Generic Software Risk Management Framework for SCADA System

Abdelghafar M. Elhady
Lecturer, Institute of Scientific Research and Revival of Islamic Heritage, Umm Al-QuraUnivearsity, KSA.

Ahmed Abou Elfetouh S. &Hazem M. El-bakry
Dept. of Information Systems Faculty of Computer Sciences and Information Systems, Mansoura University, Egypt

A. E. Hassan
Dept. of Electrical Power Faculty of Engineering Mansoura University, Egypt

ABSTRACT

Supervisory Control and Data Acquisition(SCADA) systems is one of important software systems which are used for monitoring and controlling industrial systems that are geographically spread over thousands of kilometers. These systems need to monitor and control so many field sites through thousands of devices that are varying in type, technology and usage. There are different types of people need to access SCADA systems for different purposes. Because of the sensitivity and spreading of these systems, they are vulnerable by hackers and crackers and there are many risks may causes partially or fully breakdown. To managing the SCADA systems, there are number of solutions that had been placed. These solutions varied from detecting one to more of SCADA system risk and assessed them on real system once it occurs. This way causes some damages could happen till the risk is eliminate or could need adaption that difficult or impossible to process.

We propose in this paper a new framework for assessing and managing risks of the SCADA systems before they actually implemented by using one of risk management methodologies through scanning and testing proposed SCADA system architecture and its components.

Keywords

Supervisory Control and Data Acquisition(SCADA), Attack, Vulnerability,Cyber security, Risk,Software Risk Management, Risk Assessments

1. INTRODUCTION

SCADA [1] stands for Supervisory Control and Data Acquisition, which is widely used in industrial processes for supervising and controlling infrastructures, such as water treatment and distribution, electrical power transmission and distribution, transportation services, oil and gas pipelines and so on.

Initially, SCADA systems were standalone systems or isolated systems that are operating proprietary control protocols using special hardware and software. As Internet Protocol (IP) devices become widely available and low-cost, as the trends of replacing them with proprietary solutions become more attractive. This replacement increases the chances of cyber security vulnerabilities and damage incidents [2]. SCADA systems used the promotion in IT solutions such as corporate business systems connectivity and remote access capabilities to resemble IT systems using industry standard computers, operating systems (OS) and network protocols [3,4]. This integration supports new IT capabilities, but it provides significantly less isolation for SCADA systems from the outside world than predecessor systems. Therefore it creates a greater need to secure these systems from remote, external threats which increased because of greater dependency and connectivity between SCADA system and other external systems [5]. Also, the use of wireless networking which is increasing, places SCADA implementations at greater risk from competitors who are in relatively close physical but do not have direct physical access to the devices. Threats of control systems can come from different sources, including terrorist groups, malicious intruders, hostile governments, disgruntled employees, complexities, accidents, natural disasters such as malicious actions by insiders.

To manage the SCADA systems' Risks raised from the entering SCADA into internet world, companies have two choices. First is to design their SCADA system, implement it directly and faces the risks could detected to eliminate or mitigate the impacts that happened. This choice is less effective and more cost. The second choice is to implement SCADA system first on simulation software which testing the SCADA system Architecture and discover the critical points of that architecture and provide set of recommendations to improve that architecture.

In this paper, authors will present short notes about SCADA systems, their architecture, risks, SCADA system's simulations and their ability of detecting and managing SCADA system's risks and provide advices to SCADA. Finally, they will present the proposed Risk Management Simulation (Framework) for SCADA system.

2. SCADA SYSTEMS

SCADA system can take different architectures which are varying from planet to another and from system to another. But the general architecture of SCADA system [5](see Figure 1) which consists of three main parts as follow:

2.1 Control center components

The control center is used to collect, maintain and monitor the planet and controls the SCADA system send instruction to all peripherals of the planet. To perform this functionality, control center should contain the following components:

2.1.1 Control Server

It hosts the supervisory control software of DCS or PLC that communicates with lower-level control devices over an ICS network.

2.1.2 SCADA Server or Master Terminal Unit (MTU)

It is the master device in a SCADA system which monitors and controls remote terminal units and PLC devices that located at remote field sites.

2.1.3 Human-Machine Interface (HMI)

It is a software and hardware thatenables human operators to monitor the status of a controlled process, change the control objective by modifying control settings, and override automatic control operations manually in emergency events.

2.1.4 Data Historian

It is a centralized database for auditing all process information within an SCADA system. Information stored is used to support various analyses and process control statistics needed to enterprise level planning.

2.1.5 Input/output (IO) Server

It is a control component that is used to collect, buffer and provide access from control sub-components like PLCs, RTUs and IEDs to process information.

