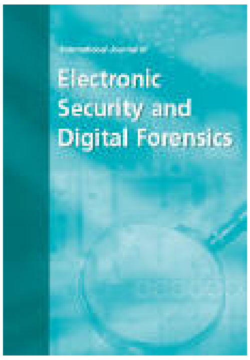


International Journal of Electronic Security and Digital Forensics

ISSN online: 1751-9128 - ISSN print: 1751-911X
https://www.inderscience.com/ijesdf

An approach towards development of a supervisory control and data acquisition system forensics framework: concerns and challenges

Ramya Shah, Digvijaysinh Rathod

DOI: 10.1504/IJESDF.2025.10068185

Article History:

Received:	24 December 2022
Last revised:	04 April 2023
Accepted:	05 June 2023
Published online:	23 December 2024

An approach towards development of a supervisory control and data acquisition system forensics framework: concerns and challenges

Ramya Shah* and Digvijaysinh Rathod

School of Cyber Security and Digital Forensics,
National Forensic Sciences University,
Gandhinagar, Gujarat, India
Email: ramyashah4@gmail.com
Email: todrdigvijay@gmail.com
*Corresponding author

Abstract: In the highly competitive technology market, supervisory control and data acquisition/industrial control systems (SCADA/ICS) have seen quick growth. They are also at the heart of operational technology (OT), which is used in businesses and processing facilities to monitor and control crucial processes in varied sectors as energy, railways and many more. However, in the event of a security incident (such as a system failure, security breach, man-in-the-middle attack or denial-of-service attack), it's critical to comprehend the digital forensics implications of such incidents, the procedures or protocols that must be followed during an investigation, the tools and techniques that an investigator should use, and where and how forensic data can be collected. It is crucial that forensic investigations start right away after a security incident due to the rising threat of sophisticated attacks on key infrastructures. This examination of current SCADA forensic researches and numerous forensic investigation methods is presented in this work. The limitations of employing conventional forensic investigative methods and the difficulties faced by forensic investigators have also been covered. The shortcomings of current research into offering forensic capacity for SCADA systems are also thoroughly reviewed.

Keywords: SCADA forensics; ICS forensics; OT; digital forensics.

Reference to this paper should be made as follows: Shah, R. and Rathod, D. (2025) 'An approach towards development of a supervisory control and data acquisition system forensics framework: concerns and challenges', *Int. J. Electronic Security and Digital Forensics*, Vol. 17, Nos. 1/2, pp.30–44.

Biographical notes: Ramya Shah is working as an Assistant Professor, School of Cyber Security and Digital Forensics, National Forensic Sciences University, Gandhinagar, Gujarat. His areas of interest are ICS/SCADA security and forensics, incident response and threat intelligence, digital forensics blockchain security and forensics. He received his Master of Technology (2019) for Cyber Security and Incident Response from Gujarat Forensic Sciences University, Gujarat, India after completion of Bachelor of Technology (BTech) for Computer Engineering (2017).

Digvijaysinh Rathod received his BSc (Electronics) and Master's in Computer Application (MCA) respectively. He completed his PhD in Computer Application from Ganpat University (GUNI), India. He is currently working as an Associate Professor (Cyber Security) in the School of Cyber Security and

Digital Forensics, National Forensic Sciences University (Institution of National Importance), India. He has around 18 years of teaching and research experience, and has published more than 30 research papers in the reputed journals, conferences, and seminar and workshop proceedings. His area of interest includes mobile and web application security, blockchain and ICS/SCADA security.

1 Introduction

The world and the technology being used in there are evolving at a rapid rate. information technology has been prevailing and ruling the world since years. The use of computer systems has been escalated in last decade to connect and control all the aspects of enterprise information technology (IT) enterprise (Krishnan and Wei, 2019). But coming to the modern era where operational technology (OT) are evolving, not only in terms of operations but also in terms of security. The soaring new disciplines for research such as CPS also stated as cyber physical systems (Rajkumar et al., 2010), SoS also stated as systems of systems (Lane and Epstein, 2013), Unicom also stated as ubiquitous computing (Friedewald and Raabe, 2011), IoT also stated as internet of things (Khodadadi et al., 2017) clearly represents the need of the emerging technologies and their implementation in real world life scenarios.

The hardware and the associated software that detects the change and monitors/controls the industrial equipment or assets or critical infrastructures (power stations, dam, telecommunication, refineries) can be termed as OT. If we state it in simple terms, control systems accumulate information and performs the operation based on functional parametrised inputs (DHS, 2009. The first use of control systems was in 1960s to monitor incidents that were executed by humans. But in last three decades, control systems have evolved as a major technological trend).

Industrial control system/SCADA system is a major segment within the OT umbrella and is the core of digital society. They are the underpinning technologies which ensures the proper functionality and operation of national critical infrastructure. The SCADA systems generally are used to automate the processes of power generation plant or power distribution plant or petroleum refineries or water management or many more. From being a part of standalone systems to getting the complete infrastructure connected to internet is the whole new paradigm shift. Initially, due to the its standalone nature, modern day security threats were not a part of the threat model. However, since recent times, industrial control systems have evolved to communicate over various types of network and networking protocols, which eventually leads them exposed to varying class of threats that can harm the digital infrastructure. SCADA systems as they interact with the real-world aspects, they were designed with an emphasis for safety than security (Krishnan and Wei, 2019).

