Tryfonas, T., & May, J. H. R. (2013). Can we learn from SCADA security Incidents? European Network and Information Security Agency.

Can we learn from SCADA security incidents?

1 Introduction

Security experts across the world continue to sound the alarm bells about the security of Industrial Control Systems (ICS).[1] Industrial Control Systems look more and more like consumer PCs. They are used everywhere and involve a considerable amount of software, often outdated and unpatched.

Recent security incidents in the context of SCADA and Industrial Control Systems emphasise greatly the importance of good governance and control of SCADA infrastructures.[2] In particular **the ability to respond to critical incidents and be able to analyse and learn from what happened is crucial.**

The EU recognized the urgency of this problem and the recently proposed cyber security strategy for the EU is focussing on improving the security of network and information systems used for critical infrastructures[3]. The strategy calls EU member states, the industry, and ENISA to increase the level of NIS in critical sectors, and to support exchange of best-practices.

ENISA responded to this call by launching several activities on security of ICS and SCADA[4].

Network level monitoring comprises mature technologies that have been used successfully for analysing security incidents in traditional networking environments for many years. Deployment of intrusion detection sensors and traffic logging becomes more acceptable practice, especially as a lot of contemporary systems are IP-enabled. Increasingly more relevant advisory bodies issue guidelines and standards that are applicable to the domain of security of this type of environments.

Technical background: ICS and SCADA

Industrial systems and critical infrastructures are often monitored and controlled by simple computers called Industrial Control Systems (ICS). ICS are based on standard embedded systems platforms and they often use commercial off-the-self software. ICS are used to control industrial processes such as manufacturing, product handling, production, and distribution. Well-known types of ICS include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and programmable logic controllers (PLC).

SCADA systems historically distinguish themselves from other ICS by being the largest subgroup of ICS systems and large scale processes that can include multiple sites and large distances. A Supervisory Control and Data Acquisition (SCADA) system can be typically viewed as an assembly of interconnected equipment used to monitor and control physical equipment in industrial environments. They are widely used to automate geographically distributed processes such as electricity power generation, transmission and distribution, Oil and gas refining and pipeline management, water treatment and distribution, chemical production and processing, rail systems and other mass transit.

This white paper explores the concerns mentioned above and provides recommendations for the implementation of a proactive environment that will facilitate agile and integrated response to incidents and their ex-post analysis.

ENISA identified several key activities that can contribute to this goal:

- Facilitating the integration of cyber and physical response processes with a greater understanding of where digital evidence may be found and what would be the appropriate actions to preserve it;

[1] http://threatpost.com/hackers-aggressively-scanning-ics-scada-default-credentials-vulnerabilities

[2] http://www.wired.com/threatlevel/2012/01/10000-control-systems-online/

[3] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[4] http://www.enisa.europa.eu/publications/programmes-reports/work-programme-2013

- Designing and configuring systems in a way that enables digital evidence retention,
- Complementing the existing skills base with ex post analysis expertise and understanding overlaps between cyber and physical critical incident response teams,
- Increasing inter-organisational public and privately held and cross-country collaboration efforts.

2 Target audience

The goals of this white paper are to inform the related community of SCADA operators and security engineers and to provide another interface between policy makers and technology specialists in the sensitive domain of critical infrastructure protection.

In particular, ENISA aims at:

- Informing operational teams about the logging and ex post incident analysis capabilities that they should consider when designing and implementing ICS systems, based on the current level of the threat existing in their operating context,
- Informing security engineers about the opportunities and the challenges that this largely proprietary domain can pose,
- Proposing a set of recommendations for developing a proactive environment of an appropriate level of preparedness with respect to ex post incident analysis and learning capability
- Facilitating further debates between the first two groups of stakeholders and policy makers in their struggles to facilitate the development and maintenance of secure and resilient critical infrastructures.

