THE DEVELOPMENT OF A CROSS-DISCIPLINARY APPROACH IN INDUSTRIAL CONTROL SYSTEM COMPUTER FORENSICS

A Thesis

Presented in Partial Fulfillment of the Requirements for the

Degree of Master of Science

with a

Major in Computer Science

in the

College of Graduate Studies

University of Idaho

by

Theora R. Rice

May 2014

Major Professor: Jim Alves-Foss, Ph.D.

Authorization to Submit Thesis

This thesis of Theora Renae Rice, submitted for the degree of Master of Science with a Major in Computer Science and titled “The Development of a Cross-Disciplinary Approach in Industrial Control System Computer Forensics”, has been reviewed in final form. Permission, as indicated by the signatures and dates given below, is now granted to submit final copies to the College of Graduate Studies for approval.

Major Professor ____________________________________ Date: _______________
Dr. Jim Alves-Foss

Committee
Members ____________________________________ Date: _______________
Dr. Paul Oman

____________________________________ Date: _______________
Dr. Brian K. Johnson

Department
Administrator ____________________________________ Date: _______________
Dr. Gregory Donohoe

Discipline's
College Dean ____________________________________ Date: _______________
Dr. Larry Stauffer

Final Approval and Acceptance

Dean of the College
Of Graduate Studies: ____________________________________ Date: _______________
Dr. Jie Chen

Abstract

Many industrial control systems are vital components of modern life, and have proven vulnerable to some computer-based attacks. Because of this, professionals seek to ensure their continued service by exploring methods of defense and incident response. Applying computer forensics to critical infrastructure is a problem that researchers must face to ensure system resilience. If those involved in securing critical infrastructures don't understand what has happened to the system after an incident, then they cannot protect it in the future.

A solution to this problem is to integrate the beginning stages of forensics investigation into the operators' and/or process engineers' incident response plan. Implementing new training seminars, moderately changing system structure, and developing software features can help mitigate certain problems. There are, of course, new complications that this solution creates. However, with adequate research and resource dedication it can be tested, and provide the progressive momentum that this field needs.

Acknowledgements

I would like to thank my major professor Dr. Jim Alves-Foss for all the guidance and support he has given me since I first came to his office, all those years ago. I'd also like to thank Dr. Oman for furthering my education in industrial control systems, and teaching me so much that is not written in any book or article. Dr. Brian K. Johnson has my thanks as well, for agreeing to be on my thesis committee.

Dr. Craig Rieger, Dr. David Manz, and Thomas Edgar all deserve special recognition for igniting and then fanning my interest in control systems cyber security.

I would also like to thank my office-mates for letting me bounce ideas off of them throughout the process of developing this document.

Dedication

I dedicate this thesis to my family. To my parents, who taught me that hard work is something to be proud of and who have always cheered me on as I pursue my aspirations. Also to the family I have gathered on my own, for supporting me and providing the stability to reach towards my goals.

Table of Contents

Table of Figures

Table of Tables

Chapter 1. Introduction

There are many ways to damage a country and its people. Even lone individuals can perpetrate enormous crimes that shake a nation's economy and attitude. Since the September 11th attacks of 2001, terrorism has been at the forefront of many United States citizens' minds. Yet many Americans may be surprised to know that many of the greatest attack vectors are not associated with violent events and a large amount of media coverage.

For years the United States government has been concerned with the security of its critical infrastructures [1]. These are the systems by which the country operates. Every day, the life of the average citizen of the United States is supported and impacted by industrial control systems (ICS). They provide electricity, water, food, medication, and any number of other process-controlled services. Losing these systems can indirectly cause as much or more damage than a focused physical attack on highly-visible targets.

Physical security and incident response plans have always been of some priority when creating critical infrastructures. Corporate espionage and other malicious attackers have been known to cause problems by breaking into a facility. Natural disasters and other errors in the system can also provide their fair share of trouble that must be manageable for production continuation to be assured. With the advancing march of technology, however, it is becoming readily apparent that these are not the only dangers control systems face.

In recent years, concern over the vulnerability of industrial critical infrastructure to cyber-attacks has become a hot topic. Due to technological progress, systems that were once created as solitary entities are now being connected to enterprise domains. This exposes these systems to the same risks that plague IT networks, and links them to more possible attack routes. There have been documented cases where control systems have been compromised due to network viruses, and malevolent hackers affecting the system [2]. Malicious software is also becoming more advanced, and has manifested in forms such as the Stuxnet worm which succeeded in working its way into a system not directly connected to the outside world [3]. These risks and exploitations have drawn a lot of attention from the professional community, who have responded by directing a great deal of research towards the cyber security of ICS for the purpose of building reliability in the system.

Within the United States, citizens must be able to rely upon the continuous service of ICS industries. If companies are not able to guarantee their clients access to electrical power, for instance, problems could arise in terms of clean water, food supplies, hospital energy, and so forth. One crucial aspect of maintaining this reliability is incidence response. This phrase defines the actions taken when an incident or problem occurs with the system. Most steps of response are involved with maintaining service or getting the process back online. However, an important step of incident recovery is knowing exactly what happened within the system to cause the problem, and whether there may be a perpetrating party. This is where the computer forensics field comes into play.

1.1 Objective

The inclusion of detailed computer forensics procedures in ICS system incidence response is crucial to analyzing the situation and maintaining future resilience of the system. When an incident occurs, it is important that the facility know exactly what machines and data have been affected. This allows professionals to take steps in damage control, such as replacing system components or analyzing stolen or lost information. When presented with a new threat, the best way that professionals can understand how to defend against it is by dissecting it. However, conducting forensics within an ICS environment is notoriously challenging [4]. Because of this and the tendency to think of forensics as something that happens after system recovery, there have been only a few implemented advances in the domain.

This document addresses these challenges, and specifically lingers on the subject of cross-disciplinary teamwork in the ICS work atmosphere. There is a great amount of variety in ICS structure, physically, logically, and professionally. Because of this, it presents unique challenges that are only conquerable with the cooperation of many different disciplines. Implementing computer forensics in ICS is no different. Cyber security has already realized the need to include professionals who understand the system in the incident response framework [5]. Due to the unique knowledge presented by systems operators and process engineers, it is logical that they be included as part of the forensics investigation as well.

Specifically, ICS operators must be incorporated into forensics procedures to ensure that system-specific, potentially volatile, information is gathered in an efficient and timely manner. To accomplish this, a combination of training and automation is required to prepare and aide these workers with their new tasks. By integrating a variety of disciplines to carry out this proposal, communication will be stimulated for greater potential advancements. This document discusses the importance of cross-discipline integration, and outlines what topics need to be addressed by new training curriculum and automation development.

1.2 A Lens

In computer science, the greatest challenge is making the material understandable to an audience. This is particularly true concerning the field of cyber security. There are some who understand technical concepts regardless of writing style, but for each of those individuals there are dozens more who need the constructs explained in a more intuitive manner. If the realm of technical-based cyber security is to grow and recruit more professionals, the academic aspect will need to address this problem accordingly.

Part of what I have dedicated myself to in the writing of this thesis is to make it comprehensive to a large and varied audience. Most technical literature seems to be aimed specifically at small groups of individuals. Considering the scope and cross-disciplinary aspects of my topic, it would be crippling to only address the cyber security professionals in my audience. Therefore, I have attempted to widen the scope, and include literature and vocabulary that can be understood by many different fields.

1.3 Structure

This document is structured to provide a clear explanation and analysis of the problem area. Chapter 2 revolves around the background of this thesis. It addresses industrial control system history and development, as well the application and methodology of computer forensics.

In Chapter 3, the problem space that this thesis centers on is explained in more detail. There are many aspects of ICS that make forensics difficult, and they must all be understood in order to suggest any solutions. Chapter 4 looks at the professionals that work within ICS and are often confronted by the problem space. Engineering, computer science, and psychological viewpoints are considered and discussed.

Chapters 5 and 6 detail a proposed solution to the ICS/Forensics problem, its benefits, and drawbacks. The meeting of system operator and pre-investigative forensics is analyzed in detail. The fifth chapter predominantly deals with methods that could be integrated into modern facilities to create more secure forensics capabilities. In the sixth chapter, these methods are analyzed for their validity and logical premises. Chapter 7 will crystallize the conclusions of this thesis, as well as identify future research that can be done in the field.

1.4 Acronym Chart

Acronym	Meaning
DCS	Distributed Control System
DOS	Denial-of-Service
HMI	Human Machine Interface
ICS	Industrial Control System
ICS-CERT	Industrial Control System – Cyber Emergency Response Team
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IO	Input/Output
IT	Information Technology
LAN	Local Area Network
MTU	Master Terminal Unit
NIST	National Institute of Standards and Technology
PCS	Programmable Logic Controller
PLC	Process Control System
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition System
SIEM	Security Information Event Management
WAN	Wireless Area Network

Table 1-1. Acronym chart

Chapter 2. Background

In order to discuss the problem of control system forensics, one must first understand the two fields separately. Each has a long history of development and implementation that have been sources of thesis and dissertations in their own right. To set the scene for this thesis' problem space, this chapter provides a brief description of each field.

2.1 Industrial Control Systems

The term "control system" refers to an automated group of machine equipment, generally run by a central or shared control paradigm. Control systems may come in a variety of forms, and are usually managed by a computer system. The amount of flexibility available within these systems has led to their inclusion in most modern factory-type processes. A simple example would be a device that measures and controls temperatures. The systems can also manage more complicated tasks, such as controlling electrical power distribution for a large city.

In the field of cyber security, important control systems are often identified as "critical infrastructures." This terminology came about as focus shifted from maintaining infrastructure adequacy to insuring its protection. However, the definition and limitations of this term have been subjects of constant reassessment. In 1996, President Clinton signed Executive Order 13010, which defined "infrastructure" as

> The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole. [1]

This marks the first well-known government attempt at prioritizing certain infrastructures in terms of United States security. As the area of infrastructure defense became a greater priority, new definitions were formed. The Department of Homeland Security references the latest terminology iteration in the USA Patriot Act of 2001:

> [control systems are]...systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would

Sector	Responsible Department
Chemical	Department of Homeland Security
Commercial Facilities	Department of Homeland Security
Communications	Department of Homeland Security
Critical Manufacturing	Department of Homeland Security
Dams	Department of Homeland Security
Defense Industrial Base	Department of Defense
Emergency Services	Department of Homeland Security
Energy	Department of Energy
Financial Services	Department of the Treasury
Food/Agriculture	United States Department of Agriculture and Department of Health and Human Services
Government Facilities	Department of Homeland Security and General Services Administration
Healthcare and Public Health	Department of Health and Human Services
Information Technology	Department of Homeland Security
Nuclear Reactors/Materials/Waste	Department of Homeland Security
Transportation Systems	Department of Homeland Security and Department of Transportation
Water/Wastewater Systems	Environmental Protection Agency

Table 2-1. Infrastructure sectors and their agencies [6]

> have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters [7].

This latest explanation infers why a critical infrastructure is important, but does not give a comprehensive list of services it includes. This causes a problem, as there are numerous infrastructures that could be referenced by this definition. Resources for defending them are limited, and so certain facilities must be prioritized above others. As of Presidential Policy Directive 21 (PPD-21), published in February of 2013, there are 16 critical infrastructure sectors (Table 2-1) [8]. Each of these sectors has been assigned a particular governmental department to oversee it [6].

The goal of these definitions and categorization is to highlight an underlying area of United States stability that is vulnerable. “Critical infrastructure” technology undergoes radical development as the industry advances, yet a comprehensive understanding of system security and reliability does not always progress as quickly. In order to ensure that the nation's safety can be protected, a greater understanding of the underlying mechanics is required.

2.1.1 History and Development

The first examples of automatic control were recorded over 2000 years ago, in the form of water clocks. Scientific discovery led to their further development, where feedback controls were used to regulate process temperatures. Near the end of the 18th century, the steam engine was invented and undergoing intensive developments. New automatic controls were needed to aid in its management [9].

In the beginning of the 20th century, further use for control systems became apparent as electricity began to spread throughout the modern world. Growing complexity was required in the field so that feedback controllers could distribute electric current to meet rising consumer demand. At the same time, temperature controls and engine regulators were further refined and advanced [9].

World War II invigorated scientific and technological progress in many fields. Pressure was placed on independent developers to automate processes and help the war effort. Anti-aircraft gun aiming systems were mechanized. Information relays were created and refined. Nuclear science and engineering, in particular, underwent a great deal of rapid development. This war also marked one of the first times in which mechanical, electrical, and electronic engineers were put together to develop new applications [9].

Automated control has proven to be useful and efficient since its inception. What was once primarily used as a method for controlling temperature evolved through the ages to control electrical current and weapons systems. After World War II, the area of control systems further diversified into the variety of sectors mentioned in Table 2-1. It has been effectively woven into the structure of modern-day life in the United States.

