IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Remote Offshore Oil and Gas Platform SCADA System Fault Tree Design and Minimal Cut Sets Analysis

M.V. V. Siva Prasad[1*], P.S. Avadhani[2]

[1,2] Department of Computer Science & Systems Engineering, AU College (A) of Engineering, Andhra University, Visakhapatnam, India

[*] *Corresponding Author:* *mvvsprasad62*@gmail.com, *Tel.: +91-08912504938*

DOI: https://doi.org/10.26438/ijcse/v7i6.775781 | Available online at: www.ijcseonline.org

Accepted: 11/Jun/2019, Published: 30/Jun/2019

Abstract: Safety of the remote oil and gas production platform is vital. Supervisory Control and Data Acquisition System (SCADA) system ensures safe operations at remote platform by remote monitoring and control from main process complex. SCADA system at remote platform comprises of remote radio, field router, and remote telemetry unit (RTU). A frame work in designing fault tree for SCADA system at remote offshore oil and gas production platform presented in this research work. It is presented here to analyze the risk to SCADA system as it is available on corporate LAN. Appearing on internet exposed the SCADA system cyber security threats. Analysis of designed fault tree carried out by applying minimal cut sets (MCS) theorem. Fault tree analysis (FTA) is a failure analysis in which an undesired state of a system is analyzed using Boolean logic to combine a series of lower-level events. FTA is an effective technique to support probabilistic risk assessment; it can also be used as a valuable design tool. Minimal Cut Set is a set such that if any basic event is removed from it, the top event will not necessarily occur if all the remaining events in the cut set occur. MCS analysis performed to identify vulnerable faulty sub systems and their components. This analysis guides us to take appropriate action in advance to mitigate the any eventuality. Present analysis contributes directly in safety analysis. It is essential for human safety and preventing oil spill thus, contributing in environment protection.

Keywords— ICS, SCADA System, DCS, CIs, RTU, TDMA, MTU, Remote Offshore Platform, Fault Tree Analysis, Minimal Cut Sets (MCS).

I. Introduction

Industrial Control Systems (ICS) is a general term describing Supervisory Control and Data Acquisition Systems (SCADA), Distributed Control System (DCS). Industrial Control Systems (ICS) are widely deployed in nation's critical national infrastructures such as nuclear energy, transport, banking and health-care. Whilst Supervisory Control and Data Acquisition (SCADA) systems are commonly deployed to monitor real-time data and operations taking place in the ICS they are typically not equipped to monitor the functional behaviour of individual components [1].

The SCADA systems in the oil and gas industry are used in production, well, remote platform, pipeline systems, and drilling for offshore oil and gas monitoring and control purpose. Contemporary SCADA systems exhibit predominantly open-loop control characteristics and utilize long distance communications. The communication link with remote locations deployed here is time division multiple access (TDMA) microwave radio.

The Remote platform SCADA consists of remote telemetry unit (RTU), field router and subscriber radio. Fail proof, reliable operation is the major concern in SCADA systems. As they often control physical processes whose wrongful behaviour might severely impact the safety of humans, offshore environment and leading to production loss directly impacting company's economy and nation's energy security. SCADA network is a process control network and is on corporate LAN, vulnerable to cyber security threats. Its security is vital. According to Suman Sarma et.al, [2] say cyber security, despite often being used as an analogous term for information security, differs from information security. Information security is the protection of information, which is an asset, from possible harm resulting from various threats and vulnerabilities. Cyber security, on the other hand, is not necessarily only the protection of cyberspace itself, but also the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace.

Industrial processes existing in the physical world are monitored and regulated by computer-controlled systems called Industrial Control Systems (ICS). SCADA

(Supervisory Control and Data Acquisition) falls under the category of Industrial Control Systems [3], and in recent years all SCADA vendors have moved to Windows NT, Windows XP and Windows Server 2003. Campos [4] says advanced control and optimization system can play an important role to improve the profitability and stability of industrial process and discussed the problems and challenges of advanced control and optimization in petroleum industries.

The purpose of the contribution statement

1. This article articulates designing of Fault Tree for remote Oil and gas production platform SCADA System. Fault Tree Analysis is a diagnostic tool used to identifying those events, can potentially contributing failure of control system at remote platform.