3 Ex post incident analysis

The primary goal of an ex post incident analysis is to obtain valuable information regarding security incidents in order to form an in-depth knowledge of what happened. By examining the various parts of the system, valuable knowledge can be obtained. However, it is not only important for the understanding of the circumstances under which a security incident occurred but it also gives the ability to:

- Create a body of robust evidence in order to respond to the changing nature of domestic and alien threats, minimize the outages of ICS-SCADA systems[5],
- Ensure that enough learning takes place in order to deploy resilient systems.

Collecting evidence related to incidents can reveal the actions that took place during the incident along with the incentives and perhaps the identity of the attacker.

There exist many places in a networked system where evidence can be recovered. Network traffic and operating system (OS) log files form the most significant sources of evidence; however the diverse nature of industrial control systems hinders the usage of a single, consistent methodology.

Ex post incident analysis forms a fundamental part of security management. Although it is the first stage of digital forensic process, one should distinguish these two terms because a digital forensic

[5] *By investigating a security incident, valuable knowledge can be gained which can be used to strengthen the system against future attacks and mitigate the effects of such incidents by incorporating the appropriate proactive defence mechanisms.*

analysis involves the preparation of results so as to allow them to be presented as evidence to a court of law and engagement with legal enforcement authorities is mandatory, while an ex post incident analysis aims primarily at:

- Identifying the target of an attack,
- Inferring the attacker's actual goal if possible,
- Identifying the vulnerabilities of the system on which the attack was based,
- Discovering a possible data theft and traces that can be used to unveil the source of the attack.

3.1 The process

The first steps of incident analysis in the domain of industrial control systems involve the examination of the system and the identification of the impacted components. Next, all OS logs and transaction logs relative to these components are gathered and analysed based on well-known guidelines that are widely available[67].

There are five basic steps when it comes to performing an ex post incident analysis of any device[89] as shown in Figure 1.

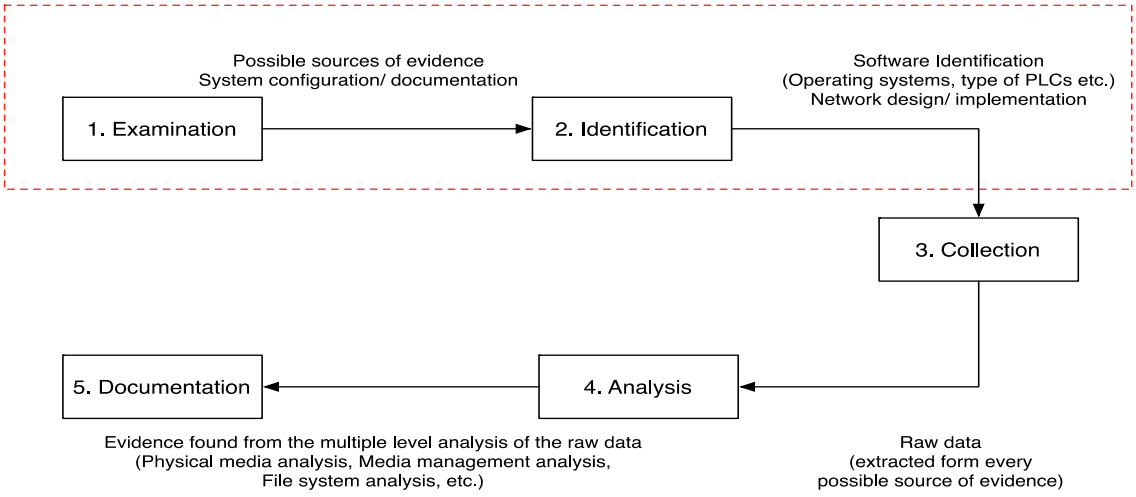

Fig 1. **Ex post incident analysis process in SCADA systems.**

These steps are:

1. **Examination**: In the examination phase the investigator has to understand all the potential sources of evidence in a SCADA system. In addition, any other system related to the SCADA system under investigation also needs to be taken into account. This includes access terminals, logging servers and routers.

