GROUP No: 12

Project Title: The system include each components of SCADA operation is to be monitored using artificial intelligence method and machine learning algorithm for reconnaissance process for collecting and analyzing data coming from scada operations

Members:

Ayush Shah, Gurkirat Sarabjeet Singh Nagpal, Atharva Marathe and Sarvesh Yenarkar

Contents:

1) Introduction and Abstract... (2)

2) Cyber Forensics in Industrial Control Systems...............(4)

3) Project Requirements.. (5)

4) Functional Architecture.. (7)

5) Subsystem Description.. (10)

6) Project Management... (17)

7) References... (19)

01) Introduction and Abstract:

Control system security is the practice of using security methods to prevent intentional or unintentional interference with the operation of industrial automation and control systems. These control systems manage the production or use of electricity, petroleum, water, transportation, and many other services This Industrial Control System (ICS) contains a few underlying technologies and approaches, all of which function and report information in different ways–and over different geographic distances.

SCADA (Supervisory Control and Data Acquisition) is mainly used in Industrial Control Systems (ICS) in order to remotely collect real time data to automate and control networked equipment such as Programmable Logic Controllers (PLC). SCADA/ICS systems are used to support and monitor the types of critical infrastructures that serve as pillars for many industrialized areas, such as municipal services, oil, and other types of large-scale energy industries.

The significance of SCADA system is based on the data acquired from a remote location in order to control the environment conditions. For instance, SCADA collects data regarding where the leaks have occurred in a pipeline infrastructure.

The SCADA system analyzes the real-time data and alerts the system about the detection of such incident. In the earlier design of the SCADA, it did not require internet connection therefore the system was isolated from the public network. In recent years, the system evolved with the technology and SCADA started to use the public network and become exposed to possible cyber-attacks.

SCADA/ICS have achieved rapid growth within the competitive technology market as well. As a result, it has encountered serious security problems. Possible intrusion attacks may cause not only the financial loses, it may also be endangerment of public safety. Hence, security methods are needed to secure ICS from such targeted attacks. The information security vulnerabilities of ICS have been studied extensively, and the vulnerable nature of these systems is well known. However, in the case of a security incident (e.g. IP flooding attack), it is important to understand what are the digital forensics consequences of such attack? What procedures or protocols are needed to be used during an investigation? What tools and techniques are appropriate to use by the investigator? Where can forensic data be collected and how? In this area, there is a serious gap in the literature as forensic attack analysis is commonly guided by experience and by intuition rather than by a systematic or scientific process. Therefore, we would like to close this gap in this study by performing specific attacks and presenting our observations in the system.

Abstract:

Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS) have achieved rapid growth within the competitive technology market. As a result, it has encountered serious security problems. Hence, security methods are needed to secure ICS from targeted attacks.

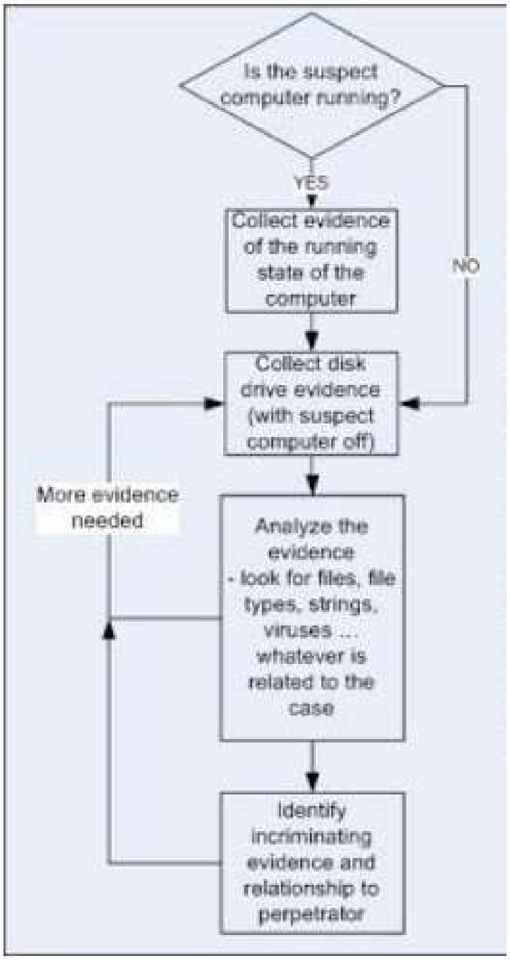
The information security vulnerabilities of ICS have been studied extensively, and the vulnerable nature of these systems is well-known. However, in the case of a security incident (e.g. system failure, security breach, or denial of service attack), it is important to understand what the digital forensics consequences of such incidents are, what procedures or protocols are needed to be used during an investigation, what tools and techniques are appropriate to be used by an investigator, and where the forensic data can be collected from and how.