The modern time critical infrastructure including oil, water, natural gas, power, various other manufacturing industries rely heavily on computers, their connected networks, the control systems and the constrained embedded devices in preview to provide safe and reliable operations. Abundance of researches have been carried out with a plethora of cyber security assessment tools in IT domain to identify and patch the vulnerabilities existing in the ecosystem, however a similar effort has not been noticed in the domain of in the umbrella domain of OT (Onyiego and Abade, 2020).

Attacks on the critical infrastructures have gained a momentum over last few years. According to the report by Kaspersky ICS CERT (2022) in their threat landscape, 39.6% of the industrial control system computers were attacked in 2021.

Figure 1 ICS threat sources globally (see online version for colours)

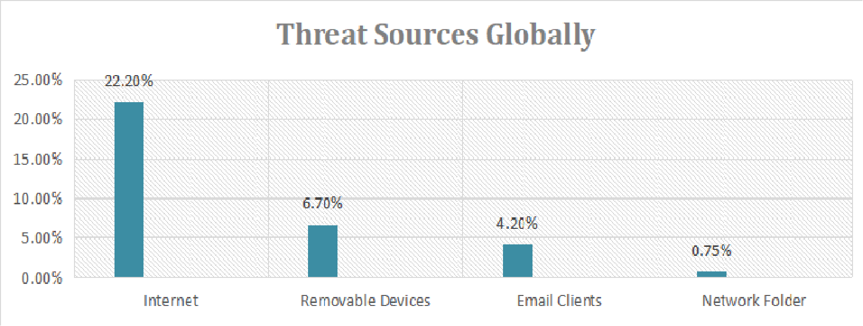
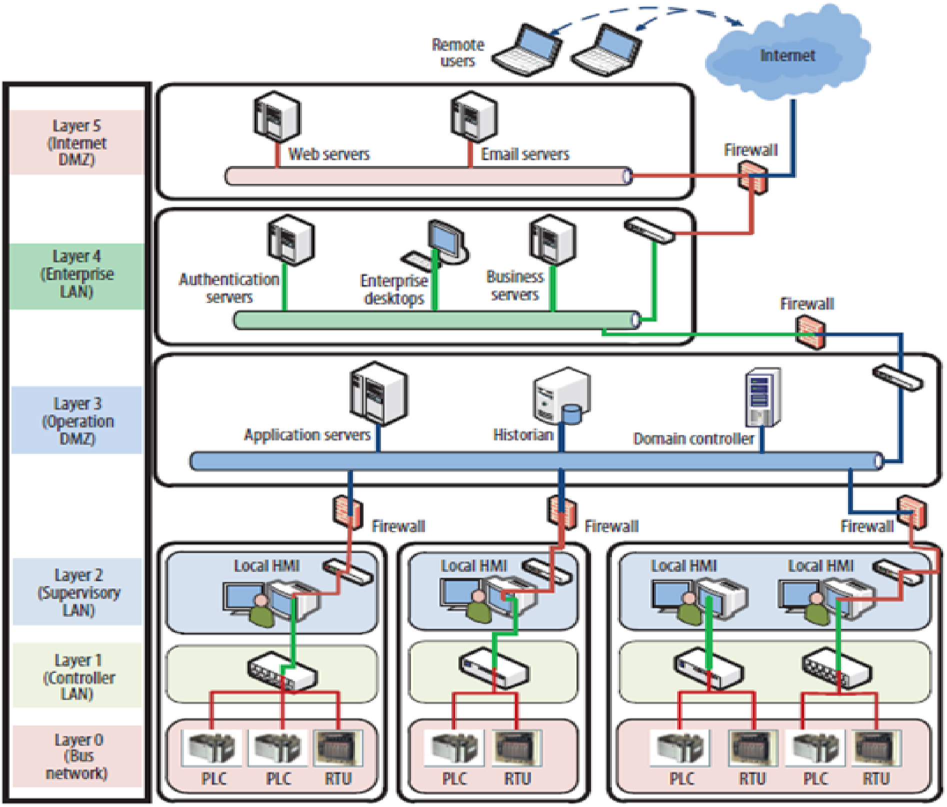


Figure 2 SCADA system layers (see online version for colours)



Source: Ahmed et al. (2012)

2 Background study

SCADA system generally can be categorised into following components:

- Control components: This includes programmable logic controllers (PLC), intelligent electronic device (IED), human machine interface (HMI), data historian and data acquisition server, sensor and actuators.
- Network components: This includes network topologies such as star topology, bus topology, mesh topology and many others and control networks (connecting network from control level to lower level).

