An Incident Response Model for Industrial Control System Forensics Based on Historical Events

Ken Yau, Kam-Pui Chow, Siu-Ming Yiu

Chapter 16

AN INCIDENT RESPONSE MODEL FOR INDUSTRIAL CONTROL SYSTEM FORENSICS BASED ON HISTORICAL EVENTS

Ken Yau, Kam-Pui Chow and Siu-Ming Yiu

Abstract Cyber attacks on industrial control systems are increasing. Malware such as Stuxnet, Havex and BlackEnergy have demonstrated that industrial control systems are attractive targets for attackers. However, industrial control systems are not limited to malware attacks. Other attacks include SQL injection, distributed denial-of-service, spear phishing, social engineering and man-in-the-middle attacks. Additionally, methods such as unauthorized access, brute forcing and insider attacks have also targeted industrial control systems. Accidents such as fires and explosions at industrial plants also provide valuable insights into the targets of attacks, failure methods and potential impacts.

This chapter presents an incident response model for industrial control system forensics based on historical events. In particular, representative industrial control system incidents – cyber attacks and accidents – that have occurred over the past 25 years are categorized and analyzed. The resulting incident response model is useful for forensic planning and investigations. The model enables incident response teams and forensic investigators to decide on the expertise, techniques and tools to be applied to ensure sound evidence acquisition, analysis and reporting.

Keywords: Industrial control systems, incident response, forensics

1. Introduction

The critical infrastructure is defined as processes, systems, facilities, technologies, networks, assets and services that are essential to the health, safety security or economic well-being of citizens and the effective functioning of government [14]. Critical infrastructure assets can be stand-alone or interconnected, and interdependent within and across cities, states and nations. Disruptions or

damage to critical infrastructure assets could result in the loss of life, adverse economic effects and loss of public confidence [14].

Industrial control systems are indispensable to the safe and efficient operation of critical infrastructure assets. An industrial control system can be a single embedded system such as a programmable logic controller (PLC) that controls an automatic door or an elevator; or it could be a large and complex distributed control system connected to multiple supervisory control and data acquisition (SCADA) systems in a nuclear power plant [24].

Modern industrial control systems are increasingly connected to corporate networks and the Internet over TCP/IP and wireless protocols to improve their performance and effectiveness [22], exposing the previously-isolated systems to myriad remote attacks. According to an IBM report [12], cyber attacks on industrial systems in 2016 increased by 110% over the previous year (2015). Because of the importance of industrial control systems, it is crucial to protect them from remote cyber attacks as well as from undesirable incidents such as hardware failures, malicious intruders, accidents and natural disasters [23].

Digital forensics is an important part of an incident investigation. It helps reconstruct past events and activities based on timelines in order to prevent recurring attacks and undesirable incidents from occurring. Industrial control systems may comprise hundreds to thousands of interconnected devices. The devices include programmable logic controllers and remote terminal units (RTUs), which are highly specialized embedded systems that often have limited computational and memory resources, and functionality. As a result, it can be difficult to acquire data from industrial control systems. Traditional digital forensic techniques are also inadequate for industrial control systems. Moreover, standard forensic guidelines, procedures and tools are not as yet available for investigating incidents involving industrial control systems.

Several frameworks, processes and tools have been developed for industrial control system security and forensics; these are primarily based on attack patterns of real or synthetic industrial control system malware. However, only a portion of industrial control system incidents involve malware attacks. This chapter presents an incident response model for industrial control system forensics based on historical events. In particular, representative industrial control incidents – cyber attacks and accidents – that have occurred over the past 25 years are categorized and analyzed. The resulting incident response model is useful for forensic planning and investigations. The model enables incident response teams and forensic investigators to decide on the expertise, techniques and tools to be applied to ensure sound evidence acquisition, analysis and reporting.

2. Forensic Challenges

Digital forensic techniques and tools are required to collect evidence for legal proceedings and internal investigations, as well as to handle malware incidents and unusual operational problems. Regardless of the application, digital forensics involves four basic processes: (i) collection; (ii) examination;

Figure 1. Digital forensic process [10].

(iii) analysis; and (iv) reporting (Figure 1). The implementation details of these processes vary based on the specific forensic needs.

Although digital forensics is becoming a mature domain, investigators need to modify traditional digital forensic processes for use in industrial control system environments. The following forensic challenges are encountered in industrial control environments [7]:

- The availability of industrial control systems is a top priority. Therefore, it is often not possible to shut down devices such as programmable logic controllers for evidence collection and forensic investigations.

- Most modern industrial control environments provide only some of the required data collection features (e.g., identifying, recording, copying and labeling materials from a variety of data sources in the information architecture). Many industrial control systems do not support forensic data collection.

- Contemporary forensic tools, such as those used to examine running processes and services, automate evidence collection through precompiled scripts or programs, bit copy processes and programs that generate checksums for image verification, are often not designed to accommodate industrial control system technologies. Many forensic tools cannot be adapted to operate in industrial control environments.

3. Industrial Control Networks

Operational technology (OT) refers to the hardware and software that monitor and/or control industrial processes. Industrial control systems and SCADA systems are examples of operational technology. The protection of critical infrastructure networks is commonly considered to fall in the domain of SCADA security [4]. However, this is not necessarily true.