2.1.2 System Configuration and Operation

The instrumentation that supports critical infrastructure is referred to as an ICS. This tends to be a catch-all phrase to describe a variety of network configurations, industrial machinery, and computing processes. The National Institute of Standards and Technology (NIST) *Guide to Industrial Control System (ICS) Security* recognizes two popular types of ICS: Supervisory Control and Data Acquisition (SCADA) systems and distributed control systems (DCS) [2].

SCADA systems (Figure 2-1) monitor and control industrial plants by means of telemetry and data acquisition [10]. They regulate communication between a SCADA host computer, remote units, and terminals used by the operators [11]. The advantages of this set up are that the system can gather and store a large amount of information, and then display it for the operators in real-time or from records. A large number of sensors can be connected to this system regardless of geographical location, and collect a variety of different data. Another benefit is that the information recorded by a SCADA system can be viewed remotely, as well as on-site. These concepts may be difficult to understand without an example. One common system that SCADA is used for are water municipal utilities. The system would monitor and display the amount of water pressure in certain tanks that may be a great distance removed from the station, and report it to a human-machine interface (HMI) for the operator to view.

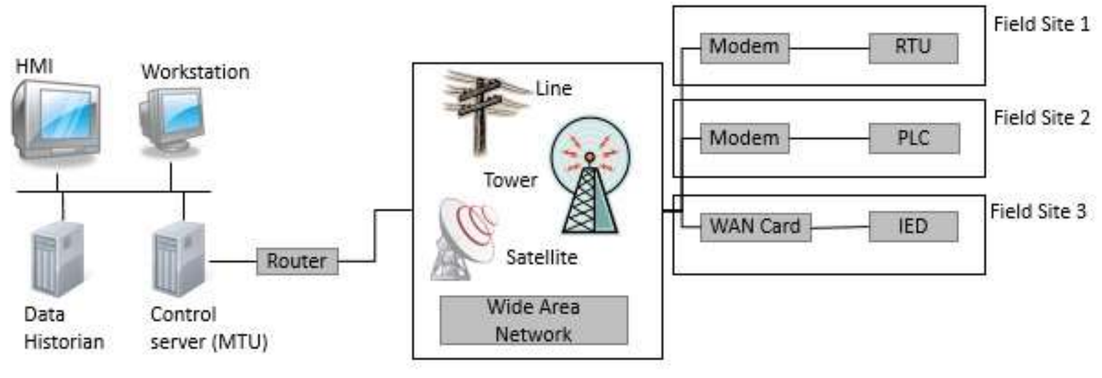

Figure 2-1. Generalized SCADA diagram

DCS (Figure 2-2) are generally used in systems where all resources are within the same geographic location, and where process manipulation is prioritized over data gathering [2]. They contain an architecture consisting of a supervisory control “overseer” that manages multiple sub-systems. These systems each receive tasks to complete that aid in the overall production process. They are generally comprised of localized controllers that are responsible for handling specific tasks. To complete these tasks, the supervisory system gives the controllers set points to operate by, and collects data to ensure that these points are being met. Set points are essentially status quo or ideal conditions to be met by the system. DCS can be expanded to nest multiple supervisory “loops” within the architecture, depending on the amount of control necessary to complete the process [2]. There are also many occasions in which a DCS is folded into the architecture of a SCADA system. With the SCADA architecture taking care of the larger picture, which may be spread across a great deal of distance, the DCS can focus on maintain system productivity [10].

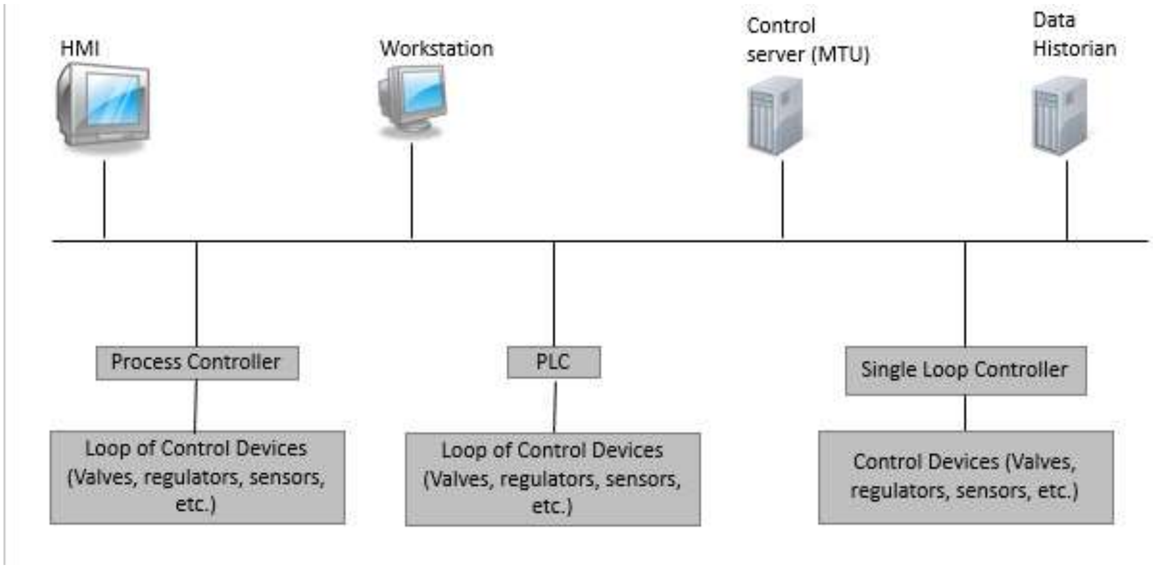
HMI
Workstation
Control server (MTU)
Data Historian
Process Controller
PLC
Single Loop Controller
Loop of Control Devices (Valves, regulators, sensors, etc.)
Loop of Control Devices (Valves, regulators, sensors, etc.)
Control Devices (Valves, regulators, sensors, etc.)

Figure 2-2. Generalized DCS diagram

ICS share some common components. They can generally be divided into two categories: monitoring and sensing. The monitoring category includes:

- Master Terminal Unit (MTU)
- Control server
- Input/Output (IO) servers
- Data historians
- HMIs

The MTU is a SCADA device that acts as the host computer, and regulates communication between itself and remote devices. It acts as a master, and controls remote devices such as remote terminal units and programmable logic controllers as slaves. Control servers are the DCS equivalent of an MTU [2].

An IO server manages collecting, buffering, and presenting information from remote units. It can also be used as an interface between third party components such as an HMI and control server. Data historians are used to keep a log of process information in the systems. The information stored here can be used for specific analysis by the engineers and enterprise statisticians [2].

A HMI is the software or hardware that creates a display interface that a human operator can use to better understand and interact with the system [2]. It monitors the state of the process, and reflects observations onto some sort of interface for the human operators to watch. The HMI also provides operators with the ability to manipulate the variables of the system to better achieve the set point. How an HMI is represented may vary greatly between systems.

The most common sensing components of an ICS are:

- Remote Terminal Units (RTUs)
- Programmable Logic Controllers (PLCs)
- Intelligent Electronic Devices (IEDs).

RTUs are units that are designed to report to SCADA systems from a remote field, and also allow the host system some amount of operable control over remote devices. Usually they are outfitted with some form of wireless radio interface, as many of these environments may not allow for wired communications [2].

PLCs are small, solid-state electronic devices that are very similar to RTUs, except that they tend to be more flexible among systems and capable of more complexity. What this means is that they can fulfill more roles in the system, and complete more tasks than the average RTU. The PLC is a very popular device in modern industry, and may even be used in place of an RTU due to their flexibility and prevalence in the field [2].

IEDs are smart sensors that operate at a higher functionality than RTUs or PLCs. They have been designed to enable communication, local processing, and data acquisition. Their main function is to "[allow] for automatic control at the local level" [2].

Within these hardware configurations a variety of software can be used to successfully run the system. In ancient times, this "software" concerned the laws of metal expansion given different temperatures. As automated control developed into ICS, the computer software developed in a less straightforward manner. It is within this software that many of the security risks posed to ICS exist.

2.1.3 Security Concerns

Existing software in ICS are generally divided into two sections based on their chronological creation: legacy and modern. Both are still used in the field, though the legacy group is shrinking as time goes on. Each presents their own unique security vulnerabilities that can be exploited by criminal elements.

Legacy systems refer to ICS that have been active for over fifteen years and do not have the same computing ability of systems made more recently. Often they run on proprietary technology that is no longer fully supported by the vendor [12]. This often causes problems, as the term proprietary means that the software and hardware configurations are vendor-specific, and have little-to-no support outside of the company of origin. Because of this, a variety of problems may exist.

Because the software configurations are older, they probably run on outmoded operating systems that lack the most recent updates and protections. Older proprietary technologies were also never truly designed to interface with anything outside of their own facility. Therefore, when greater complexity and connectivity is added, the risk becomes greater because these systems lack certain secure communication features. Another problem is that these architectures generally lack resources that could be used to detect or defend against cyber-attacks. Very few older systems have tools such as tailored virus protection, intrusion detection systems (IDS) or even comprehensive logging resources [13].

Modern systems can also be based on proprietary technology, though there is a burgeoning push towards using some standardized, shared methods. To qualify as modern system, both the vendor-specific and more “open” systems must both be fully supported and understood. The difference comes from where this knowledge originates. In the case of proprietary information, it resides within the company. For more common implementations, the ICS community at large may be able to provide support [12]. Many of the systems built within the last ten years were designed with more of an eye towards the future. Inter connectivity between ICS and corporate networks began to look like a promising advancement. Many articles have been written in recent years that extol the benefits of integrating ICS technology with the internet and new wireless protocols [14][15][16].

Many of these advancements, however, were implemented without enough preparation for the consequences. Network security has developed over many years, in response to the field's rise in importance and the advancement of malicious hacking techniques. ICS-specific security, though, has not been matured at the same pace. Many of the safety measures taken in DCS and SCADA systems were physical, such as building fences and installing heavy-duty locks. Cross-applying network security concepts is not always the most effective solution, either. Due to their intense cyber-physical nature, security must be more tailored to specific communications and hardware configurations than in an average information technology (IT) network.

The importance of maintaining secure critical infrastructure cannot be understated. If compromised, the stability of the American public may be at risk due to lack of provided services. There are a number of risks to ICS’s, ranging from simple natural disaster scenarios, to system error, and cyber-attacks. ICS’s are in control of many fields that are needed for modern security and life, and as such are prime targets for malicious computer-based aggression. Whether single attacker or an organization of malicious entities, there is obvious power to be gained from being able to manipulate or incapacitate the control system life lines of a country.

There are many stories that reflect the fragile nature of ICS's worldwide. The Maroochy Shire sewage spill is arguably one of the most famous stories to be reported. In 2000, a disgruntled former employee of an Australian manufacturing software development company used a few stolen devices and his knowledge of the system to release approximately 264,000 gallons of raw sewage into nearby public areas [2]. Stuxnet is also a well-known news story, as the first worm targeted specifically at debilitating an ICS, followed by its successor, Duqu [3][17]. These are headline examples of how an ICS can be compromised.

The importance of usable forensics in this field is plain. When an incident occurs, the full scope of what happened must be understood, and documented. In order to secure resilient ICS and persecute malicious attackers, professionals must be able to identify and document system events in a forensically sound manner.

2.2 Forensics

The term computer forensics can be generally defined as “the process of applying scientific methods to collect and analyze data and information that can be used as evidence” [18]. The intent is to gather facts from any type of computer system that has been involved in some type of incident.

These facts are then intended to hold enough integrity that they could be presented as findings in a court of law.

The episodes which might spawn such an investigation are not always malicious in nature, nor do they always directly involve the computer media itself. After a large system error has occurred, such as a blackout, a forensic investigation might take place to examine the damage to the system, and verify that it was caused by an accident. In certain criminal cases a subject’s computer media might be seized in order to search for evidence relevant to the case, such as illegal bank transactions or criminal planning.

Of course, computer forensics is also invaluable in researching cybercrime. In this area, the investigation often becomes extremely detailed and focused on a certain subject and its effects, such as malware or software exploits [3]. By digging down into the functions and mechanics of these malicious attacks, investigators can ascribe a sense of logic, motivation, and area of effect to the action.

Computer forensics is different from incident response and recovery. The Industrial Control System Cyber Emergency Response Team (ICS-CERT) identifies the key elements of incident response as planning, incident prevention, detection, containment, remediation, recovery and restoration, and post incident analysis/forensics [19]. Essentially, professionals must plan a response scenario, detect the event, contain the damage, stop the problem, recover system functionality, and then analyze what happened for future defense purposes. This is an extremely important field that has been integrated into other growing sectors of ICS security, such as resilience and reliability. Computer forensics is included within incident response as a key component, but goes to a deeper level of detail and data-integrity that sets it apart as its own field. By going to these lengths, specific details about an event can be found and explored in greater depth, and the perpetrating party may be identified.

2.2.1 Common Components of Computer Forensics

There is a sequence of steps to be followed when conducting a cyber-forensics investigation. The titles of these steps tend to vary between different scholars, but they usually fall into three broad categories: collection, analysis, and reporting [5]. These three topics are the foundations upon which forensics is based, and represent the strength upon which the evidence is presented.