Taking into these questions consideration, there is a serious gap in the literature as forensic attack analysis is commonly guided by experience and by intuition rather than by a systematic or scientific process. Therefore, in this study, we aim to close this gap by developing fairly complex SCADA/ICS laboratory at any Industry level Architecture.

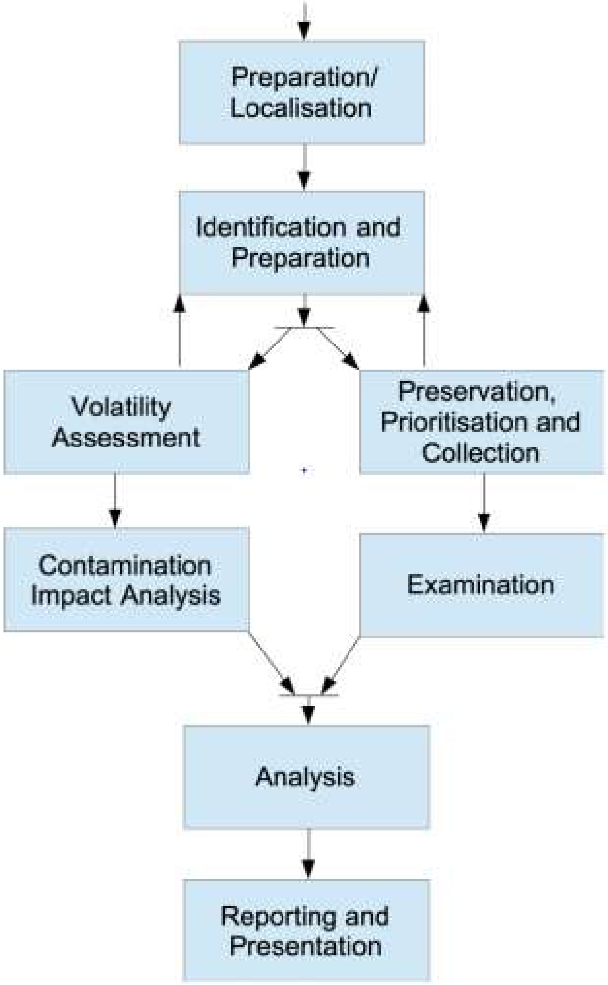
Industrial Control Systems (ICS) are used worldwide in critical infrastructures. An ICS system can be a single embedded system working stand-alone for controlling a simple process or ICS can also be a very complex Distributed Control System (DCS) connected to Supervisory Control and Data Acquisition (SCADA) system(s) in a nuclear power plant. Although ICS are widely used today, there are very little research on the forensic acquisition and analyze ICS's artefacts. In this paper we present a case study of forensics in ICS where we describe a method of safeguarding important volatile artefacts from an embedded industrial control system and several other sources.

02) 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.


Is the suspect computer running?
YES
NO
Collect evidence of the running state of the computer
Collect disk drive evidence (with suspect computer off)
More evidence needed
Analyze the evidence - look for files, file types, strings, viruses ... whatever is related to the case
Identify incriminating evidence and relationship to perpetrator

Digital Forensic process


Preparation/ Localisation
Identification and Preparation
Volatility Assessment
Preservation, Prioritisation and Collection
Contamination Impact Analysis
Examination
Analysis
Reporting and Presentation

SCADA incident response and Forensic Process

03) Project Requirements

The following requirements are derived from an objectives tree by taking in consideration the mission goals and expectations. The requirements will be categorized as mandatory and desirable requirements. These categories are further divided and the requirements are classified as performance requirements which are functional requirements with an associated performance measure and non-functional requirements.

3.1 Mandatory Performance Requirements

M.P.1 Phase 1- Identification and Preparation: Identify the potential sources of evidence, including the systems, the network and connected devices.

M.P.2 Phase 2- Identifying data sources: Identify the type of systems to be investigated including; operating system, manufacturer, serial numbers and model of PLCs, and network design and implementation

M.P.3 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.

M.P.4 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

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

M.P.6 Phase 6- Reporting and Presentation: Compilation of findings and analysis into a report(s) for management. This should include recommendations for engineers and consider carefully the requirements and operation of a SCADA environment

M.P.7 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.

