TECHRISK –A DECISIONAL FRAMEWORK TO MEASURE TECHNICAL DIMENSIONS OF LEGACY APPLICATION FOR REJUVENATION THROUGH REENGINEERING

Er. Anand Rajavat [1] and Dr. (Mrs.) Vrinda Tokekar [2]

[1]Department of Computer Science & Engineering, Shri Vaishnav Institute of Technology and Science, Indore, M. P., India
anandrajavat@yahoo.co.in
[2]Department of Information Technology, Institute of Engineering and Technology (DAVV), Indore, M. P., India
Vrindatokaker@yahoo.co.in

ABSTRACT

Competitive business environment wants to modernize existing legacy system in to self-adaptive ones. A variety of options are available to renovate legacy system in to more contemporary system. Recently the phenomenon of "software reengineering ", a methodology to allow old ways of thinking to be replaced with new, fresh approaches to increase productivity and quality of system, has been reported. However evolving legacy system through reengineering is a risky and error –prone task due to extensive changes it requires in the majority of cases. Therefore cost effective reengineering requires identifying and measuring impact of system, managerial and technical risk. We present a technical domain framework TechRisk to identify and measure quality and functional dimensions of legacy system. The objective is to identify those risk factors of technical domain which are critical to the success of reengineering. Proposed decision driven framework TechRisk provide support to identify and eliminate the highest impact risks in the software reengineering process and help to create a successful reengineering solution.

KEYWORDS

TechRisk, Reengineering, Risk engineering, Legacy system, Software quality, Domain

1. INTRODUCTION

Legacy systems and the information they process are essential assets for the organization that use them. The organization's evolution through the years requires synchronized evolution of the legacy systems, without this synchronization legacy systems provide low quality and, as a consequence, their maintenance becomes very costly. Increase in competition and soars in technology have forced organization to adopt innovative approaches to renovate their legacy system with respect to process, product & services. In recent years software reengineering has emerged as a dominant system evolution technique which helps in effective cost control, quality improvements and time and risk reduction. Software reengineering involves reorganizing and modifying existing software systems to make them more maintainable. [1] [2].

However recent experience shows that many reengineering efforts fail, because they only concentrated on functional aspects of reengineering, however, system managerial and technical aspects play an important role in system evolution task. Software reengineering projects is often

faced with unanticipated problems which pose risks within the reengineering process. These risks are especially severe in reengineering efforts, and we have therefore stressed the implications of these risks for the high rate of failure of software reengineering. The success of reengineering effort requires an understanding of the current and desired system state and available reengineering technology by identifying and controlling risk from system, managerial, and technical domain of legacy application. [3]

System domain represents a structural component that is responsible for maintaining a system that offers products and services to its customers. Issues of System domain involves planning and structuring the system infrastructure efforts, systematizing the stakeholder's tasks and defining and maintaining the organization's goals and objectives.

Managerial domain covers issues related to market factors and effect of competitive products, on quality [4] & cost of target system. Managerial Domain identifies and measure organizational economic strategy in accordance with requirements of target system.

Technical domain covers issues related to software functionality and software quality. Technical domain analyze and measure legacy system to better understand the function's capabilities and quality features in accordance with functional requirements and desired quality level of target system. Technical domain identifies and assesses the impact of the proposed changes.

Present work portrays the preliminary development of a Technical domain risk framework TechRisk to identify and measure risk components of technical domain in accordance with requirements of target system. Proposed framework enabled us to make some predictions, through identification and measurement of technical domain risk to take decision about when reengineering efforts are likely to succeed and when they are likely to fail. [5][6]. TechRisk framework is applied to an operational legacy system to identify and categories risk components of technical domain and to measure cumulative effect of different risk components. Finally, this paper contributes to identify, analyze and categories risk components and measurement factors for functional and quality perspectives of legacy system.

2. RELATED WORK

To improve the quality of legacy system, software reengineering should enable new functions and new technologies to ensure efficient management of the information container in the legacy system. The software reengineering involves restructuring and redocumenting legacy system by adding evolution effort to make them easier to maintain Increase in competition and soars in technology have forced organization to adopt innovative approaches to renovate their legacy system with respect to process, product & services. As system evolution technique software reengineering helps to achieve effective cost control, quality improvements and time and risk reduction.