2. Present FTA frame work helps in avoiding any costly design changes of present control system SCADA.

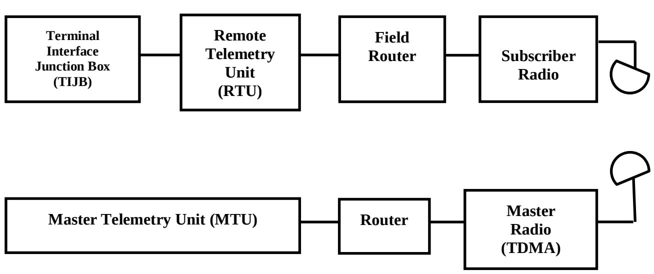

Fig: 1. Schematic SCADA Diagram at Remote Oil and Gas Production Platform

The present paper is organized into following sections for better understanding and clarity. Section I presents introduction, covering various details of remote offshore oil and gas production platform. Next point is, briefly discussed about SCADA system function at remote production platform as a control system. Section I gave details of application of FTA as a probabilistic risk analysis method.
Section II presents methodology describing about Fault Tree Analysis origin and their utility in failure analysis. It is followed by outlining about FTA Design and construction covering in various steps. Section II further proceeds with introduction about various digital gates, events and probability calculations for failure analysis. The important part of methodology is introduction of minimal cutset theorem and its application to SCADA system. Final part section II is about designing fault tree for SCADA system and performing its MCS analysis.

Section III presents results and discussion of fault tree design and MCS analysis performed for remote platform SCADA system

Section IV presents conclusion and future scope of Fault Tree Analysis of SCADA system with field instrumentation system installed at remote platform for better safety analysis.

II. METHODOLOGY

(1). Introduction to Fault Tree Analysis

Fault Tree Analysis (FTA) originally developed in 1962 at Bell Laboratories by H.A Watson [5] to evaluate the Minutemen Intercontinental Ballistic Missile (ICBM) Launch Control System. The standard or Static Fault Trees (SFTs) are the most basic fault trees. They have been introduced in sixties at Bell Labs for the control analysis of the ballistic missile [6]. Mohammad Sadegh Javadi, Azim Nobakht, Ali Meskarbashee et.al, [7] says it is an essentially a top down approach to facilitate failure analysis, starting with a potential undesirable event (accident) called a TOP event, is a box displaying a description of the failure event of interest. The logic relations presented in fault tree models can be equivalently represented in Boolean algebra formulas [8]. The Boolean algebra representation has several advantages over the original fault tree representation. The most significant one is that the Boolean representation can easily be simplified to get a so-called minimum cut representation.

C.C. Fong, C.H. Grigg [9] says FTA as a failure analysis in which an undesired state of a system is analysed using Boolean logic. By employing FTA we can improve the system by finding better components, which lowers the individual failure rates, by designing simpler systems, or by adding redundancy.

Fault identification and its diagnosis is an important aspect in present scenario of power system, as huge amount of electric power is utilized. A. Yadav and V.K. Harit, proposed on-line fault detection and identification of fault-type by using Neuro-Fuzzy method in substation [10]. H. Haroonabadi and M. R. Haghifam [11] say engineers developed of fault tree analysis of the system to be analyzed. But Ahmed Ali Baig, Risza Ruzli, and Azizul B. Buang [12] say reliability engineering for the most part has been developed by mathematicians. They also say that fault tree analysis was developed by engineers.

(2) FTA design and construction involves the following steps:

1. **Define the top event:** The top event the type of failure to be investigated must be identified. Determine all the undesired events in operating a system. Separate this list into groups having common characteristics. Several FTAs may be necessary to study a system completely. Finally, one event should be established representing all events within each group. This event becomes the undesired event to study;

2. **Know the system:** All available information about the system and its environment should be studied;

3. **Construct the Tree:** This step is only the few symbols are involved and the actual construction and is straightforward. The tree must be constructed using the event symbols. It should be kept simple. Maintain a logical, uniform, and consistent format from tier to tier. Use clear, concise titles when writing in the event symbols. The logic gates used should be restricted to the AND gate and OR gate with constraint symbols used only when necessary. An example would be the uses of the oval constraint symbol to illustrate a necessary order of events that must happen to have an event occur. The transfer triangle should be used sparingly if at all. The more the transfer triangle is used, the more complicated the tree becomes. The purpose of the tree is to keep the procedure as simple as possible;

4. **Validate the Tree:** This requires allowing a person knowledgeable in the process to review the tree for its completeness and accuracy;

5. **Evaluate the Tree:** The tree should then be scrutinised for those areas where improvements in the analysis can be made or where there may be an opportunity to utilise alternative procedures or materials to decrease the hazard;

6. **Study trade-offs:** In this step any alternative methods that are implemented should be further evaluated. This will allow evaluators to see any problems that may be related with the new procedure prior to implementation;

7. **Consider alternatives and recommend action:** This is the last step in the process where corrective action or alternative measures are recommended.