3.2 Mandatory Non-Performance Requirements

The Network shall:

M.N.1 Operate using hardware that meets the specification of overall system.

M.N.2Operate within a windows operating system environment

M.N.3 be compatible with different type of intrusions possible to your SCADA systems.

M.N.4 Operate normally when any major risk is experienced by the system.

In addition to the mandatory performance and non-functional requirements, we have also identified certain desirable requirements. These additions are nice to have and extend the project scope in exchange for having a more robust, reliable and valuable system. The desirable requirements are formulated to extract the greatest amount of information even when operating under different conditions.

3.3 Desirable Performance requirements

D.P.1 Developing a forensic Toolkit:

1) Imaging/Acquisition of data

2) Analysis of acquired data

3) Forensic Reporting of findings

D.P.2 Preservation, prioritizing and collection

1) As described by Wu et al [20] "The procedure for collecting from data sources on the SCADA system depends on the volatility of data". This is a key area for investigation as the data sources will provide a mixture of live and static data vital to the artefact discovery of the investigation

3.4 Desirable Non-Performance requirements

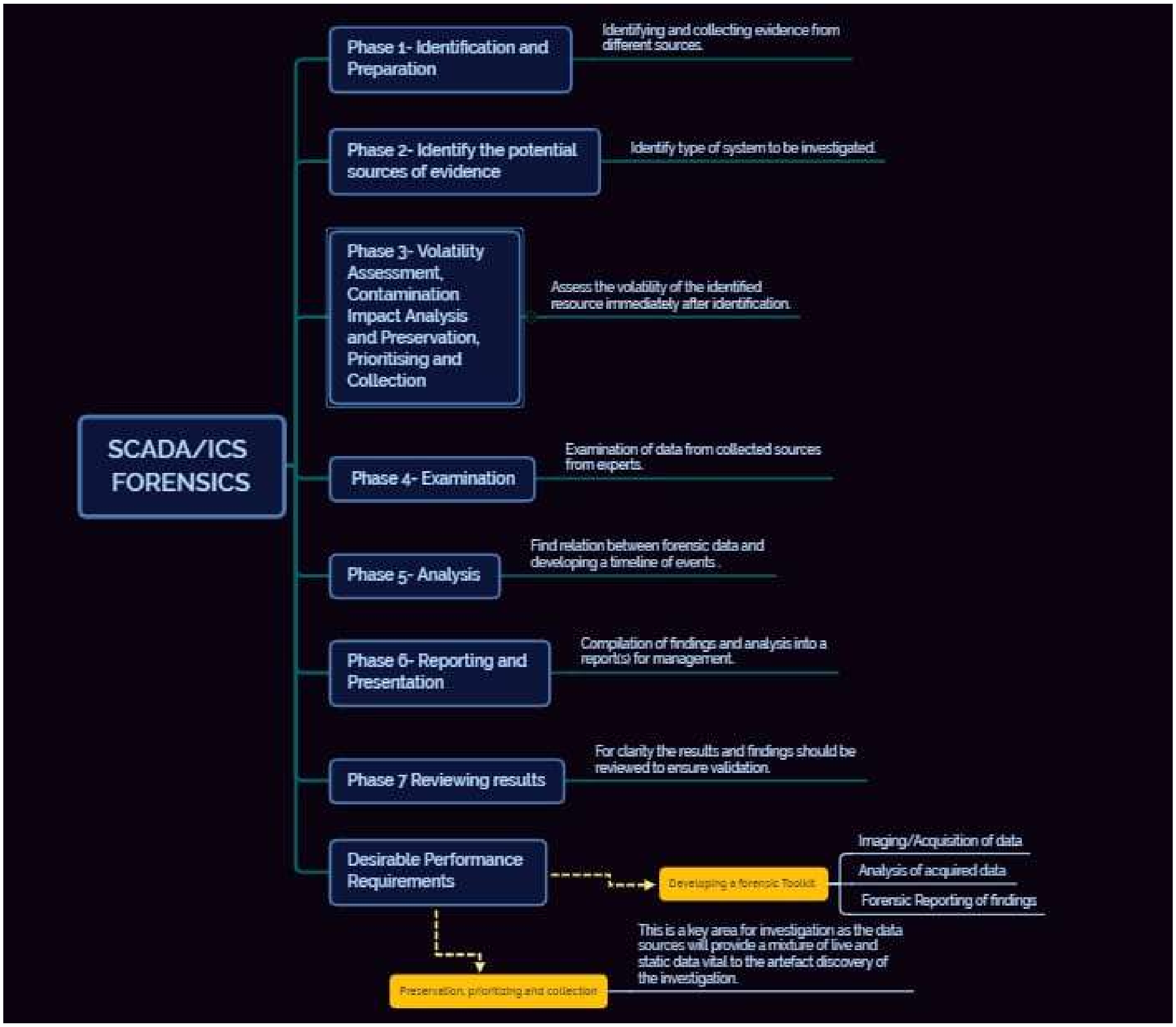
D.N.1 Checking over the parameters of the SCADA systems during an intrusion to the system.