Irfan and his colleagues in their paper divided the SCADA system architecture into 5 layers as shown in Figure 2, where the lower layer or the layer 0 includes all the field devices viz. Sensors, Actuators, many more which are connected through the bus network. The above layer, layer 1 acts as a controller layer that receives input signals from the various connected field devices. Layer 2 in the Figure 2 acts as a supervisory network, basically to connect the lower layers and get the view points in the HMI. The DMZ, data historian belongs to layer 3, where layers 4 and 5 are represents the enterprise IT network (Ahmed et al., 2012).

The ICS/SCADA systems runs on various protocols. The protocols that are being used ICS/SCADA systems are BITBUS, DC-BUS, EtherCap, PROFIBUS, DNP3, MODBUS, IEC 60870, IEC 61850 and many more.

2.1 Security incidents on industrial control systems

The attacks on SCADA systems have grown in wider ranges since its connectivity to the external world through internet.

The various major ICS/SCADA Systems incidents can be identified from the stated Table 1.

Table 1 ICS/SCADA systems security attacks

Year	*Incident description*	*Attack industry*	*Ref.*
1982	CIA Trojan causes Siberian gas pipeline explosion	Petroleum	11
1989	Oil Company SCADA system impacted by RF interference	Petroleum	11
1992	Computer sabotage at nuclear power plant	Power and utilities	11
1994	Salt river project hack	Power and Utilities	11
1995	Oakland Air-traffic control centre outage	Transportation	11
1996	Omega engineering sabotage	Electronic manufacturing	11
1997	Worcester air traffic communications system hack	Transportation	11
1998	Hackers attack NZ and Aust. for joining gulf taskforce	Power and utilities	11
1999	Navy radar shuts down SCADA systems	Water/waste water	11
1999	Hacker takes over Russian gas system	Petroleum	11
2001	DoS attack shuts down port of Houston	Transportation	11

Table 1 ICS/SCADA systems security attacks (continued)

Year	*Incident Description*	*Attack industry*	*Ref.*
2001	Electronic sabotage of petroleum company's gas processing plant	Petroleum	11
2003	Slammer impact on Ohio nuclear plant	Power and utilities	11
2003	London August 2003 power blackout	Power and utilities	11
2003	Iranian hackers attempt to disrupt Israel power system	Power and utilities	11
2007	California canal system hack	Water/waste water	11
2008	Blackout in Florida	Power and utilities	11
2008	Georgia nuclear power plant shutdown	Power and utilities	11
2010	Cyber-attack on Texas electricity provider	Power and utilities	11
2010	Malware targets uranium enrichment facility (Stuxnet)	Power and utilities	11
2011	Malware shuts down hospital	Healthcare	11
2011	Iranian oil terminal offline after malware attack	Petroleum	11
2014	Malware attack on electricity – blackenergy3	Power and utilities	11
2014	German steel mill cyber attack	Metals	11
2016	Ukrainian PowerGrid	Power and utilities	11
2017	Dragon Fly 2.0 – disruption of energy sector	Power and utilities	12
2017	Malware attack – triton	Petroleum	
2021	Colonial pipeline attack	Petroleum	13
2021	Solarwinds supply chain attack	Others	

The most critical factor is to carry out forensic investigation soon after the attack to prevent the damage/loss of the artefacts that can be retrieved from the SCADA systems. There should be a strategy to carry on with the investigation in place. The investigative purpose should be to identify the incident, the perpetrators who committed them by identifying the leftover footprints (Wu et al., 2013).

2.2 Role digital forensic investigation in ICS/SCADA systems

Digital forensics is a branch of forensic science that deals with data acquisition and analysis of data acquired from the digital device which can be related to the scene of incident. In the environments of industrial ecosystems such as SCADA, the forensic investigator play a prime role and responsibility to determine the causes of incident and the potential location of the artefacts along with a comprehensive report which can establish the crime (Ahmed et al. 2012).

The Malware attack – Stuxnet in June 2010 (Markoff, 2010), Colonial Pipeline Attack in 2021 (One password allowed hackers to disrupt Colonial Pipeline, CEO tells senator, 2021) and many more provides a strong presentation for the development and deployment of forensic capabilities to help through the post-incident investigations.

The traditional computer forensic tools and the forensic approaches are rapidly getting outdated in terms of upcoming technological advancements and their needs be upgradation on tools and approaches to achieve an immediate result with proper investigative approach (Wu and Nurse, 2015).

Also, James and Gladyshev (2013) showcased that there is a need to adopt the automated forensic solution for investigators which can improve the quality and the speed of investigation, which also spares time for the forensic investigators to research on various challenges and come up with advance manual investigative techniques. In the forte of OT, the use of digital forensics is quite limited, the available research focuses on SCADA systems in making them more secure (Iqbal et al., 2019).

A view point of digital forensic investigation of SCADA systems can be seen or noticed in different layers based on the connectivity of different components to their local networks or interconnection of components or connection of various components to the internet (Bailey and Wright, 2003). Also taking about artefacts, a small modification of PLC memory can be stated as a digital forensic artefact and it can be further used to reconstruct a timeline of events (Iqbal et al., 2019).

The below stated tools are traditional forensic analysis tools used for IT systems. These tools can be used for forensic analysis of the IT workstation systems existing on higher layers (layers 3, 4, 5) of SCADA systems.

