# Quality Assurance of Security Requirement Engineering in Socio- Technical Systems

Rida Zainab
Fatima Jinnah Women
University Rawalpindi, Pakistan

Sundas Ashfaq
Fatima Jinnah Women
University Rawalpindi, Pakistan

Mehreen Sirshar
Fatima Jinnah Women
University Rawalpindi, Pakistan

## ABSTRACT
Quality assurance is a continuous process to check whether specified requirements are being fulfilled by a system or service. Quality assurance checks for the defects before they get into the final product. In this research a comprehensive survey of various literatures has been carried out to ensure quality standards. Different quality assurance techniques have been employed in this research that help in improving the quality of the socio technical systems from the perspective of security requirement engineering. The analysis of various type of literature reveals that after applying techniques presented in the literature review shows improvement in the performance of the socio technical systems. Tropos, SeeCo (Security via commitments), formative user centered evaluation technique, three-layer framework, Si*(Secure i*) ontology are the different techniques discussed throughout the research that ensures the quality standards. Some of the quality evaluation tools like STS-tool and STS-ml are also used in the research for quality assurance. This research also assesses the improvements of security requirement engineering in socio technical systems after applying Quality evaluation techniques.

## General Terms
Quality Assurance, Socio technical systems, Tropos, SeeCo (Security via commitments), Si*(Secure i*) ontology, Security Requirement Engineering

## Keywords:
Quality Assurance, Socio technical systems, Tropos, SeeCo (Security via commitments), Si*(Secure i*) ontology, Security Requirement Engineering

## 1. INTRODUCTION
Quality guarantee is important for the achievement of the system and to achieve the excellence that essential for going to the new or next level of controlling. It is necessary to check whether a system amenities being developed is meeting identified requirements or not and to guarantee that Quality is consistently upgraded. The increasing demand of Quality products in worldwide market enforced organizations to emphasis on Quality. International Organization for Standardization (ISO) 9000 is a worldwide standard that many organizations used to confirm that their Quality guarantee product is in place and operative. Conformance to ISO 9000 is said to assure that an organizations supplies Quality products and facilities. The ISO 9000 states several features of quality controlling and includes some of ISO's best standards. ISO 9001:2008 defines the requirements of a Quality controlling appliances[23]. ISO 9000:2005 includes the simple ideas and linguistic. ISO 9004:2009 gives importance on how to make a Quality controlling appliances more efficient and effective. ISO 19011:2011 states direction on inner and outer reviews of Quality controlling appliances[23]. It was found that socio technical system significantly contributed in our daily life so quality of this system are important for the advancement of social life. The aim of this survey research is to establish that how much Quality parameters especially security and safety are important in socio technical systems. During our survey different authors have discussed different quality parameters in order to ensure quality in the system which are; performance, scalability, extendibility, reusability, efficiency, portability, effectiveness, verification, validation, maintainability and ease of use etc.

The paper is organized as follows: Section 2 discusses the various Quality Assurance techniques and tools presented in different research papers used in the requirement engineering process of socio technical systems. Comprehensive analysis of described techniques discussed in Section 3. Section 4 concludes the study.

## 2. QUALITY ASSURANCE TECHNIQUES IN DIFFERENT RESEARCH PAPERS FOR REQUIREMENT ENGINEERING OF SOCIO-TECHNICAL SYSTEMS

### 2.1. Applying Tropos to Socio- Technical System Design and Runtime Configuration[1]
In socio technical systems, human agents are also an integral part of a system along with hardware and software. In this paper a number of tropos features are discussed which are important for the design and development of STS's. Risk analysis and local variability are the two critical design issues that are focused in this paper and also how they are integrated and evaluated in choosing the best design alternative is explained. Finally the runtime self- reconfiguration is also discussed. The methodology used in this paper is tropos i.e. agent oriented software engineering methodology [1] which models the system as set of interacting agents. Goal Risk framework and location variability are the additional techniques used along with tropos. Goal risk framework minimizes the risk and location variability relates to the location where an agent is situated at runtime. The advantages of this paper are that we can prevent the system from violating the requirements. We can also minimize the risk as much as possible. The disadvantage is that the design and runtime properties of system present a lot of challenges and therefore there is a clear need of engineering tools and techniques.The approaches described in this paper are applicable on all type of real time safety critical systems.

