DOI: http://dx.doi.org/10.14236/ewic/ICS2016.16

Forensic Readiness for SCADA/ICS Incident Response

Peter Eden
Information Security Research group
School of Computing and Mathematics
Department of Computing, Engineering and Science
University of South Wales
Pontypridd, CF371DL
UK
peter.eden@southwales.ac.uk

Andrew Blyth
Information Security Research group
School of Computing and Mathematics
Department of Computing, Engineering and Science
University of South Wales
Pontypridd, CF371DL
UK
andrew.blyth@southwales.ac.uk

Pete Burnap,
Yulia Cherdantseva
Computer Science and Informatics
Cardiff University, Queen's Buildings
5 The Parade, Roath
Cardiff CF24 3AA, UK
BurnapP@cardiff.ac.uk
CherdantsevaYV@cardiff.ac.uk

Kevin Jones,
Hugh Soulsby
Airbus Group Innovations
Quadrant House Celtic Springs
Coedkernew
Newport NP10 8FZ, UK
kevin.jones@airbus.com
hugh.soulsby@airbus.com

Kristan Stoddart
Department of International Politics
Aberystwyth University
Penglais, Aberystwyth
Ceredigion
SY23 3FE, UK
kds@aber.ac.uk

The actions carried out following any cyber-attack are vital in limiting damage, regaining control and determining the cause and those responsible. Within SCADA and ICS environments there is certainly no exception. Critical National Infrastructure (CNI) relies heavily on SCADA systems to monitor and control critical processes. Many of these systems span huge geographical areas and contain thousands of individual devices, across an array of asset types. When an incident occurs, those assets contain forensic artefacts, which can be thought of as any data that provides explanation to the current state of the SCADA system. Knowing what devices exist within the network and the tools and methods to retrieve data from them are some of the biggest challenges for incident response within CNI. This paper aims to identify those assets and their forensic value whilst providing the tools needed to perform data acquisition in a forensically sound manner. It will also discuss the key stages in which the incident response process can be managed.

SCADA; critical infrastructure; digital forensics; incident response; SCADA forensics

1. INTRODUCTION

Over the years as technologies have developed, SCADA (Supervisory Control and Data Acquisition) systems, that are common amongst much of the world's CNI (Critical National Infrastructure) and manufacturing plants, have also developed. Their convergence with TCP/IP and corporate networks has allowed for a more efficient monitoring and control process and an increase in statistical and analytical elements ultimately resulting in better productivity. Systems that were once isolated networks, air-gapped from any other communications are now communicating over the Internet leaving them increasingly vulnerable to external attacks. As these systems expand the number of data sources and types of data sources also increases making any forensic analysis and incident response very challenging.

Section two of this paper discusses the available data sources within the SCADA environment that can potentially hold forensic artefacts of interest in an investigation. It will discuss the issues with knowing what assets exist and potential tools that can be used to identify those assets. It will also identify which assets typically exist in which part of the SCADA system and the type of artefacts it may contain.

Section three will discuss the tools and techniques available to a forensic investigator in order to acquire, analyse and report on data retrieved for the various particular SCADA devices.

Section four is aimed at forensic readiness and discusses the different options for incident response management, the importance of an incident response team, and also the guidelines, good practices and frameworks available to them.

2. FORENSIC DATA SOURCES WITHIN A SCADA NETWORK

2.1. Knowing your Assets

The key to a successful forensic incident response, within ICS, begins with knowing what assets are present in the network under investigation. This may seem trivial but over the years as SCADA systems adapt and grow to fit business needs, and through their convergence with IT and new technology, this is sometimes not as easy as it seems. Not knowing exactly what assets you have poses two problems. Firstly, it increases the vulnerability of the system to an attack. Secondly, potential vital information may be ignored in an investigation.

Simply creating an inventory of physical assets within a SCADA network is not enough for a forensic incident response. Device configurations, firmware and software is also essential to document in an asset inventory along with device location within a network. Communication between IT and OT (Operational Technology) engineers is essential for creating an accurate asset management process.

