RESEARCHERID
THOMSON REUTERS

[Hossain* 4(7): July, 2017] ISSN 2349-4506
Impact Factor: 2.785

Global Journal of Engineering Science and Research Management

MEASURING THE CYBER SECURITY RISK ASSESSMENT METHODS FOR SCADA SYSTEM

Nazmul Hossain*, Md. Alam Hossain, Taposh Das, Md. Tariqul Islam

* Assistant Professor, Department of Computer Science and Engineering, Faculty of Engineering, Jessore University of Science and Technology, Jessore-7408, Bangladesh.

Assistant Professor, Department of Computer Science and Engineering, Faculty of Engineering, Jessore University of Science and Technology, Jessore-7408, Bangladesh.

Department of Computer Science and Engineering, Faculty of Engineering, Jessore University of Science and Technology, Jessore-7408, Bangladesh.

Department of Computer Science and Engineering, Faculty of Engineering, Jessore University of Science and Technology, Jessore-7408, Bangladesh

DOI: 10.5281/zenodo.824955

KEYWORDS: SCADA, RTU, PLC, IED, IT methods, cyber security

ABSTRACT

The current situation with supervisory control and information procurement (SCADA) framework security is not similar with the vulnerabilities, dangers as on today and potential results. A large number of the SCADA frameworks are moderately shaky frameworks with endless and inescapable vulnerabilities. Seen data security dangers are once in a while talked about and assessed at administration level. Data security part of PC controlled basic foundations must be basically broke down. PC controlled foundations ought to be subjected to an extreme investigation. Challenges for SCADA framework security are examined in this paper. Suggestions have been made to fortify the safety efforts at PC controlled basic foundations like savvy matrix, transportation control, water circulation and others. These suggestions, when executed, will cut down essentially the danger of disappointment at basic foundations. In this paper we most survey diverse dangers states and their effect on Supervisory Control and Data Acquisition (SCADA framework). We likewise audit diverse philosophy in digital security hazard appraisal for SCADA framework. We examination distinctive dangers and place them into various classes. We additionally portray diverse hazard appraisal techniques, their points, applications, affect on up and coming dangers, contrast and distinctive strategies. We additionally investigate distinctive parts of helplessness in the framework.

INTRODUCTION

SCADA is the acronym of Supervisory Control and Data Acquisition [1], which is a correspondence innovation conspire for gathering information from far off offices and furthermore controlling them on control frameworks. SCADA frameworks have been being used over 30 years, and have turned out to be best in class and mind boggling as PC innovation has progressed. They are today fundamental for working basic frameworks, for example, electric power frameworks. SCADA framework is additionally a sort of Industrial Control System (ICS). An ICS controls forms in the mechanical division and in the parts which frame a Critical National Infrastructure (CNI) [2].

Amid the most recent ten years, the quantity of associations with SCADA frameworks and the utilization of web based systems have expanded quickly. SCADA frameworks have likewise moved from utilizing exclusive conventions and programming to utilizing an indistinguishable principles and arrangements from managerial IT frameworks. As an outcome, SCADA frameworks are presently being presented to dangers and vulnerabilities they have never been presented to, and to a considerably more prominent degree than prior [3].

The smooth and dependable operation of SCADA frameworks is key for such segments of CNI as vitality, water and transportation where both information obtaining and control are basically imperative. A boundless, enduring blackout of SCADA and, subsequently, CNI may make genuine unsettling influence a state and. The outcomes of a glitch of a SCADA framework might be unfavorable and may go from money related misfortune because of a gear and ecological harm to the loss of human life.

ISSN 2349-4506
Impact Factor: 2.785
Global Journal of Engineering Science and Research Management

Current SCADA frameworks are exceedingly refined, mind boggling and in light of cutting edge innovation frameworks. The heightening complexity and modernization and also constant persistent operation and circulated, multi-part engineering support the development of digital dangers to SCADA frameworks. SCADA frameworks are presented to an extensive variety of digital dangers additionally on account of the institutionalization of correspondence conventions and equipment segments, developing interconnectivity and inheritance.

In reality, the capacity to complete a digital assault discredits the requirement for a physical assault if the frameworks inside the site can be closed down or put into an undesired and maybe insecure mode from outside, maybe abrogating interlocks, and bringing about weights, temperatures, rotational speeds and levels to go past safe points of confinement. The digital assault might be viewed as the simple alternative by aggressors, which might be attempted from another nation, with attribution of source hard to demonstrate.

Essentially, as opposed to voyaging hundreds or thousands of miles to play out a physical assault on a very much safeguarded website, following quite a while of arranging, an able combative is at risk to rather to utilize SHODAN to decide the IP number of a SCADA framework situated on the opposite side of the world, download misuse code for the SCADA frameworks from Metasploit, then dispatch the assault by means of the obscurity administrations of TOR, maybe inside the time span of 1 hour or less. To put it plainly, SCADA/ICS frameworks must be shielded more vigorously than they are presently [4].

A scope of general IT hazard appraisal philosophies is utilized as a part of industry: Operationally Critical Threat and Vulnerability Evaluation (OCTAVE) [5], Central Computer and Telecommunications Agency Risk Analysis and Management Method (CRAMM), Consultative, Objective and Bi-functional Risk Analysis (COBRA) and CORAS, a model-based hazard evaluation strategy for security-basic frameworks [6]. Likewise there is an expansive scope of scholarly proposition such as Information Security Risk Analysis Method (ISRAM); Cost estimation, Benchmarking, and Risk Assessment (COBRA); SPRINT, a rearranged down to earth chance investigation philosophy; and the Business Process: Information Risk Management (BPIRM) system to give some examples.