Within the collection phase, tasks gravitate towards planning and gathering resources for the investigation. An initial plan is made, which involves outlining the approach that will be taken for a specific case. This often includes creating a checklist and gathering the resources needed to conduct the investigation. Resources such as forensics software, hardware, and containment units need to be carefully chosen to maintain the integrity of the data. Then investigators must obtain the devices they will be gathering the evidence from, such as hard disks, USBs, entire computers, or any other removable media associated with the case [18].

Once this has all been done, the risks associated with analyzing the evidence must be reviewed. This step is important to ensure the data remains intact and unblemished by the process. A risk may be physical, such as ensuring that a fragile case does not break, or virtual, such as ensuring that a drive is not wiped clean when the incorrect password is entered. Before evidence can be analyzed, the risks must be mitigated to ensure that the evidence contained within the computing unit is not destroyed. For a fragile case, certain containment units can be padded to ensure adequate protection. In the case of a possible disk-wipe, multiple copies of the original data can be made, so that multiple tries can be attempted [18].

When the plan has been written and the resources gathered, investigators can proceed to analyze the data. One can extract data from electronic media while it is “live” or “static.” Live analysis occurs when the computer being examined cannot be shut down. Generally, rather than conducting an entire forensics investigation using live analysis, an image will be taken of such a system while it is alive, so that the contents can be examined in a more secure manner.

Static analysis takes place when the system is or can be safely put in a static state. By doing this, the information contained within a system can be retained, without worry of constant modifications from the operating system. Static analysis can be performed on a computer that is shut down, on write-protected hard drives and disks, as well as on system images and a variety of other media [18].

Once the data has been extracted, it is the investigator's job to know what to look for. They must comb through the evidence to find problems, discrepancies, or media objects that allude to criminal activity. These bits of evidence can be found in a variety of places in a computer. The case may be as simple as critical documents in the 'My Documents' folder of a Windows computer. However, some forensics investigations may need to dig down into the operating system or software code mechanics in order to understand what has happened or is contained within a system.

When evidence is discovered on a system, it must be further investigated to ensure that it pertains to the case at hand. For instance, if the case involves money laundering, then specifically mentioned bank accounts should be noted and categorized for their possible connection. If certain files look as though they've been deleted, then an investigator should attempt to recover the files. In the case of a malicious software (malware) or system error, the affected components of the system must be observed in greater detail. With malware, an investigator might dive deeper into the code, to discern what its target and motivation might have been. The data discerned in these processes can generally be used to provide proof of a wrong doing, and aid in pinpointing the culprit [18].

In the reporting stage, investigators organize all of their findings into a case report, or series of reports. Every step of the investigative process should be documented, from how the devices were stored to where pieces of evidence were found and how they contribute to the forensic objective. Within this documentation the specifications of every piece of equipment that was examined should be catalogued, as well as how it relates to the crime, and other "facts" about the resources used in exploration. It should also contain a list of the evidence found, and in what manner it was extracted and preserved. One crucial component of the final report is documentation of the chain of custody.

This is a recording of every individual and group that has had access to the data since its designation as a possible evidence resource. By keeping track of these entities professionals are able to maintain the trust that the data has not been tampered with. Finally, the results and how they relate to the mission should be relayed in a clear concise manner. The outcome of this entire process should be a clear document that points out factual data that has been found in the system that pertains to the malicious/illegal/coincidental event in question [18].

This is the simplified overview of how a forensics investigation should operate. In reality, however, things rarely operate so smoothly. There is an entire litany of factors that can go wrong should mistakes be made throughout this process. On top of this, there are technological limitations of computer forensics capabilities.

Forensics software, hardware, and human professionals often experience difficulties interfacing with certain types of media. The location where data is stored on a system can vary widely between system specifications and user modification. It can add many frustrating hours of research to the investigation. Sometimes data loss cannot be prevented, if the device cannot be imaged or kept in a static physical and virtual state. In addition, social media information and cloud computing are only now beginning to be considered problems in the field, as more users keep information in non-local repositories [20]. These problems and the many others that exist are the current focus of professionals who seek to advance the computer forensics field. These questions must be solved to allow investigators to continue to provide the in-depth research needed for these cases.

There is a massive amount of research being thrown at solving these problems. Yet in this sprint for knowledge, it seems that smaller off shoots of computing such as mobile devices, hardware microchips, and ICS, have fewer forensic-centric professionals eager for development. However, within these fields the need for forensic advancement is just as great as their mainstream IT counterparts.

2.2.2. Forensics in SCADA

ICS and forensics have developed apart. When ICS's were first being implemented, most scientists and engineers focused on achieving more efficient automation in the system. Planned forensics procedures more likely revolved around physical activities, such as break-ins or damage to the system parts. Computer forensics arose out of a need to look through digital data in personal and professional network media, and has in many ways been tailored for this service. This has resulted in a dearth of information, procedures, and technological ability to conduct a forensics evaluation of an ICS, should an incident occur.

Only in recent years has forensics in ICS become a primary focus of some technical documents [5][13]. Even so, there are very few of these in the large pool of academic and industry research on computer forensics. There is even less information available about circumstances in which a forensics plan was enacted, and how the resulting investigation and case were carried out. The main problems that exist within this cross-disciplinary field are that technologies need to be adapted, architectures expanded, and plans need to be developed in order to provide forensic capabilities in ICS.

Chapter 3. The Problem Space

There are many problems that confront those wanting to develop the area of forensics in ICS. Most spawn from the fact that the ICS systems have not been developed to aid in traditional forensics tactics, and forensics have not been bent to fit the ICS mold. The following sections discuss some of the main problems that are currently being discussed in the research community.

3.1 Technical Problems in Control Systems Forensics

Due to their non-traditional (when compared to IT) structures, ICS have a number of technical difficulties when attempting to implement forensics. They have a different priority ranking than their corporate network counterparts. Thus, some exceptions for forensics that an IT network may allow cannot be tolerated within an industrial system.

In cyber security, there is a common acronym known as CIA, though it would be better represented as CIA^2N. This refers to the concepts of Confidentiality, Integrity, Availability, Authenticity, and Non-repudiation [21]. These are key concepts in the field of information security, which form the basis for a strong network. In the case of most systems, confidentiality, integrity, and authenticity are likely to be prioritized above availability and non-repudiation. After all, it is important for an individual to be able to access their bank account at all times, but it might be slightly more important to be able to authenticate the connection that gives them access.

With ICS, the case is the reverse. Availability is one of the highest priority goals of any given process. If the system is not accessible then it is not serving the client base. An example would be that if a SCADA system that is part of the electrical power grid was no longer available, then power would not be distributed to consumers with an adequate level of quality. This is obviously bad, and so the first and foremost goal of an ICS is to keep the process running and available. This, in turn, causes problems with the data collection aspect of forensics.

As mentioned previously, forensics professionals prefer to conduct their investigations upon static information. This is to ensure that the data is not changing and losing credibility as it is examined. It is unrealistic to expect that an ICS can be taken offline for investigation [5]. Thus, live analysis techniques must be applied to the system, and real-time forensics tools need to be developed and used.

The idea of copying the system for further analysis is further hampered by how an industrial control system operates. Huge amounts of data are generated by the average control system as it tracks different alarms, set points, and monitors sensors [13]. Many messages are needed in order to keep communications between the master and remote sensors flowing smoothly. There is an aspect of volatility here, along with storage concerns. Most systems have a rolling time frame in which they log information. Due to the sheer amount of data being tracked, there is a tendency to discard data that is no longer directly useful. For instance, low-level registers and caches are constantly rewritten as they service the system, and this data is not archived due to its usually temporary nature [5]. If an event occurs, forensic examiners want to be able to amass as much relevant data as possible about the event. At the same time, any organization would be challenged to store every single piece of data in a SCADA or DCS over any given time. As such, it becomes a question of storage capacity and realistic goals. Being able to tell the difference between useful information and system noise is a problem known as data mingling [5]. Due to the amount of data produced in an ICS, those pieces affected by an incident and those that are unrelated are likely to be mingled and indistinguishable within memory. This is a result of inadequate system labeling and description.

Possibly the greatest technical problem hampering ICS forensics is that the software and hardware configurations are exceedingly proprietary and vendor-specific [5]. The main goal of an ICS vendor is to provide efficient software for the client. Their aim is to create a system with high availability that is easy to use. Concepts such as security and forensics have not been a high priority until recent years. The sheer variety available in the ICS domain also causes a problem. In order to operate a system, one must be trained in how to use that specific vendor’s technology. Thus to conduct a proper examination, one must first be versed in where the vendor may store important data in their software.

An essential part of forensic science is the knowledge of where to look for data. Understanding where things may be cached, stored, and hidden is extremely important, especially at higher levels of incidents. In network forensics, there is a lot of knowledge in the community about how the main-stream operating systems (Windows, Linux, Mac, etc.) work, and where things are recorded within the system framework. SCADA and DCS, however, often operate on modified or custom-built kernels for process control [4]. Not only does this mean that forensic investigators need more vendor-specific knowledge concerning the kernel, but that much of the data acquisition software in use today may not be able to interface with the system. Most modern forensics devices lack the ability to understand some unique features about ICS systems, such as their specific protocols or formats [4]. The alternative to these tools is to have an individual comb through the data, which would be horrifically inefficient, error-prone, expensive, and cumbersome.

Concerning live analysis on ICS, further constraints are put upon investigators in the form of time and resource effect. Extracting data from an ICS system causes certain system resources to be used. There is no way to guarantee that forensic investigations may not tax certain system components to where they are unable to maintain high availability [4]. In the process of an examination, there have even been cases where specific investigative tools have caused as much of a problem in the system as a malicious event would have. In one specific incident, a simple ping sweep on an active SCADA network led to the destruction of $50,000 worth of assets. This was caused when a robotic arm suddenly activated, swung 180 degrees, and broke a collection of expensive wafers [2]. The explanation for this occurrence is that the ping interacted with the arm in an unanticipated manner. There have also been reports that simple scripts or tools may damage remote devices such as PLCs and RTUs, due to their limited resources. In effect, it is possible that exploration and questioning might cause them to experience a type of denial-of-service (DOS) attack, in which they are receiving more requests than they can service.

The technical questions of how to collect and analyze evidence taken from an ICS system are not simple to answer, nor have any good technical solutions been thoroughly documented in the public

Forensic Methodology	ICS Problem
Static Analysis	Need for constant availability
Data Analysis	Huge amount of data produced in the system due to amount of monitoring, automation, and control commands
Data cache analysis and image copying	Proprietary software and hardware with a high amount of variance in storage methods, and few standardized practices
Use of forensics tools on the system	Heavy taxing of resources, and occasional misinterpretation of commands

Table 3-1. Summary of ICS technical problems in forensics

purview (Table 3-1). However, the problem of forensics in ICS cannot simply be solved in the technical arena. Problems to the field extend beyond the boundaries of technological limitation. It is also a matter of manpower.

3.2 Man and Machine

One of the most fascinating aspects of ICS is its cross-disciplinary nature. In order to create a functioning facility, one needs a variety of engineering professionals, computer scientists, and daily operators. On top of this, initial development often requires the aid of corporate financiers to fund the venture and human factors psychologists to design an efficient and ergonomic structure. Each of these individuals, in one way or another, becomes involved in the life of the system.

For instance, in the case of a natural disaster, each profession is involved. The engineers make sure that the physical properties of the system (the machines, electrical current, etc.) will be as resilient as possible. Computer scientists (hopefully) ensure that the system is recoverable, with software and backups. Daily operators may be on the scene to enact emergency procedures to ensure the system suffers as little harm as possible. Even the financiers and human factors individuals are indirectly involved, due to the need for an “emergency fund” and secure escape routes for workers.

Thus, a successful forensic examination must also involve professionals from these separate aspects of ICS. Computer forensics officials are not always there at the first sign of an incident, and even if they are they may not have extensive enough knowledge of the system to make the best use of their time. In a volatile ICS system, evidence must be collected in a timely fashion in order to ensure its usefulness [5].

3.3 Financial Cost

Few companies would be willing to take on the cost of having a computer forensics professional on staff at all hours, particularly when their main function comes into effect only when an incident occurs. Thus, another solution for collecting data before the forensic investigator arrives is needed. Data logging is an essential part of this solution, and is implemented in many forensics circumstances. However, as mentioned before, this logging may not be adequately labeled for forensics circumstances. Another layer of difficulty involves the fact that vendors have designed the logging services to track process disturbances and errors, rather than security-specific problems [4]. As such, it falls to the software developers and financial supporters to create and invest in a higher level of logging program. This would be very expensive, and there has not, as of yet, been a surge in SCADA forensic logging software.

3.4 Security Vulnerabilities

There are many types of security vulnerabilities that can affect a computer system. In February 2013, the SANS institute conducted a survey on SCADA and Process Control Security. This revealed that the top threat vectors industry is concerned about are: malware, internal threats, external threats like hacktivism or nation state attacks, phishing scams, industrial espionage, and extortion [22]. When incidents occur that involve these vectors, forensics is essential in determining the details of what happened and who is responsible.