In fact, critical infrastructure networks are hybrids of operational technology and information technology [4]. Industrial control systems are often connected to corporate networks (Figure 2). Whether they reside in large critical infrastructure assets or small localized controller-run assets, industrial control systems integrate operational and information technologies.

Stuxnet, a most sophisticated and complex malware, was designed to target industrial control systems. It was launched from a conventional information technology network to attack programmable logic controllers in an operational

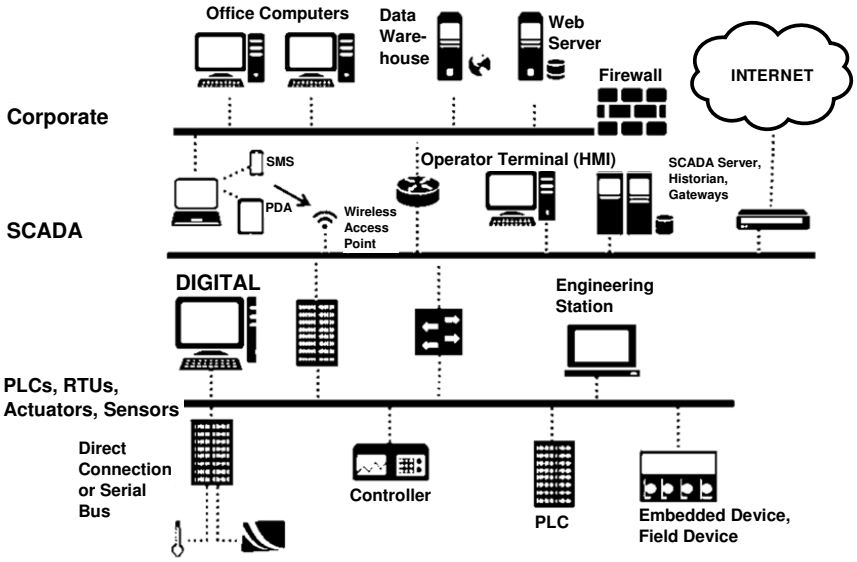

Figure 2. Example industrial control network [4].

technology network. The Stuxnet attack demonstrated that an air gap between information technology and operational technology can be breached [4].

4. Literature Review

Research on industrial control system and programmable logic controller security and forensics significantly ramped up after Stuxnet was discovered in 2010. The research has generally focused on vulnerabilities in industrial control systems and protocols. Several types of simulated cyber attacks have been investigated to advance security and forensic efforts.

Spenneberg et al. [20] developed a worm that propagates to programmable logic controllers. The worm scans a network for programmable logic controllers, attacks the targets and then replicates itself on the targets. Spenneberg and colleagues have analyzed the impacts of the worm on various targets and have suggested possible mitigations.

Abbasi and Hashemi [1] have investigated the security implications of embedded system input/output pin control. They demonstrate how an attacker can affect the integrity and availability of embedded system inputs and outputs by exploiting pin control operations. Such attacks on programmable logic controllers can be difficult to detect.

Ben Aloui [2] has demonstrated the ease with which dynamic code injection can be executed on a Siemens S7-300 programmable logic controller without shutting down or restarting the device. The program, which is written in the C language and uses the Snap7 library, pushes a new program segment

(organization block) into the CPU. A small human-machine interface (HMI) was developed to illustrate dynamic modifications of the execution flow. Several countermeasures and protection strategies were proposed to combat dynamic code injection.

All these research efforts are useful for industrial control system threat analysis and forensics, but they focus on simulated, not real, cyber attacks. Thus, the results do not reflect real situations. Indeed, realistic solutions for industrial control system forensics are unlikely to be developed by considering only simulated attacks.

Eden et al. [6] have proposed a forensic incident response model for industrial control systems. The model has four stages: (i) prepare; (ii) detect; (iii) triage; and (iv) respond. Eden and colleagues outline the forensic triage process and highlight the differences and challenges involved in performing forensic incident responses on industrial control systems compared with traditional systems. The forensic incident response model is useful, but is generic as opposed to incident-specific.

5. Classification of Incidents

In order to develop a practical methodology for industrial control system forensics, representative incidents since 1992 discussed in newspaper articles, technical reports and research papers were examined. The incidents were first organized into two types: (i) attacks; and (ii) accidents. They were then classified into four categories: (i) general computer malware; (ii) unauthorized access; (iii) industrial control system malware; and (iv) accidents.

The classification model is based on categories of malicious activity [3] and accidents. Tables 1 and 2 summarize the incidents.

5.1 General Computer Malware

General computer malware targets traditional information technology systems such as office computers and human-machine interfaces. However, malware attacks can indirectly shut down or otherwise impact industrial control system operations.

A variant of the Sobig worm was introduced into the CSX Railroad headquarters in Jacksonville, Florida in August 2003 [3]. The malware installed applications and created backdoors while continuing to spread by infecting e-mail attachments. Although the worm was not specifically designed to target railroad systems, it propagated to the control center and proceeded to disrupt signaling, dispatch and other related systems. Reports indicated that Amtrak trains in the area were also affected by the malware in CSX Railroad systems. The malware attack caused multiple train delays and expensive clean-up activities.

Table 1. Selected incidents classified into four categories [3, 12].