D.N.2 Operate over various types of intrusions.

04) Functional Architecture

The architecture outlined below shows the functions that the system must execute to fulfill the previously mentioned requirements. The functions are derived assuming we have already have the image we want to complete or implanting.

The main functions of Cyber Forensics on SCADA/ICS Systems:


SCADA/ICS FORENSICS
Phase 1- Identification and Preparation
Identifying and collecting evidence from different sources.
Phase 2- Identify the potential sources of evidence
Identify type of system to be investigated.
Phase 3- Volatility Assessment, Contamination Impact Analysis and Preservation, Prioritising and Collection
Assess the volatility of the identified resource immediately after identification.
Phase 4- Examination
Examination of data from collected sources from experts.
Phase 5- Analysis
Find relation between forensic data and developing a timeline of events.
Phase 6- Reporting and Presentation
Compilation of findings and analysis into a report(s) for management.
Phase 7 Reviewing results
For clarity the results and findings should be reviewed to ensure validation.
Desirable Performance Requirements
Developing a forensic Toolkit
Imaging/Acquisition of data
Analysis of acquired data
Forensic Reporting of findings
Preservation, prioritizing and collection
This is a key area for investigation as the data sources will provide a mixture of live and static data vital to the artefact discovery of the investigation.

1) Identification and Preparation:

Identify the potential sources of evidence, including the systems, the network and connected devices.

For example in an oil/gas plant the PLC connected to a pressure sensor or in an electric substation Plc connected to a relay might start disfunctioning or the network systems such as IP/ARP or MAC address might have been affected.

2) Identifying data sources:

Identify the type of systems to be investigated including; operating system, manufacturer, serial numbers and model of PLCs, and network design and implementation.

A factory can be divided into two parts control center and field sites.

Field sites contain PLCs connected to various sensor which send data via WAN to control center. The control center consists of various network components as well as servers, Main Terminal Unit and historian (a database).

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.

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.

Forensic examination usually involves which includes whether the attack was at network level or at device level. Network level includes MITM and Reconnaissance whereas at device level the attack happens on firmware resulting in denial of service.

5) Analysis:

Finding relationships between the recovered forensic artefacts and piecing the evidential data together to develop a timeline of the incident and its impact on the control environments.

This involves steps such as logging the PLC by tracking the values at specific memory addresses and noting down the time.

6) Reporting and Presentation:

Compilation of findings and analysis into a report(s) for management. This should include recommendations for engineers and consider carefully the requirements and operation of a SCADA environment.

The details of attack, type and damage is analyzed by digital forensic experts in industrial control systems and SCADA.

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.

The end report is prepared and accordingly future course of action is decided.

8) Developing a forensic Toolkit:

1) Imaging/Acquisition of data: An UI can be built which will be configured with all types of components such as PLC, networking components and workstations.

Data can be acquired by data logging methods.

2) Analysis of acquired data: Analysis can be performed to detect the type of attack.

3) Forensic Reporting of findings: By comparing values at different timestamps the report will be prepared by forensic investigators.

9) Preservation, prioritizing and collection:

The procedure for collecting from data sources on the SCADA system depends on the volatility of data. This is a key area for investigation as the data sources will provide a mixture of live and static data vital to the artefact discovery of the investigation

05) SUBSYSTEMS DESCRIPTIONS:

1) Vulnerability and Typical Attacks of SCADA/ICS Systems

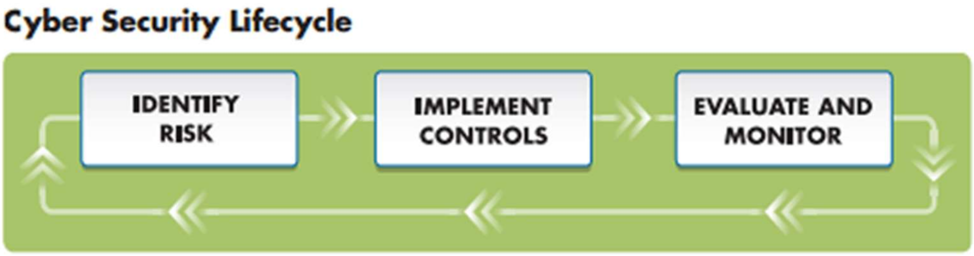
When SCADA systems were originally designed they were isolated from the network and engineers focused on providing availability of data and operations rather than confidentiality and integrity. This isolation is commonly referred to as an “air-gap”, and while originally designed as a complete physical 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, SCADA systems 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 mainstream Business IT environments.