2.1.1. Active vs Passive Discovery

There are two main approaches to identifying devices on a network; Active scanning; and Passive scanning. Active scanning involves sending additional traffic into the network and analysing the responses. Passive scanning avoids generating any additional traffic by simply monitoring network flow as it traverses a network. Chason et al. (2014).

Traditional methods and tools for actively scanning enterprise networks cannot simply be applied to ICS. Doing so would raise many safety concerns as introducing extra traffic into an ICS control environment could interrupt critical processes. Wedgbury and Jones (2015). For instance using NMAP (Network Mapper), MetaSpolit, or Nesses to scan an ICS network may introduce latency to critical processes. However, there are various tools available that can be used to automatically scan and generate inventory lists of IP and non-IP based devices for ICS when safe do to so.

2.1.2. ICS Network Mapping

Already established network maps, documentation and asset lists should be collected and used to help begin the asset inventory and accurate network map process. These should be confirmed by validating what is documented to what actually exists, through a physical assessment. In order to safely expand on this a combination of both passive and active scanning should be carefully implemented to identify those devices not already documented, proceeding with a passive scan initially and then followed by an active scan if safe to do so ie. during downtime of operations.

The following are examples of asset identification tools:

- ARP Tables: Scanning and obtaining ARP tables from managed switches will correlate an IP address to its corresponding MAC address, ultimately identifying physical devices on that network
- Wireshark Endpoints: Wireshark is an open source protocol analyser and can be used to capture packets being sent across a network. Wireshark Endpoints is a feature in Wireshark that allows the identification of logical endpoints of separate protocol traffic of a specific protocol layer.
- Wireshark Conversations: Feature in Wireshark that displays all traffic between two endpoints.

2.2. Asset Management Tools

There is an array of asset discovery and management tools available but not all are compatible or designed with ICS in mind. There are, however, some tools that are specifically designed for ICS asset discovery, inventory and management that understand the critical nature of low level control communication and bespoke ICS protocols.

2.2.1. Industrial Defender ASM (Automation Systems Manager)

Lockheed Martin's Industrial Defender Automation Systems Manager takes into consideration a control system's critical and volatile nature including ultra-low bandwidth constraints and the array of proprietary protocols available. Industrial ASM collects information, such as hardware and software versions across the ICS network, by scanning IP and non-IP based devices. It utilises both agent and agentless methods. Using an ARP watch alerts are generated when unknown drives are attached to the network by comparing IP and MAC addresses with those that are present in the ASM.

2.2.2. Dragos Security CyberLens

CyberLens is an ICS asset discovery tool that implements passive listening to identity ICS and IT assets on a control network. It is able to do this by monitoring communication between devices, utilising deep packet inspection on both IT and ICS protocols. It uses sensors around the network to carry out live and passive network data captures before processing the data offline to provide an interactive graphical representation of the network and device communication.

2.2.3. AlienVault USM (Unified Security Management)

AlienVault USM offers both active network scanning and passive network scanning for asset discovery and inventory management on an ICS network. In parallel with asset management it also performs behavioural monitoring, vulnerability assessment and intrusion detection.

2.2.4. PAS Cyber Integrity

PAS's Cyber Integrity tool is part of the Integrity Software Suite that identifies both OT and IT assets within a control environment. The tool offers an alternative to the manual inventory practice and provides an accurate inventory of device configuration data for both IT and OT assets.