## 2.2. Security Requirements Engineering via Commitments[2]

Security Requirements Engineering (SRE) [2] is related to specify the security requirements and security needs. In this paper the SecCo(Security via commitments) methodology [2] is used to derive security requirements from security needs. Security requirements can be specified as social commitments or promises. The advantage of the paper is that the commitments view can be derived from the operational view. The downside is that a lot of things are still not explained in the paper and a lot of future work is needed like development of a tool for SecCo and to give detail of how and validation of the approach can be carried out on industrial scale.

## 2.3. Using Commitments to Specify Socio-Technical Security Requirements[3]

In this paper a CASE tool for socio technical system is presented that is used for modelling and analysis of STSs. This STS-Tool helps the designer to model the system at high level of abstraction to derive security requirements. STS-ml (Socio-Technical Security modelling language), is used which allows actors to express security needs and uses the concept of social commitment among actors to specify security requirements [3]. Once the modeling is done we can derive the security requirements in form of social commitments. The advantage of this paper is that a modeling language and tool is introduced which helps in mapping security needs to gain security requirements. Also a security requirement document is generated at the end which is a helping material. The downside of the paper is that the security needs come from different stakeholders and are different due to which conflicts arise. Also they are modeled at high level of abstraction and are not detailed. The approach described in this paper can be applied in real world any field where we do not want to disclose our personal details or to make our data secure from a third party interference.

## 2.4. STS-Tool: Socio-Technical Security Requirements through Social Commitments[4]

In this paper security issues that we encounter using socio technical systems are discussed. These issues arise due to the interaction between actors during information exchange. Security needs are expressed in terms of social commitments. The methodology used in the paper is STS-Tool which is used to gather security requirements through security needs. The positive point of the paper is that STS-Tool provides different views on a diagram i.e. social view, information view, and authorization view[3]. The diagrams made through STS-tool can be exported to different formats like jpg,png etc. The negative side is that the paper should also include the techniques like embedding automated reasoning capabilities to identify inconsistencies in requirements; and implementing a plugin management system to add functionalities to STS-Tool [3]. The tool can be be applied to all real life systems that involves interaction among actors.

## 2.5. Managing Security Requirements Conflicts in Socio-Technical Systems[5]

Requirements come from different stakeholders and are conflicting. In this paper a framework is proposed on the basis of automated reasoning that identifies and manages the conflicts in security requirement models. The framework or methodology used in this paper is a revised version of STS-ml. Two types of conflicts are discussed in the paper which is among authorization requirements and between business policies and security requirements [5]. The positive side of the research is that the paper has identified the conflicts among security requirements which were not cater before in the previous researches. The downside of the paper is that we have resolved conflicts using only the technique of automated reasoning and we have to devise further reasoning techniques to resolve conflicts. And also we have to explore the possible ways to resolve the identified conflicts.

## 2.6. Specifying and Reasoning over Socio-Technical Security Requirements with STS-Tool[6]

In previous researches we have presented STS-Tool for modeling and analysis of socio technical systems. The tool helps in designing the systems in such a way that we can derive security requirements from security needs via social commitments. Also the conflicts among requirements are discussed previously. In this paper a set of automated reasoning techniques are presented that will check that whether STS- ml model is well formed and to determine the consistency of the specification of security requirements. The methodology applied in implementing techniques is disjunctive datalog programs [6]. Security analysis is implemented in disjunctive Datalog and compares the possible actor behaviors that the model describes, against the security requirements that constrain possible behaviors [6]. Well formedness analysis is carried out to determine that the model complies with the syntax restrictions of STS- Tool. The positive side of the paper is that the whole process of extracting the security requirements from security needs as well as the identification and management of conflicts in requirements are explained in a flow with consistency. The downside is that more techniques should be introduced to cope with conflicts other than that which are already explained. The techniques explained can be applied on any type of real world socio technical system.

