IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

A Survey on Security Challenges and Research Opportunities in Smart Grid based SCADA Systems

A. W. Mir[1*], K. R. Ram Kumar[2]

[1, 2]Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India

[*]*Corresponding Author: wahids@live.com, Tel.: +91 9958197525*

DOI: https://doi.org/10.26438/ijcse/v7i3.689706 | Available online at: www.ijcseonline.org

Accepted: 14/Mar/2019, Published: 31/Mar/2019

***Abstract*—** Supervisory Control and Data Acquisition (SCADA) systems have emerged as critical systems of national importance in the recent times due to their deployments at critical infrastructures. Since SCADA systems are of critical importance and being high value targets, these systems attract large interest for being target for security fissures. SCADA systems security exemplifies a critical challenge in present world. High profile cyber security threats are the recent phenomenon, yet the systems running critical industrial processes are typically a generation older. There are many legacy systems that may be vulnerable to cyber-attack because cyber security was simply not a consideration at the time of initial design and implementation stages. The security of even recently deployed systems may also pose a challenge. This paper explores and discusses the security challenges, publication trends in terms of graphical representation, and research opportunities in the SCADA system.

***Keywords*—** SCADA, Smart Grid, Publication Trends, Security Challenges, Threats

I. INTRODUCTION

The smart grid refers to the electricity grid consisting of power generation stations, transmission lines, substations, transformers and other related infrastructure to supply power to domestic and commercial customers. The two-way technology which helps the utilities to manage and control the entire operations makes the smart grid possible in reality. The smart grid consists of typical technological infrastructure like servers, storage, networking devices, computers, automation, and specialized applications which work together with the electrical grid to manage, monitor and control electric demands of the business.

The smart grid provides an opportunity to migrate the energy industry into a new age of efficiency, reliability and availability centric sector [1]. It can highly contribute to the environmental and economic issues world is facing today. There are many benefits that the smart grid will result in such as efficient transmission of electricity, faster restoration of electricity after power failures, less operations and management costs, competitive consumer rates, reduced peak demand, increased integration of large-scale renewable energy systems such as solar and wind, integration of customer owned power generation, and improved security [2].

Supervisory Control and Data Acquisition (SCADA) systems were developed to support in the management, controlling and monitoring of critical infrastructural operations of electricity, water, gas, waste, traffic, etc. These types of systems had limited connectivity to the internet in the past. This was due to the complexity of their architectural design of proprietary control protocols and vendor monopoly as they used to supply specific hardware and software. Usually the deployment was on dedicated or segregated networks only which resulted in SCADA systems to be somehow secure, avoiding threats and vulnerabilities associated with the Internet [12]. The present requirements need the remote connectedness for various reasons such as support, data collection and data analysis of multiple locations resulted in SCADA systems necessarily to be getting connected to corporate networks and the internet. At present, SCADA systems are not immune to threats and vulnerabilities of the cyber-attacks. There are number of incidents which have been reported that targeted SCADA systems [8].

SCADA networks comprises of computers and applications that execute crucial operations in providing vital services and supplies i.e. electricity, gas, gasoline, water, waste treatment, transportation, etc. It is the part of very critical infrastructure which requires security from various threats and vulnerabilities that persist in this domain [20].

SCADA systems security is very critical as it is core component of the smart grid. The fact that technology is

fast changing the world cannot be denied. It includes the threats to the SCADA system which is integral part of functioning of smart grid and the utility business [6]. The security domain related to SCADA is very complex and security controls needs to be put in place adequately as the consequences of overlooking the threats or applying the insufficient controls may have consequences involving loss of life, reputation as well as financial losses.

In the past, SCADA systems were installed as isolated networks. With this isolation architecture, SCADA Host platforms were not necessarily designed to be part of corporate or public networks. The result of such an isolated architecture left many SCADA host platforms prone to attacks as they were not designed to protect themselves in smart grid deployments [7]. Security in SCADA systems is of paramount importance and there should be holistic approach to it.

The Section I of the paper provides the introduction of SCADA systems with respect to security perspective, Section II comprises of the overview of the SCADA architecture, Section III covers the security threats in SCADA systems, Section IV summarises the related work of the security in SCADA systems, Section V depicts the publication trends of security SCADA system publications, Section VI elaborates the research opportunities in smart grid based SCADA systems and architecture and Section VIII concludes research work with future directions.

II. SCADA ARCHITECTURE

SCADA is a system of software and hardware components which allows the following functions for any industrial organization [3] [41]:

- Monitoring, gathering and processing of real-time data generated from the field devices.
- Controlling the industrial processes locally or from remote locations.
- Direct communication with field devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) software.
- Recording of all the events related to the field devices into a log database.

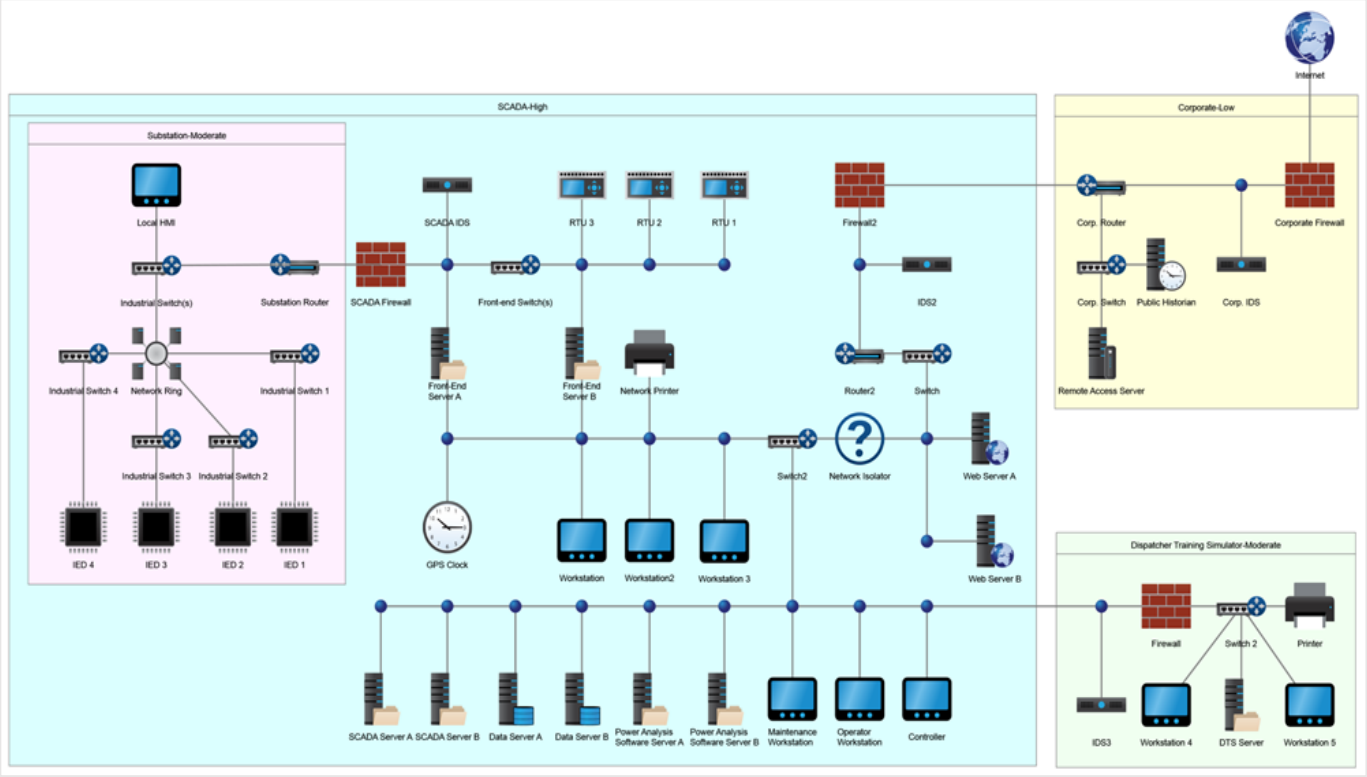

Figure 1: Typical SCADA Deployment Architecture

The typical SCADA network is depicted in the figure 1 consisting of main four zone as [58]:

1. **SCADA HIGH**
   SCADA network main zone with high security rating as this zone is rated high from any security risk eventualities.
2. **SUBSTATION MODERATE**
   Substation zone with moderate security ratings as this zone is rated moderate from any security risk eventualities.

3. **DISATCHER / TRAINING / SIMULATOR MODERATE**
   Dispatcher training simulator zone with moderate security rating as this zone is rated moderate from any security risk eventualities.
4. **CORPORATE LOW**
   Corporate zone with low security rating as this zone is rated low from any security risk eventualities.

