ANALYSIS OF RISK MANAGEMENT IN COTS COMPONENTS

S. Nirenjena , M.Tech Final Year student ,Department of Computer Science Pondicherry University ; Dr.M.S.Saleem Basha ,Assistant Professor ,Department of Computer Science ,Pondicherry University

Abstract

In recent years Commercial-off-the shelf components has become a great demand in IT industry due to its various advantages. They are defined as components which are easily implemented into existing system without a need for customization. COTS components include hardware or software products readily available for sale by third party organizations, which the user or developer can purchase from them. Many quality models were developed in order to evaluate the quality of the COTS components. Various risks are involved if quality of COTS component is not verified. Risk management is defined as set of actions that help the project manager plan to deal with uncertain occurrences. Coding, debugging, unit testing and code inspections are reduced, while design and testing are modified thus, various risk management methods are proposed which serves as a guide to both developers and the end users. This paper deals with various risk management in COTS components. The objective of this work is to enable the extension of research in the field of COTS components.
Keywords: COTS components, Risk factors and Management, Verification and Validation.

Introduction

The need and usage of COTS components has been increasing day by day in many IT industries. Many companies depend on third party organizations in purchasing COTS components because they considerably reduce effort, cost and amount of custom development by integrating COTS into their system. COTS systems have the following characteristics: the buyer has no access to source code; the vendor controls its development; and the software has a nontrivial installed base. Both the developer and the end user should be able to analyze the quality of the COTS components because it may lead to unexpected failure to the system. In order to analyze the quality of COTS components many Quality models were developed. Many research journals help in handling the various risks of COTS components during software development cycle. Risk factor results in uncertain danger which leads to failure in development of the software.

Risk identification mechanism plays a vital role in estimating the probability of the risk occurrence. Risk attack on different development phases vary with respect to different nature of projects.

Formula for risk prevention costs and risk probability helps us to avoid many risks during development cycle of the software. This kind of risk assessment technique builds trustworthiness of COTS components to the end users. There are certain factors which contribute to project failures they are:
- Mismatched skill on the evaluation and deployment teams.
- Inexperience with COTS.
- Overly optimistic expectations.
- Overly aggressive deployment schedules.
- Weak planning and managing of the project life cycle.

The risk of COTS component is due to following factors [3]:
- Black – box nature of COTS software
- Lack of component interoperability standards.
- Disparity in component – vendor evolution cycles.
- Quality of COTS software components.

Related Work

Many researches prove that there is a possibility of arrival of risks at the development stages of software process. They can be resolved using various techniques like CARE/SA and PORE; these methods handle the requirement mapping with developers and end users.

The discussion below points out various researches on risk management in COTS components.

i. ***Awais Rashid and Gerald Kotonya proposed*** **[1]**. A risk management mechanism based on identifying risk management techniques for each individual risk cat-

egory and integrating various individual techniques into a global strategy. Risks were classified into six main categories namely *evaluation, integration, context, quality, evolution and process risks*. Overlapping and cross cutting nature of risks are analyzed.

The checklist along with 9 considerations was included during selection of component based framework. Risks involved in six main categories were listed out and the solution was provided for each of them. They have also highlighted various risks that cut across a component based development cycle. The individual risk mitigation strategies are then integrated into one global strategy. The figure below is global risk strategy.

Fig1: Global risk management strategy [1]

ii.   *Amandeep Kaur Johar and Shivani   Goel* stated that risks can be due to the nature of COTS components development process, component technologies and vendor support [2]. They found a solution by identifying risks during selection, procurement, integration and maintenance of COTS components.
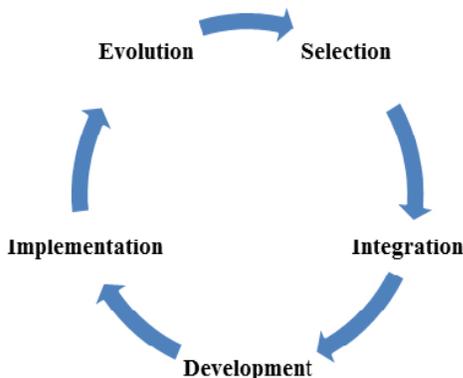