2.2 Fields sites components

These components are used to monitor the field devices, receive instructions from master stations and control field devices that are directly connected with. These components are as follow:

2.2.1 Remote Terminal Unit (RTU)

It is adata acquisition and control unit that is designed to support SCADA remote stations.In remote situations where wire-based communications can't use, RTUs are connected with wireless radio interfaces to support remote situations.

2.2.2 Programmable Logic Controller (PLC)

It is a small industrial computer that is designed to perform the logic functions executed by electrical hardware such as switches, relays, and mechanical timer/counters. In SCADA system, PLCs are often used as field devices because they are economic, versatile, flexible, and configurable than RTUs.

2.2.3 Intelligent Electronic Devices (IED)

It is a "smart" sensor/actuator that is containing the intelligence needed to communicate to other devices, acquire data, and perform local processing and control.

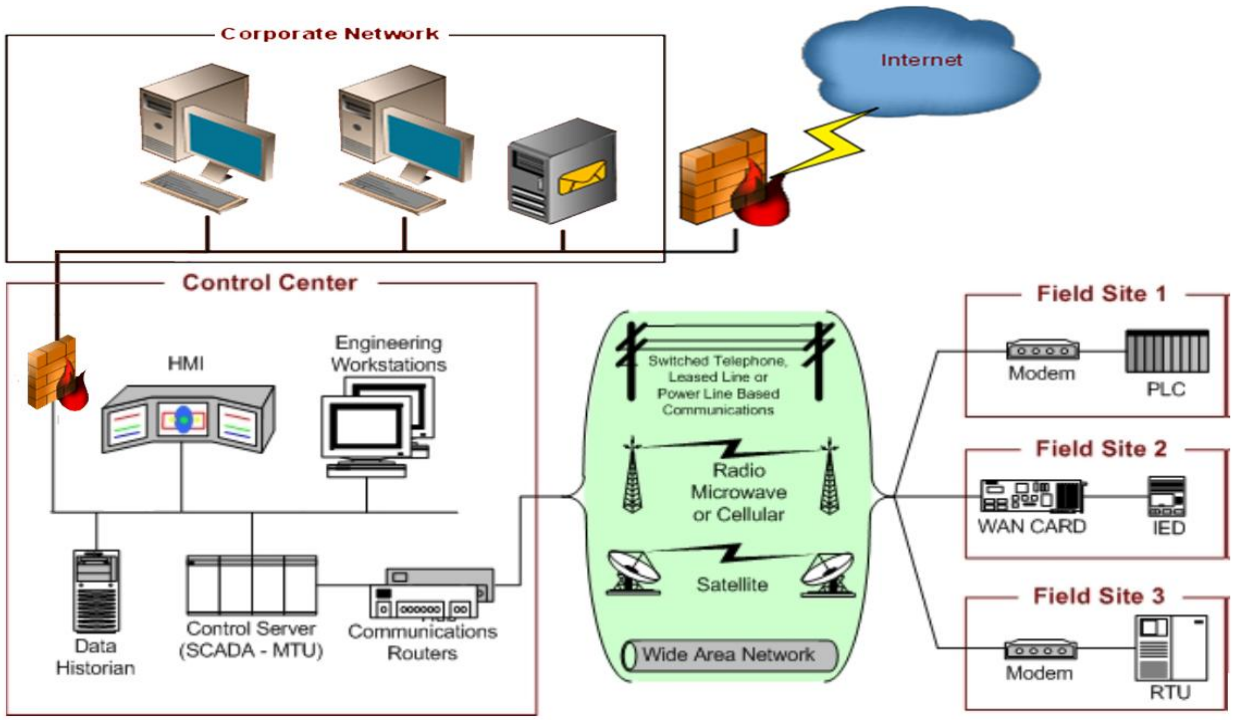


Fig 1: SCADA System Architecture

2.3 Network components

These components are responsible for connecting all devices in the field sites with the control center of SCADA system and connect SCADA control Network with corporate management network. These components are as following:

6.2.1 Fieldbus Network

It links sensors and other devices to a PLC and other controller. The messages transfer between the sensors and the controller are uniquely identified for each of the sensors.

6.2.2 Control Network

It connects the supervisory control level with lower-level control devices.

6.2.3 Communications Routers

It transfers messages between two networks.it is used to connect a LAN to a WAN, and connect MTUs and RTUs over a long-distance network.

6.2.4 Firewall

It protects network devices by monitoring and controlling communication packets that are predefined filtering policies. it is useful in managing SCADA control network segregation strategies.

6.2.5 Modems

It converts between serial digital data and analog signal that is suitable for transmission via telephone line to allow communication between devices.