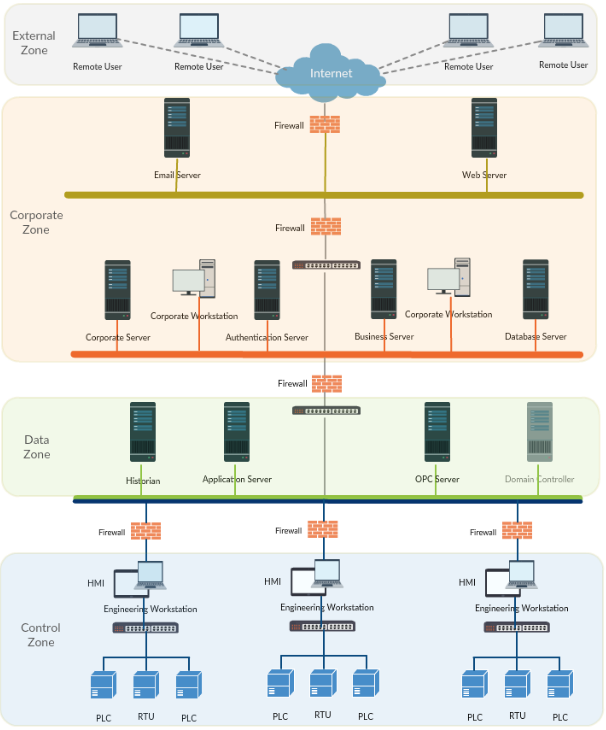

Figure 1: *SCADA Network Data Zones*

2.3. SCADA Assets of Forensic Value

SCADA systems can span huge geographical areas and contain thousands upon thousands of physical data sources. As described in Figure 1. these assets can exist within various zones within the SCADA network. The following set of tables represent the various devices that can be found within each zone and the potential forensic artefacts they may yield.

2.3.1. Control Zone

Device:	Forensic Value:
PLC/RTU	Logs, active processes, timestamps, ladder-logic, program codes, SD card firmware versions
HMI:	Logs, Issued commands, program codes, reports
Engineering Workstation	RAM, connected devices, PLC/HMI baseline images
Switches	CAM (Content Addressable Memory)

2.3.2. Data Zone

Device:	Forensic Value:
Historian	DMBS logs, client data, boolean alarms, boolean events
OPC Server	Field device logs, communication logs
Application servers	DHCP logs,
MTU	Logs, connected devices PLC/RTU I/O data
Engineering Workstations	Program/File execution, Account usage, attached devices, logs, browser usage
Routers	Event Logs, IP tables MAC addresses, routing tables
Switches	CAM (Content Addressable Memory)
Domain Controller	Logon Events, security events

2.3.3. Corporate Zone

Device:	Forensic Value:
Workstations	Program/File execution, Account usage, attached device logs, browser usage
Corporate Server	Server logs, event logs communication logs
Database Server	Data Files, server logs, system event logs, trace files
Email Server	Server logs, email transactions,
Web Server	Server logs, event logs, IP addresses, session data
Firewall/IDS/ IPS	Log data, Event data, IP addresses, port log files
Routers	Event Logs, IP tables MAC addresses, routing tables
Switches	CAM (Content Addressable Memory)

2.3.4. External Zone

Device:	Forensic Value:
Firewalls	Log data, Event data, IP addresses, port log files

3. FORENSIC ACQUISITION OF SCADA ARTEFACTS

Firstly, a SCADA forensic artefact can be thought of as any data that provides explanation to the current state of a SCADA system, device or media. Data of forensic value within SCADA systems can exist in two separate streams; data that is communicated across a network; and data that is stored in a device. Knijff (2014). The latter can be further categorised as to which zone, within the SCADA architecture, that device exists. This section will aim to highlight the key tools and methods for forensically acquiring data from both a SCADA network and from the physical assets.

3.1. Network Data Acquisition

Data passing over a SCADA network can be captured in various ways and using a variety of tools. The following is a list of current tools available to perform network data acquisition within a SCADA environment.

3.1.1. In-line Network Taps

Sniffing traffic over a network can be achieved through the use of network taps and placing them at keys points within a network, known as 'choke-points'. Ideally, they would be placed between switches, on ethernet lines or in-between individual assets. A network tap is a device that copies network traffic passing through it to a monitor port. Hjelmvik (2011). Implementing the use of link aggregation taps allow for both downlink and uplink traffic to be captured. Network taps can only be connected onto a SCADA network when it is safe to do so, during downtime of operations or during maintenance periods. This will eliminate any disruption to critical processes. The tap can then be connected to a separate machine dedicated for the collection of that data.