Threats such as malware can be insidious, and difficult to find. One of the most famous cases of malware in ICS is the Stuxnet worm. It targeted and infiltrated a specific nuclear facility in Natanz, Iran, and destroyed around 1,000 IR-1 centrifuges at the site [3]. Stuxnet is an exceedingly complicated piece of software that managed to go undiscovered for a prolonged period of time. It is a potent weapon, and the first of a generation of such malware developed for attack purposes, as evidenced by Duqu, the first Stuxnet successor [17]. Due to its complexity, the worm required a great deal of forensic investigation in order to understand its design and structure. Through this analysis, professionals were able to understand how this feat of cyber-weaponry was accomplished, and were able to patch the vulnerabilities it exploited [3]. Without such detailed analysis, many computer systems might still be vulnerable.

The intent behind an attack is often as important as the attack itself. When a vulnerability is exploited, there is motivation to compromise the system. However, a teenager disabling part of the public telephone network and a nation state developing a specifically targeted worm are two vastly different scenarios, and require different responses [9]. Computer forensics can help determine this motivation, and dictate what the proper response is. It can also raise the likelihood that the perpetrators can be found and properly punished.

3.5 In the Courts

Computer forensics and its weight in the court system is a changing field of study and application. Digital evidence can be easily corrupted, and thus can be easily thrown out of court for lack of integrity. There are specific rules on how the evidence must be gathered, stored, and analyzed in order for it to hold any weight in an investigation.

One of the ways that the integrity of a piece of digital evidence can be ensured is by creating a digital copy and comparing the two [18]. However, in some circumstances, this is too cumbersome a solution. Some forensics investigators choose to verify their data by computing a cryptographic “hash” of the original data. They then create another hash of the copy they are analyzing, and can compare the two to ensure that they are the same. If anything is changed about the copy, then that change would be reflected in the copy’s hash [18].

Live analysis of ICS systems presents a problem with this method. Due to the priority of availability, the ICS must be kept live, which means that the system data will change. The hash of the original system and that of the system copy will not match. After the forensics professional has examined the image, though, the hash of the original copy taken from the system should be able to be used to determine integrity. This raises the question, however, of whether the data could have been tampered with as it was being copied from the system. The stability traditionally offered by the hash algorithm comparison has been shaken by this assumption [18].

Another problem with live analysis is that the system may change even as the data is being extracted. States will change as the system runs and overwrites certain data, meaning that the copy being analyzed may not adequately reflect the system as a whole. There have been cases when the image taken was not able to be fully explored due to a lack of recorded preset data [18].

These problems allude to the difficulty of verifying evidence in a forensically sound manner. Without integrity checks, the data cannot be treated as trustworthy, as it may have been tampered with. In order for ICS data evidence to lead to any legal action, the data must be verified and compliant with the Federal Rules of Evidence [12].

3.6 Summary

There are a number of problems that exist where ICS and computer forensics meet. Technical problems have existed for decades, due to the rapid development of both individual fields. Human matters, such as machine interaction and financial support have also hampered advancement in the field.

In spite of these problems, however, there are greater needs that demand better ICS forensics procedures. Security vulnerabilities are a growing concern in ICS, and industry must be able to understand what is affecting their facilities and how to defend against it in the future. In order for the evidence gathered from an ICS to hold up in a court of law, new methods of ensuring evidence integrity and presenting the facts must be established. If ICS are to maintain their integrity, professionals must work together to integrate forensics into modern industrial systems.

Chapter 4. Those who Use ICS Systems

Most technological fields are cross-disciplinary. In traditional information technology networks electrical engineers, computer engineers, and computer scientists are only the skeleton crew of professionals that need to be involved. From the design of the chips used in the PCs, to the IT staff managing the email server, there is an intensive amount of varied knowledge integrated into network deployment and maintenance. However, in IT it can generally be said that all of these professionals need not be deployed during the entire life cycle of the network. An electrical engineer will rarely be called in specifically to fix a broken chip in an employee's desktop (though it may be sent back with a warranty.) Once the network has been set up, the IT staff – generally made up of computer scientists and technicians – is tasked with handling the burden of maintenance.

With ICS, this is not the case. In the field, physical technology, software, and humans are expected to interact flawlessly in order to get the process done in an efficient manner. Several different professionals are involved in the design, implementation, and upkeep of an ICS. In order to do this, many of these specialized workers must have some semblance of an idea about what each other field is responsible for. Each has a purpose and effect upon the system. Thus, in order to make any adequate advancement in the technology and techniques employed in ICS, each field must work together.

4.1 Engineers

Depending on the control system, many types of engineers may be employed. There are different requirements to be met, depending on the size and complexity of the ICS. For instance, a large electric municipality may need to keep track of thousands of statistics, whereas a canning company may only need to keep track of a handful of data points [23]. The engineers of these systems are responsible for creating and maintaining the plant equipment, and ensuring that the production receives no physical disruption. They are also expected to ensure that the site is safe and "within specification" [24]. Obviously, these tasks can require the use of many different sects of engineering, such as mechanical, electrical, process-related, etc. The cooperation of these fields is integral to the success of the system.

In order for the process to execute, the ICS needs machinery for production. What the process involves and how it can be completed efficiently are the key aspects of design. In a historical context, this is manifested in the temperature management of certain procedures. Engineers realized that metal swelled as it reached certain temperatures, and so used that observation as a rough gauge to implement automated system temperature control [9]. In modern times, other aspects that are factored into the process machinery are fault tolerance and redundancy [25]. If an accident occurs, the process equipment must be protected so that production can be resumed as soon as possible. Fault tolerance increases the durability of the structure, whereas redundancy means that if something is damaged, then its spare is already in place for system continuation.

Along with the process, it is the engineers' burden to ensure that the system can run consistently (usually continuously) and reflects real-time information and commands [25]. Continuous system operation requires high-endurance technology to function without breaking down from wear. Any moving parts, such as pistons, valves, and even the motherboard of a server can be worn down after enough uninterrupted use.

In Chapter 2, the definition of a critical infrastructure was presented, that generalized the industry and focused more on security concerns. Within the engineering field, ICS are mostly viewed as real time systems:

> A real-time system is one in which the correctness of a result not only depends on the logical correctness of the calculation, but also upon the time at which the result is made available [26].

This definition touches upon the fact that most engineers view a control system as a test in determinism and reliability. When building the system network, engineers aim for predictability, responsiveness, and support for other features such as parallelism. They desire a small operating system with good context switching and scheduling features [26]. If a structure routinely meets scheduled expectations, then it will successfully continue production and serve the clients.

In digitally controlled systems, engineers are tasked to base some of the control system operation on digital hardware. This is where more involved electrical engineering can come into contact with computer science. In order to fully utilize the system using scheduling and controller software, both professions are needed. There are errors that enter the process in this stage, however. Software development problems, sampling times, and/or control jitter caused by algorithm execution time variations can undermine the consistency of the process. The ultimate goal of implementing a digital control system is to reduce controllers to polynomial equations that can then be plugged into algorithms. During a defined sampling period, the controller algorithm will be executed to complete the task. Said process may be further divided by the system into multiple tasks, and multiple equations [26]. This is an overly simplified view of the system, but provides a brief outlook into what the engineers must calculate for an ICS to function.

4.2 Computer Science

ICS systems were created to be efficient and predictable. However, as time passed, desktop computers, servers, and computing power overall decreased in price while they increased in efficiency. Many industrial systems leapt on to this rapidly advancing technology in order to make productive advances of their own. However, this has caused the line between IT and control networks to become blurred. This lack of distinction only increased as more enterprise systems integrated themselves with ICS in the name of convenience and practicality [27].

With this in mind, in 2008 DiFrank created a network pyramid to describe a modern SCADA system setup (Figure 4-1). Levels 0-3 form control layers, whereas levels 4 and 5 are more associated with the attached enterprise infrastructure [27]. By using this type of model, it is easy to see the rising levels of abstraction in computing.

In Level 0, we see the base process that is being manufactured by the system. This is a level more associated with electrical and process-specific engineering than computer infrastructure. Higher up, Level 1 constitutes the various sensors and their interfaces to the Level 0 process, while

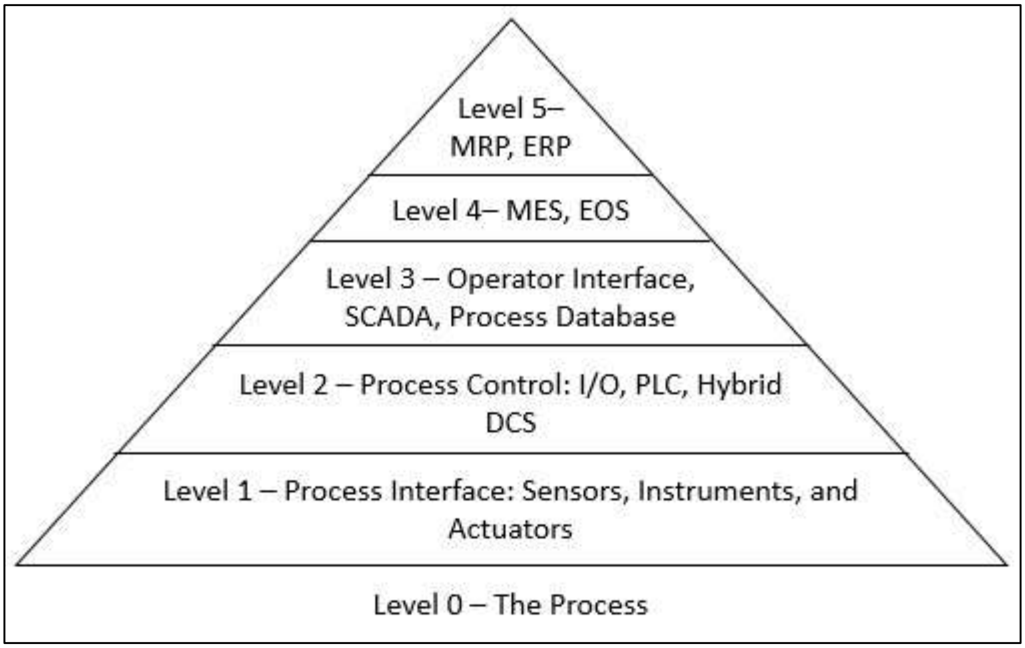
Level 5–
MRP, ERP
Level 4– MES, EOS
Level 3 – Operator Interface,
SCADA, Process Database
Level 2 – Process Control: I/O, PLC, Hybrid
DCS
Level 1 – Process Interface: Sensors, Instruments, and
Actuators
Level 0 – The Process

Figure 4-1. DiFrank Functional Enterprise Computing Model, derived from [16]

Level 2 begins to involve slightly more advanced control software. In Level 3, there are the recording databases, the SCADA supervisor, and operator interfaces [27]. It is within this section that most operators function, and marks the last area that should have any type of direct control over the lower levels.

Within Level 4 there exist the beginnings of enterprise interconnectivity. This layer contains the Manufacturing Execution Systems (MES) or Enterprise Operations Space (EOS), which are usually associated with managing operations and the control environment. A few examples of devices that might live at this layer are application servers, local area networks (LAN) and wireless area networks (WAN), as well as the interfaces to Levels 3 and 5. Level 5 contains all the remainder of the corporate computing network, such as financials and other business-level computing needs [27]. Many facilities view their system architecture this way, rather than as separate function- and IT-based networks. This attitude promotes a more unified company structure, and also allows for the creation of more convenient communications. By utilizing interfaces between Levels 3 and 4, professionals are able to maintain communication with some level of security through use of firewalls and transaction managers [27].

4.3 Operations and Human Factors

Those who use the deployed system most frequently are typically called operators or process engineers. In the two previous sections, the contractor or employee goal was to create and maintain an optimized, productive environment for process execution and business communication. The operators are present within the facility to maintain it and directly manipulate the process. They are generally more specifically trained in the production itself rather than the other fields, and their main goal is successful process completion. By working in the system, they also contribute another layer of complexity by adding human error and ergonomic concerns.

From the operator standpoint, a process control system can be seen as having manipulated variables, disturbances, and controlled variables. Manipulated variables are the devices in a system that can be changed to affect the process output. Disturbances cannot be controlled by the operator, and will generally drive the process output away from the desired goals. The controlled variables are the process output. This output manifests itself as certain conditions that must be maintained for system health. Operators will pair manipulated variables with these control variables in order to exert influence over the process conditions [28]. An example of this setup would be opening a valve to increase the flow of water into a system. The manipulated variable is how much flow the valve allows. A disturbance could be the environmental temperature, which could cause the water and metal in the system to expand. The desired output is consistent water pressure.

To manipulate these variables, the process engineer or operator must understand the system process, measurement, evaluation, and control. A process is defined as some type of equipment and/or material assembly accomplished by mechanical operation or sequence of actions. It is the machinery used and the act of accomplishing a task. For example, in a brewing facility, the distillation machines are part of the process, as is the distillation itself [28].