[6] S. Wilkinson, "Good Practice Guide for Computer-Based Electronic Evidence," Assoc. Chief Police Off., 2010.
[7] M. Fabro and E. Cornelius, "Recommended Practice: Creating Cyber Forensics Plans for Control Systems," Dep. Homel. Secur., 2008.
[8] R. Radvanovsky and J. Brodsky, Eds., Handbook of SCADA/Control Systems Security. CRC Press, 2013.
[9] T. Spyridopoulos and V. Katos, "Requirements for a Forensically Ready Cloud Storage Service," Int. J. Digit. Crime Forensics Ijdcf, vol. 3, no. 3, pp. 19–36, 2011.

2. **Identification of evidence**: The starting point of this stage is the identification of the type of system under investigation[10]. Once the type of system has become known, the next step is to identify the operating system of the system that is used, the types and manufacture of the PLCs, and the network design and implementation. Towards this direction information gathered from the system's Point of Contact (POC) can provide valuable data. The manufacturer's documentation, the design specifications, network diagrams and the Human Machine Interface (HMI) itself can assist the identification process.

3. **Collection of evidence**: The collection phase involves the collection of data from all the systems with memory components that have been identified in step 2. Network traffic between the identified system's components, such as network traffic between the control network and the management network, and between the SCADA system and the Internet should also be captured.

4. **Analysis of evidence:** In the analysis phase evidence is identified in the data collected. Eventually, a timeline of activities based on the data that was gathered in the collection phase is created. The major categories of ex post incident analysis can be defined using the notion of abstraction layers[11].

    - **Physical Media Analysis:** The analysis of the physical media translates the contents of a storage layout to a standard interface (e.g. IDE or SCSIs). Examples include a hard disk, compact flash, and memory chips.
    - **Media Management Analysis:** In the analysis of media management, evidence sources are organized based on certain criteria linked to data structures. Examples of this activity include dividing a hard disk into partitions, organising multiple disks into a volume, and integrating multiple memory chips into memory space.
    - **File System Analysis:** The analysis of the file system layer of abstraction, which translates the bytes and sectors of the partition to directories and files, involves viewing directories and file content leading to the recovery of deleted files.
    - **Application Analysis:** Analysis in this layer includes viewing log files, configuration files, images, documents and reverse engineering executable. The input data will typically come from the file system, but applications such as databases may read directly from the disk.
    - **Network Analysis**: Analysis in this layer includes managing network packets and IDS alerts. Analysis of logs generated by network services, a firewall or web server for instance, falls under the Network Analysis.

[10] The type of the system can be RTU, PLC, HMI, etc and final scope is to find the proper tools that can be used, based on the hardware and software specifications.

[11] B. Carrier, "Defining digital forensic examination and analysis tools using abstraction layers," Int. J. Digit. Evid., vol. 1, no. 4, pp. 1–12, 2003.

- **Memory Analysis:** Analysis in this area includes identifying the code that a process was running and extracting sensitive data that was stored in this code.

5. **Documentation of the process and results:** In every ex post analysis process, it is imperative to maintain comprehensive documentation. Detailed notes have to be kept with records of time, date, and the person responsible plus other essential information. This way it helps that no evidence has been tampered with by someone from inside during the ex post analysis and in the case of future incidents the documentation will be a baseline for the handling.

3.2 Organisational structures and procedures

For the above capabilities to be enabled within an organisation the appropriate structure and processes have to be in place with respect to incident responding and ex post analysis and investigation. Traditionally, an ex-post incident analysis program will be initiated after mitigation of incident and restoration of systems have been finalised by the existing incident response capability. Setting up an incident response capability is not trivial but there exist many resources describing the essential functions and organisational roles with their responsibilities.[12]

Incident response operations are important because, if they are badly designed, they have the potential to hinder any follow on ex post investigation effort, as vital evidence may have been removed or otherwise affected during mitigation, recovery and restoration activities. However, if planned well, integrating ex post analysis capability within incident response procedures may work, with the investigative function being a contained aspect of the incident response capability, up to and including any submission of data for prosecution purposes.