3.1.2. Port Mirroring

When network taps cannot be implemented an alternative can be to use port mirroring or SPAN (Switch Port Analyzer) to obtain SCADA network data from managed switches. By connecting a monitoring system to a managed switch, a copy of the packets sent through that switch, or separate ports on that switch, can be mirrored to a single port. That port can then be used to acquire the data. To acquire the data a monitor session must be started. CA (2015). This includes;

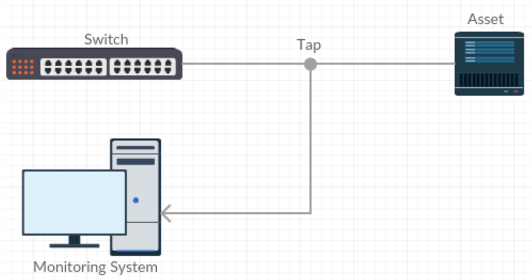

Figure 2: *In-line link aggregation network tap*

- the session number: to identify the monitoring session
- session source: the desired ports to mirror
- session direction: specifies the direction of the mirrored traffic, i.e. receive (RX) or transmit (TX) or both

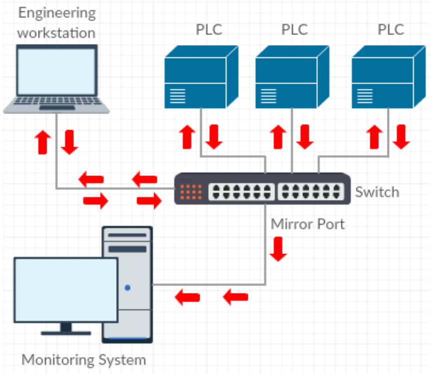

Figure 3: *Port mirroring to obtain network traffic*

3.1.3. TCPdump

Much like Wireshark, but less labour intensive, TCPdump can be used as both a network monitoring tool as well as a tool to acquire network data from within a SCADA network. Data obtained via TCPdump will include timestamps, network protocol used, source IP and port, and destination IP and port. Green and VandenBrink (2012).

3.1.4. Wireshark

Wireshark is an open source protocol analyser and can be used to capture packets being sent across a network. Acquired data will be stored as .pcap files for later analysis or can be monitored live in real-time as data is communicated. Wireshark also supports many ICS and SCADA protocols.

3.1.5. Serial RS232 and RS485 Taps

Many devices found within SCADA networks rely on serial communication and although Wireshark also supports serial communication data there are several other tools that can be used. Much like implementing the ethernet tap an RS232 or RS485 network tap could be introduced to the network during scheduled downtime or maintenance periods to obtain serial communication data.

3.1.6. PortMon

Portmon is a utility found within Windows based systems and allows for monitoring and capturing of serial data. Simply executing the portmon.exe program file will start to capture serial communication data.

3.2. Device Data Acquisition

3.2.1. PLC:

Acquiring data from PLCs is dependent upon certain factors, such as whether the PLC needs to remain active or whether it can be powered down. The first instance poses many problems. If a PLC has to remain live for critical processing any interference to those processes may result in disastrous consequences. When this is the case sometimes the software used to program the PLC can be used to monitor and record certain vital data such as memory variable values as they alter. Wu et al. (2013). Examples of this would include using Siemens STEP7 software to record the data from any Siemens S7 PLCs, or Schneider Electric's SoMachine software to record memory address alterations in their Modicon PLC range.

Over the years there has been a distinct lack of dedicated forensic tools for PLCs and similar embedded devices Ahmed et al. (2012) but some software tools are starting to emerge to overcome the problem. As well as using the PLCs manufacturing tools to retrieve data there are tools such as PLC Analyzer Pro and PLCLogger that perform similar functionality. PLC Analyzer Pro is a software tool designed for acquisition and analysis of recorded data on Siemens SIMATIC devices.

PLCLogger is an open source software tool and provides similar functionality to PLC Analyzer Pro with the addition of supporting any device using Modbus-TCP or Modbus-UDP.