Type	Category	Year	Representative Incident
Attacks	**General Computer Malware**	2003	The SQL Slammer worm disabled a nuclear power plant in Ohio, USA
		2003	The Sobig worm was introduced in the CSX Railroad headquarters in Florida, USA
		2005	The Zotob worm infected 13 automobile plants in Ohio, USA, causing shutdowns and delays
		2006	An attacker penetrated a water treatment facility network in Pennsylvania, USA
		2014	The modified Gh0st RAT Trojan infected a fast-breeder nuclear reactor in Tsuruga, Japan
Attacks	**Unauthorized Access**	1992	A fired employee hacked into Chevron systems in New York and California, USA, and reconfigured the emergency alert network
		1997	A teenager connected to a dial-up loop carrier system servicing an airport in Massachusetts, USA and sent a series of commands that disabled the system
		2000	A former consultant attacked a sewage treatment plant in Maroochy, Australia
		2007	Striking workers (insiders) penetrated a traffic system in California, USA
		2008	An attacker used a homemade device to remotely derail a train in Lodz, Poland
		2009	A disgruntled former IT contractor hacked into leak detection systems on multiple oil platforms off the coast of California, USA
		2011	A hacker used Shodan to access HMIs in a water utility network in Texas, USA
		2013	A sophisticated attacker penetrated the U.S. Army Corps of Engineers National Inventory of Dams, USA
		2014	A hacker accessed a SCADA server in the USA that operated mechanical equipment

5.2 Unauthorized Access

These incidents involve unauthorized persistent access of control center systems or field devices from another network such as a corporate network or

Table 2. Selected incidents classified into four categories [3, 12] (continued).

Type	Category	Year	Representative Incident
Attacks	**Industrial Control System Malware**	2003	An attacker sabotaged a marine terminal in Venezuela
		2010	The Stuxnet worm destroyed uranium hexafluoride centrifuges in Natanz, Iran
		2014	The Havex Trojan entered OPC servers and tried to exfiltrate data from industrial control systems in the USA and Europe
		2016	The BlackEnergy Trojan caused power outages in the Ivano-Frankivsk region of Ukraine
Accidents	**Accidents**	2013	Two mechanics died in a fire in the nacelle of a wind turbine in The Netherlands [12]
		2013	An elevator dropped on its way up a building in North Point, Hong Kong [11]
		2014	Nickel sulfate was discharged into a river from a mine in Harjavalta, Finland [13]
		2015	Water mixed with molten metal in a foundry in Feurs, France to cause an explosion [13]
		2015	Pressurized flammable gas leaked into a petrochemical complex in Gonfreville-l'Orcher, France [13]
		2017	An escalator suddenly accelerated and then reversed its direction in a mall in Mong Kok, Hong Kong [15]

the Internet. The attackers can be insiders (e.g., employees, contractors and vendors) or outsiders.

One of the most famous SCADA system breaches occurred at Maroochy Water Services on Queensland's Sunshine Coast in Australia [18]. Vitek Boden, a former Maroochy consultant, used a laptop computer and a radio transmitter to take control of 150 sewage pumping stations. Over a three-month period, he released one million liters of untreated sewage into a water drain from where it flowed into local waterways. Mr. Boden launched the attack because he was denied a fulltime position with the Maroochy Shire Council.

5.3 Industrial Control System Malware

Industrial control system malware specifically targets field devices such as programmable logic controllers. The incidents may involve firmware tampering or exploiting device vulnerabilities.

Stuxnet is a most sophisticated industrial control system malware that leveraged four zero-day vulnerabilities and two compromised digital certificates in its attacks on Iran's uranium hexafluoride centrifuges [3]. The malware exploited

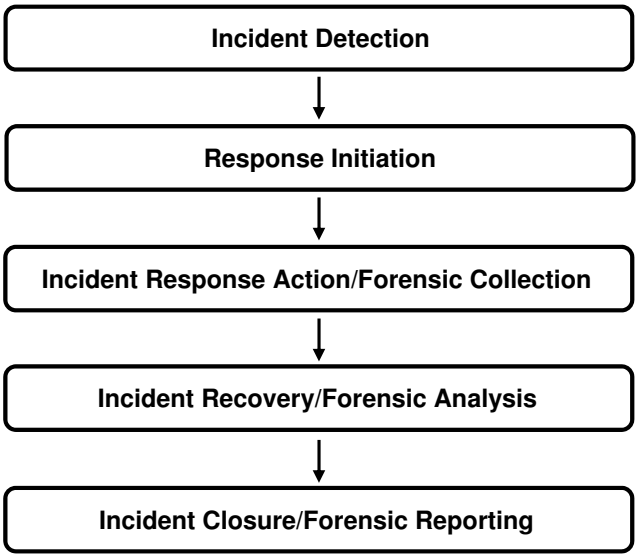

Figure 3. Cyber incident response model with an embedded forensics component.

application software to control Windows systems that could modify the control programs of Siemens programmable logic controllers, inducing abnormal operations and eventually destroying several centrifuges.

5.4 Accidents

Accidents include incidents such as incorrect control, power disruptions, hardware failures and fires that are not due to cyber attacks or cyber criminal activities [5]. They are typically caused by design flaws, human error and natural phenomena.