MATERIALS

SCADA Architecture

A SCADA framework comprises of equipment and programming parts, and of an interfacing network(s). Fig. 1 indicates bland equipment engineering of a SCADA framework. Engineering is framed by at least one control focuses and various field gadgets, for example, a RTU, Intelligent Electronic Device (IED) and Programmable Logic Controller (PLC) associated by a correspondence framework. A RTU gets information from field gadgets, changes over it to advanced information and sends it to the control focus and in addition gets computerized orders from the middle and handles alerts. A PLC is a computerized PC that screens sensors [7] and takes choices in view of a client made program to control valves, solenoids and different actuators. A control focus

Incorporates a MTU, which issues orders to and assembles information from RTUs, it additionally stores and procedures information keeping in mind the end goal to show data to human administrators to bolster basic leadership. Human operators monitor and control the system from a control centre via Human–Machine Interface (HMI) displays.

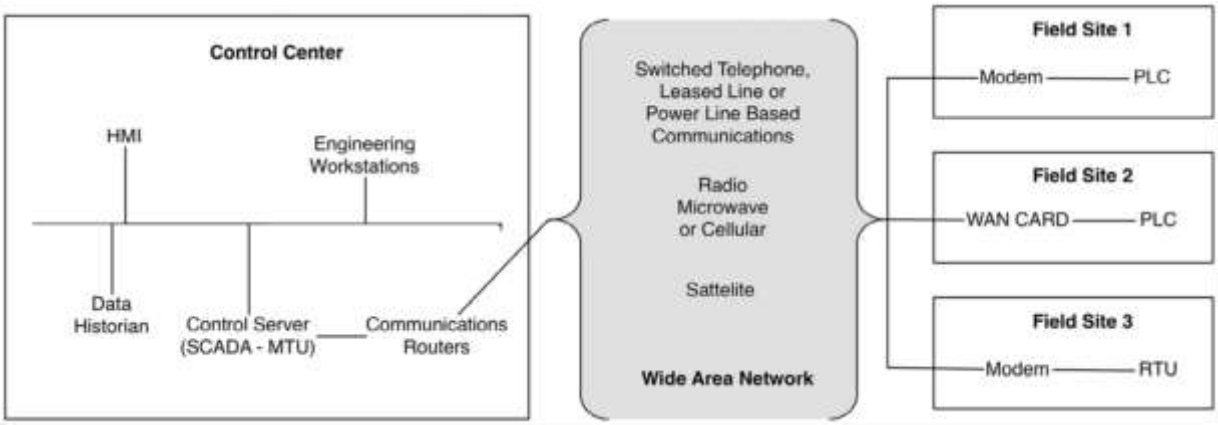

Fig 1: Generic SCADA hardware architecture (Source: NIST SP 800-82)

Generally the SCADA system includes the following components: local processors, operating equipment, PLCs, instruments, remote terminal unit, intelligent electronic device, master terminal unit or host computers and a PC with human machine interface which is show in fig 2.

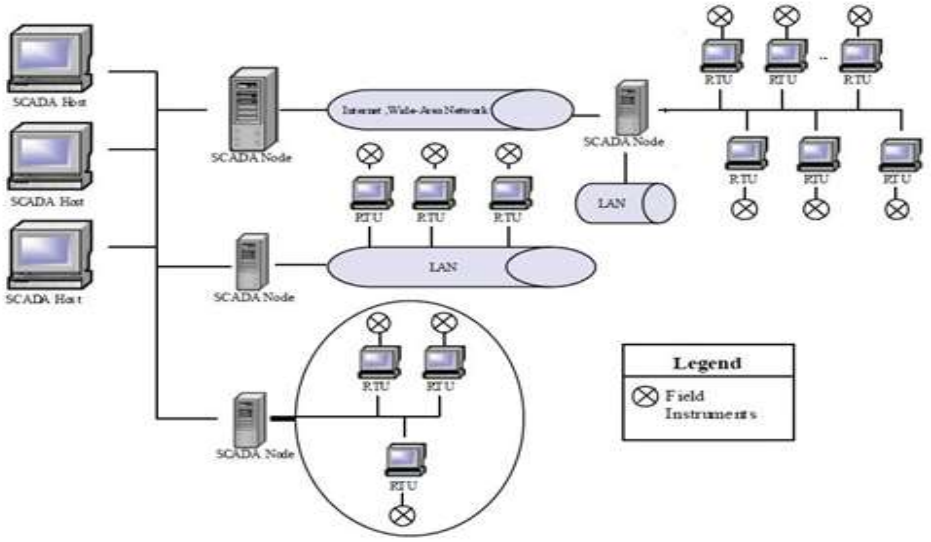

Fig 2: Human machine interface in SCADA

Cyber Security Challenge

The security of SCADA frameworks is observed to be more entangled than that in the customary IT or Internet world. The early ordinary SCADA outlines don't give modern frameworks the security against digital assaults. Old control framework offices are still being used today and they are completely or incompletely associated with corporate IP systems reaching out to Internet [8].

This association is defenseless against digital fear based oppressors' focused on assault when any ensuring system and measure, for example, specific firewall comes up short. IT methods and offices at first were not intended for control frameworks, but rather are broadly utilized as a part of SCADA frameworks. These strategies and offices cannot fulfill the strict needs of SCADA security in the event that they are not changed or improved. For instance, IP based Sensor Network is not made for control frameworks, but rather their utilization is developing quickly in mechanical control interchanges.

In the next section we will discuss different categories of threat and their impact on SCADA system.