There has been some research into the development of a solution for the security monitoring of low level SCADA devices which could potentially aid a forensic investigation within a SCADA environment. Cruz et al. (2015) suggests the use of the SSU (Shadow Security Unit) which is placed in parallel to field devices for continuous monitoring of a device. The device can check for abnormal behaviour of a PLC and through physical probing go the I/O modules can provide real-time data acquisition capabilities. Cruz et al. (2015). A similar concept is discussed by Janicke et al, implementing a run-time monitoring framework using an Ardruino Yun device, alongside a field device to ultimately capture snapshots of PLC states, i.e. values for inputs/outputs, counters and timers etc, to aid in the forensic analysis after an incident has occurred. Janicke et al. (2015).

If a PLC can be powered down for forensic analysis or is already powered off as a result of an attack then certain techniques can be used to read data from the on-board memory chips themselves through JTAGging, chip off or ISP (In-System Programming).

JTAGging and In-System Programming are both non-invasive methods for achieving the same results. JTAGging is the process of interacting with the Test Access Points (TAPs) of the microcontroller in such a way to acquire raw data from any connected memory chips.

In-System Programming is a way to acquire data by bypassing the CPU itself and connecting directly to on-board storage chips, such as eMMC or flash storage and then pulling the raw data from them. Hardsploit is a hardware and software device designed with critical electronic and embedded devices in mind. It allows for both ISP and JTAGging to be carried out and a dump of the raw data to be obtained. The raw data can then be interpreted using a hex editor such as WinHex or HxD.

Chip off is regarded as an invasive acquisition procedure as the memory chips are physically desoldered and removed form the PLCs PCB and then read using specific chip readers to acquire the image. Chip off may be the only option if chips are already physically damaged and need to be repaired before imaging. Tools and equipment for this process would include a desoldering station to remove the chip and Hardsploit to acquire the data from it.

Once a raw image has been acquired it can then be interpreted to establish program code and ladder logic such as function

- **Physical Acquisition Tools:** Hardsploit, Desoldering Station, Chip reader
- **Software Acquisition Tools:** Vendor-specific Software, PLC Analzyer Pro, PLCLogger
- **Analysis Tools:** WinHex

3.2.2. HMI:

Much like a PLC the HMI typically has a fairly limited amount of on-board storage. However, the data stored on the chips could be crucial in a forensic investigation. The HMI is the interface at which a human interacts with the control devices. Decisions are made based on information passed back from field devices to the HMI. The HMI can store critical information such as event logging, alarm logging, issued commands, diagnostics and reports on the most recent status of particular field devices. Fabro and Cornelius (2008).

Performing data acquisition from HMI devices will mirror very closely the approach used with PLC devices. Vendor-specific software tools used to program the HMIs will often have monitoring and recording features which should be enabled when possible. Physical interrogation of the devices will involve ISP, JTAG and Chip-off to recover an image of the raw data, as explained in 3.2.1.

- **Physical Acquisition Tools:** Hardsploit, Desoldering Station
- **Software Acquisition Tools:** Vendor-specific Software
- **Analysis Tools:** WinHex, Vendor-specific Software

3.2.3. Engineering Workstations/General Workstations/Servers:

Workstations and Servers found at the control, data and corporate zones can all be approached in the same manner when it comes to a forensic response. Each system is going to contain different types of forensic artefact depending on the role its plays within the SCADA environment. The underlying fundamental elements are that they will all contain data stored in both memory and on physical storage that may be vital to investigation. Therefore, different tools are generally needed for RAM acquisition and for physical media extraction.

Disk Imaging: There is an array of disk imaging software tools that can be used to extract a forensically sound full image of internal and externally attached disks from a machine. Different tools have varying levels of capabilities and the preferred tool of choice may be dependent upon which operating system is running on the source machine.

AccessData's FTK (Forensic ToolKit) Imager is a common software tool used to create digital images of physical drives as well as the ability to obtain a full memory dump. FTK Imager Lite is a variation of the tool on USB format which eliminates the need to install any software on the source machine.