The core components of cyber incident response with an embedded investigative component would be modified as follows:

1. Detection
2. Response Initiation
3. Incident Response Action**/Evidence Collection**
4. Incident Recovery**/Evidence Analysis**
5. Incident Closure**/Process Reporting**

Due to the uniqueness of the data and the relationships amongst the information resources in the control systems domain, a team comprised of individuals that have an advanced understanding of the system should complete an analysis of collected evidence.

Therefore, besides the traditional incident responders, the team members would need to include roles and responsibilities such as[13]:

- **Control Systems Incident Manager (CSIM)** – a person with oversight of the responding operations in the control systems (CS) domain. They will have oversight of the activity ensuring liaisons with operations and IT personnel and ensure that requirements from both domains can be communicated in a manner that is understandable to all parties.
- **Control Systems Security Specialist (CSSS)** – involved in ascertaining what critical assets may have been impacted. The CSSS will also work closely with both engineers and incident

[12] "CPNI Good Practice Guide, PROCESS CONTROL AND SCADA SECURITY GUIDE 3. ESTABLISH RESPONSE CAPABILITIES."
[13] M. Fabro and E. Cornelius, "Recommended Practice: Creating Cyber Forensics Plans for Control Systems," Dep. Homel. Secur., 2008.

managers supporting both investigation and containment activities, and will have specific tactical activities supporting restoration, reporting, and analysis.

- **Control Systems Engineering Support (CSES)** – Being able to have someone from the control systems engineering support contributing to primary functions such as containment, recovery planning, and restoration (as well as system upgrade), will provide significant value to the ex post analysis.

Table 1.Roles matrix for incident response and analysis in control systems[14].

Incident Response Activity	Incident Handling Team	IR Coordinator (with CS)	Primary Security (POC)	Incident Response Director	CS Incident Manager	CS Security Specialist	CS Engineering Support	(CS Vendor Coordinator)
Detection								
Detection	P	S	P					
Initial Reporting and Documentation	P	P	P					
Response Initiation								
Incident Classification	P		P	S	P			
Escalation			P	P	P	S		
Emergency Action	P		P	P		S	S	P
Incident Response/ Evidence Collection								
Mobilization	S	P	S	P	P	S	S	S
Investigation	S	P	P	S	P	P	S	S
Containment	P	P	S	S	P	P	P	S
Incident Recovery/Evidence Analysis								
Recovery Planning		S	S	S	P	P	P	S/P
Restoration		S	S	S	P	P	P	S
System Upgrade		S	S	S	P	P	P	S
Incident Closure/ Process Reporting								
Summary Report		P	S	S	S	P	S	
Mitigations/ Reporting			P	P	P	P	S	S
System Upgrade	P		P	P	P	P	S	

Illustrated above as P are primary activities; and S – secondary functions.

[14] M. Fabro and E. Cornelius, "Recommended Practice: Creating Cyber Forensics Plans for Control Systems," Dep. Homel. Secur., 2008.

3.3 The evidence and its integrity dimension

To ensure the analyst has a concise and effective framework for executing a post mortem analysis in a control systems environment, the following traditional elements have to be examined[15]:

- **Reference clock system**[16]: Many SCADA systems, due to the nature of the processes that they run, require activities and transactions to be accomplished within milliseconds. Taking also into account the volatility of evidence in a control system, the analyst needs clock reference of high precision in order to carry out the ex post analysis. Time stamping and recording activities during the investigation requires a high precision reference clock.
- **Activity logs and transaction logs**: Depending on the nature of a SCADA system different data can be extracted from its various components during an ex post analysis.

Table 2.Types of data that can be extracted from the components of a SCADA system, based on the underlying control technology and the acquisition tools used.