The following table 1 lists the various components in the typical SCADA network deployment architecture with respect to components, security assurance level, criticality, asset type, zone, subnets and description:

Table 1: Components in SCADA Architecture

Component Name / Tag	Security Assurance Level	Criticality	Asset Type	Zone	Subnets	Description
Internet	Low	Low	Web	-	External Network	Part of corporate network used to connect to internet for various services e.g. patches, updates, support, etc.
Corporate Firewall	Low	Moderate	Firewall	Corporate	External Network	Part of corporate network to protect from threats from internet.
Corp. IDS	Low	Moderate	IDS	Corporate	External Network	Part of corporate network and used as Intrusion Detection System.
Corp. Router	Low	Moderate	Router	Corporate	External Network	Part of corporate network and used to connect to SCADA network zone.
Corp. Switch	Low	Moderate	Switch	Corporate	External Network	Part of corporate network and used to connect various services within the corporate network e.g. remote access server, public historian, etc.
Remote Access Server	Low	Moderate	RAS	Corporate	External Network	Part of corporate network and used to provide remote access to vendors of SCADA systems typically for support calls.
Public Historian	Low	Moderate	Historian	Corporate	External Network	Part of corporate network and used for historian of data to be accessed typically over internet or within the corporate network.
Switch 2	Moderate	Moderate	Switch	Dispatcher Training Simulator	SCADA Network	Part of Dispatcher Training Simulator network and used to connect various components within the network e.g. dispatcher training simulator server, workstations and printer.
Firewall	Moderate	Moderate	Firewall	Dispatcher Training Simulator	SCADA Network	Part of Dispatcher Training Simulator network to protect from threats arising within this zone as well as from incoming traffic from SCADA zone.
Workstation 4	Moderate	Moderate	HMI	Dispatcher Training Simulator	SCADA Network	Part of Dispatcher Training Simulator network to facilitate human machine interaction and operations.
Workstation 5	Moderate	Moderate	HMI	Dispatcher Training Simulator	SCADA Network	Part of Dispatcher Training Simulator network to facilitate human machine interaction and operations.
Printer	Moderate	Low	Network Printer	Dispatcher Training Simulator	SCADA Network	Part of Dispatcher Training Simulator network to facilitate printing for workstation users.
DTS Server	Moderate	Moderate	Application Server	Dispatcher Training Simulator	SCADA Network	Part of Dispatcher Training Simulator network to host the application server and services for the users in the zone for various operations meant for the zone.
IDS3	Moderate	Moderate	IDS	Dispatcher Training Simulator	SCADA Network	Part of Dispatcher Training Simulator network and used as Intrusion Detection System within the zone.
Firewall2	High	High	Firewall	SCADA	External Network	Part of SCADA network zone to protect from threats arising within this zone as well as from incoming traffic from Corporate zone.
SCADA Firewall	High	High	Firewall	SCADA	SCADA Network	Part of SCADA network zone to protect from threats arising within this zone as well as from

						incoming traffic from Substation zone.
SCADA Server A	High	Moderate	Application Server	SCADA	SCADA Network	Part of SCADA network zone with role of application server for SCADA system.
SCADA Server B	High	Low	Application Server	SCADA	SCADA Network	Part of SCADA network zone with role of application server for SCADA system typically acting as load balancer or fail over server.
Data Server A	High	Low	DB Server	SCADA	SCADA Network	Part of SCADA network zone with role of database server for SCADA system.
Operator Workstation	High	Moderate	HMI	SCADA	SCADA Network	Part of SCADA network zone to facilitate human machine interaction and operations for workstation operators.
Front-end Switch(s)	High	Low	Switch	SCADA	SCADA Network	Part of SCADA network zone and typically used to connect field devices like RTU's, PLC's, etc.
SCADA IDS	High	High	IDS	SCADA	SCADA Network	Part of SCADA network zone and used as Intrusion Detection System within the zone.
Router2	High	High	Router	SCADA	External Network	Part of SCADA network zone used to connect to corporate network zone.
IDS2	High	Moderate	IDS	SCADA	External Network	Part of SCADA network zone used as Intrusion Detection System within the SCADA zone to corporate zone.
Data Server B	High	Low	DB Server	SCADA	SCADA Network	Part of SCADA network zone with role of database server for SCADA system typically acting as load balancer or fail over server.
Power Analysis Software Server A	High	Moderate	Application Server	SCADA	SCADA Network	Part of SCADA network zone with role of power analysis server for SCADA system.
Power Analysis Software Server B	High	Moderate	Application Server	SCADA	SCADA Network	Part of SCADA network zone with role of power analysis server for SCADA system typically acting as load balancer or fail over server.
Front-End Server A	High	Moderate	Application Server	SCADA	SCADA Network	Part of SCADA network zone to act as data accumulator application server from RTU's.
Switch2	High	Moderate	Switch	SCADA	SCADA Network	Part of SCADA network zone and acts as entry point for network isolation for components of corporate network zone within the SCADA network zone.
RTU 1	High	Moderate	RTU	SCADA	SCADA Network	Part of SCADA network zone to connect to remote terminal unit RTU 1.
RTU 2	High	Moderate	RTU	SCADA	SCADA Network	Part of SCADA network zone to connect to remote terminal unit RTU 2.
RTU 3	High	Moderate	RTU	SCADA	SCADA Network	Part of SCADA network zone to connect to remote terminal unit RTU 3.
Maintenance Workstation	High	Moderate	HMI	SCADA	SCADA Network	Part of SCADA network zone to facilitate maintenance of the SCADA system typically for application configuration changes.
Controller	High	Moderate	HMI	SCADA	SCADA Network	Part of SCADA network zone to facilitate any control operations on the field devices like open or close of circuits, etc.
Front-End Server B	High	Moderate	Application Server	SCADA	SCADA Network	Part of SCADA network zone to act as data accumulator application server from RTU's, typically acting as load balancer or fail over server.
GPS Clock	High	Moderate	Clock	SCADA	SCADA Network	Part of SCADA network zone to facilitate synchronization of date and time with the SCADA network components.
Workstation	High	Moderate	HMI	SCADA	SCADA Network	Part of SCADA network zone to facilitate access to data accumulator application server and operations with field devices connecting to RTU's.
Workstation 2	High	Moderate	HMI	SCADA	SCADA Network	Part of SCADA network zone to facilitate access to data accumulator application server and operations

						with field devices connecting to RTU's.
Workstation 3	High	Moderate	HMI	SCADA	SCADA Network	Part of SCADA network zone to facilitate access to data accumulator application server and operations with field devices connecting to RTU's.
Network Printer	High	Moderate	Network Printer	SCADA	SCADA Network	Part of SCADA network zone to facilitate printing for workstation users.
Switch	High	Moderate	Switch	SCADA	External Network	Part of SCADA network zone used to connect to corporate network zone.
Web Server A	High	Moderate	Web Server	SCADA	External Network	Part of SCADA network zone which is isolated to facilitate services for corporate network zone.
Web Server B	High	Moderate	Web Server	SCADA	External Network	Part of SCADA network zone which is isolated to facilitate services for corporate network zone, typically acting as load balancer or fail over server.
Network Isolator	High	Moderate	Unknown	SCADA	External Network, SCADA Network	Part of SCADA network zone to be used to isolate components required for various services access to corporate network zone.
Substation Router	Moderate	Moderate	Router	Substation	SCADA Network	Part of Substation network zone and used to connect to SCADA network zone.
Industrial Switch(s)	Moderate	Moderate	Switch	Substation	SCADA Network	Part of Substation network zone which are used to connect to field devices.
Local HMI	Moderate	Moderate	HMI	Substation	SCADA Network	Part of Substation network zone that will facilitate human machine interface for field devices.
Network Ring	Moderate	Moderate	Optical Ring	Substation	SCADA Network	Part of Substation network zone, all the field devices are connected to specific switch in the network and all the switches are connected to network ring for proper data packets management.
Industrial Switch 1	Moderate	Moderate	Switch	Substation	SCADA Network	Part of Substation network zone which are used to connect to field devices.
Industrial Switch 2	Moderate	Moderate	Switch	Substation	SCADA Network	Part of Substation network zone which are used to connect to field devices.
Industrial Switch 3	Moderate	Moderate	Switch	Substation	SCADA Network	Part of Substation network zone which are used to connect to field devices.
Industrial Switch 4	Moderate	Moderate	Switch	Substation	SCADA Network	Part of Substation network zone which are used to connect to field devices.
IED 1	Moderate	Moderate	IED	Substation	SCADA Network	Part of Substation network zone which are connected to intelligent electronic device (IED) that receives data from sensors and power equipment.
IED 2	Moderate	Moderate	IED	Substation	SCADA Network	Part of Substation network zone which are connected to intelligent electronic device (IED) that receives data from sensors and power equipment.
IED 3	Moderate	Moderate	IED	Substation	SCADA Network	Part of Substation network zone which are connected to intelligent electronic device (IED) that receives data from sensors and power equipment.
IED 4	Moderate	Moderate	IED	Substation	SCADA Network	Part of Substation network zone which are connected to intelligent electronic device (IED) that receives data from sensors and power equipment.