EnCase Forensic Imager can be used as an alternative to FTK Imager and ultimately performs the same functionality offering similar imaging formats and capabilities. However, a case study carried out by Muir (2015), of a comparison between EnCase version 7.10.00.103 and FTK Imager 3.3.0.5, showed that EnCase created more of a footprint than FTK when being run live on a target machine. This would be a factor to consider when acquiring a memory dump of a system as vital processes may be overwritten.

DD is a Linux command-line tool built in as standard on Linux and Unix systems and one that can also be installed on Windows machines. The dd command can be used to copy entire mounted drives both locally and remotely.

- **Physical Acquisition Tools:** Write-blocker
- **Software Acquisition Tools:** FTK Imager, Encase, dd
- **Analysis Tools:** FTK, Encase, Winhex
- **Reporting Tools:** AccessData FTK, Encase

RAM Acquisition: There are also various tools that can be used to acquire memory from a device that is running such as running processes, services, drivers, registry data, network data and event logs. Tools need to be carefully selected when dealing with memory acquisition as the tools being loaded to acquire the memory will also run in memory. This could potentially overwrite vital artefacts. Running command line tools are much more advantageous then GUI tools as they use less memory space.

Dumpit, a tool created by MoonSols for Windows systems, is an open source memory acquisition tool than can be run from a USB.

Memoryze, created by Mandiant, is very similar to dumpit and is run from a USB using the command-line. It is also a free tool and allows a complete memory dump to be passed to an externally connected drive or over a network.

Mandiant Redline is capable of extracting and auditing a full memory image of a workstation in a forensically sound manner. It was designed to detect malicious activity within memory. Its IOC (indicators of Compromise) functionality allows for the identification of malicious files and processes.

LiME can be used to acquire a memory dump from a linux system. Again, this can occur locally buy installing LiME on the host machine or can be acquired over the network via TCP.

Volatility is a cross-platform tool that can also be used to extract digital artefacts from live volatile memory and also provides analysis functionality. Stirland et al. (2014)

- **Acquisition Tools:** FTK Imager Lite, Volatility, dumpit, Memoryze, Redline, LiMe

- **Analysis Tools:** Mandiant Redline Suite, Winhex, FTK, Encase
- **Reporting Tools:** AccessData FTK, Encase

3.2.4. Continuity of Evidence

Digital forensic evidence collected during an investigation needs to be collected in a forensically sound manner to be admissible in court. If it is not then it cannot be relied upon in a court of law.

In the UK any evidence collected should adhere to the 4 ACPO (Association of Chief Police Officers) principles that provide a best practice guide for computer-based electronic evidence;

- No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
- In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to. QPM (2012).

All evidence collected needs to have a digitally signed hash value associated with it for authentication purposes to ensure no data is intercepted and changed between leaving one party and arriving at another. When evidence is passed on a chain of custody must be in place to ensure continuity of evidence. This will include a record of the seizure, custody, control and transfer of the evidence.

4. FORENSIC READINESS

It is important to understand clearly the difference between incident response and digital forensics when it comes to ICS and SCADA incidents. Digital forensics is essentially a subset of the incident response process and involves the use of specific tools and techniques to acquire, preserve and analyse electronic data recovered from the SCADA system. The results are then used to formalise a report that could be used as evidence in a court of law. Incident response shares many of the same goals as digital forensics but differs in its overall main focus which is to recover from an incident and restore normal operations. The two go hand-in-hand to providing more resilient systems post-incident with digital forensics identifying the cause of an incident and highlighting weaknesses within a SCADA system and incident response helping to restore normal functionality.

4.1. In-house or Outsource?

Incident response is a process and should be clearly established within an organisation via an incident response team and with the involvement of senior management. This way clear requirements can be identified and defined. The level of activity partaken by an internal team will essentially determine what is outsourced externally to third-party services and when.

Cost will also play its part in determining how much is performed in-house. With SCADA systems often containing many varied groups of assets and specialised and proprietary technologies it is often difficult and expensive to develop and train in-house teams to handle each aspect of the incident response process and therefore is sometimes cheaper overall to outsource to specific incident response companies. Torres and Williams (2014). It may also be cheaper for a company to outsource in the event of an incident over the costs involved in maintaining and training and development of an in-house team.

