ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 3, March 2020

Incident Analysis of Cyber Forensics for SCADA Industrial Control System

S.Natarajan[1], R.Muralikrishna[2], Ajay Joseph Rayan[2], U.Arun Kumar[2], V.Abinesh[2]

Assistant Professor, Department of Electrical and Electronics Engineering, Vel Tech, Chennai, Tamil Nadu, India [1]

UG Student, Department of Electrical and Electronics Engineering, Vel Tech, Chennai, Tamil Nadu, India [2]

ABSTRACT-A large number of industries including: critical national infrastructure (electricity, gas, water, etc.) and manufacturing firms rely heavily on computer systems, networks, control systems, and embedded devices in order to provide safe and reliable operations. These networks can be very complex and are often bespoke to the types of product the industries may provide. In recent years we have seen a significant rise in malicious attacks against such systems, ranging from sophisticated intelligent attacks to simple tool based delivery mechanisms. With the rise in the reliance on industrial control networks and of course the increasing attacks, the lack of security monitoring and post forensic analysis of SCADA networks is becoming increasingly apparent. SCADA systems forensics is not like standard enterprise file-system forensics, the forensic specialist often has to be an expert in such systems/networks and SCADA related devices in order to identify where potential Forensic evidence could be located.

KEYWORDS- SCADA, ICS, Cyber Forensics, Cyber Security

1. INTRODUCTION

Industrial Control Systems (ICS) and specifically Supervisory Control and Data Acquisition (SCADA) are the underpinning technologies that ensure the operation and functionality of control systems used in many industries including Critical National Infrastructure (CNI) for example; electricity grids, water treatment facilities, hospitals, transport networks. In recent years there has been an increasing number of attacks directly targeting these systems [1] including the well publicisedStuxnet APT [2], Flame [3], and Havex [4]. Control systems used in businesses have also been found as the entry point for major security breaches as was the case with Target [5] receiving malware through heating, ventilating, and air conditioning (HVAC) system. Therefore, there is a need to be able to undertake post incident forensic analysis of these systems to determine; if a breach has occurred, the extent to which the system is compromised, what functional operations and assets are affected, how the breach or incident occurred, and if possible work towards attribution.

II.INTRODUCING INDUSTRIAL CONTROL SYSTEMS /SCADA

ICS and SCADA are specialized computer networks and devices that work in sync to monitor and control key processes involved in the management of machinery, equipment and facilities. SCADA systems communicate with the control system using proprietary protocols such as DNP3 and MODBUS. SCADA systems often include the following components:
Human Machine Interface (HMI) Programmable Logic Controllers (PLC) and Remote Terminal Units (RTU) used to convert the signals from process sensors to digital data and relay them to supervisory .

- Engineer workstations and servers An example SCADA environment is shown in Figure 1 inclusive of control devices, sensors, management consoles and links to the corporate network.

2.1. Vulnerabilities in SCADA Systems

When SCADA systems were originally designed they were isolated from the network and engineers focused on

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 3, March 2020

providing availability of data and operations rather than confidentiality and integrity. This isolation is commonly referred to as an "air-gap"., and while originally designed as a complete physical separation, this increasingly has become to mean technological separation by the means of configurable firewalls or similar mechanism. Originally these systems often used

Bespoke and manufacturer independent protocols and architectures and were therefore very difficult to understand and affect without physical access.

More recent SCADA systems however, have moved to more interoperability and open standards for cost efficiency and integration into management IT systems. For example, communication is now common over Ethernet TCP-IP including more standardized control protocols and applications. Thus, SCADAsystems are now susceptible to external attacks and IT based vulnerabilities.

Many SCADA systems are safety critical and must be operational for a large proportion of time, as they provide services that are vital to the economy and well-being of citizens. Downtime is managed carefully and scheduled maintenance periods are often irregular and infrequent. Therefore, many critical infrastructures are still running legacy components and systems including amongst others; Windows 95, XP, and 2000. Access to these systems for patching is a problem and therefore many IT vulnerabilities still remain that are considered resolved in the more main-stream Business IT environments.