In the past years a variety of risk management and reengineering frameworks was developed, but very few research works identify risk factors in reengineering process of software systems to create a successful reengineering risk solution. Cristiane S. Ramos in [7] developed a framework of metrics to evaluate the complexity of a legacy software system to support outsourcing. The framework considers two dimensions of a legacy system: its documentation and its source code. However many other dimensions of legacy system such as system, managerial and technical dimensions play an important role in system evolution process. Alessandro Bianchi in [2] describes a process of gradual reengineering of the procedural components of a legacy system. The proposed method enables the legacy system to be gradually emptied into the reengineered system, without needing to either duplicate the legacy system or freeze it.

Peter H. Feiler in [8] focuses on technical aspects of reengineering to support the cost-effective evolution of large software-intensive systems. However system, managerial and quality aspects of a legacy system need to be considered. Eric K. Clemons Michael C. Row Matt E. Thatcher in [6] focuses on functionality risk and political risk that causes failure of reengineering efforts .However there is other serious risk such that modularity risk, availability risk, reliability risk, usability risk, performance risk, security risk, technology risk, complexity risk are also causes the reengineering efforts to fail.

Identification and measurement of reengineering risk is a required competence for a successful software reengineering effort, which helps to provide an effective cost control, quality improvements, and time & risk reduction strategy for legacy system evolution. Proposed TechRisk framework analyzes various functional and quality risk components of Technical domain and measure cumulative impact of risk due to different risk components. TechRisk framework attempts to identify and measure most critical functional and quality risk factors of legacy system in accordance with requirements of target system.

3. TECHRISK (TECHNICAL DOMAIN RISK FRAMEWORK)

Technical domain has a significant impact on software and systems engineering. Technical domain helps in analyzing and testing the legacy system to better understand the function's capabilities and quality features and assess the impact of the proposed changes. The Technical domain covers the technologies of legacy system as compared to technologies being considered for the proposed (target) system. The element of the Technical domain consists of functional perspective model and Quality perspective model.

A simplified conceptual view of the elements in technical domain risk framework TechRisk is presented in Fig. -1, framework comprises with Perspective, risk cluster and risk factors.

Perspective is a viewpoint according to which different risk clusters are identified and measured using different risk measurement model.

Risk cluster covers risk component and the risk measurement model, which is used to measure the effect of particular risk component on system evolution decision.

Risk component contain different types of negative outcomes from technical domain of legacy application.

Risk measurement model measures different types of risk components from technical domain of legacy system in accordance with desired state of target system and reengineering strategy.

Risk factor encompasses sources of risk components from technical domain of legacy application [9] [10].

Technical domain is characterized in terms of a fundamental set of risk component and factors that are indicative of the present state of legacy and desired state of Target System. In TechRisk framework two types of perspective model i.e. functional perspective model and Quality perspective model is developed by analyzing states of legacy and Target system.