Threat Analysis

"Threat" is normally, despite the fact that not reliably, characterized as: Threat = Capability + Intent + Opportunity. From the expository viewpoint, the definition expects the presence of a risk "source" – a performer or operator representing the danger. For some reasons, the defenselessness evaluation process is creating at a quicker pace than the risk appraisal handle [9].

While powerlessness appraisal helps in evaluating the ability consider the risk condition, acceptable evaluation of Intent and Opportunity is more troublesome. Notwithstanding the troubles it is vital and important to characterize and order the solid dangers and vulnerabilities for building security countermeasures for shielding the SCADA framework from them. Along these lines it is required to indicate the dangers at any rate on the subjective level before quantitative estimations, which is the principle center of this paper.

Massoud Amin in EPRI defined three different kinds of threats related to power systems as follows:

Attacks upon the power system: In this case, the electricity infrastructure itself is the primary target-with outages rippling into the customer base. The point of attack could be a single component – a critical substation or transmission tower [10]. Or there could be a simultaneous, multipronged attack intended to bring down an entire regional grid. Similarly the attack could target electricity markets, highly vulnerable because of their transitional status [11].

Attacks by the power system: Here, the ultimate target is the population, using parts of the electricity infrastructure as a weapon. Terrorists could use power plant cooling towers, for example, to disperse chemical or biological agents.

Attacks through the power system: The target is the civil infrastructure in this case. Utility networks include multiple conduits for attack, including lines, pipes, underground cables, tunnels, and sewers. For example terrorists could couple an electromagnetic pulse through the grid to damage computer or telecommunications infrastructure.

Among three classifications first one is identified with digital security while the second and third ones are all the more near the region of physical security. Digital security issues on SCADA systems are presented from the data organizes as the systems are coordinated with each other. Be that as it may, some of issues are brought on by human physical access with the use of general digital assault technique on IT systems to SCADA or control framework systems [12].

Many threats in communication networks are also applied to SCADA systems since they are connected to each other directly or indirectly [13]. It is strongly believe that many SCADA systems are exclusive to other networks, but it has been proved many times that they are indirectly connected to the Internet through the facilities for on-line maintenance. Threats to SCADA systems are classified into many kinds according to as shown in Table 1.

(Table 1)

Table 1. Common RT Computer System Threats

1.Authorization Violation	9.Information leakage	17.Sabotage	25.Traffic Analysis
2.Bombs (Logic or Time)	10.Intercept/ Alter	18.Scavenging	26.Trap Door/ Back Door
3.Browsing	11.Interference Database Query Analysis	19.Spying	27.Trojan Horse

4.Bypassing Controls	12.Masquerade	20.Service Spoofing	28.Tunneling
5.Data Modifications	13.Physical Intrusion	21.Sniffers	29.Unauthorized Access Violations of Permission
6.Denial of Service	14.Replay	22.Substitution	30.Unauthorized Access Piggybacking
7.Eavesdropping	15.Repudiation	23.Terrorism	31.Virus
8.Illegitimate Use	16.Resource Exhaustion	24.Theft	32.Worm

The standards included in this study have a focus on countermeasures and recommendations on how to secure SCADA systems. The keywords and phrases associated with the 14 groups of threats occurred in total 876 times in the documents. The threats the standards focus on can be seen in Fig. 3, here normalized with the total number of occurrences in all standards.

More than 40 percent of the occurrences of threats mentioned belong to the group malicious code (described in TABLE 1). Denial of service attacks with the keywords "DOS", "DDOS", "Denial of Service", "Syn flood" and "Resource Exhaustion" is the second most mentioned attack with 14 percent of the hits. Threats against data communication are also given much attention, here represented by *Spoofing* (e.g. "man-in-the middle") and Replay, interception and modification of *data* (e.g. "message replay").

On fifth place, threats related to information gathering are found, for example "war dialing" and "traffic analysis". Threats from employees and Social engineering attacks are more related to the human element of cyber security. These are given modest attention with focus of 7.9 and 3.0 percent respectively.

NERC CIP 002-009 does not contain any of the keywords related to threats. In 78 percent of the occurrences are related to malicious code, while in this quotient is 50 percent. The same quotient in the System Protection Profile (published by NIST) is less than eight percent. Further, the system protection profile focus to 42 percent on *DOS* while the guide published by the same organization only focus 10 percent of the attention on this threat.