6.2.6 Remote Access Points

They are distinct devices, used to remotely accessing and configuring a control network of SCADA system in areas and location where wire based communication is unavailable.

3. RISKS OF SCADA SYSTEM

As SCADA systems transform from isolated systems into internet based systems as web based applications, online SCADA systems, and cloud based SCADA systems as more risks appears to SCADA systems [6]. Authors brief these risks as following:

3.1 Risks related to policy and procedure vulnerabilities

These vulnerabilities can exists because of lacking or nonexistent of SCADA system's Documentation like lacking of security policies and procedures, defects in system architecture or design, Inadequate auditing plan, and recovery mechanism not sufficient.

3.2 Risk related to platform vulnerabilities

These risks can occur because of misconfiguration, poor maintenance, back doors in SCADA system's Platform including Hardware, Operating system, Applications. These risks are like delaying of operating system's or application's patches, using default configuration of applications and OS, critical configuration of the system hasn't been packed up, unprotecting system's data, no password used, insufficient access controls, inadequate physical security which facilitate unauthorized personnel from accessing system equipment, and not installing malware prevention software.

3.3 Risks related to network vulnerabilities

These risks can be happened due to misconfiguration, poor maintenance, back doors in SCADA system's networks or the connections between the SCADA system and other systems. Examples of these risks are: security architecture of the SCADA network is weak, encryption not used to securing critical data transmitted, physical security of the network devices not sufficient, misconfiguring or nonexistent of firewall, un-controlling network traffic, monitoring and auditing SCADA network is not existing or inadequate.

4. SOFTWARE RISK MANAGEMENT

Risk management is a systematic approach that is continuously processing to detect and manage the risks. Software Engineering Institute (SEI) has been developed a risk management paradigm to manage risk. The SEI paradigm [7] consists of five stages (see Figure 2).

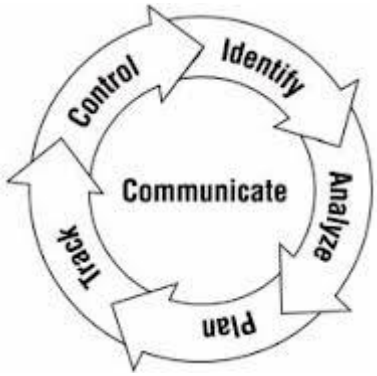


Fig 2: SEI risk management paradigm [7]

In identify stage, all risks related to the project/ system will be developed should be identified explicit and classifying these risks based on one or more criteria. This stage is done before software project is started. Any new risk will be detected after that should be identified well.

In analyze stage, data about risks are analyzing and detecting which risks are threaten to the system and form decision making information that can be used in the next steps.

In planning stage, the data and information of software risks are used to produce decision and mitigation strategies which can be one of four actions; mitigate the impact of the risk, avoid the risk, accept the risk, and transfer the risk.

In tracking stage, accurate, timely information about risk has been collect and presented to appropriate people/group which is using this information to monitor the risk and the impact of solving strategies used on the risks.

In control stage, the reports and information about risk and the software project which provided in tracking stage are studied well to check of the actions related to risks are sufficient or there are another actions need to be taken to solve the risks.

All information about the software project risks and mitigation plans should be shared across all stockholders of the software project to use it in resolve the risks.

5. SOFTWARE RISK MANAGEMENT IN SCADA SYSTEM

Risk management in SCADA system is critical issue to identify, assess and mitigate the risks could be detectedto ensure the safety and reliability of the system. In [8],Jian Guan et al presented a digraph for identifying and managing risks in SCADA system. They used probabilistic approaches to assess the impact of risk based on structural model of SCADA system. But this model didn't take threat and/or vulnerably characteristics.

E. Luiijfet al. in [9] developed a questionnaire that has been used to investigate the SCADA security posture of the ten companies comprising the Dutch drinking water sector. The questionnaire was consist of thirty nine questions cover the

main security issues (the drinking water company security policies and security posture, information and network security architectural aspects, and operational and system management issues). The output of the questionnaire was analyzed and authors developed thirty nine practices for SCADA system (eleven for company management and twenty eight practice for technical process automation).

G. Hamoudet al. in [10] presented a practical approach for assessing the risk related to the failure of the SCADA system which is used in power systems. They calculated the risk on a station by station basis and expressed in dollars. Then they developed a spreadsheet to perform calculations of all the risk they study. They applied the proposed method to the Hydro One Transmission Networks System and they used the historical operating performance data of the system.