III. SECURITY THREATS IN SCADA SYSTEMS

SCADA systems security exemplifies a critical challenge in present world. National level critical cyber security threats are recent phenomenon like Night Dragon or Stuxnet attacks. A research conducted by the Idaho National Laboratory [36] on the security of SCADA systems revealed common SCADA vulnerabilities that are faced by all SCADA systems even though functions, designs, and configurations vary among vendors, versions, and installations. Inspite of high level of threats, the systems running critical industrial processes are typically a generation older [34], [35]. Subsequently, there are many legacy systems that may be vulnerable to cyber-attack because cyber security was simply not a consideration at the time of initial design and installation. The security of even recently deployed systems may also be an issue, and often there are media reports of instances where systems are connected to the internet with inadequate protection, or the manufacturers of the

equipment have used hardcoded usernames and passwords, thereby gifting cyber intruders with inside knowledge with the ability to manipulate the system settings [36], [37]. SCADA systems are already being exposed to the continuum of threats and the systems further connected to Internet adds additional threats at an alarming rate. The adequate security should be put in place where SCADA systems are connected to the corporate IT networks. In United States only, 3920 SCADA devices were found connected to the Internet [31]. Infection can be either unintentional like Slammer, or target specific like Stuxnet, thus proving the need for added security protections on SCADA networks. Currently many SCADA networks are exempted from security protection because the impact 1-1 to operations is largely unknown. Unfortunately, mitigating attacks is not as simple as deploying IT security countermeasures. IT networks are primarily concerned with confidentiality and integrity of data, whereas SCADA networks are concerned with availability, reliability, and safety [32]. Indeed, traditional network security tools like firewalls, proxies, and Intrusion Detection Systems (IDSs) may not be compatible with SCADA; however, simply isolating SCADA systems is no longer an option.

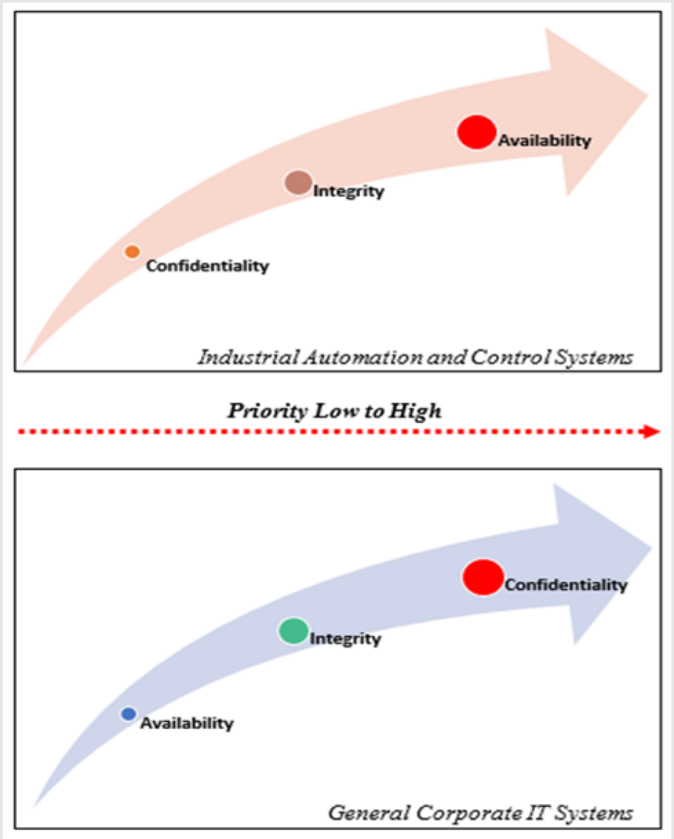

Figure 1: ICS vs IT (CIA) Triad

ICS Confidentiality, Integrity and Availability (CIA) Triad

Smart grid and corporate systems are alike in terms of IT infrastructure from the security perspective. Subsequently the risk management priorities and strategies are significantly different and domain specific [39]. In terms of SCADA systems, the service availability is more prioritized.

The figure 2 shows the transformation between ICT security vs ICS SCADA security.

In case of conventional corporate IT systems, the order of triad is:

- Confidentiality
- Integrity
- Availability

In case of ICS SCADA systems, the order of triad is:

- Availability
- Integrity
- Confidentiality

The general IT system security is prioritized and based on three fundamental dimensions of Confidentiality, Integrity and Availability. They are generally known as the CIA triad. The industrial automation and control systems security is prioritized as Availability, Integrity and Confidentiality. The dimensions are used to define characterization of security requirements, information classification and risk management priorities.

ICS Risk in SCADA systems

The following are the risks associated with Industrial Control Systems (ICS) – SCADA systems [21], [24]:

ICS vulnerabilities domains in SCADA systems

The SCADA vulnerabilities can be categorized into five major domains as shown in the Table 2 below:

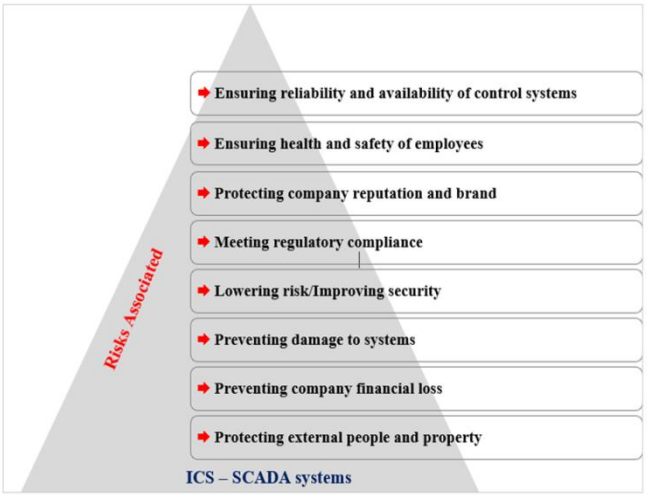

Figure 2: Risks associated with Industrial Control Systems (ICS) & SCADA systems

Table 2 : ICS Vulnerabilities Domains

SNo	Domain	Brief Description
1	Physical Vulnerabilities	Physical vulnerabilities define the characteristics and conditions of an asset that make it vulnerable to the damaging effects of a risk. For example, the open physical access to the critical SCADA data center poses a very high risk if it is not addressed.
2	Technical Vulnerabilities	Technical vulnerabilities can be defined as situation in which service denial, information comprise, or alteration risks occur due to any technical deficiencies in hardware, software, information handling, firmware bugs, design deficiencies, etc.
3	Operational Vulnerabilities	Operational vulnerabilities can be defined as a state in which critical information about the processes and actions are obtained by the attackers in order to harm or attack the critical infrastructures.
4	Procedural Vulnerabilities	Procedural vulnerabilities can be defined as a state in which the organization has inadequate procedures, policies and culture that administer control system security.
5	Personnel Vulnerabilities	Personnel vulnerabilities can be defined as a state in which the employees or contractors are the direct weak link in the system. This could be because of lack of skills, competency or any other valid reasons.

IV. RELATED WORK

The SCADA systems are used for very critical infrastructures across the different verticals in the world. The significance of SCADA systems in smart grids was recognized only after the four critical blackouts of 2003 [33]. SCADA systems being the crucial systems to monitor and control the field devices and components are prone to many types of cyber-attacks which result in loss of production, equipment and human fatalities in worst case scenarios. SCADA systems security must be given a highest priority and focus of the management [34]. The following *Table 3* lists the literature review of relevant papers highlighting major areas & security challenges in the SCADA systems. The research findings and gaps are also presented.

Table 3 : Year of Publication, Major Areas, Security Challenges & Research Findings or Gaps

Ref. No.	Year of Publication	Major Areas & Security Challenges	Research Findings and Gaps
[47]	2018	➡ ICS/SCADA systems security ➡ Architecture of ICS/SCADA ➡ ICS/SCADA vulnerabilities ➡ Attacking methods in ICS/SCADA ➡ Threats categories in ICS/SCADA ➡ Challenges to protect ICS/SCADA ➡ ICS/SCADA security objectives ➡ Security countermeasures ➡ Electronic and physical security perimeters ➡ Network communication security ➡ Product, software, and hardening ➡ Portable hardware/devices security ➡ ICS/SCADA security policies ➡ Governance and compliance ➡ Governance of the ICS/SCADA environment ➡ Regulatory compliance & standard requirements ➡ ICS/SCADA systems security in smart grid	The authors have discussed ICS/SCADA systems architecture and related security aspects. The various ICS/SCADA vulnerabilities are explained. The several attacking methods and threats types with respect to ICS/SCADA are discussed. The security requirements and challenges to protect ICS/SCADA are discussed. The ICS/SCADA governance, compliance and security policies with respect to needs and requirements are discussed. The importance of implementing the precise and proper security countermeasures for ICS/SCADA systems have been discussed. The several steps that will support to design, implement, and maintain security program with respect to ICS/SCADA systems have also been put forward. There are various research opportunities which can be explored such as the security of ICS/ SCADA systems with respect to availability, integrity and confidentiality objectives.

