Developing Cyber Forensics for SCADA Industrial Control Systems

Joe Stirland[1], Kevin Jones[1], Helge Janicke[2], and Tina Wu
[1]Airbus Group and [2]De Montfort University
Joe.stirland@eads.com, kevin.jones@eads.com, heljanic@dmu.ac.uk

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. This paper looks at the SCADA/industrial control systems, typical attacks and vulnerabilities, problems with forensic analysis and the development of a forensic methodology/toolkit for such systems.

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, and transport networks. In recent years there has been an increasing number of attacks directly targeting these systems [1] including the well publicised Stuxnet 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.

Unfortunately whilst ICS/SCADA systems do contain elements of traditional IT systems they also contain a number of bespoke control devices and software. Such systems do not necessarily contain all of the forensic prerequisites of enterprise IT systems and therefore new approaches are required.

As ICS/SCADA systems are safety critical, have the requirement of integrity of functionality during operation, and must ensure availability of systems it is important to note that engineers are trained to quickly respond to functional changes in operation by replacing components. Thus, any potential artefacts of interest to determine if the event was caused by a cyber attack or component failure are lost.

In the remainder of this paper we introduce ICS/SCADA systems design, discuss the field of cyber forensics for ICS/SCADA, present a

framework by which to undertake cyber forensics in such systems, and make recommendations for a forensics toolkit to support investigation within control environments.

1. INTRODUCING INDUSTRIAL CONTROL SYSTEMS / SCADA

ICS and SCADA are specialised 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. An Industrial Control System monitors and controls physical processes and machinery. Such systems are often distributed over a large geographic location and sometimes even through a country meaning the ability to remotely monitor and manage these is critical to their operation and efficiency. In order to facilitate control, management information, and reports, 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 systems.
- 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 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 standardised 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 main-stream Business IT environments.