Table 2 Traditional digital forensic tools for IT forensic investigation

Sr. no.	*Tools*	*Basic description*
1	Forensic toolkit	FTK or forensic toolkit is a traditional software application that is used for the forensics of the IT workstations.
2	Encase forensics	It is developed by guidance software and popular tool for computer systems forensic investigation

2.3 Study of existing studies

Krishnan and Wei (2019) state about crafting and designing a low budget SCADA lab as stated in Table 2, for allowing students to study vulnerability assessment and penetration testing. They state the problem statement in the form of communication loophole between the engineering teams and the IT enterprise network along with lack of cyber security readiness for the process control systems. The lab setup was designed vulnerable from passcode access to protocol integrity and also focused on investigating live attacks from various component sources integrated in the ecosystem.

Table 3 SCADA testbed details

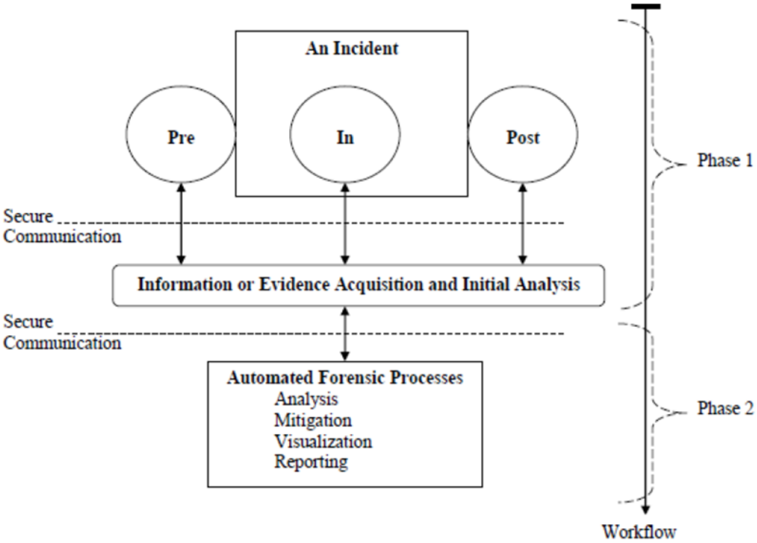
Testbed	*Major protocols*	*Purpose*	*By/mentioned*
SCADA LAB	MODBUS, TCP/IP, OPC-DA, OPC-UA, KOYO	Curriculum studies to learn VA-PT and live forensics investigation.	Sam Houston State University (SHSU)

Source: Krishnan and Wei (2019)

The author states about the approach taken for the penetration and investigation of SCADA Lab (Krishnan and Wei, 2019) setup at Sam Houston State University. The approach is divided into four stages: identifying vulnerabilities, identifying the attack methods, implementation of immediate reduction of risk policies and implementation of long-term solutions to enhance security. The paper also states about the data acquisition and analysis of attack as the major forensic challenge of SCADA systems. The authors here lacked a forensic tool to collect artefacts from the designed testbed which is a prime requirement for SCADA forensic investigation.

Wu et al. (2013) presented the various typical methods of attacks on Industrial Control Systems and various threat on SCADA systems due to enhanced technological developments. This paper also presented a draft forensic architecture for SCADA systems which focuses on memory change parameters of the PLC (S7) connected during the time of attack. The proposed forensic architecture followed the generalised incident response forensic process from identification to reporting where the theoretical approaches and the potential sources of artefacts were stated including End Point Devices, Routers, Switches, Databases, Servers, Workstation, HMI and many more. The paper also stated the limitations of traditional IT forensic process due to the connected constrained devices in the ecosystem and their protocols which aren't found normally in IT systems. The experiment environment included a scenario of traffic light system managed by S7-PLC through the OPC server and STEP-7 watch table. The future work of the paper also states the identification of artefacts on various levels, storing and analysing them needs to be conducted.

Figure 3 A conceptual framework for SCADA forensics



Source: Elhoseny and Abbas (2020)

Ahmed et al. (2012) discuss about various challenges faced by forensic investigator while investigation SCADA Systems forensically. The authors divided the SCADA systems into five layers and emphasised on forensic investigation of layer 0, 1 and 2. The lower layers of the layered architecture includes field instruments, PLC, sensors, actuators, remote terminal units and HMIs. Acquisition model for live data acquisition was considered as a major challenge in SCADA ecosystems, as the SCADA systems cannot have a down time for forensic analysis. The authors also state "It is still unclear how to acquire live data on a SCADA system in a way that minimises risk to the system's services." The paper also discussed various other forensic challenges in SCADA/ICS systems which are discussed further in this paper. The paper also emulated a resource constrained system to showcase how resource intensive data acquisition tools can be by running various versions of DD tools on the emulated system and presenting the consumption of resource. Devices like PLC and RTU can be categorised as resource constrained devices.