	Control Centre	***Field Devices***
Modern/Common Control Systems Technologies	- Network traffic capture. - Contact system administrator in case of modified OS on HMIs.	- Network logs. - Control centre's logs regarding field devices. • Device is off: Examination of device for possible evidence. • Device is on: Date and time, current active processes and current running processes.
Modern/Proprietary Control Systems Technologies	- Contemporary ex post incident analysis tools may be applicable. - Network traffic capture. - Interaction between the investigator and the vendor is mandatory.	- Network logs. - Control centre's logs regarding field devices. - Interaction between the investigator and the vendor is mandatory. - May involve embedded vendor-specific security mechanisms.
Legacy/Proprietary Control Systems Technologies	- Traditional post-mortem analysis methods cannot be applied. - No logging functionality. - No longer supported by the vendor. - Interaction with the owner of the equipment may provide some information. - Serial-based communications; network traffic cannot be captured.	- Serial-based communication; network traffic cannot be captured. - Rapid rate of sampling and data override - Rapid rate of sampling and data override. - Interaction with the vendor is imperative. - An experienced engineer should be made available to support the investigation

- **Other sources of data:** Other sources of data that should be involved in an ex post incident analysis include the various storage devices that can be found in the control centre of a SCADA system. These devices include removable media such as floppy discs, CDs/DVDs, USB

[15] M. Fabro and E. Cornelius, "Recommended Practice: Creating Cyber Forensics Plans for Control Systems," Dep. Homel. Secur., 2008.

[16] When conducting an ex post incident analysis establishing a time reference is of vital importance for the normal progress of the investigation. In control systems, time synchronisation plays a major role not only for the incident investigation but also for the normal system's operation.

devices or any other form of removable storage media that can be found in the premises of the control centre.

- **General system failures**
- **Real time monitoring**
- **Device integrity monitoring**

The documentation process also includes the generation of a detailed Summary Report that describes the entire process. This report has to include the state and status of the captured system throughout the collection process. Below we are focussing on the first three aspects, as the last three are issues that are traditionally well understood within the context of operations in SCADA systems, due to the emphasis on fault management, safety and reliability reporting.

4 Challenges

The high volatility of their data, the limited logging mechanisms that they may use and other characteristics of SCADA systems pose many challenges in the process of data collection and analysis, both from the technical and the operational perspectives. This section describes the challenges that may arise during a post mortem incident analysis in SCADA systems:

A. Challenges of data collection:

- **Inadequate logging mechanisms**: Logging mechanisms in SCADA systems are geared toward process disturbances rather than security breaches offering thus limited contribution in the incident response field,
- **High volatility of data:** The nature of control systems imposes the deletion, removal or replacement of data in some components of the system, such as high-speed data recorders, in such a rate that it is practically unviable or impossible to collect them. The cost of logging mechanisms in such devices can be prohibitively high,

Post incident investigation: When non-volatile data, such as data stored on a hard drive, are collected from a turned off system then the procedure falls into the category of post incident investigation.
Live investigation: When volatile data need to be collected, such as memory dumps or network activity, then the process falls into the category of live investigation.

- **Customised operating system kernels**: A SCADA system may utilise customised kernels running on its components in order to enhance the performance of the system, despite the fact that updating such kernels is difficult. This can render traditional data acquisition tools such as DD or memdump unable to run due to incompatibility issues or missing kernel modules.
- **Extensive lower data**: Gathering information on lower levels of a SCADA network, such as data produced by sensors, would lead to vast amounts of information that require huge amount of storage.
- **Low computational power**: Legacy systems have very little computational power for the recording and analysis of data that is produced in conjunction with control data. Therefore,

at this level no further operations can be implemented regarding other processes like incident analysis.