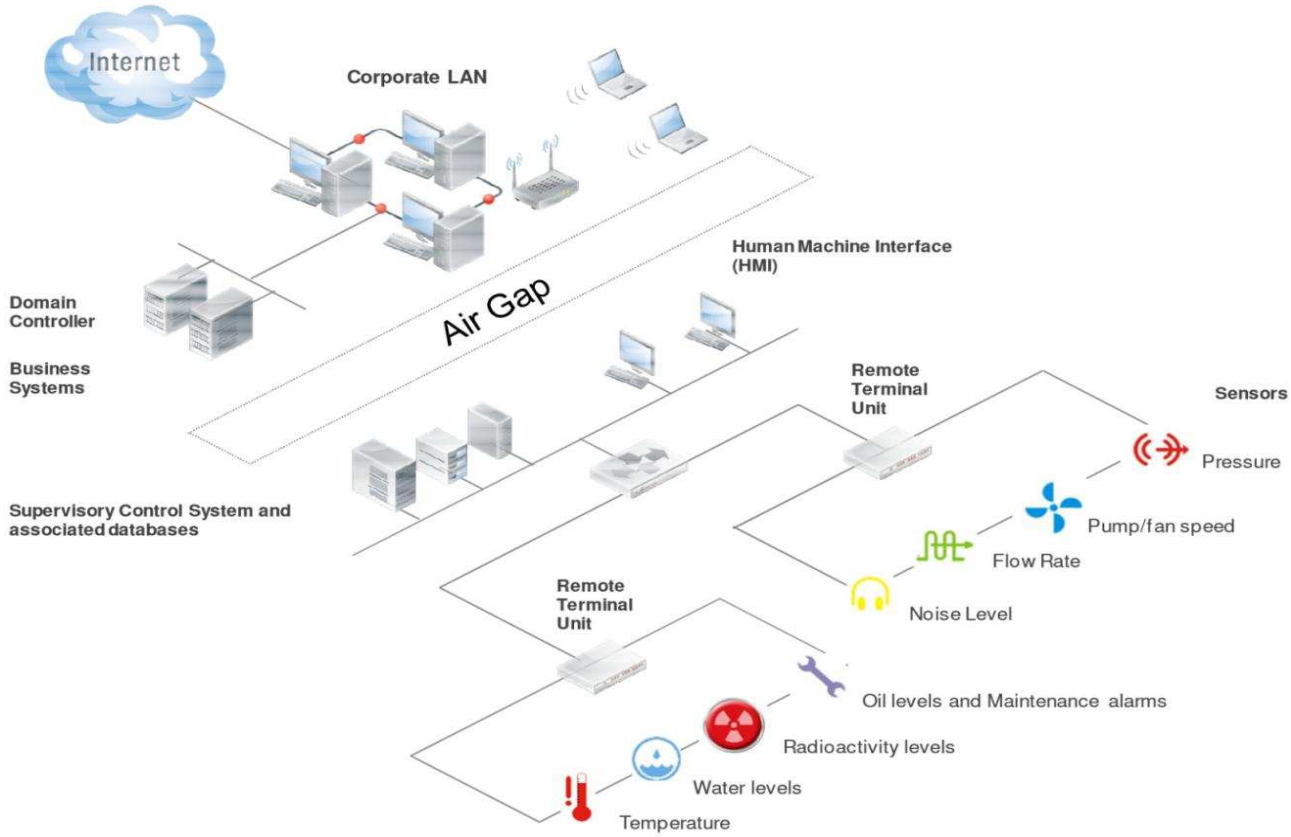

Figure 1: Industrial Control System with SCADA Network Architecture

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. Specific vulnerabilities of control devices is beyond the scope of this paper but are well documented [6,7,8,9,10,1].

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 synchronisation.

1.1 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 behaviour 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.

2. CYBER FORENSICS IN INDUSTRIAL CONTROL SYSTEMS

Computer forensics is the practice of collecting, analysing 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.

A number of key perspectives from cyber security and forensics experts provide valued understanding on the maturity and requirements for SCADA forensics.

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 very concise description regarding attacks against SCADA systems and the forensic specialities 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 defence 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/defence case.

.

3.2 Traditional Digital Forensics V SCADA

Computer forensics analysis and acquisition can generally be categorised 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).

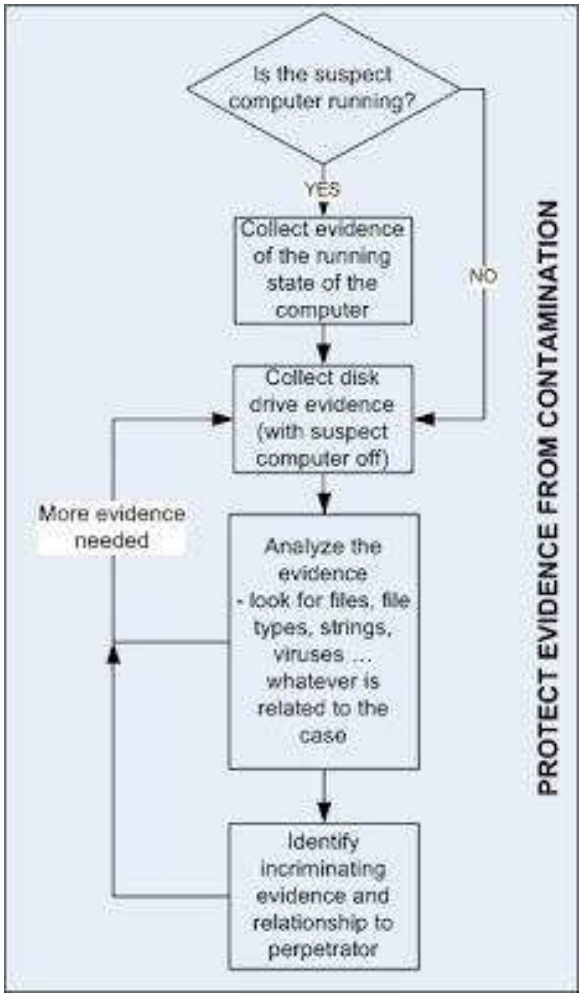

Figure 2: Digital Forensic Process [18].

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.

During a digital forensic investigation against 'standard' computer hardware, a specialist may use a variety of commercially available tools such as Encase, Xways, FTK, etc. and hardware such as Tableau write blockers, etc. in order to follow a forensic procedure similar to that shown in Figure 2. Whilst this is only a high-level view of the more complex investigation process, it captures the essential, iterative nature of a forensic investigation process. More details on traditional digital forensic investigation processes can be found in [19].

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 artefacts 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.

4. FORENSIC METHODOLOGY

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.