M. McQueenet al. in [11] proposed a methodology provides a quantitative measurement of the risk reduction achieved by modifying the control system to improve cyber security defense against external attacks. The methodology employed a graph called a compromise graph in which the nodes act as stages of a potential attack and edges represent the estimated time-to-compromise of several attacker skill levels. The time-to-compromise was modeled as function of known vulnerabilities and attacker skill level. The methodology was applied to calculate risk reduction estimates for specific SCADA system security remedial measures.

Y. Jiaxiet al. in [12] proposed two kinds of method to assess the cyber security of power industry. These methods were the probabilistic assessment and the integrated risk assessment. They finally proposed set of aspects to promote the cyber security of the power industry.

P.A.S. Ralstonet al. in [13] attempted to provide set of guidelines, best practices, security tools and new technologies developed by governmental agencies. They also, provide an update on the advances in probabilistic risk assessment that can be applied to estimate the risk (exposure or expected loss) from SCADA and DCS installations. They finally compared recently approaches used for quantifying the risk, threat impact and cyber-security of the industrial systems' networks.

Z. Anwaret al. in [14] proposed a security model which incorporated infrastructure descriptions and workflow activities of the SCADA systems. They improve existing techniques of attack graph generation for evaluating risks and give recommendation on safer workflows based on a cost-lattice. They developed a tool-chain that automates the process of generating their models from CIM specifications which can be dynamically updated to give accurate results.

D.J. Kanget al. in [15] specified the threats to SCADA system based on general cyber threats on communication networks. They analyzed and defined the points of the system where the vulnerabilities can be occurred and possible attack types based on the results.

By studying the previous cases, we find that some authors worked on real SCADA systems, other worked on simulations. Some of them concentrated on one or two phases of software risk management stages like risk assessment, risk analysis and assessment, and risk identification and assessment. Some of them have deal with one type of SCADA risks such as network attack risks, cyber security risks, data integrity risks.

We will present in the following section a generic Software risk management framework that uses all stages of software risk management paradigm in scanning, detecting, assessing, managing SCADA risks in the designing phase of SCADA system development life cycle.

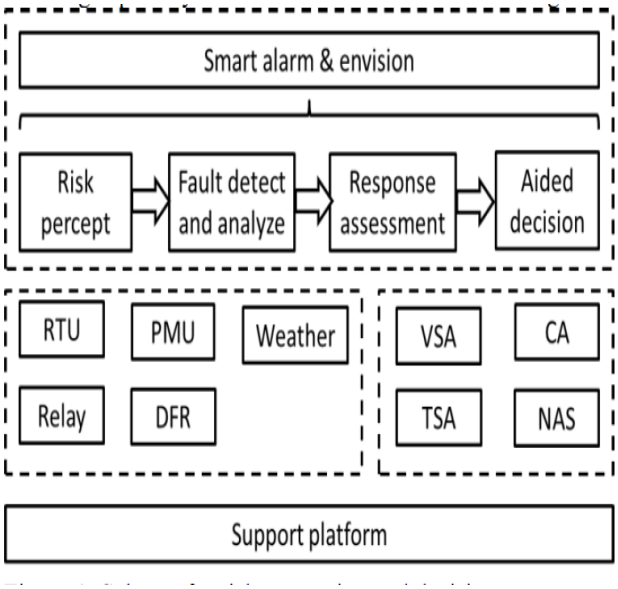
6. GENERIC RISK MANAGEMENT FRAMEWORK FOR SCADA SYSTEM

In this section, we will discuss about the most closes frameworks in more details. Then we will propose new framework for detecting, managing the risk of SCADA systems based on the proposed architecture of the SCADA system. This frame work we called "Generic risk Management Framework for SCADA system". First, we will illustrate the sequence of proposed framework by displaying the flowchart of the framework. Then, we will demonstrate the components that areforming the proposed framework by showing itsblock diagram.

6.1 The existing techniques of the proposed framework

J. J. Lu in [16] provided operational risk processing framework for risk perception, monitoring, analyzing, assessment, and aid decision making on real power system such as SCADA system. The basic structure of the proposed framework (see Figure 3).

Fig 3: Scheme for risk perception and decision support



The framework composed of four layers. The underlying layer is Support Platform layer which is responsible on resource management services for the application in upper layer. The information layer collects various types of data needed for risk perception and accident handling. The basic application layer is SOA-based used to provide network analysis and security assessment. The advanced application layer used to percept, monitors, analysis, assessment of accident risks and provide decision support.

Wang Chunlei et al. in [17] built a simulation environment to analyze and assess the security of SCADA system and its associated industrial infrastructure. They proposed reference architecture of SCADA system simulation based upon hierarchical model and communication model they previously proposed. As (see Figure 4), this architecture consists of Enterprise network, OPC server and client, SCADA protocol tester, SCADA RTUs Sensors and actuators and Industrial infrastructure. This simulation environment concentrated on specific types of attacks such as integrity attacks and denial

of service attacks on sensors and didn't study other types of SCADA risks and attacks.