Measurement provides the data that the operator needs to judge whether they need to make adjustments in the system. To do this, sensor readings are taken and then interpreted to some sort of user display. The operator depends on these reports to be accurate, so that they can evaluate and make changes if necessary. If a measurement is misrepresented, it could cause system error [28].

The evaluation component of the system involves checking the provided measurements against set points. These desired values have been calculated beforehand, and are to be maintained for peak system efficiency and production. A controller will compute the difference between the reported measurement and the set point goal. If the value is outside of acceptable error bounds, then corrective action will need to be taken. This is generally achieved by some type of automated response, or by direct action of the system operator [28].

The corrective action taken is part of the control aspect of the system. To control a process, one must control any number of dynamic manipulated variables that may contribute to its output. Those devices that exert direct influence over the process are called control elements. These are what the system or operator will change, such as a valve, motor, pump, etc. [28]. Changes can be accomplished by either physically manipulating the system, virtually interacting through an HMI, or by writing simple logic programs [29].

Operators are required to interact with the control system under a multitude of conditions. The stability of the ICS may be affected by each individual worker’s capabilities. The way that employees react under monotonous, but also potentially stressful, situations is important. The field of human factors has arisen to ensure that the system and human beings can effectively interact regardless of the environment

The goal of human factors is threefold. The field aims to enhance performance, increase safety, and increase user satisfaction during human interaction with systems. These goals manifest in the study of factors in human comprehension and the development of new methods or tools to aid the relationship between user and machine [30].

As the years advance, ICS becomes more and more automated. Ideally, this should lead to a more predictable system, as computers are supposed to only do what they are told. Many systems are run remotely, and have as little human interaction as the companies can manage. However, there is no system that is completely autonomous of human interaction, and many systems still rely heavily on the human operator component.

As outlined before, there are key elements that an operator must understand about a system, but this truly understates the sheer amount of data they are presented with to analyze the situational environment. They must supervise a complex array of controls in order to maintain the entire facility. As such, operators must be able to detect patterns or shift strategies based on changes in the system. Given the sheer amount of data that exists in an ICS, however, data overload is inevitable. Thus, being able to prioritize and filter information before it reaches the end user and decision maker is an important task of the system [31].

Under great stress, human processing power becomes more limited, and “information overload” can become a large problem [30]. Emergency response situations require careful planning beforehand, in the form of training and human factors design. Operators and process engineers must be educated in how to react in certain situations, and how to maintain a level of control. The system must also be streamlined in these cases so that the operator can effectively interact with the environment to control the problem. Human factors, in this instance, identifies the pieces of the system that can be restructured to allow for emergency reactions. By doing this, the hope is that certain disasters that are compounded and made worse by a poor interface can be avoided [31].

4.4 Cross-Disciplinary Resources

In the operation of an ICS, there are many professions that must be involved. As one can see, engineers, information technology staff, and operations engineers all see the system from a different point of view. Human factors psychologists and business financiers see ICS in different ways as well. The cooperation of all of these fields, and the understanding of all of these viewpoints, is necessary in order to ensure the resilience of the system. Forensics must also involve these fields if it is to succeed, and some researchers have considered new ideas that may help its progression.

In order for enough data to be gathered from the system, researchers state that engineers must adapt the system for more adequate space and resources. Electrical devices, in particular, must be able to record important security data as well as operation errata. In many cases, this will be an expensive task that will add more complexity to lower-level devices. By adding these features, though, it may be easier in the future to understand how the incident has affected all levels of the system [27]. Along this same vein, the devices must also be designed to be resilient against certain types of scans and examinations, so that investigators are able to probe into them without fear of causing disruption [9]. Further pushes towards standardizing software across company lines would also be of great help in the forensics cause.

Concerning computer science, studies indicate that there needs to be more individual data, documentation, and specialized security. Simply logging system traffic is not enough if it cannot be properly identified. Many SCADA systems, for instance, have specialized protocols that are not always recognized by off-the-shelf security software [5]. This needs to be remedied, so that information may be properly tagged and comprehensible to future examiners. Extensive documentation of the network and its communication pathways is also key, as it will give forensics investigators a way to narrow the focus of the investigation based on likely avenues of attack. This documentation may also help investigators in determining where important stores of information may be. Specialized security for ICS would also benefit examinations, as it may throw up alerts to potential problems and catalogue security-specific events on the corporate side that contribute to an incident.

Systems are only as secure as the humans that use them. This saying applies both before and after incidents. It has been previously mentioned that a key aspect of incidence response is to forensically analyze what has happened, so as to learn and adapt from the experience [19]. This being the case, the industry understands that it is important for the operators to know at least the basics of what a forensics investigation requires. They must understand that flushing system memory may be an effective means of restoring the system, but that they are also destroying valuable data that may contain the answer to what caused the incident in the first place [4]. Human factors can determine where forensics considerations can be placed into software during incidence recovery stages.

By working partially together, these disciplines have created systems that formed the foundation of most modern civilizations. In order to continue providing that stability, they must continue to work together. An excellent step in future development would be for these professions to make allowances and develop new strategies for executing forensics examinations. By supporting the level of detail that is output from an investigation, they are supporting the knowledge from which resilience can be built.

4.5 Summary

Many different professions are needed to design, develop, and maintain an ICS. Engineers are required to ensure the physical safety and logical structure of the system. Computer scientists must also be involved, to make sure that the enterprise level network interacts well with the industrial system. Operators carry out the true purpose of the ICS: the process. They use the system constantly, and make changes to facilitate its overarching process goals. Human factors psychologists must be involved to ensure that these operators are able to interact with the system as efficiently as possible.

Each of these individual sectors has different views of ICS. These varied viewpoints are valuable in upholding system structure and stability. To truly ensure the integrity of the system, and its ability to recover and defend against new attacks, each of these fields must work together. They must learn to see beyond their own specialties, and begin to understand how tasks need to be shared over professional boundaries in order to secure the system as a whole.

Chapter 5. A New Methodology

The importance of cross-disciplinary work and communication cannot be understated in industrial systems. This thesis proposes the idea that this multi-profession interaction be taken a step further. If operators, who interact the most with the system, could be trained in certain pre-investigation forensics techniques, there would be enormous benefits. To accomplish this many professions would need to work together to ease this burden being placed upon the operator, while simultaneously enabling them to begin the forensics process. The goals of this chapter are to outline how operators can contribute to forensic investigations, and how other industry fields can contribute to this objective.

5.1 Introduction

To accomplish any form of advancement in the control system industry, it is obvious that there must be teamwork [24]. There is a strong base of literature in ICS' that recommends cross-disciplinary teaching, integrated work environments, and strong communications skills. After all, network connectivity and cyber-security problems in SCADA have not existed long enough for many engineers or business managers to understand the dangers. In the same vein, IT security has not necessarily been integrated with SCADA or other ICS long enough to understand some of the limitations such a system presents [24]. Without working together and teaching each other, the separate disciplines will not be able to make a unified effort in protecting their systems.

To aid in this effort, many new training courses have been created to help teach about the cyber security risks to ICS. Idaho National Laboratories, for instance, sponsors a free week-long course to train engineers, management professionals, and IT staff about the difficulties presented by an industrial control system. The Department of Homeland Security strongly recommends that many different professions, from IT and engineer to lawyer and financial advisor, be involved in the incident response task force [19].

These preparations and evaluations have made progress in convincing industry that mingling disciplines is good for productivity and safety. However, many of the ideas presented involve multiple people from separate fields working together in a facility or network. This can cause problems, miscommunications, and inefficiencies. There is a difference between understanding the theory behind what a coworker is doing, and having the experience to contribute to another's work.

In forensics, there are many specialized IT personnel, government officials, and third-party contractors that are dedicated to conducting examinations in a professional, thoroughly detailed manner. This is highly conducive to obtaining the information from a system needed for intensive study and legal proceedings. They are trained in the investigative sciences, and understand how to best preserve and analyze data using a variety of toolsets [32]. However, it is inefficient to consider these individuals as the only contributors to forensics data acquisition, analysis, and reporting.

Within the staffing environment of an organization, there are generally three types of individuals associated with a forensics procedure. There are investigators, IT professionals, and incident handlers. Investigators have specialized training, as well as extensive knowledge and resources available for a forensics investigation. IT professionals include technical support staff and administrators who use lower level forensics software throughout the course of their work. Incident handlers are those who respond when something has gone wrong with the system, be it malicious or accidental [32].

Within an ICS incident response group, it is recommended to have system engineers, network administrators, management, security experts, legal specialists, public relations officials, and a whole host of others involved in the process [19]. Obviously, some individuals may be more involved in each other's work than others. It is important that everyone involved in operating on the system know what their specific task is, as well as what their fellow workers' goals are. This way, the situation can be handled as a team.

However, in the case of an incident occurring, it is unlikely that all members of the team will be physically represented and assembled immediately. In fact, it has been suggested that cyber-incident responders may be part time staff, or have other day-to-day duties that capture their attention [19]. More likely, process engineers and operators will be available at the time of malfunction, with possibly a few IT staff if the facility is located in a non-remote area. For forensics, not having the ability to immediately begin collecting information from the system is severely hampered by the mindset that data collection can come after the crisis has been averted. In certain circumstances with traditional IT networks, this has proven to be an acceptable tactic. This is because most of these networks have implemented traffic loggers, with good labeling schemes and storage [5]. An ICS, however, is a different beast. As explained in Chapter 3, one of the greatest problems in automated control system forensics is the lack of data report and storage space. By the time an incident is over, a great deal of information may be lost due to efficient, but in this case hasty, memory management.

In any system, information about an incident should be collected as soon as a problem is detected. It has been recommended that forensic collection be included along with the incident response actions taken to recover the system [5]. However, forensic specialists may not always be around when incident response actions are put into effect. If these professionals are not present, or not among the first response team, then information will be lost.

To solve this problem, a new strategy is needed, and it should include more than teamwork between multiple professions. Cross training needs to be implemented in industry to maintain the usefulness and integrity of the forensic data. In this instance, process engineers and system operators have the best working knowledge of the system, and are the most likely to be on the front lines when an incident occurs. It is logical, therefore, that they should have the knowledge needed to begin the forensics process.

Those who work with the system on a regular basis, utilize the components, and are responsible for maintaining the system process are called process engineers or system operators. They have valuable resources in terms of forensics science. Namely, they are more likely to be there when a problem occurs, and to take action to fix said problem. By training these individuals in some simple, standard forensics procedures and by working to make the collection process as easy as possible, great advancements can be made in ICS forensics examinations. The remainder of this chapter presents how operators may be trained to gather information for an investigation, and what system changes need to be made to store and carry out the new forensics actions.

5.2 Training

Operators and process engineers have extremely important jobs. They are generally specialized not only to the overall process, but to that particular facility’s process. These workers must be this specialized, due to the unique proprietary technologies and functional convenience measures that are implemented in each system. The task of maintaining such a facility is not an easy accomplishment. Suggesting an added training course in forensics is not meant to belittle this work.

The goal in training ICS operating staff members in certain forensics procedures is to enable faster collection of data with minimal risk and detriment to primary system concerns. Naturally, their first priority will be to recover from the incident quickly so as to restore the process. This does not preclude the use of certain techniques that will give later professionals, such as IT staff and investigators, more information to examine. These techniques would not be in any way intended to replace an individual with more experience in the field. It is only meant to aid the process, not compact the workforce.

Cross-disciplinary training for cyber security has been recommended, developed, and implemented before [23]. However, these courses generally give a broad overview of cybersecurity, rather than focusing on any one part. This is understandable, given the fact that the field of cyber security is constantly changing, and that specific aspects or details might quickly become outdated. However, in the case of forensics, there are a few tasks that always provide some use.

Certain forensics tasks should be left to one who understands the full resources and procedures of an investigation. These are items such as determining the scope of an examination, what tools to deploy, analysis of IDS files, traffic packet examinations, etc. Other pre-investigation and beginning

Risk Analysis Component	Operator Action
Crucial data	Observing and recording machine behavior and system communications
Time expiration	When critical components are failing a system flush or reboot must take place. Any information must be gathered before this occurs.

Table 5-1. Operator risk analysis considerations

forensics tasks are not so knowledge intensive. The “Handbook for SCADA/Control Systems Security” by Radvanovsky and Brodsky enumerates a series of actions to be taken in the beginning examination stages [24].

The preliminary steps involve evaluations that need to be done before any forensics action is taken. First is to determine the risk inherent in the system: what data is most crucial to the investigation and when may it be lost? Operators often do not know the specific underpinnings of system mechanics such as network packets and register entries, but they can use the HMIs to identify devices that seem more affected than others [23]. They also know that if devices are no longer operating, for example if they are infected with malware, they might need to be “flushed” in order to get the system back online quickly [4]. This puts them in a unique position to understand the importance of the information contained on the device, and that it will be lost if not recorded immediately. Due to their knowledge of the system, it is logical that they be involved in the risk calculations, and have recordings of their thoughts on the matter. These considerations are summarized in Table 5-1.