## 2.7. Modelling Security Requirements in Socio- Technical Systems with STS-Tool[7]

In this paper a security requirement engineering tool is introduced which is STS- Tool used for modeling the socio technical system at a level that involves abstraction and represents the limitations over the interaction between different stakeholders in socio technical systems. And as a result of this modeling we get the security requirements in terms of social commitments. The tool allows multi view modeling by providing the authority to the designer to deal with various perspectives at a time thus increasing modularity which is a positive point of the research. The negative side is that the system is too abstract to be mapped in real time scenarios because of the conflicts in the needs of actors in real time. The tool is

good enough to be applied initially on small scale scenarios.

## 2.8. Formative user-Centered Evaluation Of Security Modeling: Results from a Case Study[8]

Security modeling language is necessary to represent the aspects of a socio technical system. Developing a security modeling language is a difficult task. In this paper a technique is introduced named as formative user centered evaluation approach [8]. The technique is used to investigate any security modeling language used in designing a socio technical system. The technique involves active end users and is used in early stages of designing. The formative user centered evaluation approach identifies and explains usability problems that are related to tool and the maintenance of the graphical representations. The result of the evaluation contains both problems and solutions. The evaluation presents the new concepts introduced for STS-ml and its supporting tool. The approach presented in the paper is highly recommended for the development of security modeling language [8]. It ensures that the requirements of language are fulfilled and no concept is lacking. These are the positive points of the paper. However still the modeling language STS-ml need to be improved and updated versions of STS-ml are required. In the paper only usability aspect of modeling language is covered so far and we need to work on consistency and scalability as well. Also we need to analyze the problems when the modeling language is applied on larger scenarios since according to paper we have applied the evaluation technique on smaller scenarios.

## 2.9. Global Design for Secure Socio-Technical Systems[9]

In this paper a comprehensive framework is developed that consists of concepts, techniques and tools for designing secure STSs. In this framework, STS consists of organizational goals and security requirements, businesses and industrial processes through which requirements are satisfied. The paper consists of a systematic process to analyze and design each part of the STSs. The positive side of the paper is that a multilayer framework is developed that represents a secure socio technical system by specifying the interactions among different system components. Also a methodology is specified to cater both the organizational objectives and security requirements at the same time which was not possible before. The downside is that the methodology is carried out by a tool which is also mentioned in the paper but the name of the tool is not specified.

## 2.10. An Ontology for Secure Socio-Technical Systems[10]

In this paper the problem of security at or is discussed with the help of a modeling language at the level of organization and an ontology[10] is described model security The modeling language presents concepts on the basis of trust, delegation and permission. The modeling language is, Si*(Secure i*)[10], is based on the i* ontology[10] where specifications employ basic primitives such as actor, role, goal, task, resource, and social relationships between actors [10]. Building a model of the system that is incrementally refined and extended is based on the idea of Si*. The positive side of the proposed methodology is that it allows system designers to find more modern security requirements. Also such concepts automatically derive business processes from the requirements model. The negative side of the paper is that by applying this methodology we are unable to reduce the gap between the analysis of requirements and the description of policies. And we are unable able to derive the privacy policies directly from the requirements model.

## 2.11. Capturing Security Requirements for Software Systems [13]

This paper describes a methodology for gathering security requirement based on reusing of previous knowledge. A more organized way is needed for gathering security requirements. The methodology focus on the integration of security with software development. In this methodology a security catalog is made with the help of previous security knowledge, which help us in identifying security requirements. To model security requirements we use security problem frames and to model threats we use Abuse Frames. The basic purpose of security requirement engineering is to recognize, gathering and document the requirements that are needed for developing secure software system. In this methodology we use previous knowledge to model the problem factors of the system and to disintegrate it into sub problems then we specify the strength in the system and identify the risks that can harm such strengths. Then we model the security requirements that are intended to reduce the risks causing inabilities. We model such security requirements using security problem frames then we evaluate the requirements to assure the quality. Positive point of this methodology is that its each and every point is clearly defined and helpful in identifying security requirements. Negative points of this methodology are that this method need more empirical studies and risk analysis. This method should follow formal framework. The methodology should be extended to support more generic threats. Application that follow this methodology are banking system, e-commerce.