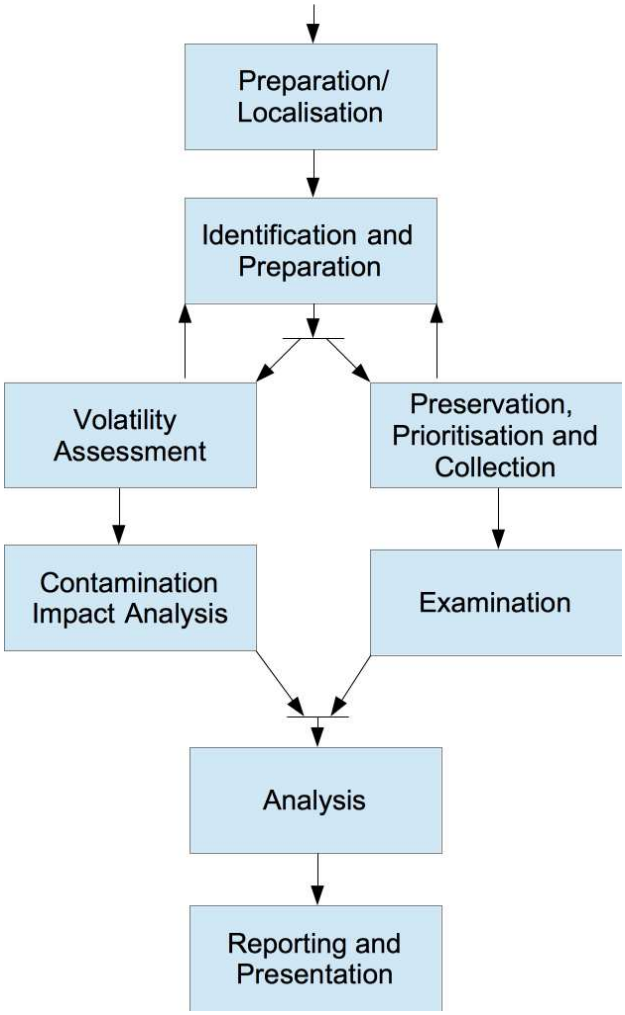

Figure 3: SCADA Incident Response and Forensic Process

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

- Phase 3- Volatility Assessment, Contamination Impact Analysis and Preservation, Prioritising and Collection: Assess the volatility of the identified resource immediately after identification in order to drive the priority list used in Preservation, Prioritisation 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 prioritised 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 artefacts 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 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.
- 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.

5. DEVELOPING A FORENSIC TOOLKIT FOR ICS

Following on from the methodology, we present the design of a forensic toolkit required to conduct a full investigation on a SCADA/ICS network. The toolkit is separated appropriately in alignment with the forensic methodology described in section 4.

5.1. What is a Forensic Toolkit?

A forensics toolkit is a pre-prepared collection of forensic software and hardware that is used for a full digital forensic investigation. Such tools could be open source and/or commercially available software/hardware installed on a forensic computer prior to conducting the investigation. The toolkit would usually be adaptable to the investigation type (i.e. what types of digital media would be involved? Can the media be accessed locally? How much media would be present? Is there any bespoke hardware involved?) In its simplest form a traditional forensic toolkit would be adapted to include tools for the following processes:

- 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.

5.2. 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:

- Phase 3- Preservation, Prioritising and Collection
- Phase 4- Examination
- Phase 5- Analysis

We now examine these steps in more detail and provide a description of the tools that are required in the toolkit for each element respectively.

5.3.Preservation, prioritising and collection

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. Additionally many of the affected devices cannot be powered off for 'static' data collection. For this part of the toolkit, the following hardware/software is chosen:

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 off devices.
- **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 the system.

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 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.
- **TCPDump** –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 exfiltration, 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.

- **Data hashing tool** – a hashing tool used to authenticate and prove integrity of your captured data. The acquisition tools often have this built in but occasionally the specialist may be required to hash and authenticate data.
- **Notepad++ or other text editor** – Extremely useful for taking evidential notes and documenting your forensic process. Can be used throughout and post investigation to keep a chain of evidential procedures taken.

5.4. 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 analysing 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.
- **Storage HDD's** – in order to store copies of all captured data.

Software:

- **Hex viewer (e.g. Xways/WinHex Forensic)** – in order to view any raw data that was dumped to hexadecimal view. Particularly with any PLC/RTU flash/RAM dumped data. This would be particularly useful in order to be able to search through the raw data for known malware binary examples. This would also provide any useful details related to the running of a field device. E.g. function codes, data payloads, running status, times, etc.
- **Encase** – To be able to process and analyse any forensic images that were taken using the write blockers (usually in E01 or DD format). There are many inbuilt processing features included within Encase, as well as the option to write bespoke data processing scripts using Enscript. This will be used to process the filesystem data from the HMI, engineering workstations, OPC and database servers.
- **Accessdata FTK Toolkit** – Can be used alongside or as an alternative to Encase as an analysis tool. This will be used to process the filesystem data from the HMI, engineering workstations, OPC and database servers.
- **Network Miner** – This is a network forensic analysis tool [21] with built-in ICS capability for parsing any captured network traffic. This may be a useful analysis tool for identifying any anomalous activities on the network. It would be useful to identify traffic flow between SCADA devices and any ICS protocols that are transferred. It may be possible to identify the incident vectors based on such traffic.
- **Wireshark** – Another network based tool that can capture and parse network traffic. It

is possible to filter the traffic in a variety of ways. This would be particularly useful when attempting to identify any anomalous activity. Again this would be extremely useful in identifying SCADA/ICS related protocols and associated 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).
- **AlienVault** – 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 AlienVault allow the analyst to create and run ICS/SCADA related rules across data and to alert the analyst 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.