A fire in the nacelle of a wind turbine in The Netherlands in October 2013 killed two service engineers [24]. Investigators working in collaboration with the Netherlands Forensic Institute, Department of Digital Technology and the wind turbine manufacturer were able to remove the controller located at the base of the turbine to extract evidence.

6. Refined Incident Response Model

Incident response requires substantial planning and resources. [19]. Digital forensics, which is a core component of incident response capabilities, covers the collection, examination, analysis and reporting of incident data [7]. A forensic program is typically initiated after incident response processes such as restoration, mitigation and initial reporting. Many organizations integrate the

forensic function in incident response processes, especially when the start of the forensic function cannot be defined clearly.

Fabro and Cornelius [7] have studied the integration trend and have defined a cyber incident response model with an embedded forensics component as shown in Figure 3. In this approach, forensic collection is embedded in incident response, forensic analysis in incident recovery and forensic reporting in incident closure.

The study of historical industrial control system incidents reveals that special skills and techniques are not always required for digital forensic examinations of industrial control systems. Some incidents can be investigated using traditional forensic techniques and tools, especially when the incidents fall in the general computer malware and unauthorized access categories. In the case of an industrial control system incident, the incident response team typically incorporates industrial control system specialists and applies special techniques and tools in the investigation. However, the historical incident data reveals that traditional forensic techniques and tools are adequate for investigating incidents in the general computer malware and unauthorized access categories, eliminating the need to use specialized techniques and tools.

Therefore, in order to increase the efficiency of forensic processes, the core components of cyber incident response in Figure 3 are refined by inserting a new incident categorization component after the incident detection component during the early stage of preparing a forensic response plan. Figure 4 shows the refined incident response model with an embedded industrial control system forensics component.

Additionally, two types of response are incorporated: (i) traditional forensics; and (ii) industrial control system forensics. Depending on the classification assigned to an incident, the investigation can employ either traditional forensics or industrial control system forensics during the early stage. This saves time, effort and resources while ensuring more precise and effective incident response.

6.1 Traditional Forensics

This section discusses the application of traditional forensics to industrial control systems in incidents involving general computer malware and unauthorized access. Since traditional information technology computers, networks and protocols are targeted, traditional forensic methods are adequate for digital investigations. Normal hard drive analysis, log analysis and network tools can be used to examine what was running on the systems and reveal the causes of the incidents.

- **General Computer Malware:** In the case of the virus attack on CSX Railroad, traditional digital forensics would have been sufficient because the incident did not involve industrial control equipment or field devices. The incident mainly involved general computer systems. Therefore, the investigation would have identified the hosts that were infected by malware, and appropriate containment, eradication and recovery ac-