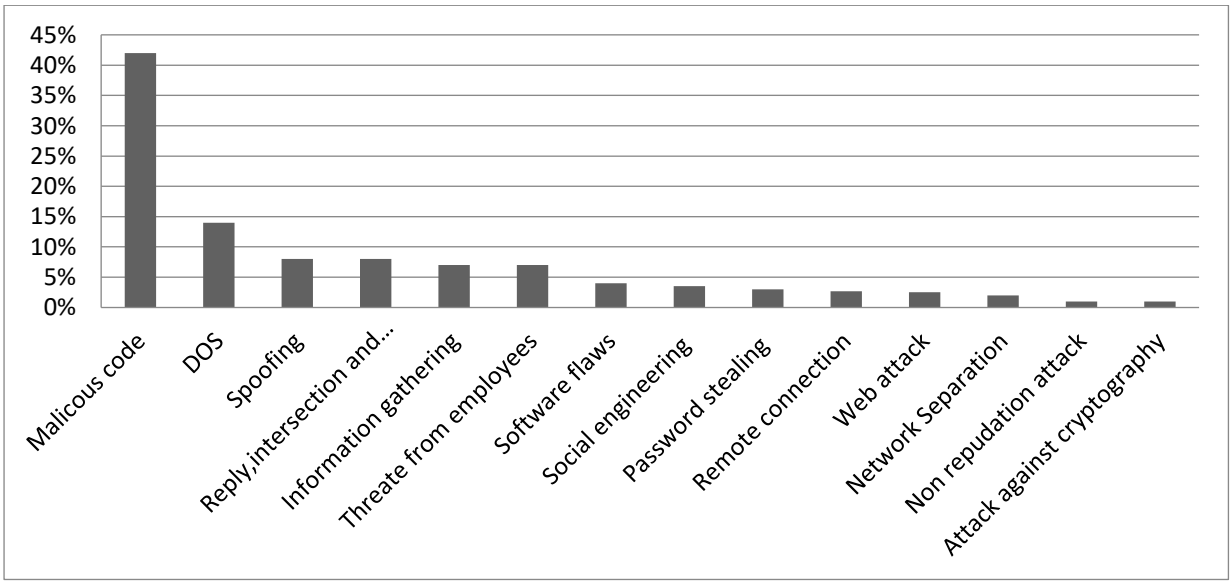

Fig 3: Focus of SCADA standards and guidelines on threat-groups, normalized.

An attack tree illustrated in Fig. 4 consists of disruptions through a power plant, substation, or web-based SCADA. The disruptions include sabotage on computer systems and power systems [14]. These combinations may result in an intrusion into the control center [15]. To derive the scenario combination, groups of attack leaves are arranged as follows:

.

Group 1a $\begin{bmatrix} G1 \\ G2xG3 \\ G4 \\ G5 \\ G6 \end{bmatrix}$ Group 1b $\begin{bmatrix} G7 \\ G8xG9 \\ G10 \\ G11 \\ G12 \\ G13 \end{bmatrix}$ Group 1c $[G14xG15]$ Group 1d $[G16]$

Group 1e $\begin{bmatrix} G17xG18 \\ G19 \end{bmatrix}$

Each gathering speaks to the security defect of a sub-arrange from power plant, substation systems, and online SCADA framework. Bunches 1a and 1b speak to an interruption of energy plant operations and substation robotization [16]. Security breaks in these gatherings may likewise bring about entrance to the control focus. Bunches 1c and 1d speak to an interruption of the reinforcement control focus and continuous administrations in the essential control focus. The significance of a reinforcement control focus is to assume control elements of the essential control focus under outrageous conditions. Correspondence, social database and ongoing application benefits in charge focuses are critical elements. Group 2 represents the disruption of Web Based SCADA system where security breaches in a web server may be exploited by intruders [17].

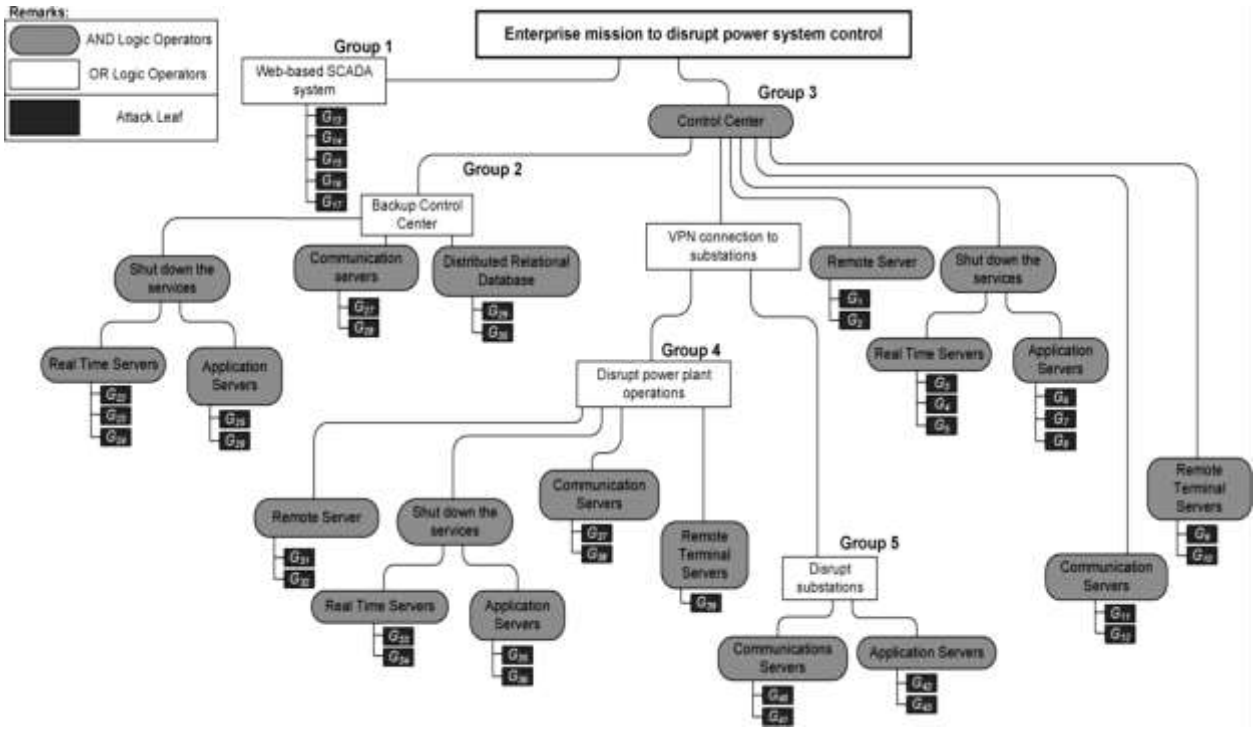

Fig 4: Attack Tree of the Power System Control Framework.