Elhoseny and Abbas (2020) discuss about forensic aspects in investigation within industrial environments – SCADA networks as primary focus and related control systems like PLC and distributed control systems (DCS) and investigates the probability of adding a new forensic framework for automated forensic investigation in SCADA systems. The initial stage of paper focuses on obstacles in acquiring data for forensic investigation – live process data acquisition, highly distributed SCADA locations, multiple SCADA operable levels and many more. The paper also presents a review of efforts taken in SCADA digital forensic investigation literatures. The authors in the paper also proposed a conceptual framework for automated forensics investigation of SCADA systems with an aim of its implementation in the coming future. The conceptual framework presented had been divided into two phases, where phase 1 monitors the security incidents while the phase 2 can be launched when an incident is detected to provide a complete analysis on the event. A conceptual security model with trust factors has also been presented.

Elhoseny and Abbas (2020) also proposed a realisation architecture for the stated conceptual model in Figure 3, where they have proposed multiple offline and online agents in connection to the SCADA network architecture.

Ji Ho and Jeong (2019) have discussed a taxonomy on SCADA forensics and various research trends that can lead to an effective investigation for ICS/SCADA systems. The authors also discussed about varying range of challenges based on layers of the SCADA system architecture.

Table 4 Taxonomy of SCADA forensics according to traditional digital forensics classification

Category		*Target evidence*
Object	Disk	Operating system, storage, historian database and internal log
	Memory	Physical memory (RAM)
	Network	Communication packet, connection information, network monitoring, security vulnerability detection
Data status	Live	Volatile data collection, analysis (such as RAM, network connection information, process information)
	Silent	Storage and static physical memory (RAM), network packet, malwares, worms

Source: Ji Ho and Jeong (2019)

Yildiz et al. (2018) have designed a SCADA laboratory to study and enhance their capabilities in concepts of vulnerability assessment and penetration testing, forensics of SCADA systems, etc. The designed lab included components such as PLC'S from varying manufactures as Allen Bradly, Schneider, Eaton, Automation Direct and software such as open platform communication (OPC) based on concepts of interoperability with various different transducers and outputs were configured in the system. The lab setup also used additional hardware like protocol convertor to ensure the compatibility, microcontroller having 802.11 abilities, network switches, WAP, desktop computers and an IP camera. The tools used through the process are:

Table 5 Tools used during the analysis

Tools (security and forensics)	*Task*
Nmap	Network mapping tool
EtterCap	Man-in-the-middle attack tool
ZED Proxy	Web app security scanner
Wireshark	Network packet analyser
MBSA (microsoft baseline security analyser)	Assessment tool (for misconfigurations in Security and updates)
LOIC (low orbit ion canon)	An utility tool to test network stress

Source: Yildiz et al. (2018)

Senthivel et al. (2017) present forensic analysis of programmable controller communication commands (PCCC) protocol for transferring the control logic files to the PLC. The PLC used in the experiment was Micrologix 1400 PLC. The programming software used here was Allen Bradly's RSLogix 500 to upload and download the PLC programming logics and the authors also identified that after compiling a ladder logic program, the software does not create low level representation of ladder logic program. The authors also prototyped a tool which can extract PLC logic as well as crucial critical information about PLC. The authors also extracted the PCCC message that has file type and file number fields. During the course of paper, the authors have also compared various ladder logic files, SMTP files to maintain a baseline for analysis. The prototyped tool named 'CUTTER' can extract SMTP configuration through the network traffic and can be parsed to obtain email address, Username and password. This prototype tool is considered to be light weight and does not require higher CPU and memory power.

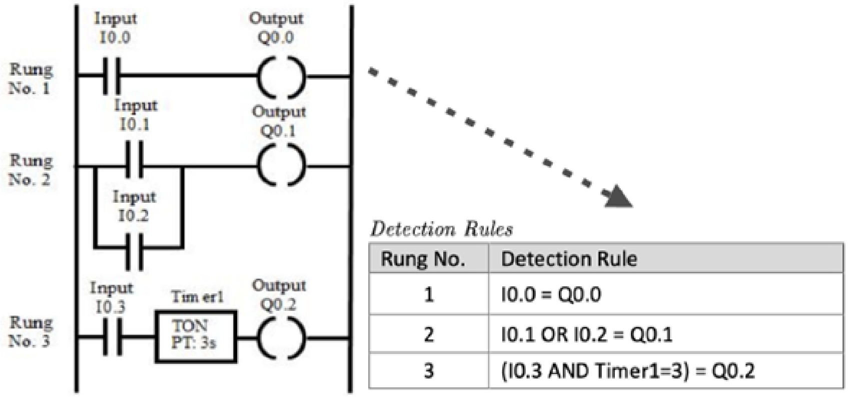
Onyiego and Abade (2020) have discussed about various aspects of digital forensics and cyber security in ICS/SCADA systems. To take a step ahead in forensic investigation of SCADA systems, they designed a testbed to collect digital artefacts from the SCADA systems. The testbed comprised of 'Modicon M340 PLC', 'BMX DDI 1602' – an input module, 'BMX DDO 1602' – a discrete output module and the various peripheral software and hardware devices. The testbed showcased worked as a minor petroleum industry where the product runs from one terminal to the other terminal (tank) and the transfer is being monitored with various sensors. John and his colleague captured the network traffic using wireshark and also performed few man-in-the-middle attack using Ettercap tool which exploited the system. The captured data was analysed using Hex Editor Toolkit, Wireshark and also a tool was developed by the authors in C# to see the current register setting of the PLC which works only on the Modbus TCP/IP of Modcon M340 PLC. The paper wasn't able to establish the forensic artefacts on similar devices/protocol and various other potential locations which play a vital role in forensic investigation.