6. APPLYING THE FORENSIC METHODOLOGY

The forensic methodology provides a clear process to follow during a SCADA investigation. This can be applied to an investigation as follows:

6.1.1. Phase 1 – Identification and Preparation

1. Ensure evidential notes are taken during every step of these processes

Table 1: Forensic Toolkit Application

SCADA Device:	Phase:	Forensic Tool:
Network	Phase 3.	TCPDump
	Phase 4.	Network Miner, Wireshark, AlienVault
HMI	Phase 3.	Write Blockers, FTK Imager, EnCase, Helix SHA-256/MD5 Hashing Tool
	Phase 4.	EnCase, XWays, Accessdata FTK Toolkit, Vclatility
PLC/RTU	Phase 3.	Bespoke PLC Flashing Software
	Phase 4.	XWays
Engineering computer	Phase 3.	Write Blockers, FTK Imager, EnCase, Helix SHA-256/MD5 Hashing Tool
	Phase 4.	EnCase, XWays, Accessdata FTK Toolkit, Vclatility
Database Server	Phase 3.	Write Blockers, FTK Imager, EnCase, Helix SHA-256/MD5 Hashing Tool
	Phase 4.	EnCase, XWays, Accessdata FTK Toolkit, Vclatility
OPC	Phase 3.	Write Blockers, FTK Imager, EnCase, Helix SHA-256/MD5 Hashing Tool
	Phase 4.	EnCase, XWays, Accessdata FTK Toolkit, Vclatility
Historian	Phase 3.	Write Blockers, FTK Imager, EnCase, Helix SHA-256/MD5 Hashing Tool
	Phase 4.	EnCase, XWays, Accessdata FTK Toolkit, Vclatility

ISBN: 978-1-941968-01-7 ©2014 SDIWC

2. Understand the problem – what type of incident has occurred?
3. Speak to the system engineers, system administrators and anyone else relevant, to capture as much information as possible related to the systems and network.
4. Obtain a copy of a network diagram (if available) and make a plan of potential forensic items.
5. Obtain timeframes for the investigation. This will allow for a more streamlined and focused effort.
6. Obtain any further relevant information related to the SCADA network which could potentially be useful for the investigation. E.g. Keywords, blacklisted IP/MAC addresses, etc.

6.1.2. Phase 2 – Identifying Data Sources

1. Using the previously gathered information, begin to map out all systems/devices to be analysed.
2. List as much information about each system as possible. What type of devices are they? List make/models, operating system, serial numbers, whether they are live/shutdown. Etc. This is a very important step, particularly with PLC/RTU devices where further research to identify flashing software may be required.
3. It is also useful to revise and create a map of networks again at this point.
4. Assess whether the forensic toolkit would cover all of the identified data sources. Does it need to be expanded?
5. In the case of the PLC/RTU devices speak to the vendors to attempt to get a copy of the flashing software and any detailed instructions of usage.
6. Write a prioritised list for forensic capture.

6.1.2. Phase 3 – Preservation, Prioritising and Collection

1. Referring to the prioritisation list in the previous step, begin to work from highest priority capture to lowest. E.g. what data is most volatile and vulnerable to loss. This will more than likely be PLC and or RTU devices.
2. If you have the flashing software for the PLC/RTU devices, follow the manufacturer's guidelines to create a memory dump of the device. Ensure that your actions do not affect the device in any way. Ensure a SCADA engineer is on hand during the process.
3. Locate all other devices relevant to the investigation and using the forensic acquisition tools in the toolkit capture the data using hashing and verification techniques. These will be engineering workstations, mobile devices, HMI devices, network devices and any other attached devices. Ensure the data is stored securely and logged in the evidential notes.
4. Create a packet capture on the network using TCPDump (or similar) and treat the data as evidential data. The specialist can hash and verify the use of any software in order to verify its credibility.
5. Obtain any relevant logs not captured from the system engineer.
6. Ensure that all devices specified in your investigation plan have been captured as necessary, and that none of your actions have affected the ICS system operations.