Countermeasures

The catchphrases and expressions related with the 26 gatherings of countermeasures happened altogether 8222 times in the eight SCADA measures. Fig. 1 demonstrates the quantity of events for each gathering standardized with the aggregate number of events in all gauges. As delineated in Fig. 5 countermeasures identified with validation represents 14.5 percent of the events taken after by countermeasures identified with cryptography with 13.6 percent of the events. On the flip side of the scale, measures identified with how to set the security association, how support can be picked up from framework administration instruments, how to make framework versatility to assaults and suggestions on solidifying of PCs and administrations are found.

The focus on these groups differs among standards. Let the focus on group *i* in standard *j* be *Fi, j* and let *Mi* be the arithmetic mean of all standards focus on group *i*. With *n* standards the absolute mean deviation for a group *i*, *Di*, can then be obtained as:

$$\boldsymbol{D_i = \sum_{j=1}^{n} \frac{||M_i - F_{i,j}||}{n}}$$

The mean of $\boldsymbol{D_i}$ over the 26 countermeasure-groups (mean absolute mean deviation) is 2.50 percent. This should be compared to the mean focus on groups in general, which is approximately 3.86 percent (1/26). Hence, the standards included in this comparison do to a large extent deviate when it comes to the number of times different types of countermeasures are mentioned in text.

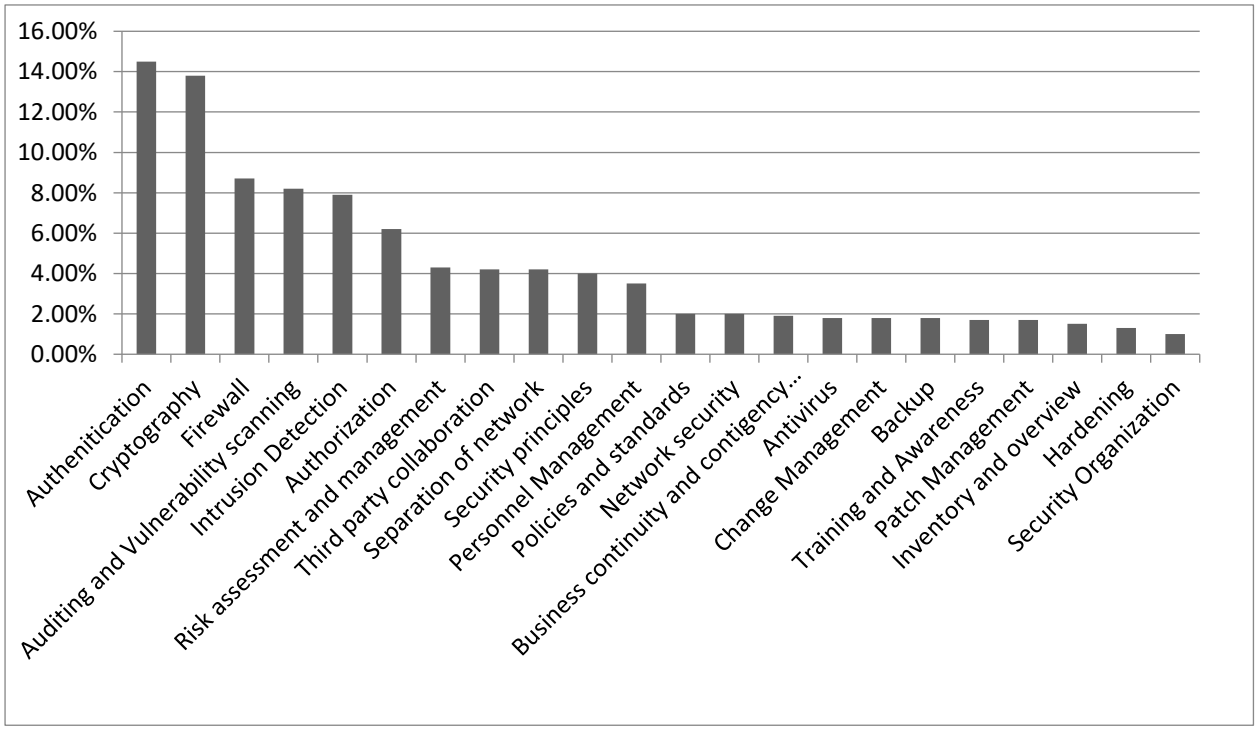

Fig 5: Focus of SCADA standards and guidelines on countermeasure-groups, normalized.

In TABLE 2 the arithmetic mean of the focus of the eight SCADA standards is shown together with the mean average deviation (MAD) of their focus. Also shown is the quotient between these, i.e. how much standards deviate in their focus compared to their mean focus on the countermeasure group.

Table 2. Focus Deviations in SCADA Standards

GROUP	MAD	MEAN	MAD / MEAN
Security Organization	0.011	0.009	1.294
System administration tools	0.006	0.006	1.090
Inventory and Overview	0.015	0.014	1.070
Business Management Commitment	0.017	0.018	0.925
System Resilience	0.008	0.009	0.900
Hardening	0.011	0.012	0.896
Network Security	0.016	0.018	0.891
Separation of Network	0.046	0.053	0.872
Incident planning/handling	0.016	0.020	0.827
Training and Awareness	0.015	0.019	0.789
Security Principles	0.040	0.052	0.765
Cryptography	0.069	0.095	0.723
Third party collaboration	0.036	0.054	0.678
Authentication	0.072	0.108	0.671
Policies and Standards	0.015	0.024	0.643
Antivirus	0.009	0.014	0.638
Firewall	0.040	0.070	0.582
Authorization	0.031	0.056	0.552

Additionally with respect to dangers there is a distinction in how much consideration they are given in the included measures. The mean total mean deviation with respect to dangers in the norms (mean of Di over the 14 risk gatherings), is 3.9. This could be contrasted with the mean concentration of gatherings, which are 6.1. NERC CIP 002-009 does not contain any of the catchphrases identified with dangers.