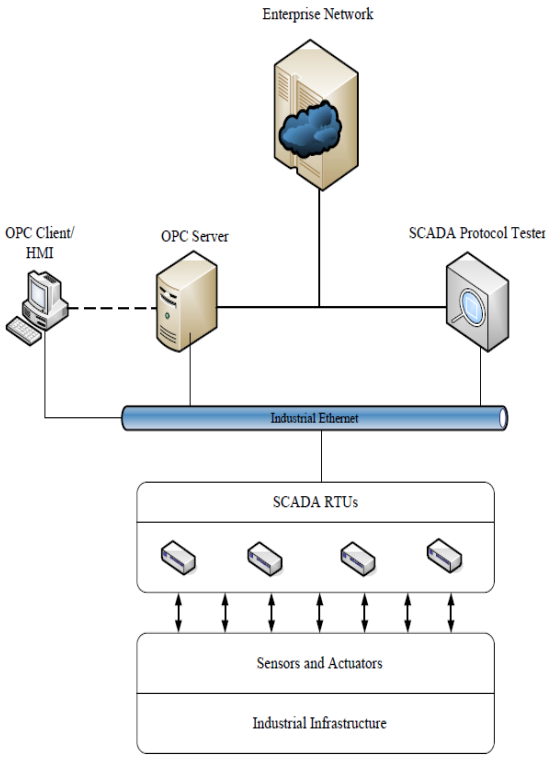


Fig 4: Reference Architecture of SCADA Simulation Environment

S. Patel et al. in [18] proposed a mathematical model used to determine the financial impact resulting from cyber-attacks on the information system of industrial plants. The authors divided cyber-attacks into sever types(see Figure 5). These types are Replay, Spoofing, Denial of Service, Control message Modification, Write to MTU, RTU- response alteration, and Write to RTU. They differentiate the financial loses into five types as follow; Control-loss, Product-Loss, Staff- Time Loss, Equip Damage, and Prevention. Based on these classifications of attack and revenue loss types, this model provides set of revenue-loss functions which is used to calculate the total loss. The values of these functions are driven from the probabilities of different attack types and the estimation of the financial losses which related to revenue loss.

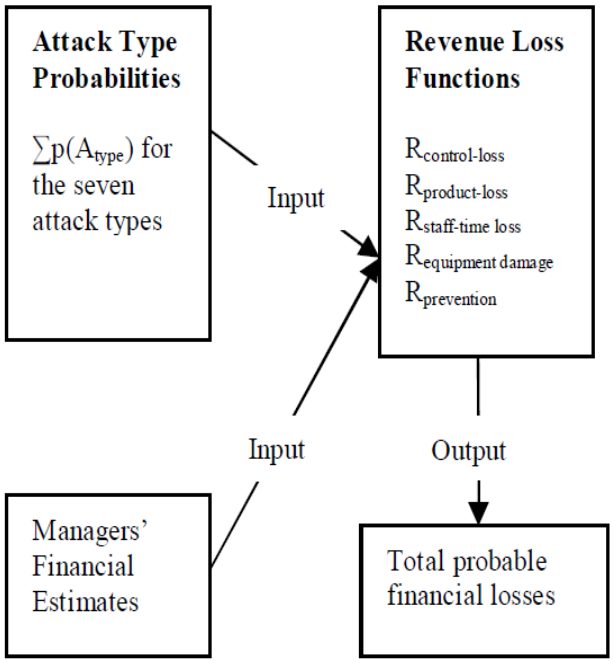


Fig 5: Proposed Model with its Inputs and the Output

6.2 The Flowchart of Generic risk management Framework for SCADA system.

The framework begins with building the proposed SCADA system architecture by SCADA system Engineer (see Figure 6). This can be achieved by one of three ways; by specifying the SCADA system description, by drawing the SCADA architecture using built-in graphical tool, and by drawing the SCADA architecture usingone of Visual Programming Language (VPL) such as labview. Then SCADA architecture is transformed into component Relationship form which has been scanned to determine the dependancy amonge architecture components and detect the risks can be happened to each component. Then, each risk is assessed by calculate the Risk Exposure (RE) as follow:

RE = Risk Probability * Risk Impact

Then all risks are sorted based on RE values and classifying these risks into three ereas and graphically repesented them using red, yellow, and green colors. Finally, Risks are being controlled to reduce risks impact by using one of risk reduction techniques such as mitigation, contingency, and crisis plan based on risk siverity. If the SCADA architecture isn't reach acceptable level, the SCADA architecture is rebuiled after risk control stage and sequence steps are being processed til the architecure be acceptable.