Attacks on SCADA systems are becoming more popular with the connection of them to wider networks like the internet. A forensics analysis needs to be made on how to protect these systems against attacks, without interfering with the always on nature of most SCADA systems. The amount of data a SCADA system uses is approximately 400 GB per day. If a monitoring and logging system is to be placed in the system it needs to be able to handle that amount of data while also not interrupting the normal flow of the SCADA system. Most SCADA systems run on old platforms that require legacy support and thus another challenge is finding forensic software that is up to date but also runs on these really old systems. A lot of data is also volatile and changes frequently, so the forensics needs to be able to read this data as fast as possible before it changes to get accurate results. As many other papers mentioned, there is no generic model for SCADA forensics and one needs to be made and be able to run without interfering with the system (Ji Ho and Jeong, 2019).

Iqbal et al. (2019) have suggested the use of Sandbox to test the malware and analyse it is behaviour in OT environment. The authors have implemented a similar technique to improvise the forensic test bed in reference to a real-time hardware configured in loop mode which was achieved by running a suspicious code without impacting the host. Through their setup of testbed for power systems, they were able to map different attacks in a WAMPAC application. The study however wasn't able to capture the memory artefacts of the PLC which holds key values in consideration of forensic artefacts.

Yau and Chow (2015) stated the need of software to identify and detect the incongruity inside the PLC by Siemens. The paper showcased a designed tool stated as "CPLCD – Control Program Logic Change Detector" that identified and captured incidents which affected the normal operations of the PLCs. The authors used rules to detect the change of working behaviour. The CPCLD has a limitation of detecting attacker or his path after an incident, so the authors suggest to use tools like 'Wireshark' for further analysis. The complete set of operation was carried on S7 programmable logic controller. They also prepared a ladder logic to rule detection converter.

Figure 3 Ladder logic to detection rules



Detection Rules

Rung No.	Detection Rule
1	I0.0 = Q0.0
2	I0.1 OR I0.2 = Q0.1
3	(I0.3 AND Timer1=3) = Q0.2

Source: Yau and Chow (2015)

The paper (Stirland et al., 2014) discussed about various approaches to SCADA forensics. The authors also provided a generic approach along with available forensic tools as a part of toolkit which can be used by the incident responders to respond to any such incidents related to cyber. The author also stated that the forensics of ICS has a different approach from standard general disk – imagining forensics, as the potential location of artefacts changes in SCADA systems that of a traditional IT system.

The research fraternity is mainly focused on security enhancements of SCADA system or ICS, but there also needs a primary focus on forensic investigation of ICS/SCADA systems. Tim Kilpatrick and colleagues proposed an architecture approach to observe and monitor the operation process flow which can eventually be used for forensic purpose. The architecture approach discussed the analysis of the process/operations behaviour through sensor data and control actions and identifying the change of trends to optimise the throughput of the plant (Kilpatrick et al., 2006).

The existing studies in forensic can be compiled in reference to the paper as:

	Title	*Year*
	Published	
Methodology	SCADA systems: challenges for forensic investigators	2012
	IEEE Computer Society	
	Towards a SCADA forensics architecture	2013
	Proceedings of the 1st International Symposium for ICS and SCADA Cyber Security Research	
	Developing cyber forensics for SCADA industrial control systems	2014
	The Society of Digital Information and Wireless Communication	
	A Forensic Taxonomy of SCADA Systems and Approach to Incident Response	2015
	Proceedings of the 3rd International Symposium for ICS and SCADA Cyber Security Research	
	Guide to Industrial Control Systems Security (NIST 800-82 R2)	2015
	National Institute of Standards and Technology	
Analysis/Techniques	Accurate modelling of the Siemens S7 SCADA protocol for intrusion detection and digital forensics	2014
	Journal of Digital Forensics, Security and Law	
	Exploring the use Of PLC debugging tools for digital forensic investigations On SCADA systems	2015
	Journal of Digital Forensics, Security and Law	
	PLC forensics based on control program logic change detection	2015
	Journal of Digital Forensics, Security and Law	
	SCADA network forensics of the PCCC protocol	2017
	Digital Investigation	
	A Forensic logging system for Siemens programmable logic controllers	2018
	IFIP International Conference Digital Forensics	
	Supervisory control and data acquisition (SCADA) system forensics based on the Modbus protocol	2020
	International Journal of Computer (IJC)	

3 Recent challenges in forensic investigation of ICS/SCADA systems

Based on various studies undergone, the following can be stated as forensic challenges for forensic investigators to carry on forensic investigation of SCADA Systems.