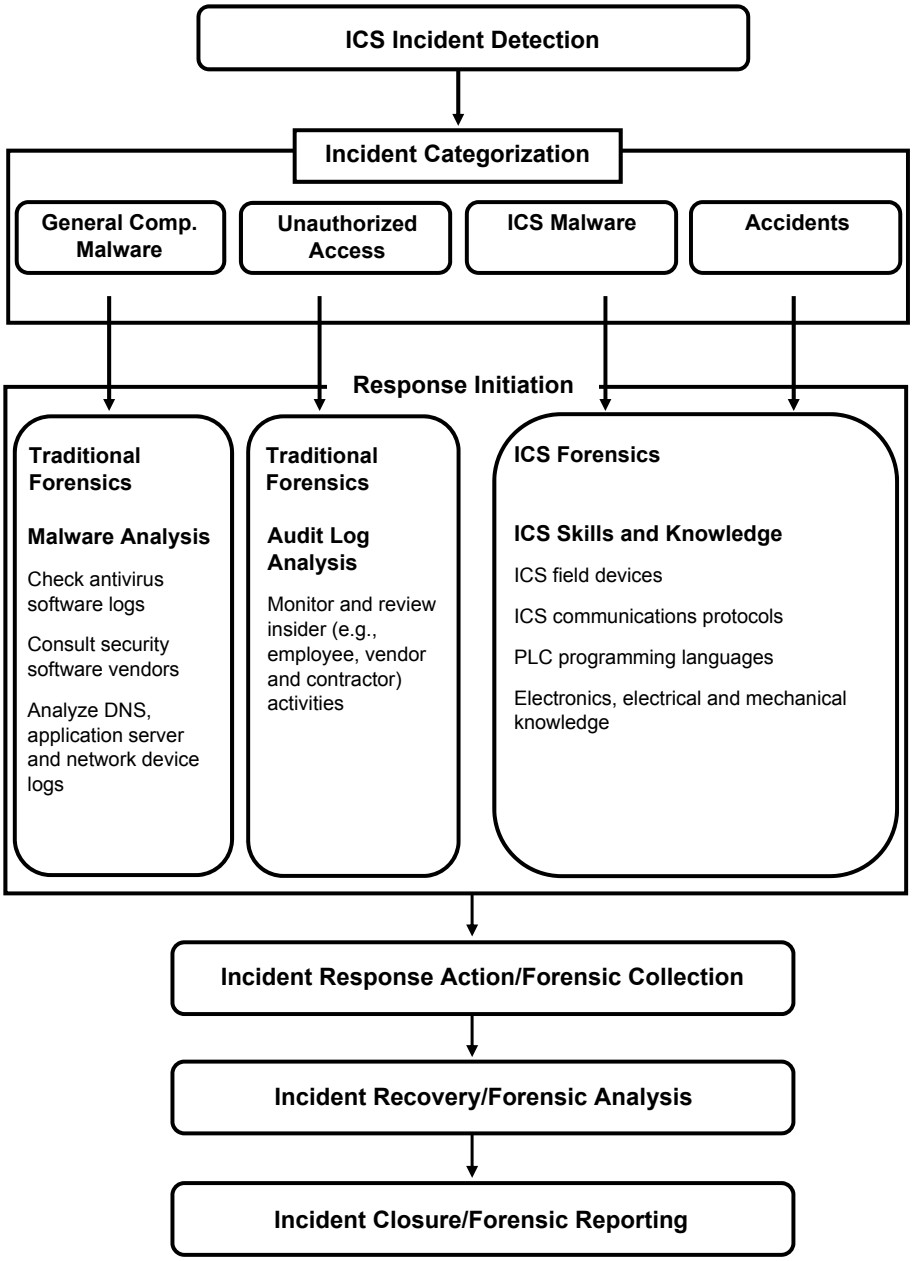

Figure 4. Refined incident response model with an ICS forensics component.

tions would have been applied to the infected hosts. Evidence would then have been collected from the domain name server (DNS) logs, application server logs and network device logs. Traditional network forensic logs would also have been analyzed to reveal detailed information about the malware activity [19].

- **Unauthorized Access:** In the case of the unauthorized access incident at Maroochy Water Services, a PDS Compact 500 process controller, two-way radio and computer laptop were found in Mr. Boden's automobile. Mr. Boden stated that he owned all the items and was using them for study, personal correspondence and work related to his family business. However, law enforcement discovered that the PDS Compact 500 controller and two-way radio were stolen from Hunter Watertech, a company contracted to install PDS Compact 500 units at pumping stations belonging to Maroochy Shire.

  The software installed in Mr. Boden's laptop computer was developed by Hunter Watertech and was required to communicate with the SCADA system at Maroochy Water Services; the software had no other practical use. The two-way radio was set to the same frequency as two of the three available repeater stations. The laptop computer startup and shutdown times were consistent with the logged intrusions. The PDS Compact 500 process controller had the same address as the one logged during the intrusions. Moreover, Mr. Boden was arrested at a location that was within radio range of the pumping station repeater and close enough to connect to the SCADA network.

  All the evidence in the Maroochy Water Services incident was collected by applying traditional digital forensic techniques and tools with the assistance of Hunter Watertech personnel. Mr. Boden was ultimately sentenced to two years in jail on 30 charges of computer hacking, theft and causing environmental damage [17].

  Industrial control system attacks are not limited to malware. Other attacks include advanced persistent threats (APTs), spear phishing, SQL injection, distributed denial-of-service (DDoS), social engineering and man-in-the-middle (MITM) attacks. However, less sophisticated methods such as unauthorized access, brute forcing and insider attacks can be just as effective [17]. As in the case of the CSX Railroad and Maroochy Services attacks, many incidents can be handled using traditional forensic methods because the incidents did not involve industrial control equipment or field devices.

6.2 Industrial Control System Forensics

Traditional forensic techniques and tools do not provide data collection functionality for programmable logic controllers, remote terminal units, intelligent electronic devices and other field devices encountered in industrial control environments [24]. Therefore, incidents that fall in the industrial control system