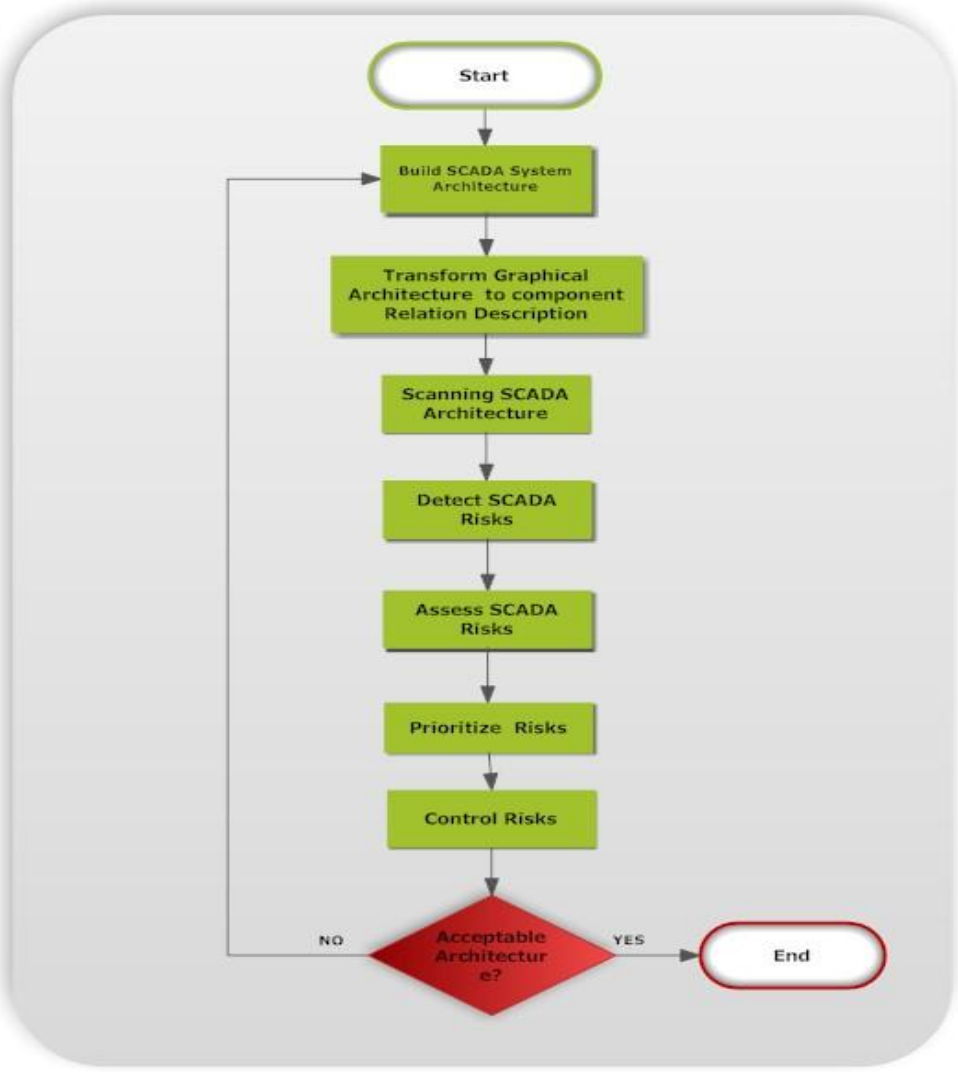


Fig 6: The Flowchart of Generic risk management Framework for SCADA system

6.3 The block diagram of Generic Software Risk Management Framework for SCADA System

The block diagram of the risk management Framework for SCADA system consists of ten components. These components are as follow:

6.2.1 SCADA Risk Identification & Classification Engine (RICE)

This component is used to define all risks could happened to SCADA system or one of its components/devices and identify the characteristics of each risk and the ways to control this risk.

6.2.2 SCADA Architecture Descriptor (SAD)

SCADA system engineer use this component to describe the proposed SCADA system he want to implement and test it for Risks. He can specify the components of the system their characteristics, interconnectionand interaction among them.

6.2.3 SCADA Graphical Designer (SGP)

This is another tool for building SCADA system architecture where it is a built-in tool used to design the prosed SCADA system using set of graphical components to represent all SCADA system components and their interconnectivity.

6.2.4 SCADA Visual Programming Language (SVPL)

SCADA system engineer can use one of Visual Programming Language (VPL) [19] such as LabView [20] to design, test that scale from small to large SCADA systems.