(3). Fault Tree Symbols

Symbols are used to connect basic events to the top event, during fault tree construction. The event symbols are logical representations of the way systems can fail. Ning Cai, Jidong Wang, and XinghuoYu et.al, [12] say that there are two kinds of fault tree symbols: gate symbols and event symbols.

(3A). AND gate

This Gate says the output event will occur only if all input events exist simultaneously.

(3B). OR gate

This Gate says the output event will occur if only one or any combination of the input events exists.

Gate symbols connect basic events and/or states to states according to their causal relation. A gate might have multiple inputs, while its output should be single. The output of an OR gate exists if at least one input to this gate exists. The output existence of an AND gate occurs if all input conditions exist for that gate.

(3C). Event Symbols

An event is a dynamic state change of a component due to hardware, software, human and environmental factors. A circle represents a basic component failure. It does not need further development. The reliability data are available for basic events. A rectangle is the symbol to designate an output event. It is also called a state, and used at the output of a logic gate to indicate that other basic events or states are connected to that output. The triangles are used to cross reference two identical pairs of the causal relations. Whenever the fault tree diagrams do not fit a page, triangles are used to show continuity.

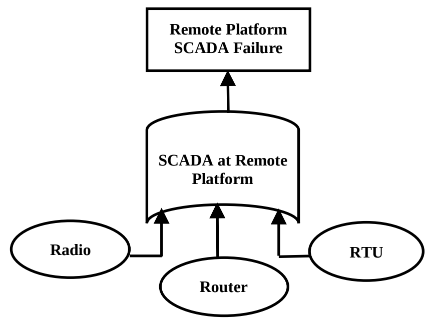

Figure: 1. Basic Fault Tree Design for Remote Oil and Gas Production Platform SCADA System

(4). Probability Calculations in Fault Trees Analysis

Events in a fault tree are associated with statistical probabilities. For example, component failures typically occur at some constant failure rate **λ** (a constant hazard function). In this simplest case, failure probability depends on the rate **λ** and the exposure time **t**:

$$P = 1 - e^{-\lambda t} \text{ And } P \approx \lambda t \leq 0.1\text{------ (1)}$$

The probability of a gate's output event depends on the input event probabilities. An AND gate represents a combination of independent events. That is, the probability of any input event to an AND gate is unaffected by any other input event to the same gate, and the probability of the AND gate output is given by:

$$P(A \text{ and } B) = P(A \cap B) = P(A)\,P(B) \text{ --- (2)}$$

An OR gate, on the other hand, corresponds to set union:

$$P(A \text{ or } B) = P(A \cup B) = P(A) + P(B) - P(A \cap B) \text{—(3)}$$

Reliability is characterised by various indices, such as failure rate **λ** (*t*), Mean Time Between Failures (MTBF), Mean Time To Failure (MTTF), Mean Time To Repair (MTTR), Availability, and Unavailability.

Failure rate is the ratio of the number of failures per unit time to the number of components that are exposed to failure. MTTF is the expected value of the time to failure If the failure rate is constant, MTTF is reciprocal of failure rate.

$$\text{MTTF} = \frac{1}{\lambda} \text{ --- (4)}$$

The average time to fix a component, MTTR, is expressed as

$$\mathbf{MTTR} = \frac{1}{\mu} \text{ --- (5)}$$

Where μ is the constant repair rate. MTBF is defined as the sum of the MTTF and the MTTR.

$$\mathbf{MTBF = MTTF+MTTR} \text{ --- (6)}$$

"Availability is the probability of finding the component or system in the operating state at some time in the future".

$$\textbf{Availability} = \frac{\text{uptime}}{\text{uptime+downtime}} = \frac{\text{MTTF}}{\text{MTTF+MTTR}} = \frac{\mu}{\lambda+\mu} \text{ ------- (7)}$$