The next aspect of the assessment involves documentation of the system. Descriptions and diagrams of structure communications are essential in a forensics review. Documents depicting the system infrastructure, critical configurations, process procedures, and device logic are crucial to understand the ICS. Some of these records will be kept by the system engineers and IT staff, as many process engineers don’t need to understand the specific network mechanics of a system. However, the process of a facility dictates what shape these systems take. Operators are able to make subtle changes to the organization, and a vital aspect of documentation is that it be kept up to date. Every time a change is made by a process engineer or operator, the change and the signature of who enacted it needs to be logged with the rest of the technical documents. This is particularly relevant if any new devices or communication pathways are added. Good documentation will allow forensic examiners to immediately understand the layout of a system, and discern “usual” from “unusual” traffic [23].

For instance, an operator can manipulate control variables via commands sent from the HMI. New programs may even be written to govern device communications. These operator actions will generate network traffic. A forensics investigator needs to know about these commands and programs, as well as who implanted them, so that they can distinguish normal device interaction from more abnormal traffic.

Actions taken and who executed them during incident response are also important, and should be documented for the examiners to look at. There are many important tasks that an operator executes in an emergency situation. One of the simplest ways to log actions taken is to record the operator’s terminal session as soon as an incident begins to occur and stamp it with their user identification. This could mean recording the HMI or terminal screen that process engineers are using to manipulate the system, and/or taking a voice recording of an operator’s steps in manipulating less-computerized aspects of the system. This logging could be triggered by the operator typing a quick command or pushing a button to begin recording the terminal, or carrying a portable microphone while making physical changes. It could also be automated, so that when an incident occurs the terminal could automatically start recording the tasks, and embedded microphones in the facility could begin to record audio. This latter solution may be costly, however, and will generate a lot of noise on the microphones.

Another important aspect to record is the exact time that the incident is occurring, as well as the router’s timestamp, preferably with screenshots (to maintain integrity). Any commands used on the system should be logged, be it by the aforementioned screen recording, audio, or preferably text

System Component	Operator Documentation
System communications	Written documentation of what components produce what communications, along with a diagram of network traffic flow
System infrastructure	Written documentation of the devices contained within the system topology and their responsibilities in the system
Critical configurations	Written lists of critical devices and structures that will endanger process completion if compromised (such as the control server, HMI displays, PLCs, etc.)
Process procedures	Written documentation of the entire process sequence, as well as a diagram depicting how the process is executed
Device logic	Written documentation of what logic has been coded in the device, including copies of active programs and applicable commands
Incident Response Tasks	Video recording of terminal sessions, audio recording of physical steps taken, along with signature of who executed actions
System Timestamps	Documented with interface display screenshot

Table 5-2. Operator documentation considerations.

document. This way, examiners know exactly what the operators have done that may affect the system data. The various documentation components that may be part of an investigation are catalogued in Table 5-2.

These are simple tasks, relatively in line with what process engineers and operators already do in the course of their work. Risk analysis and documenting circumstances are not wholly disparate concepts from current requirements for system operations. After all, calculating the risk of system failure, and maintaining good documentation leads to smoother process executions. Volatile system data recording, however, may be slightly out of their purview. It requires knowledge about the system, and of certain computer aspects such as memory storage. If this type of data could be gathered by software or firmware, however, then it is possible that the operator could be trained to understand the situation and initiate a capture process to begin pulling the data. This solution will be discussed more in subsection 5.3 [23].

During incident recovery, an important aspect that should be kept in mind by process engineers and system operators is that rebooting or running configuration commands should be a last resort. It affects the amount of data that can be collected. If flushing or a reboot is what is required for the system to function again, then the operators should document and pull as much information as they can before they take this action [23][4].

A final aspect of the training should include moderate legal briefing on the concept of a chain of evidence. If process engineers are to begin the forensics process, then they will likely be the first link in that chain [32]. This needs to be documented, and the idea of how important it is to the integrity of the data should be stressed in training courses.

If these preliminary forensics procedures were initiated or contributed to by the operators, it would solve the problems such as incomplete documentation, underrepresented command flow, immediate data collection, etc. The procedures discussed can be imparted through training, handouts, forms, and hands-on experience. The hand outs and forms can be used to outline and explain the key actions to be taken, and how to integrate these actions with the incident response plan. They can then be placed in the facility, to be referenced in emergency situations. The creation of these documents must be handled with care, so that the information is easily learned and can be reviewed quickly. Phrasing should be straightforward, and illustrations should be clear. Human factors research has many opinions on how handouts and instructions can be best written for fast, effective consumption [30].

Many professionals agree, however, that theory training only goes so far. Especially in a situation where operators will be expected to perform tasks outside of their prior knowledge base, personal experience will be the best teaching method. Both the INL ICS Advanced Cybersecurity Training and certain workshops at the University of Southern Australia have integrated practical experience labs with theoretical information to teach their clients. This enables these clients to understand the new information, and put practice in the context of their own actions [33].

This training has another advantage, in that it can be standardized among ICS systems. Some modification of training will certainly be needed, depending on whether the system is legacy or modern. However, as the technology advances, the taught procedures will likely become more applicable. Other current ICS forensics solutions in development are primarily software or hardware based. Due to the incredible variability in ICS, engineers cannot guarantee that forensics tools will be able to work on every system. The techniques taught in training courses, however, can be applied against many different architectures.

5.3 Multi-Skilling

The human factors field has conducted studies on the concept of multi-skilling, defined as:

> A way of working where the traditional divisions between work areas and separate disciplines are removed, and individuals are given responsibility for a range of different types of task [34].

This definition essentially describes the theory behind the solution presented above. Operations employees would be expected to participate in traditional forensics tasks. Within studies surrounding multi-skilling, scientists have attempted to understand possible drawbacks to this proposed methodology.

In their paper, Horbury and Wright examined certain incidents in which multi-skilling was a contributing factor [34]. Through their research they discovered that the multitasking nature being presented in the work environment was not necessarily the direct cause of the reported problems. Instead, it was the implementation that turned out to be problematic. In one case, management decided to reduce the amount of staff members due to the presence of their new multi-skilled employees. There was also a noted lack of coordination and error checking arising from an absence of established leadership and adequate training. The largest observed problem related to multi-skilling itself was the fact that errors arose that the multi-skilled individuals could not solve due to their lack of specialization [34]. In the case of forensics, if a problem were to arise with data collection software, or stress was increased with the added strain of maintaining evidence integrity, the trained operator or process engineer may not know how to make the correct decision.

The proposed solutions to these problems involve more focus on the training and maintenance of knowledge. It is important to ensure that the information dispersed in educational sessions be clear and to the point, and done in an adequate time frame to be understood [34]. Hands-on techniques should be observed and completed by the individuals [33]. Once the training has been completed, maintenance reviews should be completed to ensure that the knowledge has been retained. Supervisors should be trained in how to lead their team in a multi-skilled situation, so that leadership and an overall “big picture” can be observed [34].

5.4 Automation

The techniques discussed so far have not been definitive of one profession. Documentation and recording should be understandable by most, if not all, working individuals. However, when collecting specific data such as register values and packet information, more specialized skill sets are required to accomplish the process. Given the added stress introduced by giving more tasks to an employee’s workload, this specific information-gathering may be accomplished better by the use of automation [34].

In modern times, automation is accomplished through the collaboration of many facets of engineering and science. Fields that are continuously referenced in literature are systems engineering, computer science, and human factors. By working together, these industries can create better, more effective technologies to be utilized by process engineers and operators in the search for forensic evidence.

System engineers should be designing ICS facilities that are automated to react a certain way, should disaster strike. In most cases, this automated response is geared towards protecting the machinery, rather than protecting the process continuation. This is because the destruction of physical and virtual devices adds to the amount of time the process is out. If one protects the devices at the sacrifice of the process, then it still has the resources necessary to be resurrected. For example, if pressure is building up in a tank, the system should acknowledge the increase and shut the system down before the tank ruptures. This will prevent a damaging explosion, and will save the equipment to be used again once the reason for the pressure buildup is remedied.

This method of automated response can be leveraged to help out with forensics investigations. By placing new devices into the system network, and reworking communications structures to allow for cyber security needs, systems engineers can contribute to the resilience of their system. Base deployment designs need to be reconfigured to allow data collection to be completed quickly and effectively.

In particular, space needs to be made in the system architecture for increased storage capability. Data historians, when they are implemented, do their part in logging information by keeping track of system flow. However, the few that are usually implemented in ICS are not likely to have the capability to store the massive amounts of data that should be recorded in the event of an incident. One way to narrow this amount is by dedicating servers to particularly vital communications pathways. They would need to be connected to network capturing devices that could listen in on these major communication corridors. This will require the addition of listening devices in the network infrastructure. Hopefully by segregating the collected data and only storing recordings from those major data highways, the amount of new devices needed in the facility will be minimized. Data can also be collected from various devices on the network, and stored on the servers to analyze with network traffic. This will provide an easy database for forensics examiners to examine the moment they are on the site.

In the ICS realm, computer science mostly revolves around networks, software, and the types of procedures applied to both. In the case of automation, programming and software development become the key skill sets. To provide an automated version of data collection, computer scientists can work with cyber security researchers to augment or create programs that will cull data from network traffic and store it in a server. The program designers must also speak with systems engineers to pinpoint where exactly this data needs to be pulled from, and how it should be organized or labeled. Such programs are already enacted in many traditional IT systems, via traffic loggers. They need to be adapted for ICS use, so that they can gather ICS traffic in such a way that it can be easily investigated at a later date. Images of important machines in the system must also be made, so that any changes or machine incidents can be noted in the examination report. Further stipulations made by ICS forensics require that this storage be forensically sound and very large. This destination may vary between ICS implementations.

Traffic collection and analysis are common components of IT forensics. The network traffic of a system can show certain patterns that an investigator can analyze for possible incident causes [18]. Abnormal behavior, where it is coming from, and possibly even the source of the incident can be reflected and traced through network traffic. Network capture devices are hooked into the system infrastructure in areas where they can listen in on network packets as they move through the system. These packets are then copied, and stored on a server like those mentioned previously. By implementing more of these listening devices in key areas of an ICS, traffic can be recorded during an incident for future investigations. Developments that must take place in order to enable this implementation include adding ICS-specific labels to the categorization systems within the network capture software. Current traffic analysis software contains ways to flag packets by their protocol name (I.E. TCP, ARP, HTTP, etc.) Unlike the standardized IT protocols, however, there is a large amount of variability in the often proprietary and usually highly-specialized protocols implemented in ICS. Current software is not often given the resources to distinguish the differences between the network packet protocols, let alone to derive what their specific purpose is [5].

Data stored on individual devices can also be useful in determining what has occurred during an incident. In the case of a malicious cyber event, the device configuration and communication methods may have been changed or damaged. This could be caused by direct attacker intervention,

Forensic Need	Automation Response
Storage for massive amounts of collected data	Additional servers
Physical network traffic logging devices	Traffic capturing devices that are placed in infrastructure to listen in on communication pathways. They then store the information on servers
Network traffic logs	Develop logging software that gathers and labels network traffic packets in the ICS system
Individual device images	Critical or heavily effected device configuration can be copied for later analysis
High data integrity	Store traffic in an SIEM system. Other system documentation should be kept on secure servers, or printed on physical media depending on the item

Table 5-3. Summary of automation solutions

or malicious software. By making a copy of the device configuration and creating a recording of all the data, it can be examined later for manipulation or damage [18].

With the combined effort of systems engineers and computer scientists, progress is being made towards set goals in security. One of the most obvious is the ability to log suspicious data in a forensically secure manner. This process would essentially examine all traffic in the system, and put any suspicious packets in the Security Information Event Management (SIEM) system. The main drawback of this is that it requires an extremely large amount of memory to process these packets at any reasonable rate [35]. A possible solution to this problem is to turn on an intensive version of this program when an incident is occurring, and/or reducing the sampling rate. The first will still flood the system, but in a slightly more controlled manner. The second will not have as much detail as the first, and may miss some critical aspects. However, even a small amount of data is worth more than none.

There are many papers revolving around proposals and research done into standardized ICS-specific cyber security software that would include certain forensics measures. Two particular topics are gaining steam in the community. They are:

- Real-time adaptive security software and
- Honeypots

These two topics are not yet commonly implemented in ICS facilities. There are many reasons why they may benefit forensics.

Real-time adaptive security software can react to potential cyber security incidents whilst recording forensics data for future assessment. The ideal situation is that security processes would track traffic and logs, store them in a Security Information Event Management (SIEM) system, which would then feed into an adaptive firewall and/or IDS/IPS [35]. This may sound easy in theory, but professionals in the cyber security field have yet to be able to effectively implement such a system. Progress is being made in the field, though, and will contribute greatly to forensics investigations.