Ref. No.	Year of Publication	Major Areas & Security Challenges	Research Findings and Gaps
[48]	2018	➡ Power grid cyber security ➡ Vulnerabilities in cyber infrastructures ➡ Vulnerability assessment in a smart grid ➡ Smart grid standard and regulations ➡ Anomaly and intrusion detection systems ➡ Smart City Testbed (SCT) ➡ Cyber physical system security	The authors have provided a state-of-the-art survey of pertinent cyber security studies in power systems domain. The various reviews of the research have been demonstrated with respect to cyber security risks and various solutions to augment the security of a power grid have been presented. A survey on smart grid technologies have also been presented. The various power industry practices and standards have been discussed. The CPS testbed review from the cyber security perspective has been discussed. The various challenges and unsolved cyber security problems are also discussed. There are various research opportunities which can be explored as the current security defense and mitigation mechanisms do not essentially apply to the smart grid environment. The availability requirements of a power grid pose a big challenge and needs further research.
[43]	2017	➡ ICS/SCADA security ➡ Zero Day vulnerabilities ➡ Non-prioritization of Tasks ➡ Database Injection ➡ Communication protocol issues	The authors have reviewed the various facets of cyber-security issues in industrial control systems. The various security concerns in industrial control systems are discussed. Issues of security assessment and architectural reviewing of ICS is presented. Survey on different threat attacks on ICS is presented. There is the need of holistic approach to secure the ICS which are very critical for both private and government entities.
[44]	2017	➡ Threats classification i.e. Insiders, hackers, criminal groups, & nation states ➡ Architectural vulnerabilities ➡ Security policy vulnerabilities ➡ Software and hardware vulnerabilities ➡ Communication protocol vulnerabilities ➡ Physical attacks on technical processes ➡ Cyber-attacks on a communication network ➡ DoS attacks ➡ Simple integrity attacks ➡ Stealthy integrity attacks ➡ Attack detection and isolation methods	The authors have discussed the SCADA and its architecture in terms of layers. The security threats to modern SCADA systems has been discussed with broad classification into four main categories which include insiders, hackers, criminal groups and nation states. The investigation of SCADA vulnerabilities have been discussed. The classification by attack points and types have been discussed. The attack detection and isolation methods have been discussed.
[45]	2017	➡ SCADA hybrid testbed implementation for set of attacks for demonstration and evaluation	The authors have discussed the implementation of a set of attacks targeting a SCADA hybrid testbed. The setup used for testbed implementation has been demonstrated in a real SCADA architecture so that real operational scenarios can be attacked and tested. The various attacks have been simulated as in practical perspective manner. There are research opportunities in enhancing the process of reinventing and sustaining the fake views used by the attacker in the communication hijacking specifically targeting energy grids.
[46]	2017	➡ Common vulnerabilities and exposures ➡ Attacks on PLC's ➡ Attacks on fieldbus-level ➡ Attacks on wireless systems ➡ Physical-layer attacks	The authors have examined and discussed the known attacks on industrial systems. The investigation of the exploits that are available on public sources are examined. The various types of attacks and their points of entry are reviewed. Trends in exploitation as well as targeted attack campaigns against industrial enterprises are introduced. There are research opportunities which could be further explored such as physical segregation of industrial networks. Interconnectivity in industrial applications is another area which needs much research attention as it will lead the higher risk from the attackers. The various types of identification tools which could identify systems with vulnerabilities could be developed to help implementors to secure the industrial

Ref. No.	Year of Publication	Major Areas & Security Challenges	Research Findings and Gaps
			systems.
[50]	2017	➡ Security countermeasures for SCADA systems ➡ Password policy and restrictive network configuration ➡ Network segmentation ➡ Hardware upgrades ➡ Software patching	The authors have discussed the various countermeasures to attacks with respect to SCADA systems. The research outcomes illustrate that granular network segmentation is predominantly effective countermeasure. The implementation of a restrictive network configuration and password policy in conjunction with whitelisting of devices enhances the overall security. The network performance degradations are also matter of concern in SCADA systems which poses the big challenge with respect to active security countermeasures as well as could be leading to higher risk rating. There are various research opportunities which can be explored such as the issue of recurrent patching of systems which remains a security challenge. The need of the hour is that SCADA systems should be further explored with aim to inherently making both components of hardware and software secure.
[53]	2017	➡ Cryptographic applications for programmable logic controllers (PLC's) ➡ PLC architecture ➡ Secure application architecture ➡ Cryptographic algorithms ➡ Security properties in control applications	The author has examined and evaluated the feasibility of performing cryptographic computations at the application layer of a programmable logic controller (PLC's). The experiments on AES, SHA1 and HMAC-SHA1 have been performed to evaluate their performance against the new Speck and Simon lightweight block cipher algorithms. There are various research opportunities which can be explored as various researches have confirmed that most of control hardware equipment manufacturers don't incorporate security features. In this case, the areas like security protocols can further be researched. The key exchange and key distribution protocols integration can further be explored. The data security shall be explored in end-to-end communications flows at the application layer.
[55]	2017	➡ Semantic network-based attacks ➡ Stealthy deception attacks ➡ Dolev-Yao threat model ➡ Man-in-the-middle (MITM) attack ➡ Zero values deception attack ➡ A multi-stage attack ➡ A half-duplex attack ➡ The ICS attack markup language ➡ Attacks against ICS ➡ Anomaly detection in ICS ➡ Counter measures	The authors have presented a class of semantic network-based attacks with respect to SCADA systems. The anomaly detection like session hijacking that are usually undetectable is discussed. The test simulation for HMI and PLC's are simulated in a real test lab with various attack scenarios. A real-time security assessment tool has been proposed which could help to do real time assessment for any potential vulnerabilities. The various attacks with respect to industrial control systems are surveyed and reviewed. There are various research opportunities which can be explored as present intrusion detection and anomaly detection systems are essentially unable to detect the stealthy deception attacks. The cryptographic means to secure the communication channels can further explored and studied.
[56]	2017	➡ SCADA system characteristics and vulnerabilities ➡ Simulation and modelling in SCADA systems ➡ SCADA systems testbeds ➡ SCADA systems tools and techniques for vulnerabilities assessment	The authors have presented the surveys tools and techniques to discover various system vulnerabilities with respect to SCADA systems. The various approaches have been discussed with an inclusive review along with their applicability. The vulnerabilities scenarios like generic OS, legacy systems with long operational life, multiple points of entry and failure, communication protocols, real-time and complex interactions, conflicting priorities, social engineering and insider attacks and backdoors has been discussed and the defense strategies have also been proposed. The various SCADA security testbed simulations were also discussed. There are various research opportunities which can be explored in the areas like SCADA communication protocol level security, Cloud Computing model for SCADA systems

Ref. No.	Year of Publication	Major Areas & Security Challenges	Research Findings and Gaps
			and software defined networks (SDN's) for SCADA systems. The OpenSCADA project can be further explored for SCADA systems. The machine learning techniques with respect to SCADA systems can be further studied.
[10]	2017	➡ SCADA security measures ➡ SCADA generic security posture ➡ Network segmentation ➡ Password policies enforcement ➡ System patching	The authors have discussed various effective security measures can be taken in the SCADA deployments. The granular network segmentation is proposed as one of the possible effective solution with regular patching of the systems. The password policy enforcement and restrictive network configuration have been suggested in order to increase the security in the SCADA systems.
[4]	2017	➡ Information security ➡ System theory-based security	The authors have discussed the need for cyber– physical security in the context of the smart grid. The cyber threats and countermeasures are also presented. The future research directions which includes information security and system-theory-based security are also advocated.
[42]	2016	➡ SCADA cyber security risk assessment ➡ Risk assessment models & methods ➡ Validation of risk assessments methods ➡ Fragmentation ➡ Attack/Failure orientation ➡ Risk assessments support tools	The authors have reviewed the state of the art in cyber security risk assessment of Supervisory Control and Data Acquisition (SCADA) systems. The examination of twenty-four risk assessment methods developed and applied in the context of a SCADA system. The essence of the methods and analysis have been presented. The authors have suggested an intuitive scheme for the categorization of cyber security risk assessment methods for SCADA systems. The authors have highlighted the research challenges like Dealing with Fragmentation, Overcoming Attack or Failure Orientation, Search for Reliable Sources of Data, Improving Validation of Risk Assessment Methods and Supporting Risk Management Methods with Elaborate Tools.
[22]	2016	➡ Advanced persistent threats ➡ Lack of data integrity ➡ Man-in-the-middle attacks ➡ Replay attacks ➡ Denial of service attacks ➡ Data integrity and privacy ➡ Data logging ➡ Ownership ➡ Authentication and encryption ➡ Web applications in the cloud ➡ Risk management ➡ Embedded device protection in industrial IoTs	The authors have highlighted the security challenges that the industrial SCADA systems face in an IoT-cloud environment. The authors have provided the existing best practices and recommendations for improving and maintaining security. They also discussed future research directions to secure these critical CPSs and help the research community in identifying the research gaps. It is evident from the research paper that there is clear need to do more research with respect to securing critical power systems as the attacks on them may result in devastating effects to parties involved i.e. industrial apparatuses as well as entities related to the systems.