## 2.12. Security Requirements Engineering for Service Oriented Applications [14]

Security requirements are explicitly defined for each type of system. Security Requirements Engineering is deals with discovering and examining safety problems at initial level in system development process. This paper describes the security via commitments; it includes three opinions public, permission, and reserve. It defines the security requirements in terms of social responsibilities, obligations and contracts with authority between agents. Commitments are the result of communication between the defaulter and the customer. The aim of this paper is to model the frame work and algorithms that enable the automated detection of security threats and to evolve security requirements used to describe the functionality under development. Positive point of this model is that it is helpful in the improvement of services of the system, as currently using safety resolutions can be used again. The negative point of this model is that the security needs are not expressed by stakeholders and making of full- fledged development tool is a problem. Converting the security requirements conveyed as commitments into existing service interface

specification languages is a problem. In our daily life this model use in different industries for ensuring security requirements in service oriented applications. E.g. medical record system, therac-25, banking management system etc.

## 2.13. A Socio-Technical Approach for Event Detection in Security Critical Infrastructure[15]

In this author emphasize on planning and constructing a socio-technical system in safety critical situation. It is used to diagnose the unusual or irregular behavior. In this several behaviors of importance and communication between the software and its customers are well- defined. In this paper a smooth CCTV application is to be planned and implemented a bank office not only to encourage and enhance research and analysis but to avoid corruptions and wrong doing by noticing doubtful behavior[15]. It includes the involvement of users, officers and security workers of banks in this particular incident. The positive point of this approach is that it reduces the difficulties of overcrowding blocking and inspection in combination and analysis of the application and the essential subsequent methods are conducted. But the negative point of this approach is that it does not work properly when data are large and when it's at its peak time.

## 2.14. Toward Monitoring Organizational Safety Indicators by Integrating Probabilistic Risk Assessment, SocioTechnical Systems Theory, and Big Data Analytics[16]

Socio-Technical risk analysis consider diverse, imperfect, and unstructured data. It focuses on developing hybrid predictive technologies[16]. It works on the betterment of the theory, importance and measurement of the Socio Technical Risk Analysis framework. This theory has some positive aspect it decreases the problem of bottom up methodologies in measuring socio-technical threat in systems. There are two major challenges in this theory. Firstly the requirement of a various language among researchers and scientist for understanding deep aspects of an organization. Secondly the governing department and industries are extremely involves in the socio-technical appliances, making it problematic to check organizational features in an unbiased method[16].

## 2.15. Security Requirements Engineering: A Framework for Representation and Analysis[17]

Security needs emerge when the stakeholders wish to preserve themselves from any harm arise in the system. Security needs shall fulfill three principle description, expectations, and fulfillment. In this the author describes a structure for safety needs in requirement gathering and investigation. It constructed an environment for the software, representing security needs as non- functional requirements, and developing contentment opinions for the security needs. The framework is evaluated by applying it to a security requirements analysis within an air traffic control technology assessment plan [17]. Considering traditions, safety strategies, controlling values, and security aims in the security requirements engineering are solid ideas of the framework. One problem we encountered during the project is external argument. The external argument demonstrates that if the rules are legal and if the behavior requirement is accurate, and if there are no other presentations, then the system can be safe. It does not verify that a system will be safe and, in fact, cannot do so. In this differences, some individuals did not see the value of external opinions and required to continue directly to the internal arguments. However, it is the external argument that delivers (UEP) scheme[18]. They planned selective encryption method which offers a simple and functioning safety solution for an ECG sensor-based communication policy, where one percent of data is encrypted only without disturbing ECG data security. This percentage of the encrypted data is important to ECG data features. This mechanism significantly reduce the load of ECG encryption, while also providing a major energy saving and simulation results presented that this mechanism is capable to offer more than 40% further energy saving. But increasing the density of the ECG data does not result in considerable increase in performance. However, it is the external argument that delivers the expectations to be verified in the internal arguments, so avoiding this step is not correct. We want to discover a better method to inspire, capture, and signify the external arguments.

## 2.16. Assurance of Energy Efficiency and Data Security for ECG Transmission in BASNs[18]

Energy consumptions and safe data keeping with ECG (electrocardiographic) appliances in Body Area Sensor Networks are still two major problems to handle. In this paper the author explore the features of compressed ECG statistics for energy saving to design a selective encryption method and a two rate unequal error protection (UEP) scheme[18]. They planned selective encryption method which offers a simple and functioning safety solution for an ECG sensorbased communication policy, where one percent of data is encrypted only without disturbing ECG data security. This percentage of the encrypted data is important to ECG data features. This mechanism significantly reduce the load of ECG encryption, while also providing a major energy saving and simulation results presented that this mechanism is capable to offer more than 40% further energy saving. But increasing the density of the ECG data does not result in considerable increase in performance.