6.2.5 Graphical/Component Relationship Transformer (GCRT)

This component is responsible on translating the graphical representation of SCADA system architecture that has been built into component and relationship hierarchy to be easily scanning and risk detecting.

6.2.6 SCADA Architecture Scanner (SAC)

This component is used to scan the component/relationship hierarchy to recognize the system components and their

dependencies which used as base for determining the risk impact.

6.2.7 Risk Detection Engine (RDE)

After scanning component/relationship hierarchy of SCADA system and recognizing the system's components, this component uses knowledge base to detect the risks can be occurred in this SCADA architecture.

6.2.8 SCADA Component Risk Assessor (SCRA)

For each risk has been detected by RDCE, this component determine the probability and Impact and calculate Risk Exposure (RE).

6.2.9 SCADA Risk Prioritize Component (SRPC)

After calculate the RE for each risk, this component is responsible for sorting and categorizing the risk based on their severity in to three areas and graphically represent them by three colors ;red, yellow, and green.

6.2.10 SCADA Risk Controller (SRC)

This component uses one of reduction techniques to either eliminate or mitigate the risks have been detected.

6.2.11 SCADA Risk Repository

This is the repository which maintains data about SCADA system architectures that have been designed, SCADA risks and their data which are used for managing Risk in SCADA systems.

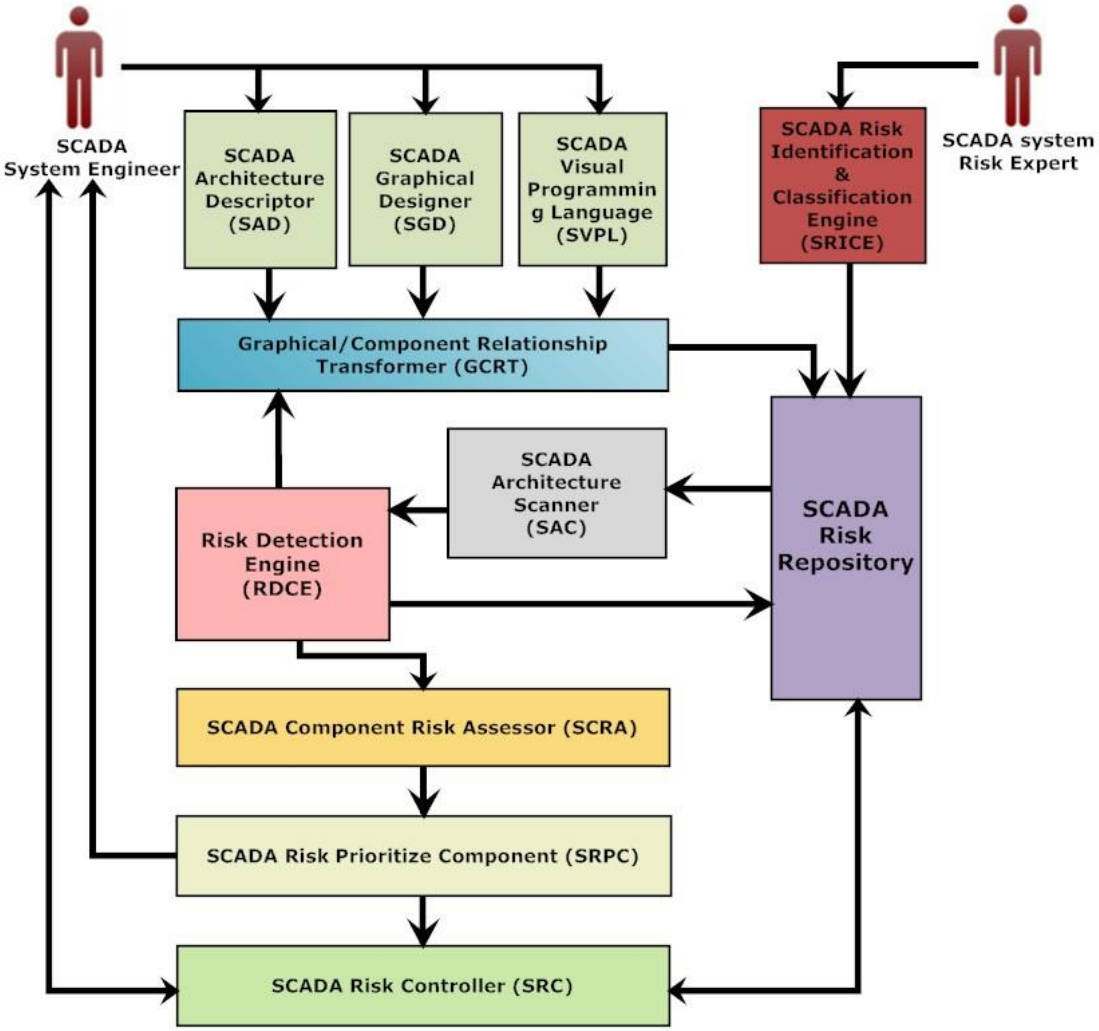


Fig 7:The block diagram of the Generic Software Risk Management Framework for SCADA System