It is the probability of finding a component or system in the non-operating state at some time in the future

$$\textbf{Unavailability} = \frac{\text{downtime}}{\text{downtime+uptime}} = \frac{\text{MTTR}}{\text{MTTR+MTTF}} = \frac{\lambda}{\lambda+\mu} \text{---- (8)}$$

$$\mathbf{P(t)} = \frac{\lambda}{\lambda+\mu}\left\{1 - e^{-(\lambda+\mu)t}\right\} \text{---- (10)}$$

$$\textbf{And P} = \frac{\lambda}{\lambda+\mu} \text{ ---- (11)}$$

Minimal Cut Set Theorem

C.L.T. Borges, D.M. Falcao, J.C.O. Mello, A.C.G. Melo [14] say if all conditions of a fault tree are verified, and if for each minimal cut set at least one of its basic events is prevented from happening, the top-level event will never happen. In other words, it is sufficient to prevent only one primary event of each minimal cut set, to avoid system failure according to Pawel Skrobanek [15]. Recently Fault Tree Minimal Cut Sets are further fine tuned with MCS time dependencies analysis.

(6). Designing Remote Oil & Gas Production Platform SCADA System Fault Tree

In designing remote platform SCADA system Fault Tree, the important components considered are DC power supply to telemetry systems, Subscriber TDMA Radio for voice and data, Field Router and Remote Telemetry Unit. The main components of communication link systems are directional antenna, radio transmitter part and radio receiver part. The Remote Telemetry Unit (RTU) main components considered for fault tree diagram are AC 800 F controller, FI 812 Ethernet Module, FI 813 Field Bus Module and FI 830 Profibus Modules. Each and every card has redundancy. Manufacturer failure data considered for most of the components. For router failure rate Cisco data has been considered.