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. Specific vulnerabilities of control devices is beyond the scope of this paper but are well documented.

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 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 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.

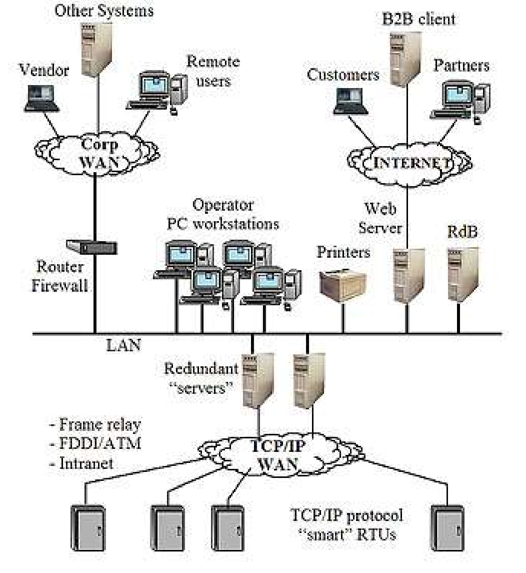
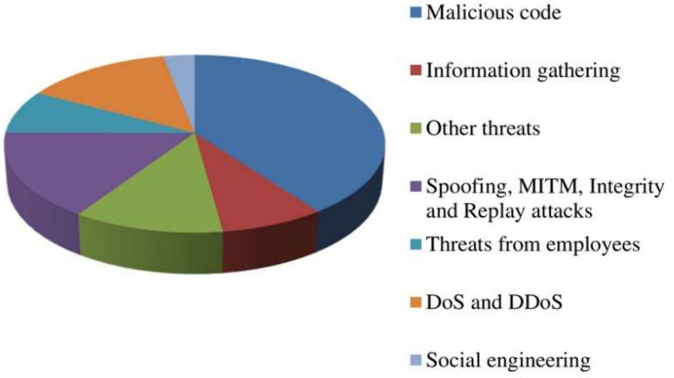
There is no privilege separation in embedded OS for example VxWorks embedded OS used in field devices provides minimum memory protection.

1) 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.

2) SCADA components especially in legacy networks are subject to accumulated memory fragmentation which can lead to programs stalling.

3) 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.

 Other Systems B2B client Vendor Remote users Customers Partners Corp WAN INTERNET Operator PC workstations Web Server RdB Printers Router Firewall LAN Redundant "servers" - Frame relay - FDDI/ATM - Intranet TCP/IP WAN TCP/IP protocol "smart" RTUs Figure 1.1 – SCADA architecture in the 2000's	
Vulnerability of Scada/ICS systems	Attacks Comparison on Scada Systems

2) ICS Forensics

2.1 ICS Forensic Challenges

Forensic acquisition tools are widely available for conventional ICT systems like hard disks, volatile memory (RAM) and common consumer electronics like mobile phones and navigations systems. Similar tools do not exist for most ICS devices. Besides, in ICS systems, safety is the main goal rather than Security. If ICT people talk about Security and Safety in ICT systems they do mean:

- Firewalls to prevent hackers from entering the system since confidential information must be protected.
- Antivirus and Antimalware for protecting the users and the systems against viruses.
- Anti-spam to protect the users against spam in their mail. However, If ICS people talk about Security and Safety in ICS systems they do mean:
- Protect the system against dangerous issues like wrong values in PLC's.
- Flow control and temperature sensors in the chemical plant.
- Voltage and current control in electrical grid installations.

Not only the other interpretation or different jargon can be an issue, also the difference between ICT people who are working mainly in the office or data centers and the ICS people working on the field inside the plant or control room. There is a big gap between the two different departments; other goals and other problems are creating completely different priorities on a daily base.