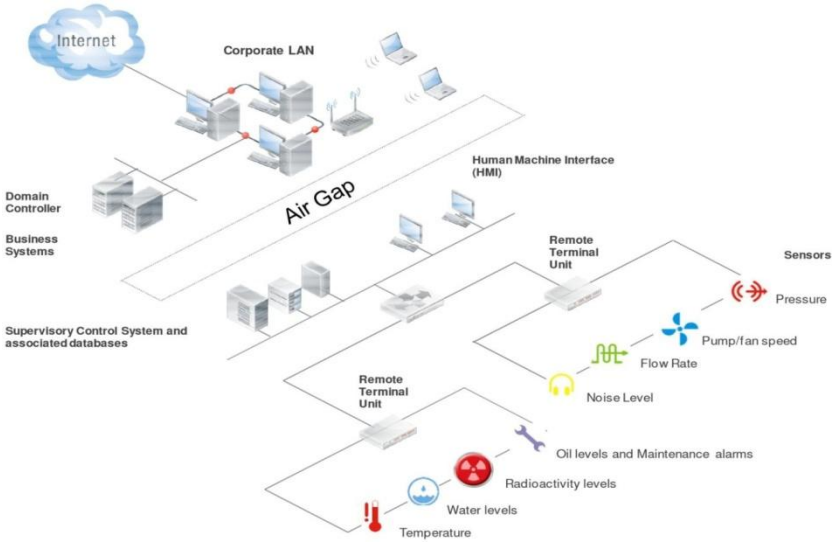

Figure 1: Industrial Control System with SCADA Network Architecture

SCADA components such as PLCs and RTUs are designed purely for functionally and are limited by their processing capability and therefore do not contain many of the authentication and access control specifications that are common in corporate IT infrastructures.

As SCADA control systems become increasingly complex and distributed, the number of potential attack vectors also increases including via; the internet, enterprise network, and direct connections to the control networks and field devices. Some of the most common types of attack vectors against SCADA are:

- Backdoors and holes in the network perimeter. Especially in the configuration of "Air Gaps" or links to corporate enterprise IT infrastructure
- Vulnerabilities in common control system protocols, Attacks on field devices Database, attacks Communications hijacking and man-in the middle attacks
- Cinderella attack [11] on time provision and synchronization.

Typical Attacks Against SCADA Systems

In order to undertake any forensic investigation we must first understand the types of attacks that are facing the systems

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 3, March 2020

and environments so as to inform the forensic process. To guide the development of a forensics framework we classify attacks against SCADA systems into 3 categories; the communication stack, hardware and software:

- Communication stack:

Attacks can occur on the network layer for example through a diagnostic server on the UDP port. Attacks can occur on the transport layer such as a SYN flood attack saturating resources by sending TCP connection requests faster than the machine can process them. At application layer many of the protocols used on a SCADA system have little security considerations. For example DNS forgery and packet replay are common.

- Hardware:

Attackers gain unauthenticated remote access to devices and change data set points that may cause the devices to fail at low threshold or an alarm not to go off.
Lack of authentication for administrative tasks on the hardware mean an attacker can reprogram the logic or values and affect the functional behavior of the device.

- Software: SCADA systems use a variety of software to provide functionality from traditional IT applications to bespoke embedded device applications and more custom HMI or Historian control applications.

There is no privilege separation in embedded OS for example VxWorks embedded OS used in field devices provides minimum memory protection.
Buffer overflow attacks are possible in bespoke applications mainly through workstations similar to standard IT systems or in industrial control automation software such as historian servers. In addition, field devices themselves that rely on real time operating systems (RTOS), are more susceptible to memory challenges by exploiting the fixed memory allocation time requirement in RTOS system. SCADA components especially in legacy networks are subject to accumulated memory fragmentation which can lead to programs stalling. Structured Query Language (SQL) is widely used to store sensor information in historians and other databases thus, if not designed properly at application level the systems are susceptible to SQL injection attacks [12].
Whilst these types of attacks are also prevalent in enterprise IT systems, and indeed some of the SCADA environments are inheriting the vulnerabilities from enterprise applications it is worth reiterating that the implementation in these environments in very different. Thus, a forensic framework for SCADA must consider the requirements of this operating environment carefully. We establish some of these particular requirements in the following section.