Fig2: Risks in various Application Development stages [2]

This identification has the risk more visible at each development stage which helps in carrying out activities that minimize their effects [2].

iii.   *Rashmi Gupta and Shalini Raghav* proposed [3] risk assessment techniques and survey method on COTS components with the help of Rational Unified Process. RUP phases include   inception, elaboration, construction and transition phase. Formula for determining risk prevention cost and finding risk probability was also included in their research. Formula for risk prevention cost(R pc) is :

$$Rpc = CPT+CPV+QAC+FC$$

Where,
CPT=Cost of Preventing Threats
CPV=Cost of preventing vulnerabilities
QAC=Quality appraisal cost
FC   =Internal/External failure cost

The formula for Risk Probability is ,

$$Risk\ Probability = (CPT+CPV) / (Rpc)$$

In this research COTS usage Risk evolution (CURE) methodology is adopted to perform risk analysis. For each risk 24 respondents were asked to provide their perception on probability occurrence of each risk and impact of each risk event.

iv.   *Amadeep Kaur Johar and Shivani Goel* extended their research by developing RIMCOTS (Risk identification and Mitigation for COTS based software development) model [4] which serves as a guide to manage multiple COTS software components in complex systems. Here in this paper risks involved in each and every phases of software development was listed out and risk scores were provided for each and every risks. Mitigation strategies were proposed to the top three high level risk scores.

v.   *Tahir Abdullah and Ahmad Mateen* proposed a general analysis of various risks of software development models [5]. They have stated that software can face various problems that can cause the different negative outcomes and sometimes to extreme cases failure of the software. This is also meant for COTS components. The factors considered in this paper are:

a.   The ease of executing the risk.
b.   Different stakeholders lack of interest
c.   A system's existing vulnerabilities
d.   Cost or impact of particular business context.

Boehm (1989) stated that risk management focuses the project manager's attention on those parts of the project that are most likely to be the   reason of some trouble and compromise participant's conditions. It is through risk management that project managers assess risks and

manage to reduce the risks to an acceptable level. In this paper Rapid Application Development is created to support the construction of business applications for the enterprise in short time and in effective manner without affecting the end product of the user. In this research it was observed that probability of occurrence of all risks is same in all type of projects. It changes in some projects where some testing is needed on some deeper level.

vi.   *Victor Sagredo, Carlos Becerra and Gonzalo Valdes* have done an empirical validation of component based software system generation and evaluation approaches [6]. Here azimuth and Ad-Hoc approach is compared. Both the approaches help to make early decisions for software architects to evaluate the COTS components. Software architects can select any one of the methods based on their project. The research has compared the usage and needs of both COTS and open source software components. Therefore this paper helps in validating the COTS components.
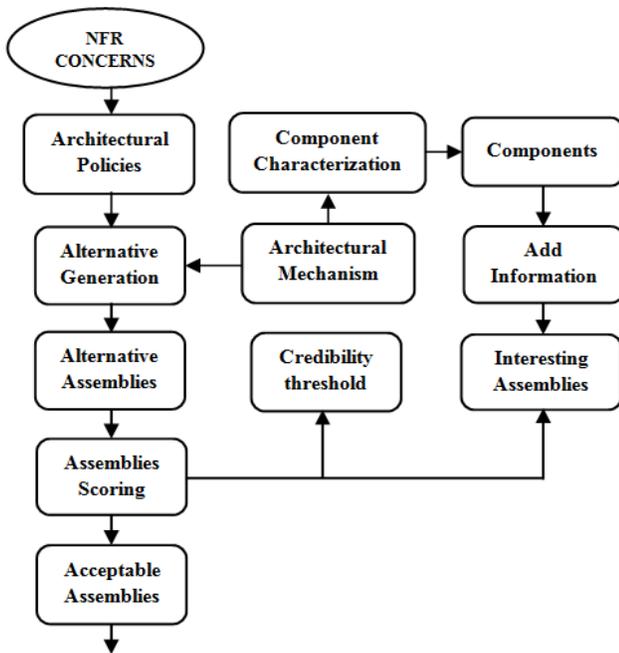