6.1.3. Phase 4 and Phase 5 – Examination and Analysis

1. At this stage the specialist should have all required data as specified in Phases 1 and 2 which can now be processed.
2. For all 'static' data provided by HMI device(s), engineering machines, database servers, network devices, etc. the created images can now be loaded into the relevant forensic software. E.g. EnCase. This software can then process this data to

remove known system files, hash and verify all files, search for specified keywords, recover deleted data, identify areas of interest, identify timelines of interest, etc.

3. For all 'live' data this can be processed using the relevant Volatility plug-ins. Depending on the operating system of the captured device this could be: running processes, dlls, registry data, API Hooks, connections, command line scripts, locating malware injection code, etc.
4. Any raw data recovered from the field devices can also be viewed and processed within the relevant hex software, e.g. XWays. A similar process can begin, searching for strings, any PLC/RTU related data such as: ladder logic data, device status, logs (if any), function codes, etc. It would be necessary to have a SCADA device engineer on hand during this section of the investigation.
5. Process the captured network data using Network Miner and/or Wireshark to attempt to identify all ICS related traffic and to tie in with the findings of your data results. For example if MODBUS is being used, are the function codes incorrect, does the data look manipulated, etc.
6. Use AlienVault at this stage to make use of SIEM. This would also produce a network timeline of highlighted possible SCADA incidents including affected devices, etc.
7. Start to identify and analyse relevant evidence related to the initial incident identified in phase 1. Further devices not captured may be identified. Return to site and image as soon as possible.
8. Further analysis to find the relationships between devices and the evidence related to the incident.
9. Produce a timeline of the incident, including a map of affected devices. This should also include detailed analyses of the impact on the control environments.

6.1.4. Phases 6 and 7 – Reporting and Presentation

1. Compile all findings and write a detailed report for the relevant parties' management.
2. The report should contain relevant recommendations for engineers.
3. The report should contain SCADA specific recommendations for future prevention, e.g. implementing/upgrading IDS/IPS solutions, implement DMZ, implement air gaps, control access to SCADA site, control device access to network, etc.
4. Review and verify all findings, and duplicate efforts using different software if possible and proportionate. Ensure all evidential notes are correct, up-to-date and follow the chain of custody.

7. 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 attacks 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 authors [20] 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 incident handling utilising 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 workstations, etc).

It is shown that a number of existing tools are suitable for elements of a SCADA forensic investigation, however, more evidence and artefacts may be discoverable as the maturity of this field develops.

8. 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 focussed 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 organisational 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 organisational and systems architecture approaches to ensure that the requirements of operation and investigation can both be met.

9. REFERENCES

[1] A. Nicholson, S. Webber, S. Dyer, S. Patel, and H. Janicke (2012). {SCADA} Security in the light of cyber-warfare. Computers & Security 31(4), 418 – 436.

[2] R. Langner (2011) Cracking Stuxnet, a 21st-century cyber weapon.

[3] E. Byres. (2012) Securing SCADA systems from APTs like Flame and Stuxnet – Part 1. Tofino Security. Weblog.

[4] Check Point Software Technologies (2014) Check Point protects from the HAVEX malware targeting ICS/SCADA

[5] M.J. Schwartz (2014) Target Breach: HVAC Contractor Systems Investigated

[6] SCADAhacker.com (2014) SCADA/ICS Vulnerability Reference . Website

[7] Digital Bond (2014) Vulnerability Notes. Website

[8] Symantec (year unknown) Vulnerability Trends - SCADA Vulnerabilities. Website

[9] G. Hale (2011) More SCADA Vulnerabilities Found. Industrial Safety and Security Source. Weblog

[10] Schneider Electric (year unknown) Support - Vulnerabilities.

[11] A. Krennmair (2003) cinderella: A Prototype For A Specification-Based NIDS

[12] B. 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 Computer Society.

[13] Forensic Control (2014) Introduction to computer forensics. Website

[14] 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.

[15] R.M. Van Der Knijff (2014) Control systems/SCADA forensics, what's the difference? in Digital Investigation Volume 11, (3), pp. 141-248.

[16] I. Ahmed, S. Obermeier, M. Naedele & Golden G. Richard III (2012) SCADA Systems: Challenges for Forensic Investigators, in Computer - IEEE. 5 (12), pp. 44-51.

[17] J. Giles (2010) Are states unleashing the dogs of cyber war? [Online]. Website.

[18] Information Security Short Takes (2008) Computer forensics process. Tutorial - Computer Forensics Process for [sic]Beginners. Website.

[19] 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

[20] T. Wu, J.F.P. Disso, K. Jones & A. Campos (2013) Towards a SCADA Forensics Architecture, in proceedings of 1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013). Leicester, UK. September 2013.

[21] Netresec (2013) NetworkMiner. Website.