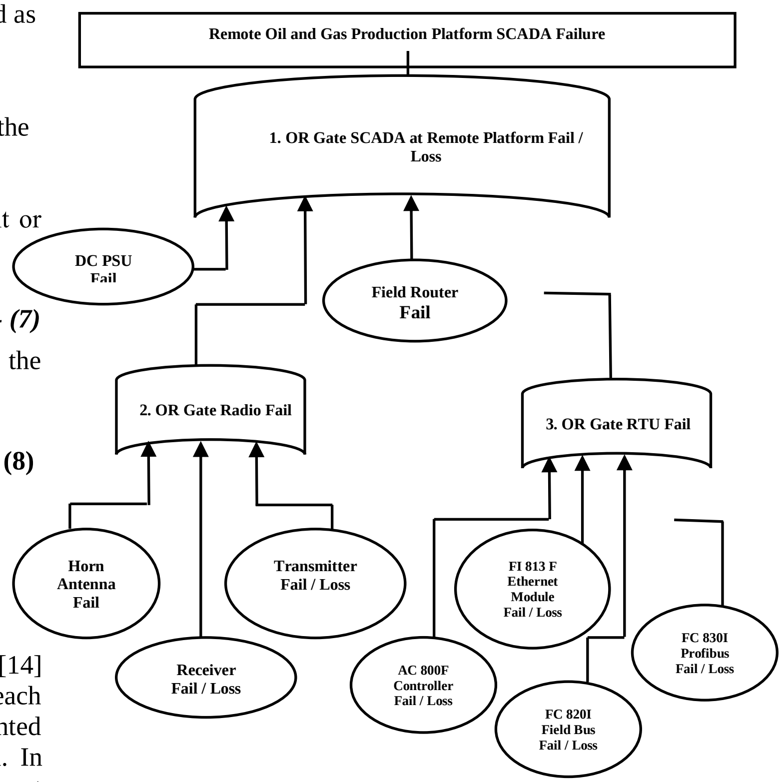

Figure: 2. Remote Oil and Gas Platform SCADA Fault Tree

Component analysis considered SINTEF-1997, OREDA [16], for manufacturer data for comprehensive fault tree analysis. The DC-DC converter Power supply Unit 0.117667 h, directional antenna with failure rate λ = 6.658E-06, and MTTR = 0.03333 h, radio receiver section with failure rate λ = 7.58E-07, and MTTR = 0.3543h, radio transmitter section with failure rate λ = 2.95E-06, and MTTR = 0.1273h, controller module with failure rate λ = 4.80E-06, and MTTR = 0.09466h, ether net module with failure rate λ = 4.80E-06, and MTTR = 0.09466h, serial module for field bus with failure rate λ = 4.80E-06, and MTTR = 0.09466h, and finally Profibus module for field instruments and devices considered with failure rate λ = 4.80E-06, and MTTR = 0.09466h**.** These are mostly industry standard figures and also observed field live failure rates. And mean time to repair, rates are also considered for calculations and analysis. Remote oil and gas production platform SCADA system Fault Tree Analysis (FTA) is employed as a valuable design tool which can identify potential accidents, and aiding in reducing costly design changes. It can also be used as a diagnostic tool, predicting the most likely system failure in a system breakdown.

III. RESULTS AND DISCUSSION

Minimal Cut Sets Analysis

Considering minimum flight time 2 hours to attend the problem time taken to rectify fault we arrive at worst probability for top event is 3.82E-05. The number of Minimal Cutsets are 9/9, and the order of Minimum Cutsets Min 1 / Max 1.

Table: 1. Remote Oil and Gas Production Platform SCADA system Fault Tree Minimal Cut Set Analysis

S.No	Event Failure	Description	Parameters	Event and Cut Set Probabilities	Remarks
1	Power Supply	DC-DC PSU Fail	a) λ = 8.350E-06 b) MTTR = 0.117667h	8.35E-06	Repairable
2	Directional Antenna	Radio link Fail	a) λ = 6.658E-06 b) MTTR = 0.033333h	6.66E-06	Repairable
3	AC 800 F Controller	RTU Controller Fail	a) λ = 4.800E-06 .b) MTTR=0.0946667h	4.80E-06	Repairable
4	FI813F 10 Base T module	RTU Ethernet Module Fail	a) λ = 4 4.80E-06 b) MTTR=0.0946667h	4.80E-06	Repairable
5	Field Router	CISCO 2600 Remote Router Fail	a) λ= 3.50E-06 b) MTTR=0.117667h	3.50E-06	Repairable
6	FI 820 F Serial Module	Serial Module For Field Bus Devices	a) λ = 0.0000032 b) MTTR=0.0946667h	3.20E-06	Repairable
7	FI 830 F Profibus Module	Profibus Module For Field Instruments	a) λ = 0.0000032 b) MTTR=0.0946667h	3.20E-06	Repairable
8	Receiver in Radio	Receiver Part	a) λ = 0.000000758 b) MTTR=0.354h	7.58E-07	Repairable
9	Transmitter Section in Radio	Radio Transmitter	a) λ = 0.00000295 b) MTTR=0.12733h	2.95E-06	Repairable

Nine failure events obtained after minimal cutest analysis. First failure event is DC power supply system to all telemetry equipment at remote platform. Its event and cutest probabilities are 8.35E-06 and 8.35E-06. It can be repaired or replaced at short notice from main process complex to make SCADA control available at remote platform. Second failure event is directional antenna; it is horn antenna at remote platform. Its event and cutest probabilities are 6.66E-06 and 6.66E-06. It can be repaired or replaced at short notice from main process complex. Third failure event is AC 800F controller, here it is RTU main controller at remote platform. Its event and cutest probabilities are 4.80E-06 and 4.80E-06. It can be repaired or replaced at short notice from main process complex. Fourth failure event is FI 813. It is RTU Ethernet module at remote platform. Its event and cutest probabilities are 4.80E-06 and 4.80E-06. It can be repaired or replaced at short notice from main process complex. Fifth failure event is router. It is Cisco 2600 router at remote platform. Its event and cutest probabilities are 3.50E-06 and 3.50E-06. It can be repaired or replaced at short notice from main process complex. Sixth failure event is FI 820. It is RTU serial bus module for field bus devices at remote platform. Its event and cutest probabilities are 3.20E-06 and 3.20E-06. It can be repaired or replaced at short notice from main process complex. Seventh failure event is FI 830. It is RTU Profibus bus module for field instruments at remote platform. Its event and cutest probabilities are 3.20E-06 and 3.20E-06. It can be repaired or replaced at short notice from main process complex. Eighth failure event is receiver section of radio. It receives voice and data from main process complex at remote platform. Its event and cutest probabilities are 7.58E-07 and 7.58E-07. It can be repaired or replaced at short notice from main process complex. Ninth failure event is transmitter section of radio. It transmits voice and data from remote platform to main process complex radio. Its event and cutest probabilities are 2.95E-06 and 2.95E-06. It can be repaired or replaced at short notice from main process complex.