In 78 percent of the events are identified with noxious code, while in this remainder is 50 percent. A similar remainder in the System Protection Profile (distributed by NIST) is under eight percent. Encourage, the framework assurance profile [23] concentrate to 42 percent on DOS while the guide distributed by a similar association ("Guide to Industrial Control Systems (ICS) Security") just concentration 10 percent of the consideration on this risk [4, 18].

METHODS

Assessment Method

1. (Risk assessment in SCADA for railways, 2004). A risk assessment framework which utilizes the Hierarchical Holographic Modeling (HHM) and is designed for GPS-based railway SCADA systems is described in Chittester and Haimes (2004). HHM is the methodology for *"capturing and representing the essence of the inherent diverse characteristics and attributes of a system"* (Haimes, 1981). HMM was used for modeling complex defense and civilian systems. It aids in assessing risks in subsystems and their effect on the system as a whole, which makes HHM useful in the context of SCADA (Chittester and Haimes, 2004).

Three sub-models are distinguished in the hierarchical holographic model of a SCADA system (Chittester and Haimes, 2004): (1) hardware and software, (2) human supervisory [19] and (3) environment. Each of these sub-models is decomposed into elements and each element is decomposed into subtopics. The framework suggests mapping the Control Objectives for Information and Related Technology (CobiT) onto the holographic model in order to facilitate risk identification.

2. Vulnerability assessment methodology for SCADA security, 2005 (Permann and Rohde, 2005). A digital powerlessness appraisal philosophy for SCADA frameworks in Permann and Rohde (2005) depends on the experience of evaluating the security of various SCADA frameworks. [20]

Directed as a piece of the national SCADA Test Bed program supported by the Department of Energy – Office of Electricity and Energy Assurance, US and the Idaho National Laboratory SCADA Test Bed program. The philosophy depicted in Permann and Rohde (2005) comprises of five stages:

- Assessment plan development: a plan outlines budget, schedule, goals, resources and the engagement of experts required, and deliverables expected from an assessment.
- Testing environment configuration: the testing environment must be safe and non-production configuration.
- Vulnerability assessment: the vulnerability assessment is performed via a penetration test conducted from an external to the tested system machine. A range of open source and commercial tools for assessing system vulnerability is listed.
- Reporting: the methodology of assessment and testing along with the results must be thoroughly documented.
- Metrics and scoring: the security of SCADA system must be measured quantitatively so that it may be benchmarked against other systems [21].

3. Vulnerability assessment of cyber security in power industry, 2006 (Yu et al., 2006). The method requires six steps to be undertaken [22]:

- Development of the base-level and expanded vulnerability trees for an original system;
- Population of an effect analysis table and calculation of threat-impact index values;
- Augmentation of the tree with threat-impact index values;
- Calculation of cyber-vulnerability index values;
- Augmentation of the tree with cyber-vulnerability index values; and
- Reproduction of steps 2–5 for a security-enhanced system and the comparison of results.

4. Cyber-terrorism SCADA risk framework, 2009 (Beggs and Warren, 2009) [23]. The recommendation for the risk assessment stage is to adjust the AS/NZS 4360:2004, an Australian risk management standard, for the specifics of SCADA systems. For the development of the cyber-terrorism capability assessment model, the level of cyber-terrorist group capability is characterized using eight indicators: (1) advanced ICT skills, (2) advanced hacking tools and techniques, (3) access to new advanced ICTs, (4) advanced knowledge of SCADA systems, (5) insiders within the organization of a selected target, (6) reconnaissance, (7) funding, and (8) motivation.

5. Evaluating the risk of cyber-attacks on SCADA systems via petri net analysis, 2011 (Henry et al., 2009). A methodology for quantifying the risk of cyber-attacks on computer network operations on SCADA systems is introduced in Henry et al. (2009). The method is based on the Petri Net state cover ability analysis and process simulation. The purpose of the method is to identify all high-consequence attack states.

The method avoids the use of such measure as likelihood since it is *"difficult to credibly evaluate in many practical applications"*, but rather represents risk as *"a function of the resources to which an attacker can gain access during an attack"* (Henry et al., 2009).The method is demonstrated on a non-automated hazardous liquid loading process which is described in Balasubramanian et al. (2002).

Two risk metrics are proposed in Henry et al. (2009): (1) centre of mass risk measure, which is the median of the set of the consequence of all inducible SCADA and process failure modes; and (2) worst-case risk measure, which is a maximum value of the set. Six types of failure modes are adopted from Balasubramanian et al. (2002).

6. Adversary-driven state-based system security evaluation, 2010 (LeMay et al., 2010). In LeMay et al. (2010), the ADversary VIew Security Evaluation (ADVISE) method is proposed. It enriches an attack graph with the characteristics of an adversary. The purpose of the method is to simulate an attack on a system, identify the

most likely attack path and to calculate the probability of the success of an attack using an executable state-based security model of a system.