2.2 ICS Forensic Process

The purpose of our approach is to safeguard the important information from the ICS system. Depending if we talk about a running system which is still intact and connected to other devices like a distributed control system, or if we talk about a standalone control system like a single PLC or a post mortem investigation after a big incident like a fire or explosion in a chemical plant, several information sources are available to acquire important digital evidence for digital forensic investigation purposes. For this reason we have to setup an ICS Forensic process. Inside this process, we split up the information from two different sources:

- Network data
- Device data

Network data acquisition: For network data acquisition network investigation (depending on our investigation) we have to decide on what level (or levels) we need to analyze the network traffic. Network Levels: A typical distributed ICS system has at least three different levels of network types:

- Device level such as sensor, programmable logic controller (PLC), actuator.
- Cell Level that irresponsible to control the device controllers.
- Plant Level that is responsible to control the cell controllers.

Beside, network data can also be historical information like backup files, logging databases etc. Sources of network data can be listed as:

- Live Network Data (raw network data, Arp tables, flow records, etc.)
- Historical Network Data (host based logs, database queries, firewall-logs, etc.)
- Other Log Files (backup archives, access point logs, historians, etc.)

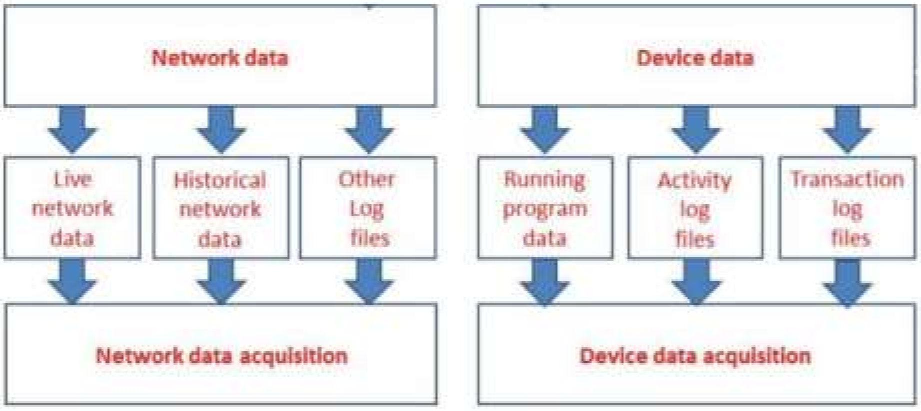


Fig.1 ICS Forensic process

Not all tools or methods are safe to use in ICS environments. ICS systems often monitor or control processes in which a failure may have disastrous consequences (or may be otherwise very undesirable). For this reason active probing (like scanning for open ports and then opening arbitrary TCP connections) should generally be avoided.

Device data acquisition:

Device data acquisition forensic tools do not exist for most ICS devices. Product specific service tools for programming a PLC, saving the program and servicing log files from a PLC to a service computer do exist. The question is can we use those service tools in a forensic matter to save important data from the PLC for later analyses? The sources of device data can be listed as:

- Running Program Data such as RAM dump, CHIP images, Memory cards…
- Activity Log Files such as RAM dump, active processes, control room logs, etc.
- Transaction Log Files such as Serial communication logs, Error logs, Event logs, etc.)

2.3) SCADA DIGITAL FORENSIC PROCESS

Digital forensics is an important part of an incident response strategy in an IT forensic investigation following an incident and will provide an effective response in a forensic manner Imtiaz (2006).There are several steps to conduct a digital forensic investigation with basic steps being; preservation, identification, extraction and documentation of digital evidence. The purpose of the digital forensic process model is to demonstrate in the court of law that the evidence has been collected in the correct manner and following legal procedures with scientific backing.

Currently a SCADA forensics model identified by Radvanovsky and Brodsky (2013) has the following investigative steps:

Step 1 Examination

Identify the potential sources of evidence, including the systems, the network and connected devices. In addition to these sources an investigation should examine other systems that have a relationship to the SCADA system such as access terminals, servers and routers.