After performing minimal cutset analysis on remote oil and gas production platform SCADA system three gates with worst case probabilities are determined. They are Gate number one OR-Gate: Platform SCADA system Fail, number two gate is an OR-Gate: Platform Radio System Fail and last and final one is gate number three is an OR-Gate: Platform RTU Failure.

Table: 2. Remote Oil and Gas Production Platform SCADA system Gates with Worst Case Probabilities

S. No	System	Description	Gate	Probability
1	Platform SCADA System Fail	Remote Oil and Gas Production Platform SCADA System	OR	3.82E-05
2	Platform Radio System Fail	Digital Microwave Radio at remote platform	OR	1.04E-05
3	Remote Platform RTU Fail	Remote Telemetry System at remote Platform	OR	1.60E-05

After observing above table, remote platform SCADA system Fail is OR-Gate number one with worst case probability is 3.82E-05, and Radio system failure OR-Gate number two is with 1.04E-05 and RTU Fail OR-Gate is with 1.60E-05.

Above data interpretation implies that if OR-Gate 1 with failure probability 3.82E-05 the telemetry data and control of remote platform not available from main process complex. It means catastrophic. It should avoided to the maximum extent, if not problem should be taken up on priority basis to restore SCADA functions. If we analyse OR-Gate 2 it implies data and control will not available to main process complex. But telemetry instrumentation functioning and once radio communication link available, data, monitoring and control will be available to main process complex over remote platform. The third OR-Gate analysis yields that RTU failure. Once RTU does not available, then total SCADA control fails at remote platform to main process complex. It is complicated one, as it may be main controller failure, or it could be ether net module failure or it could be serial module, or it could be Profibus module, or else it could be field bus module. Sometimes combinations of modules failure may impact SCADA control pertaining to remote platform. Minimum Necessary support for fault rectification may be made available at main process complex taking into logistic requirements into consideration.

IV. Conclusion and Future Scope

Over the last decade, efforts from industries and research communities have been made in addressing the security of Supervisory Control and Data Acquisition (SCADA) systems. However, the SCADA system security deployed for a critical infrastructure is still a challenging issue today.

This paper has presented a new risk identification and mitigation framework for analyzing risks to Supervisory Control and Data Acquisition system at remote offshore oil and gas production platform. The goal of this paper was to develop a probabilistic risk or fault analysis framework that uses existing risk assessment (PRA) methodology to quantify the risks of design oriented and also willful threats into Offshore Oil and Gas Production Platform SCADA system. This framework can assist decision makers in understanding the risks of cyber intrusion, consequences and to maximize the availability and survivability of the system. SCADA system possible risks using fault trees were identified

In Future scope of the work may be extended to systems including remote platform field instrumentation part. Detailed Fault Tree encompassing all field instrumentation at remote platform and SCADA system will enhance fault or risk identification and determination of exact cause of telemetry control and monitoring functions failure at remote platform.

Acknowledgment

The author is deeply indebted to his organization Oil and Natural Gas Corporation Limited for according permission to pursue his research work on SCADA system at Heera Offshore Process Complex, Neelam & Heera Asset, Mumbai, India. The author is also greatly indebted his guide Prof. P.S.Avadhani for his timely valuable guidance and scholarly suggestions in his thesis work.

References

[1]. Helge Janicke, Andrew Nicholson, Stuart Webber and Antonio Cau. "Runtime monitoring for industrial control systems", Electronics 2015, Vol: 4, pp. 995-1017, 2015.

[2]. Suman Sharma, Yogesh Verma, Amit Nadda, "*Information Security: Cyber Security Challenges*", International Journal of Scientific Research in Computer Science and Engineering, Vol.7, Issue.1, pp.10-15, 2019

[3]. Aditya Bagri, Richa Netto and Dhruvil Jhaveri. "Article: Supervisory Control and Data Acquisition". International Journal of computer Applications. Vol: 102. No: 10, pp. 1-5, 2014.