- Live data acquisition: An ICS/SCADA system needs to be in operation 24 × 7 for reasons like safety and monetary feasibility. Live forensics is the most vital and primary part of digital forensic investigation. The data of ongoing process, ongoing parameter change values can be retrieved from volatile memory of devices and hence the data is also called as volatile data. The process to acquire volatile data from digital devices is called volatile memory forensics. Live forensics is more and more useful because of the potential artefacts the investigator is searching for might be present once the system is in shut down state. The potential retrievable artefacts from the system through live forensics includes change in ladder logic, change in opcodes, manipulation of some protocol data and many more.

- Lack of compatible forensic tools and techniques: The Industrial system comprises of a greater number of resource constrained devices. Also on current phase there are no generalised and direct implemented acquisition tools that can extract data from embedded devices. This happens as there is very less demand for data acquisition vendors to add compatibility with SCADA devices or eventually to produce hardware or software-based solutions to collect data forensically from SCADA systems (Olivier and Shenoi, 2006; Fabro and Cornelius, 2008).

  In considerations of the attacks which targets the field devices like PLC, there are good chances of artefacts to find out from such devices. However, compatibility of tools is a challenge to capture RAM and flash memory of the PLC along with PLC data.

- Identification of potential data sources: The architecture of SCADA system is complex in nature as the data flow passes through varying layers through the architecture. In case of collection of the complete data, it becomes extremely difficult to normalise the data collected and identify the incident of the event. Even in such cases to identify the malicious data packet passing through adds to the challenge. It is also challenging task for the forensic investigator to identify the types of data sources that can be useful in forensic investigation.

- Varying attacks in sophisticated manner: In reference to the Table1, it can be determined that there are pool of attacks that can be performed on the SCADA systems. Each and every attack has its own tactics, techniques and procedures to execute the attack. The recent cyber-attacks have increased in their abilities to perform attacks like malicious packet injection, buffer overflow, code injection and many more. With increase of attacks in sophisticated manner, it increase challenges for the investigator to analyse the incident.

- Varying range of customised OS Kernels: supervisory control and data acquisition systems run customised kernels on its components for comparatively better performances and extended supports. For Example – 'PatriotSCADA (SAGEFirst – PATRIOTSCADA) is a firewall solution for SCADA networks that uses a customised Linux kernel to enforce access control and role-based security for every request in the kernel.' This increases the challenge for the forensic investigator to identify the compatible tools and their modules for the customised OS kernel. If the module fails to find itself compatible, data acquisition or forensics investigation would come to a halt.

- Devices used (resource constrained devices): The smaller devices with limited CPU, memory and power resources are termed as constrained devices which includes sensors, actuators, smart objects (RFC – 7228, https://datatracker.ietf.org/doc/html/rfc7228#). The field devices like RTU, sensors and PLC are all resource constrained devices. To extract data from such constrained devices lightweight data acquisition tools which adds a challenge for the forensic investigator.
- Extensive logging: In SCADA systems or any ICS ecosystems, the layer 0 comprises of field devices like sensors, actuators, motors, valves and many more creating large amount of data which can sometimes range beyond 4,000 measurements per second. To log all the created data, to capture and analyse in itself is a challenge. Also, to prove the visibility of the attack by analysing all the collected is a bigger challenge.
- Highly distributed plants/systems: In shifting paradigm towards the highly scaled system in Industrial plants including nuclear energy, power & utilities, water/waste management and many more, this system includes large number of components to come up with an forensic investigation strategy for all the devices is a challenging issue. Also as these systems are distributed physically to a large extent, automating the process also add the challenge.
- Era of legacy systems: The system developed comprises of various legacy devices or lower layer devices coming from some specific vendor. Some in-turn supports cross platform data transmission, which adds an obstacle for a forensic investigator to carry on with specific data acquisition model.
- Varying range of protocols: The pool of protocols operable in SCADA Systems are completely different apart from the IT ecosystem protocols such as TCP/IP, HTTP, FTP and many others. To handle the heterogeneity of all such protocols needs a tool that can handle all the diversities.
- Investigation approach: Having complex architecture, wide range of connected devices, wide range of operable protocols, wide range of dynamically variable data types there always lies a challenge in identifying a perfect investigative approach for forensic investigation of SCADA system.

4 Conclusions

Because of the underlying industrial processes they control, performing a forensic investigation of SCADA systems is fundamentally different from investigating corporate or home networks. SCADA-focused forensic research is essential to address the unique challenges associated with these systems. It is also desirable to encourage SCADA system owners and operators to initiate steps that can facilitate an investigation if needed – for example, by maintaining a data acquisition plan and regularly testing data acquisition tools to ensure that they will not affect the availability of SCADA system services. The designed tools should be lightweight in nature and should support the data acquisition from the constrained devices.

References

Ahmed, I., Obermeier, S. and Naedele, M. and Richard III, G.G. (2012) 'SCADA systems: challenges for forensic investigators, DOI: 10.1109/MC.2012.325, 2012.

Bailey, D. and Wright, E. (2003) 'Background to SCADA, practical SCADA for industry', *Newnes*, pp.1–10, ISBN: 9780750658058, https://doi.org/10.1016/B978-075065805-8/50001-5.