## 2.17. Automata-Based Verification of Security Requirements of Composite Web Services[19]

Due to the increase number of complex real world web application, there is a need to verify that these applications not only accomplish the essential services but also fulfils the required constraints. In this the authors describes a methods for confirming that a composite web service meets the non-functional requirements expressed by the user in the form of constraints. They presents an automata-based structure for validating that a merged service satisfies the user non-functional requirements based on the nonfunctional properties of the component web facilities .The positive point of automata-based method is that it is for verification of string operations in real world web applications based on symbolic string analysis (representative verification method that cartels two investigates with the some previous string analysis

procedures). The negative point of this method is that it can only manage those types of nonfunctional requirements which can be stated in Web Services Description Languages such as Web Service Policy, WS-Security, WS-Trust and the domain expert knowledge is needed to build the terminology mapping table[19].

## 2.18. Assuring Mission Success: Systems Security Engineering and Assurance MILCOM2008[20]

Certification and Accreditation is a methodical procedure for calculating, describing, testing activities before or after a system is in process. It is considered one of the greater problem to information technology .In this the authors discovers the description and coordination of 16 activities in Information Assurance engineering, C&A activities, network operational design, authentication design, connection activities and Information Assurance operational management[20]. These activates provide consistent advantage in implementation of technical actions like security, discovery, and reaction of elements for information technology components. There is a challenge encountered to estimate the cost of these activates in Information Assurance for both the financial mediator as well as the service supplier.

## 2.19. Dealing with Security Requirements for Socio- Technical Systems: A Holistic Approach [21]

Security requirements are necessary for the development of socio technical system like other non-functional requirements. In this the authors offered a universal approach to examine safety requirements for socio technical system. In this three layer security investigation that comprise business procedures, applications and physical structure are developed. They offered a method that manage security requirements analysis throughout the three layer structure. This approach has a benefit that it supports specialists who are not security experts by describing transformation standard and contributes to reduce the scalability issues in independent model[21]. However, this method has restrictions on its evaluation because this method is only applied to the situations, which are explanatory example rather than a real-world analysis.

## 2.20. Security and Trust Requirements Engineering*[22]

In system development process integration of security requirement is a challenging process now a days. In this paper the authors critically review advanced security requirements and talk over the inspiration that let them to propose the Secure Tropos, a proper structure for forming and analyzing security requirements. The positive point of this approach is that it well placed within the meta level modelling field. To escape the disadvantages of this approach authors focused on a segmental addition so that releasing all newly planned features makes them, return to original procedure [22].

# 3. ANALYSIS

Different techniques have been followed to ensure the quality standards to achieve quality products. F. Dalpiaz et al. [1] followed Tropos technique [2] for the design and development of Socio Technical systems. The tropos approach employed the usability standard but it did not take into account any verification standard for evaluating the technique. F. Dalpiaz et al. [2] has also described SecCo(Security via commitments) methodology to derive security requirements from security needs[2].

E.Paja et al. [3] introduced STS-Tool which is used to gather security requirements through security needs in terms of social commitments. E.Paja et al. [5] has also identified and managed the conflicts on the basis of automated reasoning in security requirement models. Consistency and security were the basic quality standards employed in [11][12]Table 1: Evaluation Parameters for Quality Assurance.