Fig3: Azimuth Framework[6]

vii.   *Nitin Upadhyay, Bharat M. Deshpande and Vishnu P. Agarwal* propose Modeling and Analysis of

Component Based Software System (MACBSS) which helps in analyzing risks and quality of software at architectural level [7]. This describes the characteristics of quality such as performance, reliability, functionality etc…The research proposes a framework based on graph theory and systems engineering approach to analyze component based software system at the architectural level.

viii.   *Jiang Zheng and Brain Robinson* conducted a research on regression test in COTS components. They presented a Light weight Integrated –Black Box approach for Component Change identification (I-BACCI) [8] , process in order to select regression tests for user/glue code that uses COTS components. This method helps in identifying changes occurring in system using COTS components with black box approach. Each function and their relations are analyzed. This method reduces the risk level to some extent so this method can also be added to verify and validate the nature of COTS components.

ix.   The other research was experimental risk assessment and comparison using software fault injection by *Moraes, J.Duraes* [9]. The research was a case study which demonstrated and evaluated a comparison scenario using two off the shelf components RTIMS and RTLinux real time operating system in realistic satellite data handling application used by European Space Agency. Their goal was to provide a quantitative measure of the risk of system having a failure. This kind of fault injection method helps in measuring the impact of faults and the risk level due to that.

Lawrence Chung and Kendra Cooper proposed COTS Aware Requirements and Software Architecting (COTS/SA) for effectively using the components that meets the needs of system under development [10]. It involves matching, ranking and selection of COTS components to match functional and non-functional requirements of COTS components. The approach was illustrated using Digital Library System. This method reduces the major risk involved in satisfying the stakeholder and end user needs. Therefore this process can be included in managing the risk of components under development. The below tabulation gives a brief idea on the above researches along with advantages and disadvantages.

Sl. No	Title/Author	Theme	Advantage	Disadvantage
1.	Risk management in component based development: A separation of concerns perspective by Awais Rashid, Gerald Kotonya .	Risk management mechanism is proposed and global strategy is developed.	Overlapping and cross cutting nature of risks are analyzed.	Testing techniques are not given.
2.	COTS components usage risks in component based software development by Amandeep Kaur Johar & Shivani Goel	Risks are identified during selection, procurement, integration and maintenance of COTS components.	All the risks are stated which occurs during the application development activities.	Solutions not provided.
3.	Risk assessment techniques and survey method for COTS components by Rashmi Gupta & Shalini Raghav.	Rational unified process is introduced, providing appropriate security and protection levels by identifying various risks.	Formula for risk prevention cost and risk probability are given.	Verification and validation strategies not proposed.
4.	Designing of RIMCOTS model for Risk identification and mitigation for COTS based software development by Amadeep Kaur Johar & Shaivani Goel	Mitigation strategy proposed for risks with high scores	COTS usage risk evaluation (CURE) & PURE methodology is used to perform risk analysis	Mitigation strategies not provided for risks with less scores.
5.	Risk analysis of various phases of software development models by Tahir Abdullah ,Ahmed Mateen, Ahsan Raza Sattar & Tasleem Mustafa.	Reduced RAPID APPLICATION DEVELOPMENT MODEL (RAD) is proposed to identify the risks.	Effects are classified based on cost , schedule, and other phases of development.	Impacts not discussed.
6.	Empirical Validation of Component based software system generation and evaluation approaches by Victor Sagredo , Carlos Becerra & Gonzalo Valdes.	Azimuth and Ad-hoc approach are compared and empirical study is done in both.	Architecture is more important for product selection, Needs of both COTS and OSS users are analyzed.	Possibility of various threats.
7.	MACBASS: Modeling and Analysis of Component Based Software System by Nitin Upadhyay , Bharat M.Deshpande & Vishnu P. Agarwal.	SWOT (Strength – weakness-Opportunities-Threats)method is supported.	Cut down at overall development cost.	Performance parameters does not correlate quantitatively with proposed system.
8.	A Lightweight Process for change identification and Regression test Selection in using COTS components by Jiang Robinson, Brian Robinson, Laurin Williams, Karen Smiley.	Integrated black box approach for component change identification (I-BACCI) integrates firewall analysis of RTS method with black box approach.	No changes in the component affect the product using the component.	Shares a limitation with the existing source based firewall methods.