III. CYBER FORENSICS IN INDUSTRIAL CONTROL SYSTEMS

Computer forensics is the practice of collecting, analyzing and reporting on digital information in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally [13]. “Traditional digital forensics is performed through static analysis of data preserved on permanent storage media. Not all data needed to understand the state of [an] examined system exists in non-volatile memory. Live analysis uses [the] running system to obtain volatile data for deeper understanding of events going on” [14]. As discussed the first problem in achieving cyber forensics for SCADA systems is that such systems are critical and cannot generally be powered off for acquisition. Additionally it is more likely that the information is generally volatile and any forensic evidence would potentially be lost if the device was powered off or interrupted. This remainder of this section looks at existing perspectives on SCADA forensics as well as the main differences between SCADA and enterprise forensics.

3.1. Existing Perspectives

SCADA and ICS forensics is slowly emerging as a key forensic topic within the cyber world. Although this has been a developing subject for a number of years, the release of the Stuxnet virus in 2010 seemed to have dramatically increased the awareness of such critical systems and their vulnerabilities, and quickly began to make people aware of the issues surrounding cyber security of ICS. It is apparent that much more work and research needs to be completed in order to secure such systems and to migrate existing best forensic practices to ICS systems.
Van der Knijff [15] states that “Immature IT security, increasing network connectivity and unwavering media attention is causing an increase in the number of control system cyber security incidents. For forensic examinations in these environments, knowledge and skills are needed in the field of hardware, networks and data analysis”. This provides a

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 3, March 2020

very concise description regarding attacks against SCADA systems and the forensic specialties that are required to conduct a forensic investigation post incident. Ahmed et. al. [16] suggest that "today, the reliability of many SCADA systems is not only dependent on safety, but also on security. The recent attacks against SCADA systems by sophisticated malware (such as Stuxnet and Flame) demands forensic investigation to understand the cause and effects of the intrusion on such systems so that their cyber defense can be improved. Not just this, but when the news of unleashing the cyber dogs [17] to attack enemies is prevalent, forensic practice becomes essential to find the traces of an attack and gather evidence against the entity that has tried to sabotage the critical infrastructure of a country." [16] This shows that a major concern in the forensic analysis of SCADA systems is the aspect of attribution which means more emphasis is placed on the identification of a perpetrator, rather than the gathering of evidence in support of an already established prosecution/defencecase.

3.2 Traditional Digital Forensics SCADA

Computer forensics analysis and acquisition can generally be categorized as static (static data - generally stored within a file-system that is not active e.g. a powered off HDD), and volatile/live (data that is currently in use by an active piece of hardware e.g.RAM). Live data is aptly referred to as volatile data as it is constantly changing, however, if captured and analysed, it can often provide an analyst with very useful information. For SCADA forensics it is necessary to look at both forms of computer forensics and in various situations, as each will provide interesting and unique evidence. This is a much more complicated process for a SCADA environment, as live data acquisition would be a priority and it would not necessarily be possible to take a system offline just for the purpose of undertaking a cyber investigation. Many of the commercially available tools will not recover artifacts of interest from control devices without additional plug-ins, development, or configurations. Thus, a forensic toolkit for SCADA should be developed and preconfigured in order to respond to any reported incidents. As the systems contain largely volatile data and are 'live' environments a new adaptation of traditional forensic processes is required.

IV.FORENSICMETHODOLOGY

A forensic methodology for SCADA systems has previously been proposed by Wu et al [20] and therefore we explore this approach with a view of developing a forensics toolkit to support this methodology. This forensics methodology for SCADA extends and modifies the existing approach to ensure that the requirements of control systems are explicitly considered. The process draws on both incident response models and cyber forensics models and can be seen in figure 3.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 3, March 2020

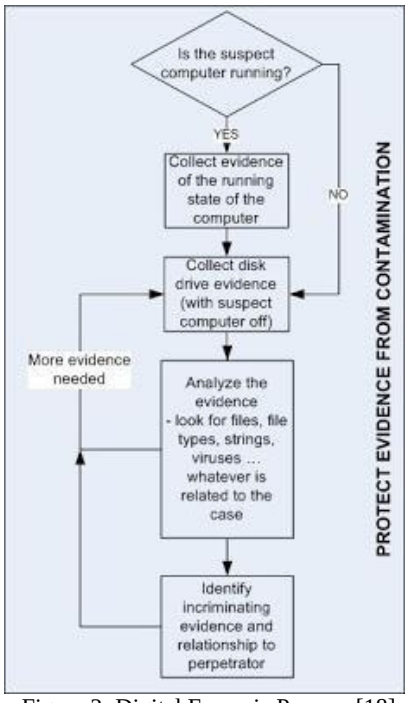

Figure 2: Digital Forensic Process [18].