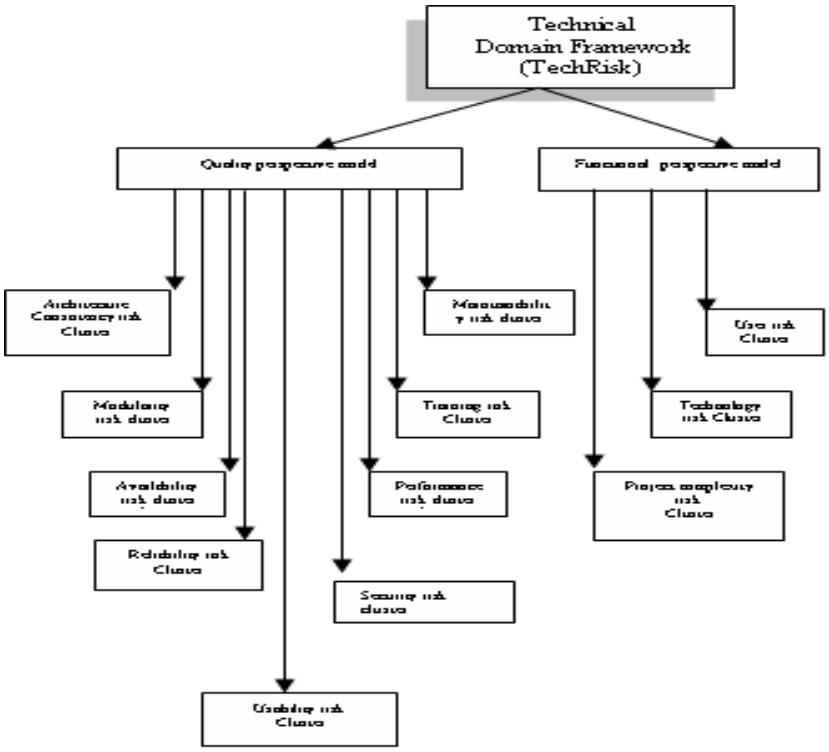

Figure1. Technical Domain Framework (TechRisk)

3.1 Functional Perspective Model

Functional perspective model highlights functional view of legacy system in accordance with functional requirements of target system. Model includes issue like complexity level of functions, user requirements, tools and technology used in legacy system as well as tools and technology used for the development of desired system. Risk clusters for functional perspective model are:-

3.1.1 Project Complexity Risk Cluster

Project Complexity Risk Component: - Project complexity risk component is the risk of loss associated with the complex legacy system functions that are hard to evolve through reengineering.

Project complexity Risk Measurement Model: - Project complexity risk measurement Model measures complexity of different functions of legacy system with the help of different software complexity measurement tools.

3.1.2 Technology Risk Cluster

Technology Risk Component: - Technology risk is the possibility that the present state of legacy system will fail to support advance technology and tools used to fulfill the requirements of target system.

Technology Risk Measurement Model: - Technology risk measurement model identify and measure technology risk by considering factors related to technology used in legacy system in accordance with desired technology required to accomplish the needs of target system. The

probabilistic approach is used for quantifying the probability of technology risk. Technology risk is comprised of the fundamental technological factors that may cause the reengineering effort to fail.

3.1.3 User Risk Cluster

User Risk Component: - User Risk is the risk of loss due to lake of user involvement during system evolution process. If the attitude of users toward a new system is unfavorable they will not cooperate during reengineering effort, leading to an increased risk of project failure.
User Risk measurement Model :- User risk measurement model identify and measure user associated risk factors which includes user resistance to change, conflict between users, negative attitude towards the evolution, users not committed to the project and lake of cooperation from users.

3.2 Quality Perspective Model

Quality perspective model measure some property of software or its specifications. Quality perspective model measures different quality of legacy system in accordance with desired quality of target system. Measurement model measure specific attributes of the development process, legacy system and target system that are used for successful reengineering effort. Risk clusters for quality perspective model are:-

3.2.1 Reliability Risk Cluster

Reliability Risk Component: - Reliability is the ability of a system or component to perform its required functions under stated conditions for a specified period of time. Reliability risk component is the probability of failure-free operation of a system in a specified environment for a specified time.

Reliability Risk Measurement Model: - Reliability risk measurement model identify and measure reliability risk at various levels, such as function, component, and subsystem of legacy application. The level of reliability risk affects the overall cost and schedule for the evolution of legacy system.

3.2.2 Usability Risk Cluster

Usability Risk Component: - Usability is a general term that encompasses everything having to do with "ease of use." That is, how easily existing user can use and control legacy system after evolution. Usability is a user-focused starting point for thought in target system design. Usability risk component is the risk of loss associated with dissatisfaction of user due to inefficient and complex operational process.

Usability defines convenience and practicality of use. This is affected by such things as the human-computer interface. The component of the software that has most impact on this is the user interface (UI), which for best usability is usually graphical (i.e. a GUI).

Usability Risk Measurement Model: - Usability risk measurement model measures the suitability of the proposed target system for its users. Identification and measurement of usability risk require measuring effectiveness, efficiency and satisfaction with which users of legacy system can achieve specified goals within the environment of the organization.

3.2.3 Modularity Risk Cluster

Modularity Risk Component:-Modularity risk component is the risk of loss associated with unmodularised legacy system. To reengineer such type of legacy system into a modularized target system requires massive restructuring and eenormous development efforts.

Modularity Risk Measurement Model: - Modularity, in general, is a broad concept, and its main driver is complexity. Value and the form of modularity vary depending on the state of legacy and target system. Modularity risk measurement model measure the modularization level of legacy system using different modularity metrics like coupling and cohesion in accordance with target systems modularity decision. Modularity decision for target system requires considering strategic preference of the organization, tactical alternatives, resource availability and external and internal uncertainty.

