integration (CMMI). Because of its extensive content, a process of filtering PAs was performed to obtain essential elements for a prototype.

A Colored Petri Net (CPN) graphical and modeling tool was used and provided detailed and unambiguously tracking features for steps of this study. Some mechanisms of analysis and assessment inherent to the CPN model helped to control and manage essential and accidental complexities development.

The major contribution of this paper was the conceptualization of a FCM using a CPN and an inspection form. The proposed model was applied to a project within the financial department of an enterprise CMMI level 5. It was able to identify, control, and manage risks of software development. At the end, a successful case study was performed involving the two experiments of a Project Planning (PP) and a Risk Management (RSKM). Their assessments have shown that after the proposed FCM execution, PENDING activities were completely fixed.

RECOMMENDATIONS AND SUGGESTIONS

Authors of this paper recommend some refinements and customizations on the proposed FCM, in order to attend at least a third experiment, involving the Project Monitoring and Control (PMC) PA. Authors suggest the application of the proposed FCM within different CMMI PA, software houses, and research groups dealing with risks management in software development.

ACKNOWLEDGMENTS

Authors thank to ITA and Tata Consultancy Services for supporting this research.

REFERENCES

[1] Moreira, Nilton Stringasci. "Segurança Mínima: Uma Visão Corporativa de Segurança de Informações", Rio de Janeiro, Axcel Book, 2001.

[2] CMMI, "Version 1.2 - CMMI-DEV, V1.3, CMU/SEI-2010-TR-033 - ESC-TR-2010-033",. Improving Processes for Better Products and Services, November 2010.

[3] Laundon, Kenneth C. & Laudon, Jane P. "Sistemas de Informação Gerenciais.", 7 ª Edition, 2006.

[4] Pressmann, R. S. "Software Engineering", 7ª Edtion, p.928, McGraw Hill, NY, 2009.

[5] Murata. Petri nets, "Properties, analysis and applications", In Proceedings of the IEEE, pages 541–580, April 1989, Newsletter Info: 33Published as Proceedings of the IEEE, volume 77, number 4.

[6] PETERSON, J. L. "Petri Nets", ACM Computing Surveys, v.9, n.3, p.223-252, 1977.

[7] PETERSON, J. L. "Petri Net Theory and the Modeling of Systems", Englewood Cliffs, NJ: Prentice-Hall, C1981. 290 p.

[8] MACIEL, P. R. M. et al, "Introdução às redes de Petri e aplicações", Campinas: Universidade Estadual, 1996, 187 p.

[9] DESEL, J. "Place/Transitions Nets I", Introductory Tutorial Petri Nets, Petri Nets, In: 21st international conference on application and theory of petri nets, 2000, Denmark, pp 111-160.

[10] GIRAULT, C.; VALK, R, "Petri Nets for Systems Engineering: A Guide for Modeling, Verification and Application", New York: Springer Verlag. 2002. 607p.

[11] AHERN, D. M. et al., "CMMI Distilled: A Practical Introduction to Integrated Process Improvement", 3 ed. Boston, MA: Addison-Wesley Professional, 2008. 288p.

[12] International Organization for Standardization. ISO/IEC 15504: Information technology - Software process assessment, ISO/IEC International Standard, 2005.

[13] A. B. Raposo, "Coordenação em Ambientes Colaborativos usando Redes de Petri", PhD thesis, UNICAMP, Univerdade Estadual de Campinas, 2000. L. P. Magalhães and I. L. M. Ricarte.

[14] SEDGEWICK, R, "Algorithms. 2". ed. Reading, MA: Addison-Wesley, c1988. 657 p, (Addison-Wesley series in computer science).

[15] CORMEN, T.H, "Introduction to algorithms", Cambridge, MA: MIT Press, c1990, 1 cd-rom.

[16] D. O. Penha, H. C. Freitas, and C. A. P. S, "Martins. Modelagem de Sistemas Computacionais usando Redes de Petri: aplicacão, análise e avaliacão", Anais da Escola Regional de Informática - ERI RJ/ES, 2004.

[17] JENSEN, K, "Coloured Petri Nets: Basic Concepts, Analysis Methods and Practical Use", New York: Springer Verlag, 1997, 265p, 3v.

[18] OLIVEIRA, C. de, "Associação de Redes de Petri com Objetos Virtuais e Reais para Controle de Ambientes Virtuais Imersivos e Telepresença", 2008, Dissertação (Mestrado) - Universidade de São Paulo, São Carlos.