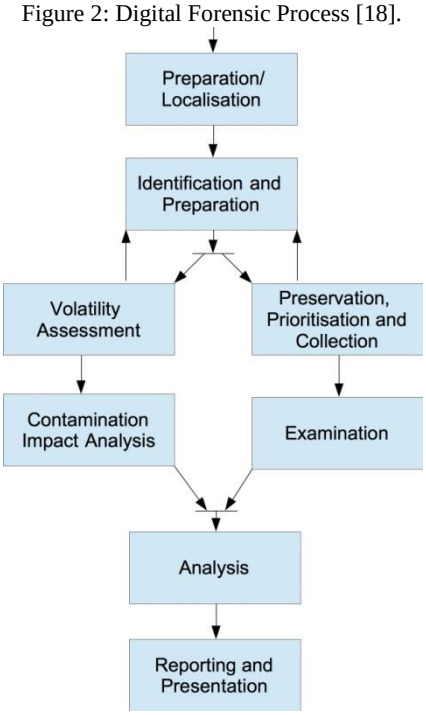

Figure 3: SCADA Incident Response and Forensic Process

- Phase 1- Identification and Preparation: Identify the potential sources of evidence, including the systems, the network and connected devices.
- Phase 2- Identifying data sources: Identify the type of systems to be investigated including; operating system,

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 3, March 2020

manufacturer, serial numbers and model of PLCs, and network design and implementation

- Phase 3- Volatility Assessment, Contamination Impact Analysis and Preservation, Prioritizing and Collection: Assess the volatility of the identified resource immediately after identification in order to drive the priority list used in Preservation, Prioritization and Collection. Document the level of volatility and the impact on the reproducibility of the investigation results. Ensure highly volatile data is forensically captured and stored to maintain integrity. Assess the impact of volatile data capture on the safety and operation and identify what is the impact of the volatility on the harvesting and analysis of other volatile data items with lower priority of the SCADA system. Collect all potential evidence from the systems that are suspected to be part of the SCADA system being investigated. It is critical that volatile and dynamic information across various network cards and controller units be prioritized to prevent any loss of data. Network traffic is also captured to discover anomalous traffic.

- Phase 4- Examination: Forensic examination of collected evidence by specialist trained forensic examiners is an important part of the process with the goal to provide answers to questions raised before the investigation. For SCADA this examination should also include engineering representatives familiar with the operation of the system.

- Phase 5- Analysis: Finding relationships between the recovered forensic artifacts and piecing the evidential data together to develop a timeline of the incident and its impact on the control environments.

- Phase 6- Reporting and Presentation: Compilation of finding sand analysis in to a report(s) for management. This should include recommendations for engineers and consider carefully the requirements and operation of a SCADA environment.

- Phase 7 Reviewing results: For clarity the results and findings should be reviewed to ensure validation and that all forensic ‘chain of custody’ for information has been met.

V.DEVELOPING AFORENSIC TOOLKIT FORICS

Following on from the methodology,
Imaging/Acquisition of data Analysis of acquired data Forensic Reporting of findings
In addition, during a traditional forensic investigation the specialist may also require additional tools dependant on what data was present on the devices. For example: email parsing, mobile device analysis, image parsing, encryption, data carving, etc.
Forensic Toolkit for SCADA/ICS
To create a forensic toolkit for a SCADA/ICS investigation, it is necessary to separate the tools and requirements based upon a number of steps in the SCADA forensic methodology. The most prevalent requiring toolkit use are:
Hardware:

- Write blockers – for Engineering systems, workstations, HMI hosts, database servers, any other compatible device that may have been connected to the SCADA network. – used to capture ‘static’ data from compatible powered offdevices.

- Firewire PCI Card - for Engineering systems, workstations, HMI hosts, database servers (whilst running) – used to capture volatile memory data. Caution should be taken as this process may cause crashes to the control system if not used appropriately.