3.2.4 Availability Risk Cluster

Availability Risk Component:-Availability risk component is the risk of loss associated with unavailability of required design and change management document of legacy system. Availability risk also concern with legacy systems operational and functional availability.
Availability Risk Measurement Model: - Availability risk quantify that a system is operational and functional at a given moment. Availability usually provided through redundancy. Measurement of availability risk requires considering reliability parameters of the system. Availability risk also reflects on the side of availability of analysis, design, source code and configuration management documents of legacy system. Unavailability of above information and document causes reengineering effort to fail.

3.2.5 Architecture consistency Risk Cluster

Architecture consistency Risk Component:-Architecture consistency risk is the risk of loss associated with inconsistency between existing and desired architecture of legacy and target system.

Architecture consistency Risk Measurement Model: - Architecture consistency risk measurement model analyzes legacy systems structure, comprising software elements, the externally visible properties of those elements, and the relationships between them in accordance with architecture of target system. Identification and resolution of architectural risk is one of the key factors in successfully reengineering effort. Architectural consistency risk often leads to project inefficiencies, poor communication, and inaccurate decision making. Identifying and controlling architectural risks can have a significant impact on the overall success of a reengineering effort.

3.2.6 Security Risk Cluster

Security Risk Component: - Security can be defines as ability to protect data against unauthorized access and to withstand malicious or inadvertent interference with its operations.

Security risk component is the probability that the important data and information of existing system is lost or misused during system evolution process.

Security Risk Measurement Model: - Security ensures that important data and information of present system is not accessed by unauthorized persons during system evolution process. Security risk measurement model measures the effectiveness of the process that will ensure the availability and confidentiality of important data and information of legacy system after the evolution through reengineering.

3.2.7 Performance Risk Cluster

Performance Risk Component:-Performance risk component is the risk of loss associated with deficit between desired and actual level of performance.

Performance Risk Measurement Model:-Performance risk measurement model measure the performance attributes like response time, throughput and resource utilization of different application provided by legacy system and measure shortfall between the desired level of performance and the actual level of performance. Identification of performance risk require to consider workload requirements, service level agreement, response time, projected growth, lifetime of application, budget and schedule for application, network consideration including bandwidth , Hardware , resource dependencies, and shared resources.

3.2.8 Training Risk Cluster

Training Risk Component:-Training risk component is the risk of loss associated with the lack of training for the existing work force on advanced tools and technology which will be used to achieve target system goals.

Training Risk Measurement Model: - Training risk measurement model measure the requirements of customized and specialized training programs and special consulting services for present user of the legacy system so that they are comfortable with operations of target system. The Training risk identifies the key elements and steps necessary for training the various staff to use of the relevant functionality of the target system.

3.2.9 Maintainability Risk Cluster

Maintainability Risk component: - Maintainability risk component is the probability that the reengineered system facilitate updates to satisfy new requirements in future.

Maintainability Risk Measurement Model: - Maintainability risk measurement model measure that the software product that is maintainable should be well-documented, should not be complex, and should have spare capacity for memory, storage and processor utilization and other resources.

4 CONCLUSIONS

Now a days organizations face with a very high competition and consequently they have to continuously improve their legacy system to satisfy current user and business needs. Legacy system reengineering has emerged as a well-known system evolution technique which helps in effective cost control, quality improvements and time and risk reduction. The goal of reengineering is to increase productivity and quality of legacy system through fundamental rethinking and radical redesigning of system. However many reengineering projects are often less than successful because they concentrate on a narrow set of risk issues for that reason there is a great need to identify and measure risk from different domains of legacy system. Without them, we are not able to assess the impact of overall risk to take decision about when evolution of a legacy system through reengineering is likely to succeed and when they are likely to fail. Proposed framework TechRisk analyzes various functional and quality risk components of technical domain and measure cumulative impact of risk due to various risk components. In this paper, we first categorize major perspective models and risk clusters of technical domain for legacy application. We then construct a technical domain risk engineering framework TechRisk to establish relationship between various perspective models and risk clusters. This work contributes for a decision driven risk engineering framework to identify and assess risk within the technical domain of legacy system. The paper proposes a technical domain risk engineering framework TechRisk which is applied to an in-use legacy system to identify and categories functional and quality risk components of technical domain and to measure cumulative effect of

different risk components. The TechRisk framework guides users through assessment of functional and quality risk by selecting assessment measures and assigning values to them. The result of TechRisk framework can be used to take decision about when evolution of a legacy system through reengineering is likely to succeed and when they are likely to fail

REFERENCES

[1] Alessandro Bianchi, Danilo Caivano, Vittorio Marengo, Giuseppe Visaggio, "Iterative Reengineering of Legacy Systems",Ieee Transactions On Software Engineering, Vol. 29, No. 3, March 2003.