7. Attack countermeasure tree, 2010 (Roy et al., 2010). In Roy et al. (2010), the risk assessment method based on Attack Countermeasure Tree (ACT), which enriches a widely used in risk assessment concept of an attack tree with information about security countermeasures, is introduced. There are three types of events in an ACT: attack event, detection event and mitigation event. An ACT may be augmented with the cost of an attack and the amount of security investment. The cost of an attack is the cost of the consequences of events leading to an attack with the minimal cost and is restricted by the budget of an attacker.

8. Risk-assessment model for cyber-attacks, 2010 (Patel and Zaveri, 2010). Another risk-assessment model for cyber-attacks on Information Systems is introduced in Patel and Zaveri (2010) and its application is demonstrated on a test SCADA system of a chemical plant. The model may be used for risk assessment, cost–benefit analysis supporting the acquisition of IT components, and for the calculation of insurance premium by insurance companies.

9. Digraph model for risk identification and management in SCADA systems, 2011 (Guan et al., 2011). A digraph model of a SCADA system for a chemical distillation column of a laboratory scale is presented in Guan et al. (2011).The model provides a formal representation of the structure and behavior of a SCADA system and may be exploited for risk impact assessment and fault diagnosis. The vertexes of the graph are the components of a SCADA system and a directed edge exist between two vertexes if a security risk at an initial vertex may affect security of a terminal vertex.

The reach ability matrix of a graph and its partitioning may be used to separate the components that are more likely to be impacted from those that are less likely to be impacted if the component represented by the initial vertex of a digraph is found at risk. For fault diagnosis a digraph is used in a deductive manner in a way similar to fault trees.

10. A PMU-based risk assessment framework for power control systems, 2013 (Yan et al., 2013). In Yan et al. (2013), a Phasor Measurement Unit (PMU)-based risk assessment framework for SCADA systems of power grids is introduced. The application of the framework is demonstrated using a simulation on the IEEE 10 Generator 39 Bus System. The steps of the framework are as described below [24]. First, the configuration of a system is identified. Next, vulnerabilities within the system are identified and quantified using the Duality Element Relative Fuzzy Evaluation Method (DERFEM). Then, an attack graph is designed and used in order to find intrusion scenarios, the probabilities of which are also calculated [25].

11. Quantitative methodology to assess cyber security risk of SCADA systems, 2014 (Woo and Kim, 2014). A methodology for quantitative assessment of cyber security risk in SCADA systems based on the optimal power flow and power flow tracing is introduced in Woo and Kim (2014). The fifteen types of threats and the four components of a SCADA system (EMS server, a SCADA server, and RTU and communication network) are distinguished in Woo and Kim (2014). For the quantification of vulnerabilities, first, the relevance of each threat to each component is defined [26].

Then, a vulnerability index is assigned to each component of a system. The vulnerability index of a component is based on historical data, where available, and on the security characteristics of the component. For the quantification of threats, a normalized weighted index is assigned to each type of threat for each component of a SCADA system. It is based on the applicability of the treat to the component, the vulnerability index of the component and the damage capacity of the component. The asset value is calculated based on the outage cost..

CONCLUSION

This paper has exhibited a quantitative assessment of SCADA measures and the correlation with ISO/IEC 17799 [27]. It can be inferred that with this positioning strategy, more than each fourth countermeasure specified in the SCADA benchmarks concern cryptography or confirmation. Moreover, the dangers most regularly said are those

identifying with vindictive code or dissent of administration assaults, which together make up 50 percent of the aggregate events of watchwords related with dangers. There is likewise a solid concentrate on countermeasures in the SCADA measures, henceforth less concentrate on dangers. Likewise concentrate on various techniques for hazard evaluation.

In the paper, we laid out some methodologies that may be taken to security challenges. The steady tending to of the predefined examine difficulties will improve future research about digital security hazard evaluation techniques in the SCADA setting. We welcome all around situated analysts and experts to augment the rundown of the difficulties, and to proceed with the exchange.

Shared comprehension of the difficulties confronting the area will encourage its quick developing.