- A HD camera – extremely useful for taking photos and documenting your data collection process. Particularly useful when capturing volatile data in order to evidentially document monitor layout, desk layout, any changes to thesystem.

Software:

- Bespoke PLC flashing software – this will be vendor specific to the PLC/RTU which is used to issue commands to the PLC in order to attempt to dump any volatile data from it. This may not be a forensically sound practice and may make the investigation void however, would support rapid incident response initiatives when required.

- FTK Imager - This software is used to acquire data in a forensically sound manner from a compatible operating system. This will be used for the HMI, engineering workstations, OPC and database servers. The software can handle

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 3, March 2020

static and live data but is required to be installed on the target device.

- EnCase– Similarly to FTK Imager this software is used to acquire data in a forensically sound manner from a compatible operating system. This will be used for the HMI, engineering workstations, OPC and database servers for static and live data.

- Helix – A bootable application used to acquire data in a forensically sound manner, including live data. This will be used to capture volatile data from the HMI, engineering workstations, OPC and database servers.

- TCP Dump–used on the SCADA network to capture and dump network data post incident. This may not be useful if all traces of an incident have since passed, however certain indicators of an attack may be still be present. E.g. existing data exhilaration, anomalous activity, etc. It will be useful to capture any SCADA specific protocols such as Modbus, any associated data, such as data payloads or function codes for the PLC devices.

Examination and Analysis

Due to the often complex nature of a SCADA/ICS system the examination and analysis section relies heavily on the examiners notes and 'reconnaissance' of the system/network during phase 1 and 2 (Identification and preparation, and Identifying data sources). At this stage there will be a significant amount of varied data to process and examine. A detailed understanding of the network itself and the configuration of the devices would be extremely useful. The tools included in this section relate to processing, examining and analyzing the captured data:

Hardware:

- High specification forensic computers - capable of processing large amounts of data quickly and efficiently, with multiple connection points to access the captured data.

- Volatility – a live data processing tool to be used on the acquired live data from the HMI, OPC, engineering workstations, database servers, etc. This can be configured for finding interesting information within the captured memory data. This includes running processes, dlls, command line commands, and tcp binding information, etc. It would be useful to highlight any SCADA specific modules located within the RAM that may be targeting the communication devices or even the field devices via the HMI (for example).

- Alien Vault– this is a security management system with integrated forensics and SIEM (security incident events management). This system can parse captured network data, and has a number of integrated processing functions such as Snort (an open source intrusion prevention system). The built in features of Alien Vault allow the analyst to create and run ICS/SCADA related rules

when such rules are met. The user can create their own rules and security events to be monitored. This could be pre-configured to contain all known SCADA attacks to allow for efficient identification within network data.

This list is in no way comprehensive; however it should provide a basic toolkit for the capture and analysis of SCADA/ICS systems. It is important to understand the bigger picture with regards to a forensic investigation against an ICS system. All manner of attached devices could potentially hold key forensic evidence. It is important to be able to understand how these systems function and what information you may be able to capture, without system downtime.

VI.CONCLUSIONS

With the increased interest in the security of Industrial Control Systems / SCADA there is a need for improvements in incident response and cyber forensics to support the investigation into the increasing number and complexity of cyber tacks targeting these systems. In this paper we have described the implementation of a cyber forensics methodology specifically considering the requirements of SCADA systems and have gone on to make recommendations for a forensics toolkit for use in such environments. In order to achieve this we have considered carefully the vulnerabilities and threats that exist within SCADA environments and the unique requirements that exist in operations in this domain, above and beyond traditional enterprise IT cyber forensics. The C.Nagarajan et al [15-17] have previously discussed a phased methodology to follow when conducting a forensic investigation on an industrial control system. This paper follows that proposed methodology and provides an example use of the specified toolkit in each of the respective phases. The contribution of this paper is the careful consideration of implementation and operation with regards to

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 3, March 2020

incident handling utilizing the cyber forensics methodology. A number of existing and bespoke tools can be used to create a forensics toolkit ready to equip operators to better respond to cyber events. Whilst a number of difficulties remain with such an investigation, including: volatile data, bespoke architecture for SCADA field devices and data forensic verification, this paper provides a continued methodological approach highlighting that a full forensic investigation of an ICS system can take place within each part of the system (e.g. PLC, RTU, HMI, Network data, database servers, engineering work stations, etc). It is shown that a number of existing tools are suitable for elements of a SCADA forensic investigation, however, more evidence and artifacts may be discoverable as the maturity of this field develops.