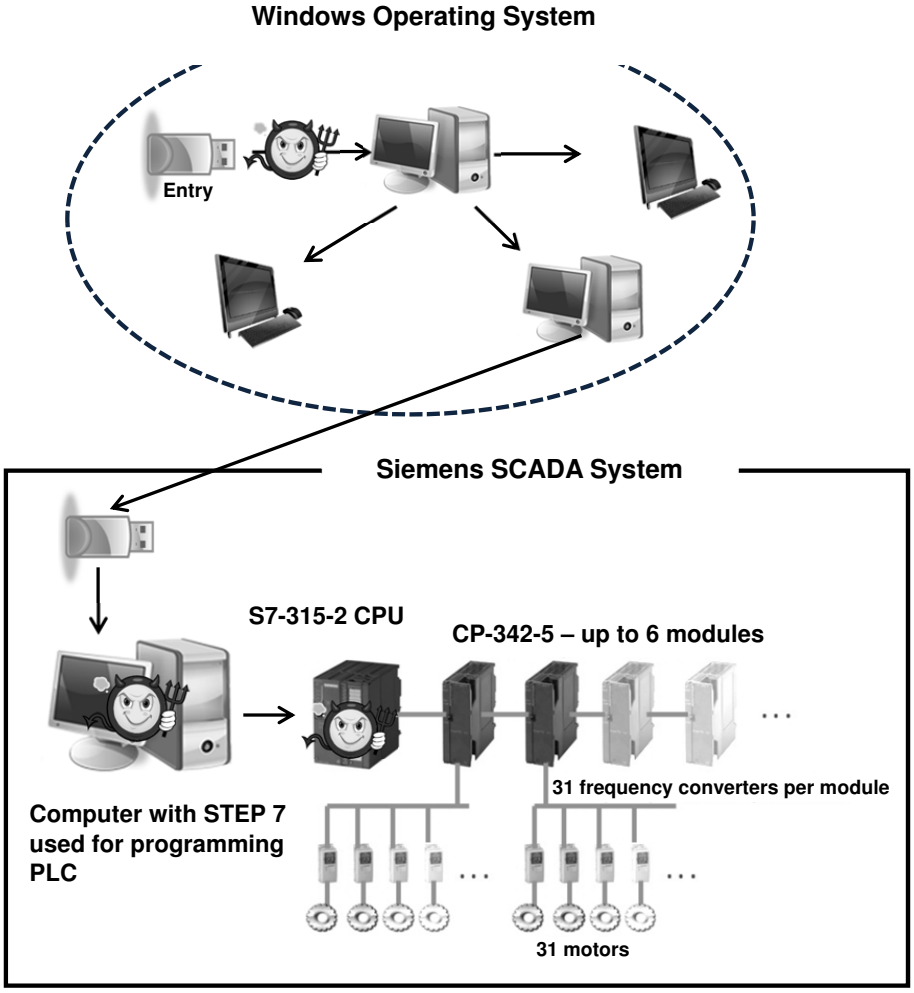

Figure 5. Stuxnet infection.

malware and accidents categories require the application of industrial control forensic expertise and tools.

- **Industrial Control System Malware:** The Stuxnet malware was developed to target specific industrial control systems. The malware conducted a layered attack against three systems: (i) Windows operating system; (ii) Siemens PCS 7, WinCC and STEP 7 industrial software applications that run on Windows (SCADA system); and (iii) Siemens STEP 7 programmable logic controllers (SCADA system).

  Figure 5 provides an overview of the Stuxnet infection. The malware entered and infected a target system via a USB flash drive, following which

it searched for, propagated to and infected other target systems. It originally leveraged four zero-day Windows vulnerabilities to propagate and infect systems. Stuxnet was designed to sabotage centrifuges that employ Siemens SCADA systems by reprogramming the programming logic controllers to command the centrifuges to operate outside their designed parameter ranges [8].

In order to conduct a forensic investigation of a Stuxnet-type incident, incident response personnel must have substantial knowledge about SCADA systems, especially programmable logic controller and field device hardware, firmware and software (applications) as well as SCADA communications protocols. Furthermore, highly specialized techniques and tools are required to collect and analyze data from industrial control devices in a forensically-sound manner.

- **Accidents:** In the case of an accident like the wind turbine fire in The Netherlands discussed above, investigators were required to have adequate industrial control system expertise and sophisticated tools because evidence pertaining to the accident had to be collected from the RAM chip in the programmable logic controller located at the base of the turbine. Therefore, the accident investigators worked closely with professionals from the Netherlands Forensic Institute, Department of Digital Technology and the wind turbine manufacturer to collect and analyze the evidence.

  On March 25, 2017, a serious escalator accident occurred in a busy Mong Kok, Hong Kong shopping mall. A 45-meter escalator linking the fourth and eighth floors and carrying about 120 patrons malfunctioned and suddenly moved in the reverse direction, injuring 18 people [16].

  The technical investigation report [9] stated that the escalator accident was due to the failure of the main drive chain and a broken chain safety device. There was no overloading of the escalator. The investigators worked closely with escalator workers, a registered escalator engineer, the escalator contractor and personnel from the mall management company to collect evidence for examination.

  Investigating incidents involving industrial control systems is not only about finding evidence about potential criminal activities. This is because incidents are often the result of accidents such as equipment malfunctions and fires [24]. Accident investigators must have adequate technical expertise and the appropriate tools to collect and analyze evidence from industrial control systems that are directly or indirectly connected to accidents, or are proximal to the accidents [24].

7. Discussion

This study has some limitations. A large number of industrial control system incidents go unreported and, in other cases, details about the incidents

are not published. The number of incident categories proposed depends on the representative incidents considered in the study and different selections of incidents would likely yield different incident categories. Moreover, information about the incidents considered in the study was collected from various sources, and may have various assumptions and biases. All these factors are expected to affect the results of the analysis.

This study reveals that a large proportion of industrial control system incident investigations can be conducted using traditional forensic processes. However, some incidents are more difficult to handle because embedded systems such as programmable logic controllers are specialized devices with their own communications protocols, connection interfaces, operating systems and programming languages [24]. Therefore, in the case of incidents related to embedded systems, investigators may have to work with experts who have the appropriate tools to collect and analyze data from industrial control equipment. Some tools are able to extract evidence from RAM chips in the devices, but this may not always be done in a forensically-sound manner [24].

Programmable logic controllers are arguably the most important components in industrial control systems. They are attractive targets because successful attacks on programmable logic controllers can result in significant industrial process malfunctions and equipment damage. Each vendor usually provides custom software for programming, communicating and configuring its programmable logic controllers. For example, STEP 7 software running in Windows environments is used to program, communicate with and configure Siemens programmable logic controllers.

The following STEP 7 features are useful in forensic investigations of programmable logic controllers:

- **Logging communications between a programmable logic controller and STEP 7 software:** Communications events of interest include Program Change, Start PLC and Stop PLC (Figure 6). For example, the logged information enables an investigator to identify who changed the control program and when it was changed.