Compliance is another factor that may force a company to outsource its incident response process if it doesn’t have the capabilities in-house or if third-party verification is required by law. In the United States, NERC (North American Electric Reliability Corporation) has “the legal authority to monitor and enforce compliance with NERC Reliability Standards and impose penalties or sanctions for non-compliance.” NERC (2013). This is enforced through NERC CIP (Critical Infrastructure Protection) v5 standards and includes mandatory incident reporting requirements for all Energy sector asset owners.

4.2. Good Practices, Guidelines and Frameworks

There are many guidelines and frameworks for establishing incident response capabilities for industrial control systems depending on which country a company operates in. In the UK the SICS (Security for Industrial Control Systems) Framework was developed by CPNI (Centre for Protection of National Infrastructure) and CESG (Communications-Electronics Security Group), to provide security guidelines across all aspects of ICS. The framework consists of eight good practice guides, the last of which focusses on establishing response capabilities. CPNI (2015).

In the US, Homeland Security have developed recommended practices entitled "Developing an Industrial Control System Cybersecurity Incident Response Capability." These guidelines help provide guidance on incident response planning, incident prevention, incident management and post-incident analysis and forensics. ICS-CERT (2009) NIST (National Institute of Standards and Technology) also provide a "Guide to Industrial Control Systems (ICS) Security" which includes guidance on ICS incident response. NIST (2011).

After consulting the relevant guidelines and good practices, and with senior management involved, the key to a successful incident response is in the policies and planning of procedures.

4.3. Establishing an Incident Response Capability

Every company that relies on ICS and SCADA environments as part of the service they provide should have a dedicated incident response capability that is both well planned and well maintained. For smaller companies this may be in the form of a single person whose responsibilities include managing and overseeing third-party investigators and external incident response teams ensuring contracts are formed in line with business and operational needs. For the larger organisations roles may be assigned to certain employees on top of their normal day-to-day responsibilities who would ultimately come together to form the incident response team in the event of an incident.

Some organisations may employ a dedicated full-time incident response team as part of their business plan. CPNI (2015). Regardless of where a company is operating there are some key processes that need to be established within an incident response team working within an organisation.

4.3.1. Define an Incident Response Policy and Plan
When an event occurs within a SCADA environment, without a clear incident response policy or plan, it is possible for incorrect and rash decisions to be made as a result of being under extreme pressure. This can cause even further damage to an organisation through loss of production and financial loss or even environmental or public safety issues. A policy containing clear procedures of what to do in the event of an incident should be formed before an incident occurs, as part of business operations. This should include planning objectives, discovery, reporting, analysis and response actions, including forensics and communications. ICS-CERT (2009). There should also be detailed documentation regarding response team personnel, all critical assets within the ICS environment and scenario-based procedures. CPNI (2015).

4.3.2. Roles and Responsibilities
Team members should be selected based on their specialist knowledge and technical skills, and should include all areas of an ICS organisation i.e. Business management, Engineers, Legal, IT etc. From a forensic perspective having the ability to start recording network traffic as soon as an event is identified is essential. Setting up a SOC (Security Operations Centre) is advisable as it provides a central point within the organisation from which to work.

4.3.3. Exercise the Plan
In order to be able to respond appropriately, in light of an incident occurring within an ICS/SCADA environment, it is essential that regular exercises are carried out using fabricated scenarios to maintain and update response plans using lessons learned. CPNI (2015). This will prepare the team and help them to stay focussed when an actual incident occurs.

5. CONCLUSION

As we move forward with technology and as SCADA systems grow and become more and more at risk from outside cyber attacks, the ability to recover from and analyse an incident has never been more important. The incident response and forensic investigation within a SCADA environment needs to be separated from those of traditional IT networks. It is essential that when an event occurs there is a process in place to respond safely and accurately, with the correct tools and methodologies.

This paper has attempted to provide an overview of the various approaches specific to SCADA forensics and incident response. It has discussed the most applicable tools and techniques needed to undertake a forensic investigation considering the various levels and different data sources within a SCADA network. It has also emphasised the key elements needed for a successful incident response plan and how to prepare for the forensic response. It is clear that a more dedicated approach to SCADA forensic response and analysis is required in terms of tool development for SCADA specific devices and incident management.