VII. FUTURE RESEARCH

Whilst we continue to make progress toward methods and tools for undertaking a cyber forensic investigation in SCADA systems there are still a number of key areas that must be addressed in future research. Firstly capturing volatile data from PLC's is still a fine-art and ensuring continued operations whilst the capture is ongoing has only been possible on a limited number of controllers within laboratory conditions. New methods and tools should be considered for the recovery of memory and processes from a live controller (e.g. PLC, RTU). Additionally the controller's logic (ladder logic), variables, and timers are critical artefacts in determining functional changes in a system. Whilst recovery for this information is possible it is often complex to correlate and timestamp and should be processed carefully as part of an investigation. Thus, verification of volatile forensic data is an extremely prevalent topic within forensics. Live data is constantly changing and so to verify the acquired data is very difficult. This is an area particularly for SCADA forensics that needs further research.

To recover the required information, development of PLC/RTU specific forensic software that can identify and provide RAM acquisitions of the common field devices (e.g. Siemens, Schneider, etc.) is required. This is complex as architectures are vendor specific and each vendor has bespoke software for their developed devices. Further work needs to be completed with vendors on writing such software. This paper has focused on the technical element of incident response and cyber forensics in the implementation of a cyber forensics methodology however, it is noted that SCADA operators also require the organizational and procedural means to enable a cyber forensics investigation. This is often due to the need for operations to meet safety and/or economic objectives and much of the volatile "live data" sources will be replaced before an investigation can even begin. Therefore we will continue to explore organizational and systems architecture approaches to ensure that the requirements of operation and investigation can both be met.

REFERENCES

[1] M.J. Schwartz (2014) Target Breach: HVAC Contractor Systems Investigated
[2] SCADAhacker.com (2014) SCADA/ICS Vulnerability Reference . Website
[3] Digital Bond (2014) Vulnerability Notes.Website
[4] Symantec (year unknown) Vulnerability Trends-
[5] SCADA Vulnerabilities.Website
[6] G. Hale (2011) More SCADA VulnerabilitiesFound.
[7] Industrial Safety and Security Source.Weblog
[8] Schneider Electric (year unknown) Support - Vulnerabilities.
[9] Zhu, A. Joseph, and S. Sastry (2011) A taxonomy of cyber attacks on scada systems," in Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, ITHINGSCPSCOM '11, Washington, DC, USA, pp. 380-388, IEEE ComputerSociety.
[10] Forensic Control (2014) Introduction to computer forensics. Website
[11] S. Mrdovic, A. Huseinovic, & E. Zajko (2009) Combining static and live digital forensic analysis in virtual environment. In proceedings of the 2009 International Conference on Advanced Technology (ICAT). Bosnia. 29-31 Oct.2009.
[12] Ahmed, S. Obermeier, M. Naedele& Golden G. Richard III (2012) SCADA Systems: Challenges for Forensic Investigators, in Computer - IEEE. 5 (12), pp. 44-51.
[13] J. Giles (2010) Are states unleashing the dogs of cyber war? [Online]. Website.
[14] Information Security Short Takes (2008) Computer forensics process. Tutorial - Computer Forensics Process for [sic]Beginners.Website.
[15] C.Nagarajan, M.Muruganandam and D.Ramasubramanian – 'Analysis and Design of CLL Resonant Converter for Solar Panel - Battery systems- International Journal of Intelligent systems and Applications (IJISA), Vol.5 (1),pp.52-58, 2013.
[16] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 3, March 2020

Techniques'- *Electric Power Components and Systems*, Vol.39 (8), pp.780-793, May 2011

[17] K Umadevi, C Nagarajan, "High Gain Ratio Boost-Fly Back DC-DC Converter using Capacitor Coupling", 2018 Conference on Emerging Devices and Smart Systems (ICEDSS), 2nd and 3rd March 2018, organized by mahendra Engineering College, Mallasamudram, PP. 64-66,2018