Ref. No.	Year of Publication	Major Areas & Security Challenges	Research Findings and Gaps
[49]	2016	➡ Communications and control architectures ➡ Substation architectures, threats, and vulnerabilities ➡ Cyber vulnerabilities within substations ➡ Security standards and compliance requirements ➡ Encryption and authentication ➡ Access Control ➡ Intrusions detection systems	The authors have provided an overview of the communications and control architectures with respect to modern substations that includes the network protocols and commonly used devices to support these substation functions. The cyber threats associated with the components, highlighting the different power system control applications which can be targeted by the attackers. The various security mechanisms are also identified which can be deployed to protect substations like access controls, encryption, authentication, firewalls, and intrusion detection systems. The various cybersecurity standards have also been reviewed which impact the security posture of the grid like North American Electric Reliability Corporation critical infrastructure protection (NERC CIP), IEEE C37.240, and IEC 62351. There are various research opportunities which can be explored as well as there is a pertinent need for further research and development in protecting and securing the substations. There could be many open areas were challenges exist in terms of economic, technical, and operational challenges that needs to be considered while safeguarding substations. The explicit areas that have clear need of further research consist of encryption and authentication encryption techniques with minimized communication latency. The new approaches for intrusions detection systems deployments also needs to be explored.
[52]	2016	➡ Cyber warfare ➡ Industrial control systems potential active and military response to an attack by stakeholders ➡ Schmitt analytical framework ➡ Mitigation and response ➡ Case studies of various attacks	The author has discussed the industrial control systems potential active and military response to an attack by stakeholders. The cyber warfare is discussed with respect to several frameworks, mitigation and response approaches. The various case studies of events happened around the world are discussed with comprehensive analysis. Since industrial control systems are very critical deployments in nature, these deployments can easily be used by attackers as potential targets. There are various research opportunities which can be explored such the legal angle for international cyber-attacks with respect to potential active and military response in the event of any attack on critical industrial control systems of the country.
[51]	2016	➡ Internet and external threats to SCADA systems ➡ Access control ➡ Availability ➡ Authentication ➡ Integrity ➡ Self-healing techniques ➡ Intrusion tolerance techniques ➡ Firewall security	The authors have discussed the ways to protect SCADA systems against both internal and external threats. The various security mechanisms i.e. access control, availability, authentication and integrity are explained. The implementation of ModbusSec which is secure communication protocol is also discussed. The intelligent firewall security mechanism and deployment to secure the SCADA systems is discussed. The concepts and techniques such as self-healing and the intrusion tolerance, which are used for intrusion detection in the SCADA systems are also explored. There are various research opportunities which can be explored such as internal access control application that can be applied as an access control policy for restricting access to HMIs at supervisory level. The deployment of intrusion threats tolerance for any internal and external threats for SCADA systems at supervisory level needs further study. The availability being one of the most critical factor in the SCADA system needs further study.

Ref. No.	Year of Publication	Major Areas & Security Challenges	Research Findings and Gaps
[54]	2016	➡ SCADA system testbed ➡ Cybersecurity research ➡ Forensic research	The authors have presented a supervisory control and data acquisition (SCADA) testbed which has been built at the University of New Orleans. With respect to cybersecurity and forensic research, the testbed can be an advantageous resource. The various facets of SCADA systems i.e. programmable logic controllers programming, protocol analysis, and demonstration can be evaluated with the help of the testbed.
[57]	2016	➡ Virtual SCADA security testbed ➡ SCADA system architecture and protocols ➡ Simulation platform for SCADA systems ➡ SCADA cyberattack scenarios ➡ Distributed denial of service (DDoS) ➡ False data injection attack	The authors have discussed Distributed Denial of Service (DDoS) and false data injection attack scenarios. The virtual SCADA security testbed has been proposed which could be scaled and reconfigured very easily and shall be used in development and evaluation of SCADA specific security solutions. The virtual SCADA security testbed Experimental results indicate that the testbed can be efficiently used for cyber security assessment and vulnerability assessment on SCADA systems. There are various research opportunities which can be explored with respect to evaluating the testbed with various SCADA communication protocols. The remote accessibility of testbed for researchers can also be further explored. The data compiled from the testbed can be used to develop and evaluate a new SCADA specific intrusion detection system (IDS).
[21]	2016	➡ SCADA system security challenges ➡ Lack of data integrity ➡ Man-in-the-middle (MITM) attacks ➡ Replay attacks ➡ Denial of service (DoS) attacks ➡ Advanced persistent threats ➡ Policy management ➡ Data integrity ➡ Weak communication ➡ Data integrity and privacy ➡ Data logging ➡ Authentication and encryption ➡ Web applications in the cloud ➡ Risk management ➡ Embedded device protection in industrial IoTs	The authors have highlighted the security challenges of critical infrastructures. The existing best practices and recommendations for critical infrastructures have also been emphasized. The authors have also emphasized that the further research in security for the critical infrastructure needs to be undertaken to be secure in the smart grid. The recommendations proposed to secure the SCADA systems include network segregation, continuous monitoring and analysis, log analysis, file integrity monitoring, network traffic analysis, memory dump analysis, updating and patching regularly, testing vulnerability regularly, proxy solutions and using tools for detecting malicious activity. There are various proposed research opportunities which can be further explored which include SCADA management, security, real-time data handling, cross-layer collaborations, application development, migration of cyber physical systems and the impact on existing approaches, sustainable management, engineering and development tools, sharing and management of data lifecycle and data science.
[9]	2016	➡ Physical security of plant, equipment, and networks ➡ Cyber security for networking and computing ➡ Security management for the corporation or enterprise itself ➡ Specific security issues for supervisory and control applications and networks (SCADA) ➡ Specific security issues for endpoints	The authors have discussed cyber security of smart grid and SCADA systems. The various threats and risks have also been discussed. The different types of cyber-attacks and the appropriate architectural and security strategies have been proposed. The trends and best practices in smart grid have also been discussed. The overview of assessment methodology in terms of baseline and architecture is explained.
[7]	2016	➡ Fragmentation ➡ Overcoming attack or failure orientation ➡ Search for reliable sources of data ➡ Improving validation of risk assessment methods ➡ Supporting risk management methods	The author has reviewed the cyber security risk assessment of SCADA systems. The twenty-four risk assessment methods have been analyzed and discussed. The five research challenges which include dealing with fragmentation, overcoming attack or failure orientation, search for reliable sources of data, improving validation of risk assessment methods, and supporting risk management methods with elaborate tools have also been discussed.