**Table 1. Evaluation Parameters for Quality Assurance**

| Evaluation Parameters | Meaning | Possible values |
|---|---|---|
| **Reliability** | Maintaining level of performance under different conditions for a stated period of time. Also defined as failure-free operation. | Yes , No |
| **Understandability** | How easily the software can be made understood to a layman about its functions/purpose. | Yes , No |
| **Reusability** | Components of the software to be reused in other applications. | Yes , No |
| **Maintainability** | How easily system can be corrected and modified. | Yes , No |
| **Ease of use** | Friendly to use and learn. | Yes , No |
| **Efficiency** | Performance level using minimum resources. | Yes , No |
| **Portability** | Transferring from one place to another and run in different environment. | Yes , No |
| **Functionality** | Performing according to defined requirements and specifications. | Yes , No |
| **Verification** | Comparison with specified requirements | Yes , No |
| **Validation** | How easy to test | Yes , No |
| **Performance** | Utilizing low resources, lower response time and mean time of failure and recovery. | Yes , No |
| **Extendibility** | Adapting new features. | Yes , No |
| **Effectiveness** | Completed task under stated conditions. | Yes , No |
| **Consistency** | Acting or done in the same way over time, especially so as to be fair or accurate. | Yes , No |
| **Scalability** | Function that describes its capability to cope and perform under an increased or expanding workload | Yes , No |

**Table 2. Analysis of Quality Assurance Standards Parameters**

| Ref.# | Research Papers | Reliability | Understandability | Reusability | Maintainability | Ease of use |
|---|---|---|---|---|---|---|
| [1] | **F. Dalpiaz et al., 2008** | No | Yes | No | No | Yes |
| [2] | **F. Dalpiaz et al., 2011** | No | Yes | Yes | No | Yes |
| [3] | **E.Paja et al., 2012** | No | Yes | No | No | Yes |
| [4] | **F. Dalpiaz et al., 2012** | No | No | No | No | Yes |
| [5] | **E.Paja et al., 2013** | No | No | No | No | No |
| [6] | **E.Paja et al., 2013** | No | No | No | No | No |
| [7] | **E.Paja et al., 2012** | No | No | No | No | Yes |
| [8] | **S. Trösterer et al., 2012** | No | No | No | No | Yes |
| [9] | **T. Li et al., 2013** | No | No | No | No | No |
| [10] | **F. Massacci et al., 2007** | No | No | No | No | No |
| [13] | **H.El-Hadary et al.,2014** | No | Yes | Yes | No | Yes |
| [14] | **F.Dalpiaz et al.,2011** | Yes | No | Yes | No | Yes |
| [15] | **P.Blauensteiner et al.,2010** | No | Yes | No | Yes | Yes |
| [16] | **J.Pence et al.,2014** | Yes | No | No | No | No |
| [17] | **C.B.Haley et al.,2008** | Yes | Yes | Yes | Yes | Yes |
| [18] | **T.Ma et al.,2012** | No | No | No | Yes | Yes |
| [19] | **H.Sun et al. ,2010** | Yes | Yes | No | No | Yes |
| [20] | **B.Capitan,2008** | Yes | No | No | Yes | Yes |
| [21] | **T.Li et al.,2009** | Yes | Yes | No | No | No |
| [22] | **P.Giorgini et al.,2009** | No | No | No | No | Yes |

this technique. S.Trösterer et al. [8] used formative user centered evaluation technique to categorize and examine the large quantity of handling difficulties related to the STS-Tools[8]. The technique was concerned with the usability issue. T.Li et al [9] designed a comprehensive framework that consists of concepts, techniques and tools for designing secure STSs. Along with security, efficiency and performance were also concerned. F.Massacci et al. [10] employed forming language Si*(Secure i*), based on the i* ontology [10] to solve the problem of security at organizational level. Security and integrity was the key issue handled but it lacked reliability. H.El-Hadary et al.[13] describes a methodology in which security catalog is made with the help of previous security knowledge. This methodology based on reusing of previous knowledge. B.Capitan explores the definition and coordination of 16 activities. These activities focused on validation planning. H.Sun et al. [19] design a methods for confirming that a combined web service meets the non-functional requirements described by the user in form of limitations. It focus on verification of string operations in real world web applications based on symbolic string analysis. T.Ma et al. explore the characteristics of compacted ECG data for energy conservation as a struggle to plan a selective encryption method but it does not result in much improvement in performance. T.Li et al. [21] describes an efficient process that manages safety requirements investigation during the three-layer structure. P.Giorgini et al. [22] critically review advanced security requirements and argue that the motivation let us to recommend the Safe Tropos. These tropos focused on modular extensibility. C.B.Haley et al. [17] presents a structure for gathering security requirements and to do its analysis.