7. CONCLUSION

In this paper, we take a look on SCADA systems as one of important software systems in industry environment. We presented SCADA systems, their functionality, architecture, risks could threat SCADA systems and set of experiments and efforts that had been suggested to manage these risks. Then we gave a short note on software risk management and its phases. afterthat, we proposed a new generic software risk management frame work for managing risks of SCADA systems by checking the SCADA architecture and its components to determine the risks could happened and put some suggestions to control them before the actual implementation of the SCADA system. We displayed the flowchart of the framework and illustrated the components of the framework.

8. REFERENCES

[1] http://en.wikipedia.org/wiki/SCADA, last visited 26/3/2013.

[2] McClanahan,andRobert H., "SCADA and IP: Is Network Convergence Really Here?", Industry Applications Magazine, IEEE, 9(2), pp. 29-36, 2003.

[3] D. C. Mcfarlane , and S.Bussmann, "Developments in holonicproduction planning and control", production planning & control, Taylor & Francis group content, 11(6), pp. 522-536, 2000.

[4] R. M. Murray,K. J.Astrom, S. P. Boyd, R. W. Brockett, and G. Stein, "Future directions in control in aninformation-rich world", Control systems magazine, IEEE, 23(2), pp. 20-33, 2003.

[5] E. J. Byres, M. Franz, and D. Miller, "The Use ofAttack Trees in Assessing Vulnerabilities in SCADASystems", International Infrastructure Survivability Workshop (IISW'04), IEEE, Vol. 4, 2004.

[6] K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security", Department of Commerce, National Institute of Standards and Technology(NIST), USA, 2011.

[7] J. McManus, "Risk Management inSoftware DevelopmentProjects", Elsevier Butterworth-Heinemann, ISBN 0 7506 5867 3, 2004

[8] J. Guan, J. R. Graham, and J. L. Hieb, "A Digraph Model for Risk Identification and Management in SCADA Systems",International Conference on Intelligence and Security Informatics (ISI), IEEE, china, pp. 150-155,2011.

[9] E. Luiijf, M. Alib, and A Zielstra, "Assessing and improving SCADA security in the Dutch drinking water sector", International Journal of Critical Infrastructure Protection, Elsevier, pp. 124-134, 2011.

[10] G. Hamoud, R. Chen, and I. Bradley, "Risk Assessment of Power Systems SCADA", Power Engineering Society General Meeting, IEEE, pp. 758-764, 2003.

[11] M. McQueen, W. Boyer, M. Flynn, and G. Beitel, "Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System", Proceedings of the 39th Hawaii International Conference on System Sciences, IEEE, 2006.

[12] Y. Jiaxi, M. Anjia and G. Zhizhong, "Vulnerability Assessment of Cyber Security in Power Industry", Power Systems Conference and Exposition,IEEE, pp. 2200- 2205, 2006.

[13] P.A.S. Ralston, J.H. Graham, and J.L. Hieb, "Cyber security risk assessment for SCADA and DCS networks", ISA Transactions,Elsevier, 46(4), pp. 583–594, 2007.

[14] Z. Anwar, R.Shankesi, and R. H. Campbell, "Automatic Security Assessment of Critical Cyber-Infrastructures", International Conference on Dependable Systems & Networks, IEEE, Alaska, pp. 366-375, 2008.

[15] D.J. Kang, J. J. Lee, S. J. Kim, and J. H. Park, "Analysis on Cyber Threats to SCADA systems", Conference on Transmission & Distribution: Asia and Pacific, IEEE, 2009.

[16] J. J. Lu , "Risk Awareness And Decision Support Technique For Bulk Power System"; 11th IET International Conference on Developments in Power Systems Protection (DPSP 2012), Birmingham, UK, pp. 70-74, January 2012.

[17] W.Chunlei, F.Lan and D.Yiqi, "A Simulation Environment for SCADA Security Analysis and Assessment", International Conference on Measuring Technology and Mechatronics Automation,IEEE,China, pp. 342-347, 2010.

[18] S. Patel and J. Zaveri, JOURNAL OF COMPUTERS, Academy Publisher,5(3), pp. 352-359, march 2010.

[19] http://en.wikipedia.org/wiki/Visual_programming_language, last visited 24/3/2013.

[20] http://www.ni.com/labview/, last visited 24/3/2013.