Ref. No.	Year of Publication	Major Areas & Security Challenges	Research Findings and Gaps
[3]	2016	➡ Data protection ➡ Security analytics	The authors have examined and surveyed the security advances of smart grid from a different perspective i.e. a data driven approach. The data protection either in data in transit or at rest is the security goal. With this insight, the survey has been carried out which focused around the security issues within the entire lifecycle of smart grid data comprising of four serial stages i.e. data generation, data acquisition, data storage and data processing. The review of security analytics in smart grid is also presented.
[13]	2015	➡ Cyber–physical systems modelling ➡ Unauthorized access ➡ Packet access to the network segments hosting SCADA devices	The authors have proposed a new model and simulation platform for the supervisory control and data acquisition (SCADA) systems with respect to cyber–physical systems. The SCADA systems performance is evaluated based on time delays in communications. The various methods to models for cyber intrusions assessments for cyber–physical systems security is proposed.
[2]	2015	➡ Confidentiality ➡ Integrity ➡ Authorization ➡ Authentication	The authors have presented the key security issues and challenges of a smart grid which included confidentiality, integrity, authorization, and authentication of the exchanged data.
[19]	2014	➡ Cybersecurity for power systems ➡ Security enhancements ➡ Impact analysis ➡ Mitigation of cyber attacks ➡ Simulation scenarios of cyber intrusions ➡ Intrusion-based attacks ➡ DoS attacks ➡ Real-time monitoring ➡ Anomaly detection	The authors have explained the importance of cybersecurity for power systems. The significance of security for cyber-physical systems like SCADA operated systems have been highlighted. The various scenarios of the attacks and intrusions on power grid using the testbed have also been showcased. There are various research opportunities which can be further explored such as computational methods for fast recovery in the event of an extended outage condition due to cyber-attacks.
[18]	2014	➡ Cyber-physical security of wide-area monitoring, protection and control (WAMPAC) ➡ Game theoretic approach ➡ Cyber-physical testbeds ➡ Realistic attack-defense ➡ Phasor measurement units ➡ Advanced metering infrastructure ➡ Distribution automation	The authors have discussed the smart grid technologies in conjunction with cyber developments in order to have end to end control and monitoring of electric power grid. The various technical initiatives i.e. advanced metering infrastructure, demand response, wide-area monitoring, protection and control systems that are based on phasor measurement units, large scale renewable integration of wind and solar generation, and hybrid electric vehicles. The vital security issues in wide-area monitoring, protection and control are discussed. The game theoretic framework for physical and cyber is a discussed. The testbeds for evaluating and validating cyber-physical issues are also explained.
[14]	2014	➡ Information security ➡ Privacy ➡ Securing communications and devices ➡ Data protection ➡ Incident management	The author has discussed various concerns which needs to be addressed for successful smart grid implementations with respect to the perspective of information security. The privacy, consumption data protection and incident management in SCADA are also discussed. The various standards, guidelines and risk assessments approaches with respect to the critical infrastructures are also presented.
[11]	2014	➡ Threat modeling ➡ Vulnerability assessment ➡ Security strategies ➡ SCADA reference model ➡ Security posture ➡ Protection scenarios	The authors have provided review of SCADA standards, its state-of-the-art communication and security aspects. The SCADA architecture with respect to hardware architecture, software architecture and Communication infrastructure has been explained and discussed. The various SCADA communication standards and technologies are also discussed. The SCADA security with respect to attacks on data, pathways, insecurities, vulnerabilities and possible solutions are also discussed.

Ref. No.	Year of Publication	Major Areas & Security Challenges	Research Findings and Gaps
			There are various research opportunities which can be further explored such communication infrastructure technologies, extensibility and interoperability.
[6]	2013	➡ Impersonation/identity spoofing ➡ Eavesdropping ➡ Data tampering ➡ Authorization and control access issues ➡ Privacy issue compromising and malicious code ➡ Availability and dos issues ➡ Cyber-attacks	The authors have examined the security issues and challenges on the IoT-based smart grid. The key security issues faced include impersonation/identity spoofing, eavesdropping, data tampering, authorization and control access issues, privacy issue, compromising and malicious code, availability and DOS issues, and cyber-attacks.
[5]	2013	➡ Security threats ➡ Attack prevention & defenses ➡ Network protocols	The authors have described the objectives and requirements of security in the smart grid with emphasis on identifying essential differences among the smart grid and the internet. The potential security threats, attack prevention and defenses, and network protocols and architectures were also discussed.
[27]	2012	➡ Privacy ➡ Data confidentiality ➡ Data usage ➡ Trust ➡ Fine grained access controls ➡ Tamper resistance and non-repudiation ➡ Availability ➡ Transparent auditing ➡ Verifiability ➡ Regulatory and policy aspects	The authors have highlighted the issues and the research challenges in smart grids with respect to privacy and security perspectives. The main challenges such as privacy, data confidentiality, data usage, trust, fine grained access controls, tamper resistance and non-repudiation, availability, transparent auditing and verifiability have been discussed. There are various research opportunities which can be explored with respect to security, privacy and regulatory facets.
[15]	2012	➡ Communication infrastructure ➡ Power line communications (PLCs) ➡ Challenges in terms of complexity, efficiency, reliability & security ➡ Information security domains ➡ Government coordination on SCADA security ➡ Segregation in operational SCADA/EMS and IT ➡ Privacy	The authors have discussed the communication infrastructure with respect to smart grid. The criticality of a scalable and ubiquitous communication infrastructure of a smart grid is highlighted. The background and motivation of communication infrastructures with respect to smart grid systems is discussed. The smart grid componential technologies of sensing, communications, and control technologies have been described. The security aspects of SCADA with respect to privacy, information security domains, threats, and vulnerabilities have also been discussed. The challenges in communication infrastructure in smart grid are explored. The reliability and security challenges that are really critical are also discussed. The various challenges such as complexity, efficiency, reliability and security are discussed in detail.
[1]	2010	➡ Trust ➡ Communications & Devices ➡ Privacy	The authors discussed various security issues in SCADA systems which included trust, communications and devices security, privacy, issues pertaining to complexity and scaling of future power systems.

V. PUBLICATION TRENDS

The various sources including Google Scholar, Crossref, Scopus and Web of Science were searched for the publications related to the SCADA security and its challenges. The final subset of publications i.e. total of 372 publications were evaluated for interpreting the various publication trends. The above *figure 4* illustrates the publications which have been published during the period of 2015 – 2018. All the publications are primarily focusing on SCADA security. The above *figure 5* illustrates the total number of publications which have been published during the period of 2015 – 2018 by each publisher. All the publications are primarily focusing on SCADA security.

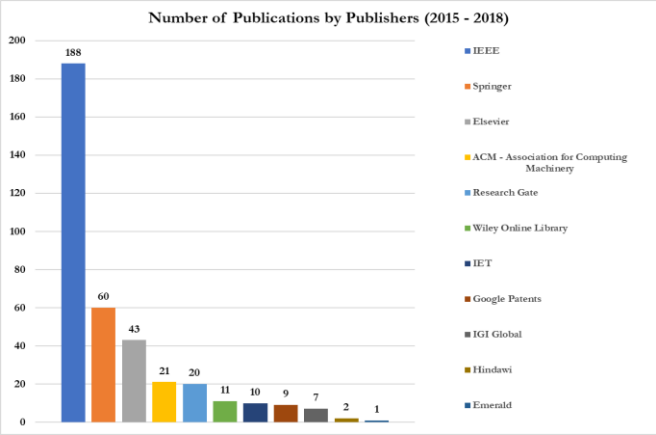

Figure 4: Publications by Publishers on Yearly Basis (2015 - 2018)

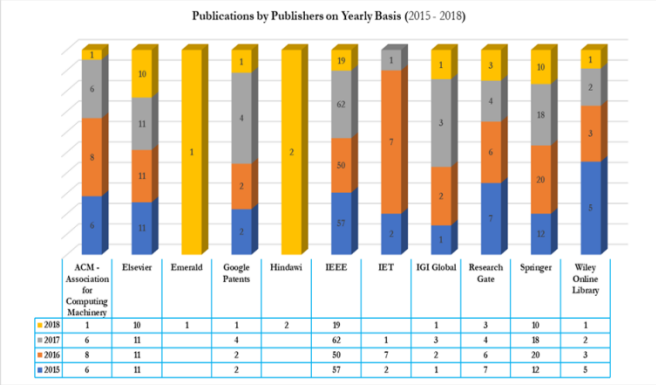

Figure 5: Number of Publications by Publishers (2015 - 2018)

The above *figure 6* illustrates the top 5 publishers who published SCADA security related publications during the period of 2015 – 2018.

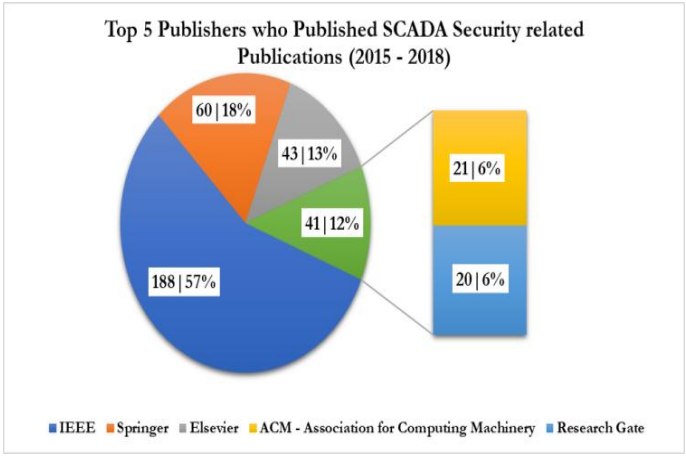

Figure 6: Top 5 Publishers who Published SCADA Security related Publications (2015 - 2018)

VI. RESEARCH OPPORTUNITIES IN SMART GRID BASED SCADA SYSTEMS

In the literature reviewed [1], [2], [3], [4], [5], [6], [7], [9], [10], [11], [14], [15], [18], [19], [21] and [27], it is apparent that the SCADA security have many open research problems. Some of the areas in which the research gaps have been recognized and further explored are listed as under:

Table 4 : Research Gaps / Opportunities

#	Research Gap / Opportunity	Brief Description
1	**Privacy**	Privacy with respect to confidentiality, integrity and availability of the SCADA systems.
2	**Devices security**	The security is considered at device level itself rather than securing the perimeter of the device.
3	**Complexity & scaling of future power systems**	The scalability of the system is very critical which is often ignored at the start of new projects. The systems should be flexible to be expanded in the future without major changes to the original setups.
4	**Trustworthiness**	The SCADA systems should be intrinsically secure, available, and reliable.
5	**Authorization & authentication**	The enhanced methods and mechanisms are to be devised to enable access to what and to whom in the critical systems.
6	**Data protection**	The enhanced methods and mechanisms to protect data from destructive forces and from the undesirable activities of illegal users that will result in cyberattack or a data breach.
7	**Information security**	The enhanced processes and methodologies to protect electronic, print or any other form of information that is confidential, private and sensitive in nature. The data should be protected from illegal access, deletion, usage,

		leak, alteration, misappropriation or interruption.
8	**Data tampering**	The enhanced methods and mechanisms to protect data tampering purposely either by modifying it or over change over the unauthorized channels.
9	**Impersonation or identity spoofing**	The enhanced methods and mechanisms to protect the SCADA system from impersonation or spoofing which can lead to fraud.
10	**Eavesdropping**	The enhanced methods and mechanisms to protect the SCADA system from an eavesdropping attack i.e. intrusion where somebody attempts to steal the information as it may not be encrypted over the transmitting medium.
11	**Access control**	The enhanced methods and mechanisms to protect the SCADA system from the risk of illegal access to physical and logical systems.
12	**Denial of service (DoS) issues**	The enhanced methods and mechanisms to protect the SCADA system from denial-of-service (DoS) type of attacks in which hackers try to prevent genuine users from accessing the services and systems.
13	**Fragmentation**	The enhanced methods and mechanisms to protect the SCADA system from Fragmentation issues that intent to bypass security measures or Intrusion Detection Systems by deliberate fragmentation of attack activity.
14	**Patching of SCADA systems**	This is one of the big and most common challenge in SCADA systems. The hands-on policies and procedures needs to be in place to make sure that the systems are always up to date with the latest patches especially security patches.
15	**Incident management of SCADA systems**	The enhanced methods and mechanisms to handle the incidents in SCADA systems needs to be devised in order to avoid the risks associated with it.
16	**Intrusion detections system**	The enhanced Intrusion Detection Systems (IDS) should be built for ensuring the detection of vulnerability exploits against a target network, computer or application.
17	**Non-repudiation**	The enhanced methods and mechanism needs to be explored for Non-repudiation to guarantee that a transferred message has been sent and received by the intended parties claiming to have sent and received the specific message.
18	**Transparent auditing**	The enhanced procedures for auditing needs to be developed for higher transparency that guarantees that high standards of correctness are the core objective of the audit along with right audit processes that workforce comply to.
19	**Segregation of duties**	The clear roles and responsibilities needs to be identified for the required roles for the SCADA systems to operate. Segregation of duties needs to be done in order to avoid any single point of failures in the future.
20	**Interoperability**	The interoperability is one of the most common issue in the power systems as the vendors usually safeguard their business interest by locking and limiting the integration of systems with other vendors systems. The proper procedures and protocols needs to be put in place to make sure that different systems can talk to each other and exchange the data irrespective of the vendor.

VII. CONCLUSION AND FUTURE SCOPE

SCADA system security is vertical of critical importance due to the critical infrastructure-based SCADA systems deployments. The threat spectrum is very huge due to the various interests and internet connectivity to the corporate networks. SCADA systems security with conjunction with Smart Grid is a very interesting research of area for government, academia and industry. In this paper, we have presented a comprehensive survey on security challenges and research opportunities in Smart Grid based SCADA systems. We have presented the typical SCADA deployment architecture with respect to components, security assurance level, criticality, asset type, zone and subnets. The various risks associated with SCADA-ICS were also presented. We have presented the publishing trends with respect to SCADA security and its challenges.

The literature review of relevant papers highlighting major areas & security challenges in the SCADA systems along with research findings and gaps is also presented. Lastly, some of the areas in which the research gaps have been recognized are discussed for further future research opportunities.

REFERENCES

[1]. Khurana, H., Hadley, M., Lu, N., & Frincke, D. A. (2010), 'Smart-grid security issues'. IEEE Security & Privacy, vol. 8, no. 1.

[2]. Delgado, V., Martins, J. F., Lima, C., & Borza, P. N. (2015), 'Smart grid security issues', Proceedings of IEEE 9th International Conference on Compatibility and Power Electronics, pp. 534-538.

[3]. Sullivan, D., Luiijf, E., & Colbert, E. J. (2016), 'Components of industrial control systems', Advances in Information Security, Springer International Publishing, vol. 66, pp. 15-28.

[4]. Tan, S., De, D., Song, W. Z., Yang, J., & Das, S. K. (2017), 'Survey of Security Advances in Smart Grid: A Data Driven Approach'. IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 397-422.

[5]. Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012), 'Cyber–physical security of a smart grid infrastructure', Proceedings of the IEEE, vol. 100, no. 1, pp. 195-209.

[6]. Wang, W., & Lu, Z. (2013), 'Cyber security in the Smart Grid: Survey and challenges', Computer Networks, vol. 57, no. 5, pp. 1344-1371.

[7]. Bekara, C. (2014), 'Security issues and challenges for the iot-based smart grid', Procedia Computer Science, vol. 34, pp. 532-537.

[8]. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016), 'A review of cyber security risk assessment methods for SCADA systems', Computers & Security, vol. 56, no. 1, pp. 1-27.

[9]. McBride, A. J., & McGee, A. R. (2012), 'Assessing smart grid security', Bell Labs Technical Journal, vol. 17, no. 3, pp. 87-103.

[10]. Safa, H. H., Souran, D. M., Ghasempour, M., & Khazaee, A. (2016), 'Cyber security of smart grid and SCADA systems, threats and risks', Proceedings of CIRED Workshop, pp. 245.

[11]. Korman, M., Välja, M., Björkman, G., Ekstedt, M., Vernotte, A., & Lagerström, R. (2017). 'Analyzing the Effectiveness of Attack Countermeasures in a SCADA System', Proceedings of ACM 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, pp. 73-78.

[12]. Gao, J., Liu, J., Rajan, B., Nori, R., Fu, B., Xiao, Y., & Philip Chen, C. L. (2014), 'SCADA communication and security issues', Security and Communication Networks, vol. 7, no. 1, pp. 175-194.

[13]. Stefanov, A., Liu, C. C., Govindarasu, M., & Wu, S. S. (2015), 'SCADA modeling for performance and vulnerability assessment of integrated cyber–physical systems', International Transactions on Electrical Energy Systems, vol. 25, no. 3, pp. 498-519.

[14]. Kim, H. (2012), 'Security and vulnerability of SCADA systems over IP-based wireless sensor networks', International Journal of Distributed Sensor Networks, vol. 12, no. 268478.

[15]. Line, M. B. (2014), 'Why securing smart grids is not just a straightforward consultancy exercise', Security and Communication Networks, vol. 7, no. 1, pp. 160-174.

[16]. Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2013), 'A survey on smart grid communication infrastructures: Motivations, requirements and challenges', IEEE communications surveys & tutorials, vol. 15, no. 1, pp. 5-20.

[17]. Tawde, R., Nivangune, A., & Sankhe, M. (2015), 'Cyber security in smart grid SCADA automation systems', Proceedings of IEEE Innovations in Information, Embedded and Communication Systems (ICIIECS), pp. 1-5.

[18]. Ashok, A., Hahn, A., & Govindarasu, M. (2014), 'Cyber-physical security of Wide-Area Monitoring, Protection and Control in a smart grid environment', Journal of advanced research, vol. 5, no. 4, pp. 481-489.

[19]. Stefanov, A., & Liu, C. C. (2014), 'Cyber-physical system security and impact analysis', Proceedings of the 19th World Congress the International Federation of Automatic Control, vol. 47, no. 3, pp. 11238-11243.

[20]. Hawk, C., & Kaushiva, A. (2014), 'Cybersecurity and the smarter grid', The Electricity Journal, vol. 27, no. 8, pp. 84-95.

[21]. Rice, E. B., & AlMajali, A. (2014), 'Mitigating the risk of cyber attack on smart grid systems', Procedia Computer Science, vol. 28, pp. 575-582.

[22]. Sajid, A., Abbas, H., & Saleem, K. (2016), 'Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges', IEEE Access, vol. 4, pp. 1375-1384.