DHS (2009) Cyber Security Procurement Language for Control Systems, USA [online] https://www.energy.gov/sites/default/files/oeprod/DocumentsandMedia/SCADA_Procurement_Language.pdf, (accessed 19 September 2023).

Elhoseny, M. and Abbas, H. (2020) 'Towards automated SCADA forensic invesitigation - challenges, opportunities and promising paradigms', *Int. J. Information and Computer Security*, Vol. 13, Nos. 3–4, p.2020.

Fabro, M. and Cornelius, E. (2008) *Recommended Practice: Creating Cyber Forensics Plans for Control Systems,* August.

Friedewald, M. and Raabe, O. (2011) 'Ubiquitous computing: an overview of technology impacts', *Telematics and Informatics*, Vol. 28, No. 2, pp.55–65.

Iqbal, A., Mahmood, F. and Ekstedt, M. (2019) 'Digital forensic analysis of industrial control: systems using sandboxing', *Energies*, Vol. 12, p.2019, DOI: https://doi.org/10.3390/en12132598.

James, J.I. and Gladyshev, P. (2013) *Challenges with Automation in Digital Forensic Investigations*, arXiv preprint arXiv:1303.4498.

Ji Ho, S. and Jeong, S. (2019) 'Research trends of SCADA digital forensics and future research proposal', *Journal of The Korea Institute of Information Security and Cryptology*, December, Vol. 29, No. 6, pp.1351–1364.

Kaspersky ICS CERT (2022) [online] https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Threat-landscape-for-industrial-automation-systems-statistics-for-H2-2021-En.pdf (accessed 25 November 2022).

Khodadadi, F., Dastjerdi, A.V. and Buyya, R. (2017) *Internet of Things: An Overview*, arXiv preprint arXiv:1703.06409.

Kilpatrick, L., Gonzalez, I., Chandra, R., Papa, M. and Shenoi, S. (2006) 'International federation for information processing', *Advances in Digital Forensics II*, Edited by M. Olivier and S. Shenoi, Vol. 222, pp.273–285, Springer, Boston, MA.

Krishnan, S. and Wei, M. (2019) *SCADA Testbed for Vulnerability Assessments, Penetration Testing and Incident Forensics*, DOI: 10.1109/ISDFS.2019.8757543, IEEE,2019.

Lane, J.A. and Epstein, D. (2013) *What is a System of Systems and Why Should I Care?, University of Southern California* [online] http://csse.usc.edu/csse/TECHRPTS/2013/reports/usc-csse-2013-500.pdf (accessed 25 November 2022).

Markoff, J. (2010) 'A silent attack, but not a subtle one', *New York Times*, Vol. 160, No. 55176, p.6.

Olivier, M. and Shenoi, S. (2006) *Advances in Digital Forensics II,* Vol. 222, p.364, Springer, Berlin, Germany.

One password allowed hackers to disrupt Colonial Pipeline, CEO tells senator (2021) https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/, (accessed 25 November 2022).

Onyiego, J. and Abade, O.E. (2020) 'Supervisory control and data acquisition (SCADA) system forensics based on the modbus protocol', *International Journal of Computer (IJC)*, Vol. 38, No. 1, pp.209–221.

Rajkumar, R.R., Lee, I., Sha, L. and Stankovic, J. (2010) 'Cyber-physical systems: the next computing revolution', Proceedings of the *47th Design Automation Conference*, June, pp.731–736, ACM.

RFC – 7228 [online] https://datatracker.ietf.org/doc/html/rfc7228# (accessed 25 November 2022).

Senthivel, S., Ahmed, I. and Roussev, V. (2017) 'SCADA network forensics of the PCCC protocol', *DFRWS 2017 USA – Proceedings of the Seventeenth Annual DFRWS USA.*

Stirland, J., Janicke, H., Jones, K. and Wu, T. (2014) 'Developing cyber forensics for SCADA industrial control systems', *Conference: The International Conference on Information Security and Cyber Forensics (InfoSec2014).*

Wu, T. and Nurse, J.R. (2015) 'Exploring the use of PLC debugging tools for digital forensic investigations on SCADA systems', T*he Journal of Digital Forensics, Security and Law: JDFSL*, Vol. 10, No. 4, p.79.

Wu, T., Disso, J.F.P. and Jones, K. (2013) 'Towards a SCADA forensics architecture', *ICS-CSR 2013: Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research 2013.*

Yau, K. and Chow, K-P. (2015) 'PLC forensics based on control program logic change detection', *Journal of Digital Forensics, Security and Law*, Vol. 10, No. 4, p.5.

Yildiz, F., Holekamp, J., Pecen, R., Karabiyik, U., Coogler, K. and Ryan, J. (2018) 'Design and development of a SCADA laboratory', *ASEE Annual Conference and Exposition – 2018, American Society for Engineering Education.*

Websites

https//www.sage-inc.com/cgi-bin/products_scadasentry.php (accessed 25 November 2022).

https://thehackernews.com/2017/09/dragonfly-energy-hacking.html (accessed November 2022).

https://www.risidata.com/ (accessed 25 November 2022).