- **Checking the integrity of the control program in a programmable logic controller:** The control program in a programmable logic controller and the source program in the device used to program it can be compared to identify alterations to the program logic.

- **Monitoring programmable logic controller inputs/outputs and control program memory addresses:** The inputs/outputs and memory address values provide valuable information about malicious activity.

- **Monitoring execution time:** A programmable logic controller executes in a cyclic manner. Every cycle has three phases: (i) read inputs; (ii) execute the control program; and (iii) update outputs [16]. A change in the execution time can indicate control program alteration.

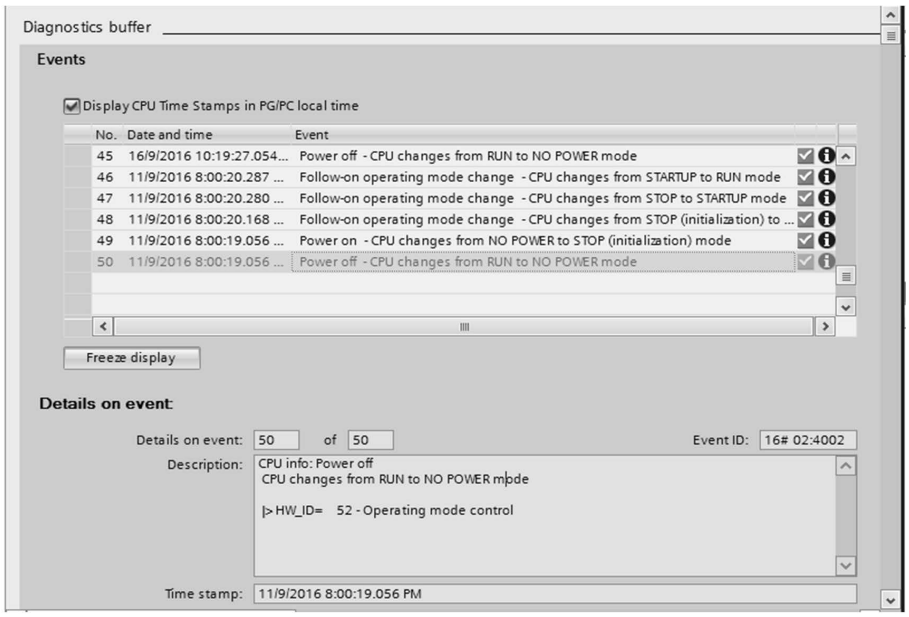

Figure 6. STEP 7 event activity log.

Other vendors (e.g., Allen Bradley) provide similar software (RSLogix) for their programmable logic controllers. The software is useful for investigating industrial control system incidents involving industrial control system malware and accidents.

The official investigative report [9] on the escalator incident in the Mong Kok, Hong Kong shopping mall attributed the cause to the failure of the main drive chain as well as a broken chain safety device. The main drive chain failure was due to metal fatigue, and the chain safety device malfunction was due to the presence of grease on the sliding surface of the moving part of the device and an improper setting of the compression springs. The incident was classified as an accident and the investigators cooperated with the escalator contractor and manufacturer to collect evidence for analysis. However, the focus was on the mechanical parts of the escalator. Clearly, the investigation would have been more comprehensive by applying digital forensic processes to extract and analyze evidence residing in the controllers.

In order to prepare an efficient plan for industrial control system forensics, incidents should be classified at an early stage if possible. In the case of incidents involving general computer malware or unauthorized access, the investigations can be handled just like they are for incidents involving conventional information technology systems. In the case of incidents involving industrial control system malware and accidents, the investigations must incorporate industrial control system experts, including vendor personnel. The investigators

Table 3. Summary of industrial control system incidents.

Category	Incidents (%)	Techniques
General Computer Malware	5 (19%)	Traditional forensics
Unauthorized Access	9 (35%)	
ICS Malware	6 (23%)	ICS forensics
Accidents	6 (23%)	

must understand the technical and tactical aspects of industrial control system forensics. Additionally, specialized industrial control system evidence recovery and analysis tools would have to be used in the investigations.

The proposed model inserts the incident categorization component before the incident detection component. However, it is not always possible to categorize an incident at an early stage. In such instances, incident categorization can be performed after response initiation, after incident response or after incident recovery, as appropriate. The important point is that, regardless of when incident categorization is performed, it enhances the efficiency of the investigation.

8. Conclusions

The incident response model presented in this chapter is useful for forensic planning and investigations of industrial control system incidents. The model enables incident response teams and forensic investigators to decide on the expertise, techniques and tools to be applied to ensure sound evidence acquisition, analysis and reporting.

Most investigations of industrial control system incidents tend to focus on malware attacks; this could obscure determinations of other causes of the incidents. The majority of the representative incidents considered in this work ($19\% + 35\% = 54\%$ in Table 3) fall in the general computer malware and unauthorized access categories, which means that they could be investigated using traditional forensic techniques. In the other words, industrial control system experts and specialized tools are not required for all investigations of industrial control system incidents. Robust guidelines and tools are available for such investigations, which greatly simplify incident response.

Another key point is that performing incident categorization early in incident response renders the entire process more effective and efficient. Based on the incident categorization, forensic investigators can decide on the industrial control system expertise, techniques and tools that are required, which reduces the time, effort, costs and resources.