Another area being examined is the deployment of “honeypots” within ICS. A honeypot can be defined as a security device “whose value lies in being probed, attacked, or compromised” [36]. They can be virtual or physical machines that will mimic other devices on the network, without carrying any essential burden in the system. Honeypots will also usually be isolated from other devices in some way, so that if they get infected they do not participate in spreading the problem. How this supports forensics is that, if the devices are attacked, well-labeled logs can be kept of what is happening to that machine, without the worry of incident response. Honeypots can be used and abused by malicious attackers without worry of loss, specifically so the tactics and malicious tools can be studied at a later date [35]. The implementation of these in ICS systems may mean that less storage is required in order to gain an understanding of what happened on the system. This will only work, however, if these machines are specifically targeted. To make the machines desirable, IT professionals would be best served talking to systems engineers, who would be able to point out vital machines in the system. By understanding prime targets, the computer scientists can replicate them as honey pots, so that whatever malicious activity is targeting valuable system aspects may infect them.

5.5 Human Factors and Automation Design

The creation of new network schematics, hardware, and software for aiding forensics investigations of ICS would help immensely in the field. Yet, it must be repeated that computer operation reflects human knowledge. If the new technologies are not easy and understandable, then they may only hurt the incident response process by confusing operators in an emergency situation. Thus, is it important to involve human factors professionals in the design of these new tools.

In the human factors field, specific terminology can get extremely complicated and detailed. Understanding the human brain and how it interprets outwardly-imposed signals is an incredibly complicated task that requires years of study to appreciate. Thus, to truly be most effective, professionals should be employed to determine the best method of new technology deployment.

The essential aspects of how an operator will react when confronted by an emergency situation with new tools depend on a number of factors. Some generalized topics that should be addressed are signal processing, stress reactions, and alert presentation. Signal processing is how a human identifies a change in the system. By adding forensics tasks to the technology an operator handles, the signal of an event must be recognizable, and the solution provided by new forensics technology should be readily apparent. Attention in information processing is described as "increased awareness directed at a particular event or action to select it for increased processing" [37]. Essentially, in the case of an incident, the operator must be able to dedicate more awareness towards the situation, and should be able to determine the best course of action.

Stress can greatly affect the way an individual will react in an emergency situation. In general, the way stress seems to effect most is by emotionally influencing one's perceptions. The motivation of every action becomes related to "one's perceived state of progress towards or away from one's goals" [37]. In Figure 5-1, an illustration is provided that shows the input considered in making an analysis of the situation under stress. As can be seen, the person, environment, computer response and task all contribute to the emergent unit of analysis. Thus, forensics data must not only be raised

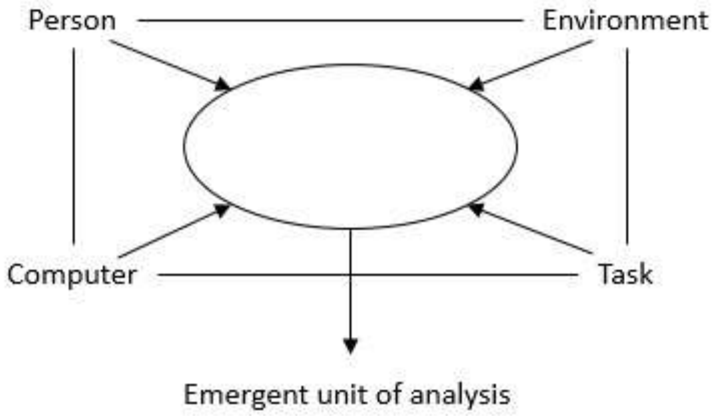

Figure 5-1. Diagram of emergent units in a given situation derived

as an important goal worth striving for, but also an important step in maintaining the resilience of the system [37].

One proposed way of easing operator stress is to specifically design collection software that is triggered automatically. A programming “script” could be written that would begin documenting and data collection software when an incident occurs. A trigger to launch such a script might be when a specific alarm is activated. This would be a simple solution that would not add any undue stress on the operator. However, it does not account for the amount of variability in systems, situations, and storage capacity.

Because most ICS are organized differently, a unique program would need to be written in order to trigger data collection throughout the network. It would be hard to adapt general software to focus on recording specific consoles, or gathering data from specific streams. As an example, there may be only one operator on duty when a minor cyber incident occurs in the system. If the forensics preliminary steps were completely automated, then wide scale system data collection would begin, and there would be a large amount of resulting data. This data would likely be rife with data mingling, and it might be hard to pick out important information from the general data.

By allowing the operator to initiate where the forensics process begins, they can prioritize where the collection begins and what is recorded first. This is important, because storage space is limited. If operators can direct where the software records from, particularly concerning their individual actions and volatile systems that may need to be flushed, then more information can be saved. Thus, it may be best to allow the operators to target particular devices and areas with certain commands that trigger automated data collection.

For instance, assume a SCADA system operator is sitting at an engineering workstation, when an alarm triggers on the system, and the computer begins to behave abnormally. Perhaps the alarm alludes to an unauthorized remote connection, or the fact that the workstation seems to not be communicating with other system components. The operator could trigger recording technology to document their preliminary steps in fixing the problem, collect traffic data coming from that workstation, and take an image of the device. The problem may be only linked to this device, or it could be more widespread. Flooding system resources by triggering a wide scale data collection would not be the best first step.

5.6 Summary

This chapter has introduced a large number of concepts that must be integrated together in order to support the proposed solution. Training and automation are both needed in order to accomplish the goal of this cross-disciplinary approach. Implementation of this methodology will provide future ICS forensics investigations with important information about incidents. It will also motivate multiple professions to work together to understand what is necessary for data collection and integrity.

To grasp what is needed to empower operators in early forensics tasks, a great deal of description is required. For quick reference, however, the new concepts proposed to support this methodology are summarized in Table 5-4. In Table 5-5, the suggested tasks are listed alongside the professions that will be responsible for implementing them.

Training	
Conducting risk analysis	• Prioritizing crucial data in the system • Understanding time frame limitations
Contributing to documentation	• System communications documents and diagrams • System infrastructure documentation • Critical configuration lists • Process procedure documentation and diagrams • Device logic documentation • Incident response task recordings • System timestamp screenshots
Legal advising	• Chain of evidence procedures
Hands-on training	• Updating documentation • Using recording tools in a simulated incident • Using data collection commands and tools in a simulated incident
Automation	
Hardware	• New devices implemented in systems for data storage and collection • High data integrity implemented through use of SIEM systems and hardened architecture
Software	• New software developed to collect and categorize data for ease of investigation • Ease-of-use assured using human factors to prioritize executing convenient data collection commands during an incident

Table 5-4. Summary of new methods to be integrated

Professionals	New Tasks
Operators	• Contribute to documentation • Record incident response actions (On screen and recorder) • Execute data collection commands
Engineers	• Integrate storage devices into system network • Integrate listening devices into system network
Computer Scientists	• Design software additions for data collection
Human Factors	• Assist in developing training documents • Assist in software design and development • Conduct user studies on resulting trained employees
Computer Forensics Investigations	• Communicate with system engineers and operators • Gather evidence from data repositories

Table 5-5. Summary of ICS professionals and their new tasks

Chapter 6. Analysis

The methodology proposed in Chapter 5 recommends new training and technology to enable operators to multi-skill and contribute to the forensics investigations of ICS. This is a challenging proposal for many reasons. There are many benefits that could arise from the intense cross-disciplinary focus both in efficiency and work environment. However, not all of the problems associated with this solution have been resolved in the technological or psychological fields. Below certain aspects of the proposed solution are analyzed for their validity and consequences.

6.1 Benefits

This proposal centers on the idea that dispersal of work across disciplines will aid in the retention of forensics data. Its main goal is to solve the immediacy imposed upon forensics data collection in the volatile ICS environment. By creating training courses and system resources for process engineers and operators, this solution hopes to enable immediate forensics work in the system, rather than beginning the process after the incident is over.

By immediately collecting information about what actions the operator has taken in the system, forensics professionals immediately gain insight into the status of the recorded data they have to analyze [24]. It allows them to examine the context of the information so that possible discrepancies can be ruled out. Making sure that documentation is up to date from the operator's point of view is also extremely valuable because it gives investigators insight into the workings of the system and who has access to the data [24].

It is also important that the investigator understand what steps an operator took in remediating the situation, who the operator was, and how those actions effected the system. By recording every act taken during incident response, the investigators can make sense of the communication flow and device configurations. They may also be able to better pinpoint the source of the incident based on the amount of interaction operators have with certain aspects of the system.

Being able to gather system data as the incident occurs is also of great value to investigators, since it allows them to see the sequence of events. By recording network traffic and pulling data from servers, data applications, and field devices, the examiner will get a large degree of information about the event. This is the most desirable outcome: that the investigator is presented with a large amount of data related to the incident [5].

By giving operators more initiating power in an investigation, good communication will be stimulated between forensic staff and process engineers. Operators will be able to more easily explain what has happened with the system, and the steps they took. Through training, they will also have a better understanding of what type of information an investigator might be interested in. This continues the cross-disciplinary teamwork that is crucial to ICS functionality [24]. Rather than replacing the forensics employees with multi-skilled operators, this solution is proposing a method that will enable these two fields to communicate with a similar vocabulary and background.

Another advantage of this methodology is that it will spur development in more intuitive software and hardware for operator use. With new skills comes new development and progress. Many of the operator-interaction systems are already the focus of human factors professionals. Adding new forensic functionality will continue this research. Intensive user studies will need to be conducted in order to develop the best methods for operator and process engineer use. However, if human factors scientists are employed properly, the final product should be very intuitive and useful even under the pressure of an emergency situation. These benefits are summarized in Table 6-1.

Method Idea	Beneficial Impact
Cross-disciplinary forensics training for system operators	Immediate data collection in a volatile environment
Continuous data collection during incident	Large amount of recorded traffic and memory data that show the effected system
Sharing power with the operations employees	Stimulates good interactions with forensic staff and process operators
Development of intuitive forensics tools for operators	Invigorates research in operator-interaction based systems in ICS

Table 6-1. Summary of benefits

6.2 Drawbacks

As with any new prospect, there are some problems that must be considered and overcome in order to accomplish the intended goal. It is easy to talk about ideals and potential future advancements. Talking about design and implementation, though, requires a realistic outlook on the complications posed by the process.

Arguably, the most evident drawback would be the added stress on the operator. There have been modern studies done on the amount of data overload a process engineer may face during their career [31]. Adding new forensics procedures may cause the individual to make more errors by exceeding the ability of the employee to learn and apply information in tense situations. It is also commonplace to experience errors in the application of multi-skilling due to a work overload upon the employee. If they already have a full docket of tasks, then adding another may only compound the problem of stress under pressure. There is also the problem of these operators being insufficiently exposed to the new tasks depending on the amount of training they receive. Forensics can be a particularly detailed area of application. If employees run into a problem that requires greater knowledge of computer forensics then they have been trained in, the stress of the situation will only increase [34].

These problems are dire, but they have theoretical solutions. The first of all is to carefully choose which individuals should be trained in these added tasks. Those who are already responsible for a great deal of work in the system should be avoided as candidates. Furthermore, those who have shown a propensity to react poorly under stress should not be taken into consideration. There is also the question of supervision. A good supervisor who has also been trained in the proposed forensics techniques and understands where they fit into the larger action of incident response should be available to help employees prioritize actions. Stress reactions can also be guided by the skills and confidence that training sessions will instill in each individual. By giving them control over certain forensics procedures, employees have a way to react to what is occurring in the system. If they are well trained, then the proposed procedures should not add greatly to the amount of stress experienced [34].

Another problematic item is that of funding. Especially in modern economies, it is hard to rationalize added expenditure. The creation of these training classes will require a lot of professional input into creating and picking teaching materials, and developing hands-on laboratory exercises for the students [33]. They will also take operators away for many hours of training, and may introduce annual courses as threats evolve and change. These training sessions will need to be general enough that non-computer scientists will be able to understand the content, but also specific enough to provide useful skills. This problem is inflated by the fact that in the United States, operators can come from a variety of skill levels and education. In certain industries, a high school diploma and training courses may be all that's required of a process engineer. In others, it may require a master's degree from a university and years of apprenticeship.

The development and adoption of the new technology is also a massive additional expense. Engineers, computer scientists and development tools will be needed to be used to create the new system layout and additional data collection features. To do it correctly, one should also hire human factors psychologists to make the system intuitive and efficient. The resulting infrastructure will be expensive.

Problems of expense versus cyber-risk are not isolated to forensics. It is a common argument between business representatives and cyber security professionals. Because of the frequency of this debate, certain components of building a business case have been singled out for the prospective technician to focus on: "prioritized threats, prioritized business consequences, prioritized business benefits, and estimated annual business impact" [2].