B. Challenges of data analysis:

- **Ex post analysis tools**: Contemporary tools for ex post analysis rely on precompiled scripts and programs that automate the evidence collection process by utilising certain techniques, such as bit copy processes and checksum generators that may not be applied in platforms and software elements of a control system in their native form so that afterwards analysis can be done. Software modifications need to be implemented in traditional analysis tools in order to meet the specifications of a control system.

- **Data analytics and correlation:** Data gathered from key data repositories (such as Data Historians and HMIs) and volatile non-persistent data collected from the various field devices (such as PLCs and I/O devices) need to be correlated in order to create an informative representation of the incident that can be considered as evidence.

C. Operational challenges:

- **The apparent culture gap** between Information Technology (IT) specialists and Operations personnel: At first sight, such division appears to be created by the differences in operational objectives between the industrial control community (availability, reliability, safety) and the traditional IT security focus (confidentiality, integrity, availability).

- **The absence of dedicated scientific studies**: There is lack of dedicated scientific studies on the performance of typical control and instrumentation equipment operating under security configurations of tight access control, strong encryption and comprehensive event logging. The end-user community appears rather conservative upon adopting security architectures that are built on these premises.

- **Management of obsolescence** and the availability of skills to handle legacy systems: Currently the user community identifies a significant skills shortage in this area, with key people retiring and the new generation of engineers not readily possessing the skills to work on older systems.

- **The fundamentally different lifecycles** of the infrastructures: Components of a traditional IT infrastructure would have a limited lifecycle in comparison to the SCADA instrumentation and control equipment (typically 5-7 years versus perceivably a few decades correspondingly).

5 Recommendations

ENISA has identified the following key areas where action can be taken in order to develop investigative capabilities that match the level of perceived risk:

A. **Facilitate integration with existing structures for reporting and analysis**:
   a. Understand where evidence may be found: As part of the traditional risk assessment process, it may be beneficial to consider along with the scenarios of security breaches where evidence is crucial and to identify where this evidence could be found.
   b. Understand the impact of data retention: It is recommended that some form of impact assessment of data retention policies is performed on a test infrastructure that resembles the operating environment. It is essential to develop an understanding of whether any overhead is introduced (and how much if so), when enabling more advanced logging features over and above the traditional fault recording and performance-tracking paradigm of operation.
   c. Manage obsolescence and the IT/Ops interface: Albeit not directly related to ex post analysis, a structured plan for obsolescence management, where applicable, will ensure that adequate knowledge of legacy systems exists and that access to the appropriate facilities for their management is possible.

B. **Safeguard systems and configurations**:
   a. Deploy adequate security controls that also perform logging – such as firewalls and intrusion detection systems: The cornerstone of effective security management is the implementation of appropriate and well-measured controls able to balance the risk and provide mechanisms to counter and follow up incidents.
   b. Design systems with evidence protection in mind: Adequate protection of data historians is essential for forensic-grade evidence retention. Contemporary systems may be able to log a variety of events but if the access to the logs is compromised an attacker could easily erase their tracks.
   c. Enable logging of common events across the system as a minimum: Most contemporary control systems and equipment at device level are capable of producing and retaining a wealth of information related to their operational status and also to contextual events. However what events can be logged and the exact form of the data may vary tremendously from one equipment vendor to another.

C. Review key roles and responsibilities:
   a. Identify gaps in digital investigation skills: It is important to understand the available level of (or the lack of) skill and knowledge of investigative expertise among existing staff.
   b. Identify physical and cyber response interfaces and overlaps: A review of organisational roles and responsibilities involved in incident response, including operational, physical security and cyber incidents, may facilitate the integration of the responding capability from both physical and cyber perspective.

D. Pursue inter-organisational public and privately held and cross country cooperation:
   a. A coordinated approach at cross-country level (e.g. pan European): This could be another dimension that could promote further community development.
   b. Experience sharing and multi-party private and public collaboration may enhance the chances of delivering a solution that is comprehensive and applies more generally: Enabling inter-state collaboration is perceivably critical, as attacks may be targeted across a number of sites, from a number of foreign jurisdictions.