J.Pence et al. [16] focuses on developing hybrid predictive technologies. It works on the betterment of the theory, importance and measurement of the Socio Technical Risk Analysis framework. P.Blauensteiner et al. [15] emphasize on planning and developing a socio-technical software in a safety critical atmosphere. But the negative point of this approach is that it does not work properly when data are large. All research papers ensure security and integrity parameter on the whole.

## 4. CONCLUSION

Quality assurance is one of the vital aspects of software development [12].It is an advantageous approach to judge the Quality of a system. It examines that the software system is upto the marked standards, processes, and procedures. Different Quality standard parameters are included in this continuous process for assuring the levels and methods that are established and followed throughout the software development process of software. The major reason of involving software Quality assurance in the process of software system development is to make sure that the final system built is as per the requirement specification and comply with the standards[12]. In this research paper different Quality assurance standards have been followed and some have been pointed out to be followed during requirement collection regarding security of socio technical systems. Security and integrity of socio technical systems have been maintained by applying different techniques and using different tools throughout the survey. But still some of the Quality standards need to be met in the process of collecting requirements for socio technical systems like scalability and consistency. Also the STS-tool should be optimized in order to get better results. The performance of the tool should be improved because when the tool is processing the data at its peak level then the performance gets down. The review of different research papers assures that quality assurance practices are very useful and should become an ongoing program. While the risk of errors is well-managed across all research papers reviewed, but our continuing effort would benefit more to further lower the risk of errors.

## 5. ACKNOWLEDGMENTS

Our thanks to our department of Software Engineering and our teacher who have contributed towards development of this research paper.

## 6. REFERENCES

[1] F. Dalpiaz, R. Ali, Y. Asnar, V. Bryl and P. Giorgini. "Applying Tropos to Socio-Technical System Design and Runtime Configuration." in Proc. of Evolution of Agent Development: Methodologies, Tools, Platforms and Languages, 2008. Available: www.troposproject.org/files/dalp-ali-asna-bryl-gior-08-woa.pdf

[2] F. Dalpiaz, E. Paja, and P. Giorgini "Security requirements engineering viacommitments." in Proc. of first Workshop on Socio-Technical Aspects in Security and Trust STAST, 2011, pp. 1-8. Available:www.troposproject.org/files/dalp-paja-gior-11-stast.pdf

[3] E. Paja, F. Dalpiaz, M. Poggianella, P. Roberti, and P. Giorgini. "STS-Tool: UsingCommitments to Specify Socio-Technical Security Requirements." in Proc. ER Workshops, 2012, pp. 396-399. Available:www.troposproject.org/view/Requirements Engineeringpapers

[4] E. Paja, F. Dalpiaz, M. Poggianella, P. Roberti, and P. Giorgini. "STS-tool: Socio-technical Security Requirements through social commitments."in Proc. RE, 2012,pp. 331-332. Available:www.troposproject.org/files/re12-demo-v03-cr.pdf

[5] E. Paja, F. Dalpiaz, and P. Giorgini. "Managing Security Requirements Conflicts inSocio-Technical Systems." in Proc. ER, 2013, pp. 270-283. Available:www.sts- tool.eu/doc/publications/paja-dalp-gior-13-er.pdf

[6] E. Paja, F. Dalpiaz, M. Poggianella, P. Roberti, and P. Giorgini. "Specifying andReasoning over Socio-Technical Security Requirements with STS-Tool." in Proc. ER, pp. 504-507. Available:www.sts-tool.eu/doc/publications/paja-dalp-pogg-robe- gior-13-er.pdf

[7] E. Paja, F. Dalpiaz, M. Poggianella, P. Roberti, and P. Giorgini. "Modelling SecurityRequirements in Socio-Technical Systems with STS-Tool." in Proc. CAiSE Forum,pp.155-162. Available: www.ceur-ws.org/Vol-855/paper19.pdf

[8] S. Trösterer, E. Beck, F. Dalpiaz, E. Paja, P. Giorgini, and M. Tscheligi. "FormativeUser-Centered Evaluation of Security Modeling: Results from a Case Study." in Proc. of International Journal of Secure Software Engineering IJSS, 2012, pp. 1-19. Available: www.disi.unitn.it/~pgiorgio/papers/ijsse12.pdf