[2] Alessandro Bianchi, Danilo Caivano,Vittorio Marengo, Giuseppe Visaggio," Iterative Reengineering of Legacy Functions", 17th IEEE International Conference on Software Maintenance (ICSM'01), Florence, Italy, ISBN: 0-7695-1189-9,November 07-November 09.

[3] Anand rajavat,Vrinda Tokaker," MngRisk –A Decisional Framework to Measure Managerial Dimensions of Legacy Application for Rejuvenation through Reengineering",International jurnal of computer application 2011 by IJCA Journal, Number 2 - Article 4 ,DOI 10.5120/1985-2674,2011.

[4] Software Maintenance and Reengineering, 1998,ISBN: 0-8186-8421-6, Digital Object Identifier : 10.1109/CSMR.1998.665778

[5] Harry M. Sneed, "Risks Involved in Reengineering Projects," in WCRE: Proceedings of the 6th IEEE Conference on Reverse Engineering, PP.204, 1999.

[6] Eric K. Clemons Michael C. Row Matt E. Thatcher, "An Integrative Framework for Identifying and Managing Risks Associated With Large Scale Reengineering Efforts," Proceedings of the 28th Annual Hawaii International Conference on System Sciences, PP.960-969, 1995

[7] Cristiane S. Ramos, Káthia M. Oliveira, Nicolas Anquetil," Legacy Software Evaluation Model for Outsourced Maintainer", published in CSMR '04 Proceedings of the Eighth Euromicro Working Conference on Software Maintenance and Reengineering (CSMR'04), IEEE Computer Society Washington, DC, USA ©2004 table of contents ISBN:0-7695-2107-X

[8] Ransom, J., Somerville, I., Warren, I.," A method for assessing legacy systems for evolution ", in Proceedings of the Second Euromicro Conference on Software Maintenance and Reengineering, 1998, ISBN: 0-8186-8421-6 , INSPEC Accession Number: 5884288,PP 128 – 134.

[9] Anand rajavat,Vrinda Tokaker," MngRisk –A Decisional Framework to Measure Managerial Dimensions of Legacy Application for Rejuvenation through Reengineering",International jurnal of computer application 2011 by IJCA Journal, Number 2 - Article 4 ,DOI 10.5120/1985-2674,2011.

[10] Anand Rajavat, Vrinda Tokekar, "ReeRisk –A Decisional Risk Engineering Framework for Legacy System Rejuvenation through Reengineering", Published in Proceedings of Second International Conference on Recent Trends in Information, Telecommunication and Computing – ITC 2011 by Springer LNCS-CCIS, March 10-11, 2011 in Bengaluru, India, CNC 2011, CCIS 142, pp. 152 – 158, 2011, © Springer-Verlag Berlin Heidelberg 2011

Authors

Er. Anand Rajavat
Assistant professor
Department of Computer Science & Engineering
Shri Vaishnav Institute of Technology and Science Indore, M. P., India
B.E. (Computer Science and Engineering)
M.E. (Software Engineering)
Ph.D (Pursuing) (Computer Engineering)
Areas of Interest:
Software Engineering, Object Oriented Analysis and Design, Computer Architecture

Dr. (Mrs.) Vrinda Tokekar
Professor & Head,
Department of Information & Technology,
Institute of Engineering & Technology,
Devi Ahilya University, Indore (M.P.) India
Ph. D. (Computer Engg.) in 2007 from DAVV, Indore
M.E. (Computer Engg.) in 1992 from DAVV, Indore
B.E. (Hons.) EEE, BITS Pilani in 1984,
Areas of Interest:
Computer Networks, Distributed Computing, Security in Wireless Networks, e-Governance, Multimedia Communication, Software Engineering