15

9.	Experimental Risk assessment and comparison using Software Fault injection by R.Moraes, J.Duraes, R.Barbosa, E.Martins, H.Madiera.	Demonstration is done in a comparison scenario (RTEMS& RTLINUX).in satellite data handling system. G-SWIFT is used to inject the faults.	Helps in tuning complex COTS components to minimize risk and increase the system dependability.	Fault injection tool used cannot be common to all domains.
10.	COTS – Aware requirements Engineering and software architecting by Lawrence Chung & Kendra Cooper.	The framework proposed supports matching, ranking and selection of COTS during development of software system architecture.	Satisfies stakeholder needs and their business process.	Only the requirement part is satisfied.

CONCLUSION

The above mentioned researches contribute a major development to risk management of COTS components at all stages. These methods can be considered for verification and validation of COTS components which is still an ongoing research topic. Since many organizations depend on COTS components there is a necessity to evaluate their quality and analyze the risks to reduce the system failures due to COTS component.

Acknowledgments

REFERENCES

[1] Awais Rashid & Gerald Kotonya, *Risk Management in Component Based Development A Separation of Concerns Perspective,* Journal ECOOP Workshop on advanced Seperation Concerns, July 2011.

[2] Amadeep Kaur Johar & Shivani Goel, *COTS components usage risks in Component based Software development,* International Journal of Information Technology and Knowledge Development July-December, Volume 4 N0.2,pp.573-575.

[3] Rashmi Gupta & Shalini Raghav, *Risk Assessment and Survey Method for COTS Components* , International Journal of software Engineering & Applications(IJSEA),Vol.3,No1,January 2012.

[4] Amadeep Kaur Johar & Shivani Goel, *Designing of RIMCOTS model for Risk Identification and mitigation for COTS–based Software Development*, Research Journal of Computer Systems Engineering: An International Journal Vol02, Issue 02, June, 2011

[5] Tahir Abdullah, Ahmed Mateen, Ahsan Raza Sattar & Tasleem Mustafa, *Risk Analysis of Various Phases of Software Development Models*, European Journal of Scientific Research ISSN 1450-216X Vol.40 No.3(2010),pp.369-376

[6] Victor Sagredo, Carlos Beserra & Gonzalo Valdes , *Empirical validation of Component Based Software Systems Generation and Evaluation Approaches*, CELEI Electronic Journal Volume 13, Number 1, Paper 6, April 2010.

[7] Nitin Upadhyay, Bharat M. Deshpande & Vishnu P.Agarwal, *MACBSS: Modeling and Analysis of Component Based Software System, World Congress on Computer Science and Information Engineering* 2009.

[8] Jiang Zheng, Brian Robinson, Laurie Williams & Karen Smiley, *A Lightweight Process for Change Identification and Regression Test Selection in Using COTS Components* , Proceedings of the Fifth International Conference on Commercial-off-the-Shelf(COTS)-Based Software Systems(ICBSS 2006), IEEE

[9] R. Moraes, J. Durlaes, R. Barbosa, E. Martins H. Madeira ,*Experimental Risk Assessment and Comparison*

Using Software Fault Injection, 37th Annual IEEE/IFIP International Conference On Dependable Systems and Networks(DSN'07), 2007.

[10] Lawrence Chung & Kendra Cooper, *COTS Requirements and Software Architecting,* Proc. Int. Workshop on Systems / Software Architecture (IWSSA'04), June 21-24 Las Vegas, NV.

Biographies

NIRENJENA.S completed B.tech in Information Technology at Perunthalaivar Kamarajar Institute of Engineering and Technology ,Karaikal. Currently final year student of M.Tech in Computer Science Final Year student from Pondicherry University,Pondicherry.

Dr.M.S.SALEEM BASHA completed B.Tech in Electrical and Electronics Engineering from Bangalore University and M.Tech in Computer Science and Engineering from Anna University Chennai**.** He is also a Ph.D holder. Currently an Assistant Professor at Pondicherry University .

ANALYSIS OF RISK MANAGEMENT IN COTS COMPONENTS