[9] T. Li, J. Mylopoulos, and F. Massacci."Global Design for Secure Socio-TechnicalSystems." In Proc. of International Symposium on Engineering Secure Software and Systems, 2013. Available: www.ceur-ws.org/Vol-965/paper07- essos2013.pdf

[10] F. Massacci, N. Zannone, J. Mylopoulos. "An Ontology for Secure Socio-Technical Systems" in Handbook of Ontologies for Business Interaction, Pennsylvania: IGI Global, 2007, p. 188-206.Available:security1.win.tue.nl/~zannone/publication/mass-mylo-zann-07-IDEA.pdf

[11] M.Sirshar et al., "Quality Assurance Standards and Survey of IT Industries, IOSR-JCE, Vol. 10, pp. 65-74, Mar.-Apr. 2013.

[12] Software Quality Attributes-Parameters Explained. 2012, Nov. 4, Retrieved from http://kedar.nitty-witty.com.

[13] H. El-Hadary, S. El-Kassas. "Capturing security requirements for softwaresystems" in Journal of Advanced Research, Journal of Advanced Research, 2014, vol.5,pp. 463–472 Available: http://www.sciencedirect.com/science/article/pii/S2090123214000332

[14] F. Dalpiaz, E. Paja, P. Giorgin. " Security Requirements Engineering for Service-Oriented Applications" in University of Trento - DISI, 38123, Povo, Trento, Italy.2011.pp.102-107.Available:http://www.sts-tool.eu/doc/publications/dalp-paja- gior-11-istar.pdf

[15] P. Blauensteiner, M. Kampel, C. Musik, S. Vogtenhuber." A Socio-TechnicalApproach for Event Detection in Security Critical Infrastructure" in Computer Vision and Pattern Recognition Workshops (CVPRW), 2010 IEEE Computer Society Conference,2010,pp.23-30. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5543164

[16] J. Pence, Z. Mohaghegh, C. Ostroff, E. Kee, F. Yilmaz, R.Grantom, and D.Johnson. "Toward Monitoring Organizational Safety Indicators by Integrating Probabilistic Risk Assessment, Socio-Technical Systems Theory, and Big Data Analytics" in Probabilistic Safety Assessment and Management PSAM 12, June 2014.Available: http://psam12.org/proceedings/paper/paper_549_1.pdf

[17] C. B. Haley, R. Laney, J. D. Moffett, and B. Nuseibeh. "Security RequirementsEngineering: A Framework for Representation and Analysis" in IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. 34, NO. 1, JANUARY/FEBRUARY 2008, pp.133-153.Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4359475

[18] Shrestha, P.L. Hempel, M. D. Sharif, H. Hsiao-Hwa Chen. "Assurance of EnergyEfficiency and Data Security for ECG Transmission in BASNs" in Biomedical Engineering, IEEE Transactions on (Volume: 59, Issue: 4), 2012, pp. 1041 – 1048.Available:http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6122058&ranges%3D2007_2014_p_Publication_Year%26queryText%3Dquality+assurance+in+security+requiremnents

[19] H. Sun, B. S. Honavar, V. Lutz, R. "Automata-Based Verification of SecurityRequirements of Composite Web Services" in Software Reliability Engineering (ISSRE), 2010 IEEE 21st International

Symposium,2010,pp.348-357.Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5635065

[20] F. Church, VA. "Assuring mission success: Systems Security Engineering andAssurance MILCOM 2008" in Military Communications Conference, 2008. MILCOM 2008. IEEE, 2008, pp.1-7. Available:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4753123

[21] T. Li, J. Horko."Dealing with Security Requirements for Socio-TechnicalSystems: A Holistic Approach" in University of Trento, Trento, Italy.Available: disi.unitn.it/~li/papers/caise_14.pdf

[22] P. Giorgini, F. Massacci, and N. Zannone. "Security and Trust RequirementsEngineering" in Department of Information and Communication Technology University of Trento – Italy, pp.25-28.Available:disi.unitn.it/~massacci/Publications/GIOR-MASS-ZANN-05-FOSAD.pdf

[23] ISO standards 9000 Retrieved from http://www.iso.org/iso/iso_9000.