[23]. Ciancamerla, E., Fresilli, B., Minichino, M., Patriarca, T., & Iassinovski, S. (2014), 'An electrical grid and its SCADA under cyber attacks: Modelling versus a Hybrid Test Bed', Proceedings of IEEE International Carnahan Conference on Security Technology (ICCST), pp. 1-6.

[24]. Dondossola, G., & Terruggia, R. (2015), 'Cyber security of smart grid communications: Risk analysis and experimental testing', Springer Berlin Heidelberg, pp. 169-193.

[25]. Zhang, Y., Wang, L., Xiang, Y., & Ten, C. W. (2015), 'Power system reliability evaluation with SCADA cybersecurity considerations', IEEE Transactions on Smart Grid, vol. 6, no. 4, pp. 1707-1721.

[26]. Kuzlu, M., Pipattanasompom, M., & Rahman, S. (2017), 'A comprehensive review of smart grid related standards and protocols', Proceedings of IEEE 5th International Smart Grid and Cities Congress and Fair (ICSG), pp. 12-16.

[27]. Ajayi, A. O., Alese, B. K., Fadugba, S. E., & Owoeye, K. (2014), 'Sensing the Nation: Smart Grid's Risks and Vulnerabilities', International Journal of Communications, Network and System Sciences, vol. 7, no. 05, pp. 151-163.

[28]. Asghar, M. R., & Miorandi, D. (2012), 'A holistic view of security and privacy issues in smart grids', Springer, Berlin, Heidelberg, pp. 58-71.

[29]. Ionica, D., Pop, F., Popescu, N., Popescu, D., & Dobre, C. (2018). SCADA Security: Concepts and Recommendations. In International Symposium on Cyberspace Safety and Security, pp. 85-98. Springer, Cham.

[30]. Igure, V. M., Laughter, S. A., & Williams, R. D. (2006), 'Security issues in SCADA networks', Computers & Security, vol. 25, no. 7, pp. 498-506.

[31]. Sebastio, S., Scala, A., & D'Agostino, G. (2016), 'Availability Study of the Italian Electricity SCADA System in the Cloud', Springer, Cham, pp. 201-212.

[32]. Leverett, E. P. (2011), 'Quantitatively assessing and visualising industrial system attack surfaces'. University of Cambridge, Darwin College, vol. 7.

[33]. Gold, S. (2009), 'The SCADA challenge: securing critical infrastructure', Network Security, vol. 09, no. 8, pp. 18-20.

[34]. Igure, V. M., Laughter, S. A., & Williams, R. D. (2006), 'Security issues in SCADA networks', Computers & Security, vol. 25, no. 7, pp. 498-506.

[35]. Chen, T. (2010), 'Stuxnet, the real start of cyber warfare?', IEEE Network, vol. 24, no. 6, pp. 2-3.
[36]. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016), 'A review of cyber security risk assessment methods for SCADA systems', Computers & Security, vol. 56, pp. 1-27.
[37]. Idaho National Laboratory, (2011). 'Vulnerability Analysis of Energy Delivery Control Systems'. [Online] Available at: http://energy.gov/oe/downloads/ vulnerability-analysis-energy-delivery-control-systems [Accessed 12 August 2017].
[38]. Dán, G., Sandberg, H., Ekstedt, M., & Björkman, G. (2012), 'Challenges in power system information security', IEEE Security & Privacy, vol. 10, no. 4, pp. 62-70.
[39]. SCADA Systems Made Simple. (2019). [online] Schneider Electric, pp. 4-11. Available at: https://www.schneider-electric.com/en/download/document/998-2095-01-19-12AR0_EN/ [Accessed 23 Jan. 2019].
[40]. Lenzini, G., Oostdijk, M., Teeuw, W., Hulsebosch, B., Wegdam, M., & Enschede, N. (2009). Trust, security, and privacy for the advanced metering infrastructure.
[41]. SCADAguardian. (2019). Retrieved from https://www.nozominetworks.com/ products/ scadaguardian/
[42]. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K.. (2016). A review of cyber security risk assessment methods for SCADA systems. Computers & security, Elsevier, 56, pp.1-27.
[43]. Babu, B., Ijyas, T., Muneer, P. and Varghese, J. (2017). Security issues in SCADA based industrial control systems. In Anti-Cyber Crimes (ICACC), 2nd International Conference on (pp. 47-51). IEEE.
[44]. Fillatre, L., Nikiforov, I. and Willett, P. (2017). Security of SCADA systems against cyber–physical attacks. IEEE Aerospace and Electronic Systems Magazine, 32(5), pp.28-45.
[45]. Rosa, L., Cruz, T., Simões, P., Monteiro, E. and Lev, L. (2017). Attacking SCADA systems: a practical perspective. In Integrated Network and Service Management (IM), IFIP/IEEE Symposium, pp.741-746. IEEE.
[46]. Antón, S.D., Fraunholz, D., Lipps, C., Pohl, F., Zimmermann, M. and Schotten, H.D. (2017). Two decades of SCADA exploitation: A brief history. In Application, Information and Network Security (AINS) Conference, pp. 98-104. IEEE.
[47]. Ali, S., Al Balushi, T., Nadir, Z. and Hussain, O.K. (2018). ICS/SCADA System Security for CPS. In Cyber Security for Cyber Physical Systems, pp. 89-113. Springer, Cham.
[48]. Sun, C.C., Hahn, A. and Liu, C.C. (2018). Cyber security of a power grid: State-of-the-art. International Journal of Electrical Power & Energy Systems, vol. 99, pp. 45-56.
[49]. Hahn, A., Sun, C.C. and Liu, C.C. (2016). Cybersecurity of SCADA within Substations. Smart Grid Handbook, Wiley, pp.1-17.
[50]. Korman, M., Välja, M., Björkman, G., Ekstedt, M., Vernotte, A. and Lagerström, R. (2017). Analyzing the Effectiveness of Attack Countermeasures in a SCADA System. In Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, pp. 73-78. ACM.
[51]. El Anbal, M., El Kalam, A.A., Benhadou, S., Moutaouakkil, F. and Medromi, H. (2016). Securing SCADA Critical Network Against Internal and External Threats. In International Conference on Critical Information Infrastructures Security, pp. 328-339. Springer, Cham.
[52]. Honkus, F. (2016). Responding to Attacks on Industrial Control Systems and SCADA Systems. In Cyber-security of SCADA and Other Industrial Control Systems, pp. 305-322. Springer, Cham.
[53]. Duka, A.V., Genge, B., Haller, P. and Crainicu, B. (2017). Enforcing end-to-end security in SCADA systems via application-level cryptography. In International Conference on Critical Infrastructure Protection, pp. 139-155. Springer, Cham.
[54]. Ahmed, I., Roussev, V., Johnson, W., Senthivel, S. and Sudhakaran, S. (2016). A SCADA system testbed for cybersecurity and forensic research and pedagogy. In Proceedings of the 2nd Annual Industrial Control System Security Workshop, pp. 1-9. ACM.
[55]. Kleinmann, A., Amichay, O., Wool, A., Tenenbaum, D., Bar, O. and Lev, L. (2017). Stealthy deception attacks against SCADA systems. In Computer Security, pp. 93-109. Springer, Cham.
[56].Nazir, S., Patel, S. and Patel, D. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. Computers & Security, Elsevier, vol. 70, pp. 436-454.
[57].Tesfahun, A. and Bhaskari, D.L., (2016). A SCADA testbed for investigating cyber security vulnerabilities in critical infrastructures. Automatic Control and Computer Sciences, Springer, vol. 50(1), pp.54-62.
[58].Industrial Control System Cyber Emergency Response Team (ICS-CERT). (2019). [online] Available at: https://cset.inl.gov/SitePages/Home.aspx [Accessed 10 Jan. 2019].

Authors Profile

Mr. A. W. Mir is Ph.D Research Scholar at Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India. He has progressive experience in Information Technology field in diverse sectors like Education, Training, Software Development, Consulting and Utilities. He has Bachelors and Masters Degree in Computer Applications. His main research work focuses on Industrial Control Sytems Security, SCADA Systems and Cyber Security.

Dr. K. R. Ramkumar is PhD in Computer Science and Engineering from Anna University, Chennai, India, having 17 years of Teaching and Research Experience. He is currently working as Associate Professor at Chitkara University , Punjab, India. His areas of expertise are Network Security, Key Management and Relational Database Management Systems with advancements. His research includes solving the routing issues, dealing with security and node failure apprehensions of wireless sensor networks. Much of his work has been on improving the understanding, design, and performance analysis of different routing and security algorithms of Wireless Sensor Networks. He also is working with the Extensible Markup Language (XML) and resolving the data integrity and consistency issues on web communications. In his rest time he does research on Green, Free and Sustainable Energy.