Step 2 Identification

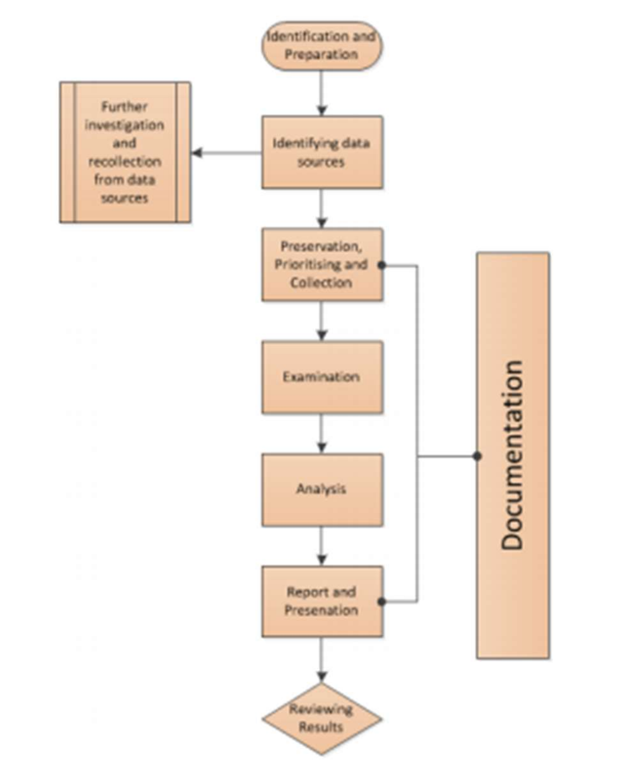
Identify the type of systems to be investigated, this includes operating system, the manufacturer including the serial numbers and model types of PLCs, the network design and implementation. Once the operating system has been identified it is important to note a system could be running more than one operating system such as a Linux variant. Many SCADA systems run a child system over a base OS. During the identification process several areas can assist, including manufacturer's documentation, design specifications, network diagrams, and the HMI (Human Machine Interface).

Step 3- Collection

Collect potential evidence from the memory 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 collected first to prevent any loss of data from network connections. Network traffic is also captured to discover anomalous traffic.

Step 4- Documentation

In this step it is critical to keep accurate documentation of the investigation to ensure chain of custody. Records need to be kept of potential evidence as well as case numbers and the time when the evidence was collected. Many investigators will photograph the entire investigation process including the systems that could be connected to the SCADA system or that are presently connected, to ensure that the examiner will be able reconnect them if needed later. A detailed report would need to be produced of the whole digital forensic process to include the captured system throughout the collection process. The last stage is to gather all the information together and store in a secure and safe location.


Identification and Preparation
Further investigation and recollection from data sources
Identifying data sources
Preservation, Prioritising and Collection
Examination
Analysis
Report and Presenation
Reviewing Results
Documentation

SCADA FORENSIC SYSTEM

Part 05: Importance

The importance of SCADA systems is automation. It allows an organization to carefully study and anticipate the optimal response to measured conditions and execute those responses automatically every time. Relying on precise machine control for monitoring equipment and processes virtually eliminates human error. More importantly, it automates common, tedious, routine tasks once performed by a human, which further increases productivity, improves management of critical machine failure in real-time, and minimizes the possibility of controllable environmental disasters.

In addition, SCADA systems are needed to monitor and control a large geographical displacement where an organization may not have enough manpower to cover. Thus, reliable communication and operability of these areas or sites is critical to profitability.

SCADA monitors and controls entire sites and systems spread out over large geographic areas. You know how your sites and systems are performing remotely, 24/7.

- LESS TIME SPENT BEHIND THE WINDSHIELD TRAVELING FOR SYSTEMATIC SITE VISITS.
- LESS FUEL
- LESS DEPRECIATION
- MORE TIME TO BE PRODUCTIVE!

SCADA systems can alert you of changes in your system, tell-tale signs that something is about to fail in your system.

06) Project Management

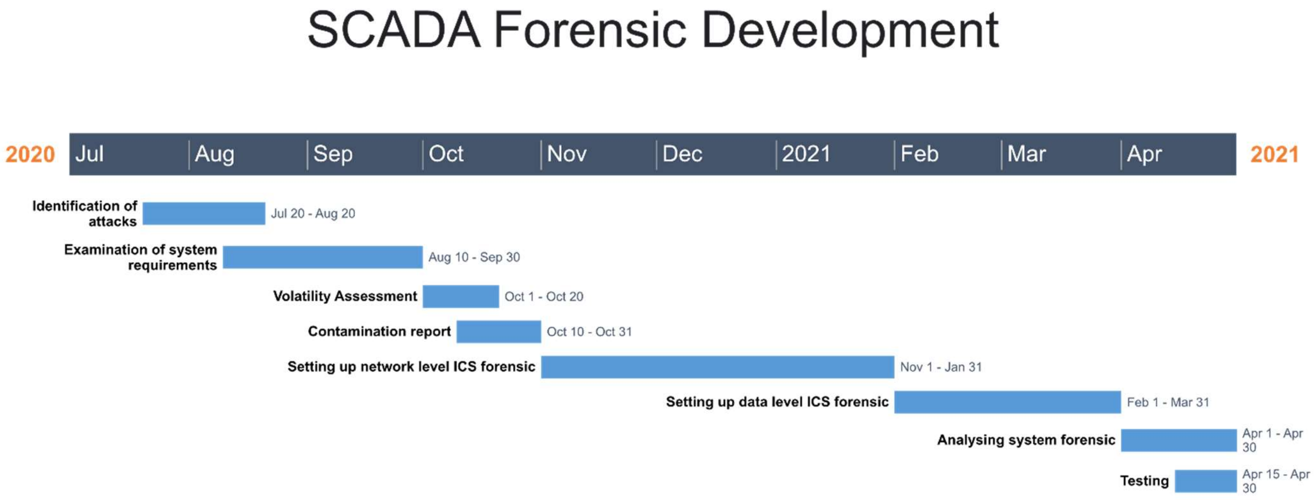
01)Work Plan and Tasks:

The majority of the work required for this project is software based. Our approach will be to focus on identifying all possible threats by typical attacks on SCADA system, examining other systems that have a relationship to the SCADA system such as access terminals servers and routers, identify the operating system, tackling these attacks independently in the odd semester, and then integrating a defence mechanism to tackle all 3- Hardware, software and communication stack attacks together in even semester. Our work plan reflects project management throughout the year.

WORK PLAN		
Identification and Examination	1.1	Identify the type of attacks possible on SCADA system and the layer it affects.
	1.2	Identify the potential sources of evidence, including the systems, the network and connected devices.
	1.3	Examine other systems that have a relationship to the SCADA system such as access terminals, Servers and routers.
	1.4	Examining the type of systems to be investigated, this includes operating system, etc.
Volatility Assessment, Contamination Impact Analysis and Preservation, Prioritising and Collection	2.1	Assess the volatility of the identified resource
	2.2	Building and imaging the contamination impact report
	2.3	Integrating a collection of hardware, software, communication stack based attacks
	2.4	Setting up priority mechanism
Setting Network level ICS Forensic process	3.1	Step-by-step procedure for forensic analysis including creating environment

		scanning for anomaly detection
	3.2	Production and replay for each vulnerability is performed
	3.3	Each vulnerability is analysed, resulting in the creation of an IDS rule set.
	3.4	Testing of each rule set is performed.
Setting Device level ICS Forensic process	4.1	Acquisition of data from suspicious PLCs
	4.2	Analysis of the data acquired
Analysis	5.1	Finding relationships between the recovered forensic artefacts
	5.2	Create timeline of the incidents and its impact on control environment
Testing and Reviewing results	6.1	Testing the system in its integrated form
	6.2	Reviewing each mechanism

02) Work Schedule GNATT CHART:



07) References:

1) E. Byres. (2012) Securing SCADA systems from APTs like Flame and Stuxnet – Part 1. Tofino Security. Weblog.
2) Detecting Anomalous Behavior of PLC using Semi-supervised Machine Learning by Ken Yau, KP Chow, SM Yiu, CF Chan Department of Computer Science The University of Hong Kong Hong Kong, China
3) Digital Forensic Analysis of Industrial ControlSystems Using Sandboxing: A Case of WAMPAC Applications in the Power Systems Asif Iqbal *, Farhan Mahmood and Mathias Ekstedt
4) Programmable Logic Controller Forensics by Irfan Ahmed | University of New Orleans, Sebastian Obermeier | ABB, Sneha Sudhakaran and Vassil Roussev | University of New Orleans
5) Towards a SCADA Forensics Architecture by Tina Wu, Jules Ferdinand Pagna Disso, Kevin Jones and Adrian Campos EADS Innovation Works Quadrant House Celtic Springs ,Coedkernew, Newport NP10 8FZ UK
6) E. Casey (2011) Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet, 3rd Edition. Academic Press 2011, ISBN 978-0-12-374268-1, pp. I-XXVII, 1-807
7) A. Nicholson, S. Webber, S. Dyer, S. Patel, and H. Janicke (2012). {SCADA} Security in the light of cyberwarfare. Computers & Security 31(4), 418 – 436.
8) Forensic Analysis of SCADA/ICS System with Security and Vulnerability Assessment by Umit Karabiyik, Naciye Celebi, Faruk Yildiz, James Holekamp. Khaled Rabieh at Department of Computer Science Sam Houston State University