[4] Campos M, Teixeira H, Liporace F, Gomes M. "Challenges and problems with advanced control and optimization technologies", IFAC Proceedings Volume 42, No. 11, pp. 1-8, 2009.

[5] H.A.Watson. "Launch control safety study". Bell Telephone Laboratories, Murray Hill, NJ, USA, 1961.

[6]. C. A. Ericson. Fault tree analysis–a history". In: Proc. 17th International System Safety Conference, Orlando, Florida, USA, pp. 1–9, 1999.

[7]. Mohammad Sadegh Javadi, Azim Nobakht, Ali Meskarbashee. "Fault Tree Analysis Approach in Reliability Assessment of Power System", International Journal of Multidisciplinary Science and Engineering, Vol. 2, No. 6, pp. 46-50, 2011.

[8]. Yang Y and Jung I. "Boolean Algebra Application in Simplifying Fault Tree Analysis". International Journal of Safety Science, Vol.1, No.1, pp. 12-19, 2017

[9]. C.C. Fong, C.H. Grigg. "Bulk power system reliability performance assessment". Reliability Engineering Systems, Saf. 46: pp. 25–3, 1994.

[10]. A. Yadav, V.K. Harit, "*Fault Identification in Sub-Station by Using Neuro-Fuzzy Technique*", International Journal of Scientific Research in Computer Science and Engineering, Vol.4, Issue.6, pp.1-7, 2016

[11]. H. Haroonabadi, M.R. Haghifam: Generation reliability evaluation in power markets using Monte Carlo simulation and neural networks, in: 15th International Conf. on Intelligent Systems, Applications to Power Systems, Curitiba, 2009.

[12]. Ahmed Ali Baig, Risza Ruzli, and Azizul B. Buang, "Reliability Analysis Using Fault Tree Analysis: A Review". International Journal of Chemical Engineering and Applications, Vol. 4, No. 3, June 2013.

[13]. Ning Cai, Jidongwang, and XinghuoYu: "SCADA system security: Complexity, History and new developments". The IEEE International Conference on Industrial Informatics (INDIN 2008), DCC, Daejeon, Korea July 13-16, 2008.

[14]. C.L. T Borges, D.M. Falcao, J.C.O. Mello, A.C.G. Melo: "Composite reliability evaluation by sequential Monte Carlo simulation on parallel and distributed processing environments", IEEE Transactions on Power Systems. Vol. 16, No.2, pp. 203–209, 2001.

[15]. Pawel Skrobanek, "Minimal Cut Sets with Time Dependent Analysis". Automatyka /Automatics, Vol 17. No.2, pp. 219-228, 2013.

[16] SINTEF, "OREDA - Offshore Reliability Data, 3rd Edition", SINTEF Industrial Management, Trondheim, Norway. 1997.

Authors Profile

1. Mr M V V Siva Prasad received his M.Sc Physics (Electronics) from Kakatiya University, Telengana State, India, and pursued his Master of Technology in Computer Science and Systems Engineering from Andhra University, Visakhapatnam, India. He is working with Oil and Natural Gas Corporation Limited as Deputy General Manager (E&T). He is serving the organization at various locations throughout India in various capacities. During his tenure at Mumbai offshore he has directly contributed in installation and commissioning of Tier-1 Enterprise wise SCADA System covering 14 remote offshore platforms of at Heera Process Complex, ONGC Mumbai. He also oversaw in Installation and Commissioning of Vessel Aircraft Traffic Monitoring System (VATMS) a joint project between ONGC, Indian Navy, and Indian Coast Guard for the first time in Western Offshore at Heera Process Complex. He is pursuing for his Doctorate Degree in Computer Science & Systems Engineering under the guidance of Prof. P S Avadhani, Andhra University.

2. Mr P S Avadhani, at present Professor, Department of Computer Science and Systems Engineering, AU College of Engineering(A), Andhra University, Visakhapatnam, India. He is Eminent Scientist in Cryptography and Network Security, Computer Algorithms. He received his Masters in Computer Science and Doctorate from Indian Institute of Technology Kanpur, India. He supervised Twenty Ph.D Theses under his guidance. He authored Fifty Four papers in various International Journals and Forty One papers in National Journals. He is Life Member, Indian Science Congress Association of India and also Life Member, Cryptology Research Society of India (CRSI).