Future research will analyze a comprehensive collection of industrial control system incidents. This research will provide valuable insights into incident handling, enabling the creation of a robust forensic investigation model for industrial control systems.

References

[1] A. Abbasi and M. Hashemi, Ghost in the PLC: Designing an undetectable programmable logic controller rootkit via pin control attack, presented at *Black Hat Europe*, 2016.

[2] N. Ben Aloui, Industrial Control Systems Dynamic Code Injection, Cybersecurity Labs, DCNS Toulon, Toulon, France (`grehack.org/files/2015/Grehack%202015%20-%20Paper%20-%20Industrial%20Control%20Systems%20Dynamic%20Code%20Injection.pdf`), 2015.

[3] N. Carr, Development of a Tailored Methodology and Forensic Toolkit for Industrial Control Systems Incident Response, M.S. Thesis, Cyber Systems and Operations, Naval Postgraduate School, Monterey, California, 2014.

[4] A. Dar, Protecting industrial control networks – It's not just about SCADA security, *Cyberbit Blog*, February 10, 2017.

[5] M. Dzwiarek, An analysis of accidents caused by improper functioning of machine control systems, *International Journal of Occupational Safety and Ergonomics*, vol. 10(2), pp. 129–136, 2004.

[6] P. Eden, A. Blyth, P. Burnap, Y. Cherdantseva, K. Jones, H. Soulsby and K. Stoddart, A forensic taxonomy of SCADA systems and approach to incident response, *Proceedings of the Third International Symposium for ICS and SCADA Cyber Security Research*, pp. 42–51, 2015.

[7] M. Fabro and E. Cornelius, Recommended Practice: Creating Cyber Forensic Plans for Control Systems, INL/EXT-08-14231, Idaho National Laboratory, Idaho Falls, Idaho, 2008.

[8] N. Falliere, L. O'Murchu and E. Chien, W32.Stuxnet Dossier, Version 1.4, Symantec, Mountain View, California, 2011.

[9] Government of the Hong Kong Special Administrative Region, EMSD releases technical investigation report on escalator incident at Langham Place, Press Release, Hong Kong, China (`www.info.gov.hk/gia/general/201706/09/P2017060900449.htm`), June 9, 2017.

[10] K. Kent, S. Chevalier, T. Grance and H. Dang, Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86, National Institute of Standards and Technology, Gaithersburg, Maryland, 2006.

[11] S. Lau and J. Ngo, Seven injured in lift accident in North Point building, *South China Morning Post*, March 3, 2013.

[12] D. McMillen, Security Attacks on Industrial Control Systems: How Technology Advances Create Risks for Industrial Organizations, IBM Security, International Business Machines, Somers, New York, 2015.

[13] Ministry of the Environment, Energy and the Sea, Lessons Learnt from Industrial Accidents, 12th Seminar, Paris, France (`www.impel.eu/wp-content/uploads/2018/01/Brochure_IMPEL2017_EN.pdf`), 2017.

[14] Public Safety Canada, Critical Infrastructure, Ottawa, Canada (publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx), 2018.

[15] Radio Television Hong Kong, Langham Place escalator malfunctions, injuring 18, *RTHK News*, March 25, 2017.

[16] K. Sacha, Translatable finite state time machine, in *Design for Dependable Systems*, E. Gaudin, E. Najm and R. Reed (Eds.), Springer, Berlin Heidelberg, Germany, pp. 117–132, 2007.

[17] N. Sayfayn and S. Madnick, Cybersafety Analysis of the Maroochy Shire Sewage Spill, Working Paper CISL# 2017-09, Cybersecurity Interdisciplinary Systems Laboratory, Sloan School of Management, Massachusetts Institute of Technology, Cambridge, Massachusetts, 2017.

[18] J. Slay and M. Miller, Lessons learned from the Maroochy water breach, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 73–82, 2007.

[19] M. Souppaya and K. Scarfone, Guide to Malware Incident Prevention and Handling for Desktops and Laptops, NIST Special Publication 800-83, Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, 2013.

[20] R. Spenneberg, M Bruggemann and H Schwartke, PLC-Blaster: A worm living solely in the PLC, presented at *Black Hat USA*, 2016.

[21] B. Sperber, Solutions emerge to prevent control system cyber-attacks, *Automation World*, May 23, 2012.

[22] T. Spyridopoulos, T. Tryfonas and J. May, Incident analysis and digital forensics in SCADA and industrial control systems, *Proceedings of the Eighth IET International System Safety Conference Incorporating the Cyber Security Conference*, 2013.

[23] K. Stouffer, J. Falco and K. Scarfone, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, National Institute of Standards and Technology, Gaithersburg, Maryland, 2011.

[24] P. van Vliet, M. Kechadi and N. Le-Khac, Forensics in industrial control system: A case study, in *Security of Industrial Control Systems and Cyber Physical Systems*, A. Becue, N. Cuppens-Boulahia, F. Cuppens and S. Katsikas (Eds.), Springer, Cham, Switzerland, pp. 147–156, 2016.

[25] C. Wueest, Targeted Attacks Against the Energy Sector, Version 1.0, Symantec, Mountain View, California, 2014.