6. FURTHER RESEARCH

Next steps will involve developing the requirement of a SCADA Forensic tool to acquire data from different vendor PLCs. A possible hardware-software solution that will aim to identify, by manufacturer and model, the technical specifications and architecture of a PLC. It will aim to display the specific data sources that can be found, and where within the device they are located, together with a forensic acquisition capability.

ACKNOWLEDGMENTS

This work is funded by the Airbus Group Endeavr Wales scheme under the SCADA Cyber Security Lifecycle (SCADA-CSL) programme with the ultimate goal of improving the forensic handling and incident response process for SCADA systems.

REFERENCES

Ahmed, I., Obermeier, S., Naedele, M. and Richard III, G. G. (2012), 'Scada systems: Challenges for forensic investigators', *Computer* **45**(12), 44–51.

CA (2015), Data acquisition: Best practices guide, Technical report, CA Technologies.

Chason, K., Dinnage, S., Lee, A., Searle, J., Widger, D. and Wright (2014), Guide to vulnerability assessment for electric utility operations systems., Technical report, NESCOR (National Electric Sector Cybersecurity Organization Resource).

CPNI (2015), Security for industrial control systems - establish response capabilities: A good practice guide, Technical report, CPNI.

Cruz, T., Barrigas, J., Proenca, J., Graziano, A., Panzieri, S., Lev, L. and Simões, P. (2015), Improving network security monitoring for industrial control systems, *in* '14th IFIP/IEEE Int. Symposium on Integrated Management (IM 2015)'.

Fabro, M. and Cornelius, E. (2008), Recommended practice: Recommended practice: Creating cyber forensics plans for control systems, Technical report, Department of Homeland Security.

Green, T. and VandenBrink, R. (2012), Analyzing network traffic with basic linux tools, Technical report, SANS Institute InfoSec Reading Room.

Hjelmvik, E. (2011), 'Intercepting network traffic', *NETRESEC (Network Forensics and Network Security Monitoring)* .
URL: *http://www.netresec.com/?page=Blogmonth =2011-03post=Sniffing-Tutorial-part-1—Intercepting-Network-Traffic*

ICS-CERT (2009), Recommended practice: Developing an industrial control systems cybersecurity incident response capability, Technical report, U.S. Department of Homeland Security.

Janicke, H., Nicholson, A., Webber, S. and Cau, A. (2015), 'Runtime-monitoring for industrial control systems.', *Electronics* **4**(4), 995–1017.

Knijff, v. d. R. M. (2014), 'Control systems/scada forensics, what's the difference?', *Digital Investigation* **11**(3), 160–174.

Muir, B. (2015), Encase imager vs. ftk imager. http://bsmuir.kinja.com/encase-imager-vs-ftk-imager-1677906594 (Accessed 21st June 2016).

NERC (2013), Request for information north american electric reliability corporation response, Technical report, National Institute of Standards and Technology.

NIST (2011), Guide to industrial control systems (ics) security, Technical report, National Institution of Standards and Technology.

QPM, D. J. W. (2012), Good practice guide for digital evidence, Technical report, ACPO (Association of Chief Police Officers for England, Wales and Northern Ireland).

Stirland, J., Jones, K., Janicke, H. and Wu, T. (2014), Developing cyber forensics for scada industrial control systems, *in* 'Proceedings of the International Conference on Information Security and Cyber Forensics', SDIWC Digital Library.

Torres, A. and Williams, J. (2014), 'Incident response: How to fight back', *SANS Institute InfoSec Reading Room* .

Wedgbury, A. and Jones, K. (2015), Automated asset discovery in industrial control systems - exploring the problem, *in* 'Proceedings of the 3rd International Symposium for ICS SCADA Cyber Security Research 2015', EWIC.

Wu, T., Disso, J. F. P., Jones, K. and Campos, A. (2013), Towards a scada forensics architecture, *in* 'Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research', p. 12.