REFERENCES

1. V. Urias, B. V. Leeuwen, and B. Richardson, "Supervisory Command and Data Acquisition (SCADA) system Cyber Security Analysis using a Live, Virtual, and Constructive (LVC) Testbed," in Proc. IEEE MILCOM 2012, November. 2012, pp. 1 - 8, DOI: 10.1109/MILCOM.2012.6415818.
2. S. Ismail, E. Sitnikova, and J. Slay, "Using integrated system theory approach to assess security for SCADA systems cyber security for critical infrastructures: A pilot study," in Proc. Fuzzy Systems and Knowledge Discovery (FSKD), August. 2014, pp. 1000 - 1006, DOI: 10.1109/FSKD.2014.6980976.
3. H. H. Safa, D. M. Souran, M. Ghasempour, and A. Khazaee, "Cyber security of smart grid and SCADA systems, threats and risks," in Proc. IEEE CIRED Workshop, Jun. 2016, pp. 1 - 4, DOI: 10.1049/cp.2016.0692.
4. K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security." Computer Security Division, IT Laboratory, National Institute of Standards and Technology Special Publication 800-82 Revision 1, Gaithersburg, June. 2011. DOI: http://dx.doi.org/10.6028/NIST.SP.800-82r1.
5. C. Alberts, A. Dorofee, J. Stevens and C. Woody, "Introduction to the OCTAVE® Approach" Networked Systems Survivability Program, Carnegie Mellon Software Engineering Institute, Pittsburgh, PA, August. 2003.
6. J. Ø. Aagedal, F. D. Braber, T. Dimitrakos, B. A. Gran, D. Raptis, and K. Stølen, "Model-based Risk Assessment to Improve Enterprise Security," in Proc. Sixth International ENTERPRISE DISTRIBUTED OBJECT COMPUTING Conference (EDOC'02), September. 2002, pp. 51 - 62, DOI: 10.1109/EDOC.2002.1137696.
7. Roy E. Fraser, Process Measurement and Control: Introduction to Sensors, Communication, Adjustment, and Control, Prentice Hall, 2001.
8. V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks" in Computers & Security, VOL. 25, NO. 7, pp. 498-506, October. 2006. DOI: https://doi.org/10.1016/j.cose.2006.03.001.
9. T. Brown, "Security in SCADA systems: How to handle the growing menace to process automation," in Computing & Control Engineering Journal, VOL. 16, NO. 3, pp. 42-47, August. 2005. DOI: 10.1049/cce:20050306.
10. A. H. Smith "Security for Critical Infrastructure SCADA Systems" White Paper, SANS Institute InfoSec Reading Room, February. 2005.
11. G. K. Chalamasetty, P. Mandal, and T. L. Tseng, "Secure SCADA communication network for detecting and preventing cyber-attacks on power systems," in Proc. Power Systems Conference (PSC), 2016 Clemson University, March. 2016, pp. 1 - 7, DOI: 10.1109/PSC.2016.7462865.
12. V. L. Do, L. Fillatre, I. Nikiforov, and P. Willett, "Feature article: security of SCADA systems against cyber–physical attacks," in IEEE Aerospace and Electronic Systems Magazine, VOL. 32, NO. 5, pp. 28-45, May. 2017. DOI: 10.1109/MAES.2017.160047.
13. R. Czechowski, P. Wicher, and B. Wiecha, "Cyber security in communication of SCADA systems using IEC 61850," in Proc. Modern Electric Power Systems (MEPS), July. 2015, pp. 1 - 7, DOI: 10.1109/MEPS.2015.7477223.

14. Y. Zhang, L. Wang, Y. Xiang, and C. W. Ten, "Power System Reliability Evaluation With SCADA Cybersecurity Considerations," in IEEE Transactions on Smart Grid, VOL. 6, NO. 4, pp. 1707 - 1721, July. 2015. DOI: 10.1109/TSG.2015.2396994.
15. J. Zhang, S. Gan, X. Liu, and P. Zhu, "Intrusion detection in SCADA systems by traffic periodicity and telemetry analysis," in Proc. IEEE Symposium on Computers and Communication (ISCC), June. 2016, pp. 318 - 325, DOI: 10.1109/ISCC.2016.7543760.
16. N. Hossain, M. A. Hossain, A. K. M. F. Islam P. Banarjee, and T. Yasmin, "Research on Energy Efficiency in Cloud Computing." International Journal of Scientific & Engineering Research, Volume 7, Issue 8, pp. 358-367, August. 2016.
17. M. Regula, A. Otcenasova, M. Roch, R. Bodnar, and M. Repak, "SCADA system with power quality monitoring in Smart Grid model," in Proc. IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), June. 2016, pp. 1 - 5, DOI: 10.1109/EEEIC.2016.7555577.
18. E. Byres, and J. Lowe, "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems" White Paper, VDE 2004 Congress, VDE, Berlin, October. 2004.
19. "Supervisory Control and Data Acquisition (SCADA) Systems" TECHNICAL INFORMATION BULLETIN 04-1, NATIONAL COMMUNICATIONS SYSTEM, Arlington, VA, October. 2004.
20. C. C. Liu, C. W. Ten, and G. Manimaran, "Cybersecurity of SCADA Systems: Vulnerability assessment and mitigation," in Proc. Power Systems Conference and Exposition (PSCE '09), March. 2009, pp. 1 - 3, DOI: 10.1109/PSCE.2009.4840120.
21. M. Stoddard, D. Bodeau, R. Carlson, C. Glantz, Y. Haimes, C. Lian, J. Santos, and J. Shaw, "Process Control System Security Metrics – State of Practice" Research Report No. 1, The Institute for Information Infrastructure Protection (I3P), August. 2005.
22. Y. Zhang, L. Wang, Y. Xiang, and C. W. Ten, "Inclusion of SCADA Cyber Vulnerability in Power System Reliability Assessment Considering Optimal Resources Allocation," in IEEE Transactions on Power Systems, VOL. 31, NO. 6, pp. 4379 - 4394, January. 2016. DOI: 10.1109/TPWRS.2015.2510626.
23. C. Beggs, and M. Warren, "Safeguarding Australia from cyber-terrorism: a proposed cyber-terrorism SCADA risk framework for Australia" in Journal of information warfare, VOL. 7, NO. 1, pp. 24-35, 2008.
24. H. Saadabadi, and M. Dehghani, "Large-scale power systems state estimation using PMU and SCADA data," in Proc. 24th Iranian Conference on Electrical Engineering (ICEE), May. 2016, pp. 906 - 911, DOI: 10.1109/IranianCEE.2016.7585649.
25. S. Pal, B. Sikdar, and J. Chow, "Detecting data integrity attacks on SCADA systems using limited PMUs," in Proc. Smart Grid Communications (SmartGridComm), November. 2016, pp. 545 - 550, DOI: 10.1109/SmartGridComm.2016.7778818.
26. J. Formea, and J. Gadbury, "Improve Power Reliability through Small-Scale SCADA Systems," in Proc. IEEE Rural Electric Power Conference (REPC), May. 2016, pp. 21 - 26, DOI: 10.1109/REPC.2016.12.
27. T. Phinney, "ISA/IEC 62443: Industrial Network and System Security" Integrated Security Technology Lab, International Society for Automation/International Electrotechnical Commission, Gaithersburg.