Prioritized threats examine what things the organization can believe could impact the ICS. With critical infrastructures, terrorism is a prevalent concern. Other factors that may be of interest are viruses, worms, malware, and insider problems. Prioritized business consequences are created so that the ICS management group will be better able to understand the impact if a cyber-incident were to occur. By explaining the system failure in terms of lost production, revenue, and compliance agreements, management may be more willing to spend money upfront on providing their facility with more technology. Prioritized business benefits are much the same, in that they explain to the ICS businessmen what advantages spending money will give them. In this case, better forensics implementations will lead to a better understanding of what has happened in the system, which can then be applied to create a more resilient implementation. Estimated annual business impact is generally represented in financial terms of loss to company profits. For instance, if a virus were to infect an ICS and result in loss of production, no stakeholder in that company would want it to happen again. By utilizing quick forensics, the virus could be analyzed and security measures enacted to protect the system. Using these arguments and a substantial amount of data can overcome the problem of restricted finances. Forensics is an important task, and deserves funding to ensure system reliability [2].

Implementing new hardware configurations and developing new software functionality is not easy. Especially in ICS systems that have no true “standard” architecture or communication flow. In many cases, the features may need to be specifically tailored in some way for the environment. Communication between engineers, computer scientists, and human factors personnel is also in early stages of development. The professional vocabularies of these individuals are different, and miscommunications can occur.

The speed of development can also be very slow, especially as more disparate parties become involved in design and production. There are many ways that features can develop, but most often software follows a spiral-type pattern where multiple prototypes are created, getting closer and closer to what is needed as time advances. In between each prototype, research and development takes place, along with risk analysis and adding features. This type of production cycle is generally referred to as Boehm’s spiral model, and tends to be one of the simplest ways of representing the evolution of software. However, the earlier prototypes are often flawed, and can cause problems [38]. In most systems, the bugs in this programming could be accepted as part of technological progress. ICS, though, hold production and availability as tantamount, and the same risks cannot be abided. If a bug in new software causes a problem in the system, then the process is at risk. Thus, more development and refinement of a product must take place before it is implemented in an ICS, as compared to most other systems. This adds to the amount of time needed before the software can be implemented in the system.

In spite of this, there is still hope for the new advancements in applied forensics. If nothing else, the preparatory work that the operators would be doing (such as gathering documentation and recording commands) would help an examination. The new software proposed may be able to build off of other software like it that is currently implemented in modern IT networks. Certain programs will monitor and filter traffic, and can navigate through a system to pull specific data from specific places. By adapting these techniques for ICS purposes, it is possible that the production time may be lessened to a certain extent.

The entire premise of this solution is that operators and/or process engineers will be present when an incident occurs, or will be among the first responders. As time passes, many facility owners are beginning to turn to remote control of their facilities to save on employee time and company funds [25][30]. This means that operators may not even be able to get to the facility in time to complete some of the information gathering before it is lost. There may even be a chance that forensics investigators may arrive before they do, depending on the environment and situation.

Yet even in this case the operator can keep track of and provide a forensics examination with more data by participating. Keeping up-to-date documentation of the system and recording whatever remote actions they may be taking in the system will help investigators to know what has occurred.

Drawback	Possible Remediation
Added operator stress	Careful consideration when choosing multi-skilling candidates. Individuals to avoid would be those who are very busy, and those who do not act well under pressure
Insufficient operator exposure	Well trained supervisors and hands-on training
Funding	Building a business case, "prioritized threats, prioritized business consequences, prioritized business benefits, and estimated annual business impact" [2]
Implementing new hardware and software features	Cross-disciplinary team work and flexible software structures
Amount of time needed to develop useful features	Time and research
Tendency towards remote facilities	Remote activation of software

Table 6-2. Summary of drawbacks

If they are able to trigger any data collection software remotely as well, then the argument for their training is also still valid. The problems presented in this subsection are summarized in Table 6-2.

6.3 Summary

There are many considerations that must be taken into account before enacting any new methodology. The advantages presented by the changes proposed in this document include immediate relevant data collection, employee communication, and technological development. These are benefits worth striving for, as they support system stability.

The drawbacks of these suggestions include operator stress, financial expense, development and implementation of the new features, and the difficulty of certain trends in ICS such as remote facilities. Yet there are possible solutions for these problems. It will require a great deal of work, but these efforts must be made in order to integrate forensics into the ICS field.

Chapter 7. Conclusion

Implementing forensics in an ICS system is currently fraught with difficulties. The technological and cultural problems that must be overcome are extensive. Chapters 2 through 4 explained the situation that ICS forensics finds itself in. SCADA-like systems are currently not ready to have intensive forensics techniques applied to them. The hardware and software hasn't been developed to work nicely with forensics applications, nor have said applications been designed to work well with an ICS environment. The two disciplines developed separately, and do not usually complement each other well.

There are also culture problems that accompany this dissonance. The professionals that must work together for an ICS to function do not often share a vocabulary. Miscommunications can abound, and there can be a lot of frustration in attempting to communicate with different parties [24]. Because of this, more effort must be placed in fostering communications and teamwork.

Expanding the role of operators and process engineers in the system can help advance forensics techniques, and aid cross-disciplinary communication. This solution provides better documentation of the system, and immediate data collection in the face of a volatile event. It further links all aspects of the system together, by placing the professions that arguably work with the system the most in direct communication with those who investigate what has gone wrong. The exchange of information could lead to great developments if certain problems can be overcome. This is where research, development, and testing must come in to play.

7.1 Future Work

There is a significant amount of work that needs to be done in the process of implementing the solution proposed in this thesis. The course of development, testing, and eventual application will require time, resources, and volunteers for testing. Research can be divided into a variety of smaller experiments, with the intent to put everything together into a final procedural application.

Training materials must be arranged for the courses to be taught. At first, while data gathering software is being created and new SCADA architectures are being reviewed, these sessions may only contain information on the pre-investigation steps. This will include maintaining proper system documentation (which should hopefully be a review of company policy), how to properly record terminal screens and commands, as well as an introduction to forensic law proceedings concerning integrity of evidence. Handouts, texts, and hands-on laboratory experience should be required for these courses.

Once the materials and a teacher have been prepared, a session should be run on a test group of process engineers and/or operators. Psychologists should be involved in this testing process, to survey the students during and after the class. If any notable problems arise during the course of the seminars, they can be observed and accounted for in later versions. Once the training has been carried out, these operators would ideally attempt to apply their knowledge in a test SCADA facility.

A simulation should be carried out to test what they have learned from their seminar experience. Once again, if problems arise, they should be noted and examined for future development of the course. During this time, the actual data the subjects are collecting should be reviewed by a forensics investigator. The ideal outcome of this would be an evaluation of how well the process works in a test environment, as decided by those observing the training and simulation, as well as those who would actually use the resulting documentation. Naturally, similar tests would need to be done with the software before it is implemented in a real-world system. Eventually, once most of the problems had been studied and resolved, researchers should test the resulting course and technological solutions on a real-world ICS.

Human factors research needs to be done in the computer forensics field to determine ways to make the process more intuitive for casual use. There is very little research in the field. Through study of current forensics techniques, human factors psychologists may be able to discern a way to design basic techniques of data collection so that they can be easily implemented by non-forensics specialists. Even simple pamphlets on what is required to maintain data integrity, as well as some basic procedures for gathering data would be useful to the field.

More research and development must also be done in the hardware, firmware, and software that exist within ICS. Some of this is already being accomplished due to the fear for cyber security that is rippling through the community. More needs to be done, though, in reference to forensics. General security concerns of logging and IDS/IPS development are important, of course, but so is the ability to analyze what happened in a system. It is through forensics that professionals will be able to understand and account for threats to system stability. Therefore, more hardware should be put in the system to properly record evidence. Firmware must be created that can withstand forensics prodding, and contribute to information about malicious or accidental activity. The need for tailored ICS software may be the greatest need yet, not only in forensics, but in cyber security. Too many protocols and communications are lost due to their proprietary nature. New programs must be created that account for ICS' peculiarities in order to protect its stability.

The United States is not alone in its fear for its critical infrastructure. Most of the modern world is caught up in a race to secure their foundational factory components. The press for cyber security in all fields of technology grows, and forensics cannot be left behind in its rapid advancement. A system will never be secure unless one can examine everything that has happened to it in the course of an incident. Standing back and waiting to investigate after an incident has occurred is not truly an option in examining ICS. There is too great a chance that information will be lost, be it to time or miscommunication between professionals. By placing more responsibility in the hands of the process engineers and operators of critical infrastructures, the field can progress from being secondary and reactionary. Instead, forensics in ICS can be of a higher priority, and lead to a stronger, more resilient United States infrastructure.

References

[1] J. Motef and P. Parfomak, "Critical Infrastructure and Key Assets: Definition and Identification," Congressional Research Service, 2004

[2] K. Stouffer et al., *Guide for Industrial Control Systems (ICS) Security,* 1st ed., National Institute of Standards and Technology, 2011.

[3] C. Nachenberg, "A Forensic Dissection of Stuxnet," Symantec Corporation, 2011.

[4] I. Ahmed et al., "SCADA Systems: Challenges for Forensic Investigators," *Computer,* vol.45, no.12, Dec. 2012, pp.44,51.

[5] M. Fabro and E. Cornelius, “Recommended practice: Creating computer forensics plans for control systems,” Idaho National Laboratory (INL), Aug. 2008.

[6] (2014, Apr. 10) *Critical infrastructure sectors*, Department of Homeland Security, http://www.dhs.gov/critical-infrastructure-sectors

[7] *United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, P.L. 107-56 (2001)

[8] *Presidential policy directive -- critical infrastructure security and resilience* (PPD-21), The White House, Office of the Press Secretary, 2013.

[9] S. Bennett, "A brief history of automatic control," *Control Systems, IEEE* , vol.16, no.3, pp.17,25, Jun 1996 doi: 10.1109/37.506394

[10] D. Bailey and E. Wright, "Background to SCADA," *Practical SCADA for Industry,* 1st ed. Burlington, MA: Elsevier, 2003, ch. 1, pp. 1-9.

[11] *Supervisory Control and Data Acquisition (SCADA) Systems,* 1st ed., National Communications System, Office of the Manager, 2004.

[12] B. Galloway and G.P. Hancke, "Introduction to Industrial Control Networks," *Communications Surveys & Tutorials, IEEE,* vol.15, no.2, pp.860,880, Second Quarter 2013.

[13] J. Slay and E. Sitnikova, “The Development of a Generic Framework for the Forensic Analysis of SCADA and Process Control Systems,” *Forensics in*

Telecommunications, Information, and Multimedia, M. Sorrell, ed., Springer, 2009, pp. 77-82.

[14] S. Brown, ”Applying Internet Technology to Utility SCADA Systems,” Utility Automation, Vol. 5(5), September 2000, pp. 25-26.

[15] D. Wallace, "How to Put SCADA on the Internet," *Control Engineering*, Sept. 2003, pp. 16-21.

[16] J. Montague, "Free at Last: How to Use Wireless on the Plant Floor," *Control Engineering*, July 2003, pp. 22-29

[17] B. Bencsáth et al., "Duqu: Analysis, Detection, and Lessons Learned," *EuroSec '12*, Bern, Switzerland, April 2012.

[18] B. Nelson et al., *Guide to Computer Forensics and Investigations,* 4th ed. Boston, MA: Course Technology, 2010.

[19] "Recommended Practice: Developing an Industrial Control System Cybersecurity Incident Response Plan," Department of Homeland Security, Oct 2009.

[20] D. Reilly et al., "Cloud computing: Forensic challenges for law enforcement," *Internet Technology and Secured Transactions (ICITST), 2010 International Conference for*, Nov. 2010, pp.1,7, 8-11

[21] W.V. Maconachy et al., "A Model for Information Assurance: An Integrated Approach," *Information Assurance and Security, Proceedings of the 2001 IEEE Workshop on*, June 2001, pp. 306-310

[22] M. E. Luallen, "SANS SCADA and Process Control Security Survey," *SANS Analyst Program,* SANS Institute, 2013, pp. 1-18.

[23] J. Slay and E. Sitnikova, "Developing SCADA Systems Security Course within a Systems Engineering Program," *Information SYstems Security Education, Proceedings of the 12th Colloquium for*, 2008, pp. 101-108.

[24] R. Radvanovsky and J. Brodsky, *Handbook of SCADA/Control Systems Security*, Boca Raton, FL: CRC Press, 2013.

[25] A. Miller, "Trends in process control systems security," *Security & Privacy, IEEE* , Sept.-Oct. 2005, pp.57,60, doi: 10.1109/MSP.2005.136

[26] A. Gambier, “Real-time control systems: A tutorial,” in Proc. 5th Asian Control Conf., Melbourne, Australia, Jul. 20–23, 2004, vol. 2, pp. 1024–1031.

[27] G. DiFrank, "The Power of Automation," *IEEE Industry Applications Magazine*, Vol 14, No. 2, March-April 2008, pp. 49-57.

[28] T. Hughes, *Measurement and Control Basics*, 3rd Ed., ISA Press, 2002.

[29] J. Karl-Heinz and M. Tiegelkamp, “The Programming Languages of IEC 61131-3,” *IEC 61131-3: Programming Industrial Automation Systems: Concepts and Programming Languages, Requirements for Programming Systems, Decision-Making Aids*, 2nd ed. New York, Springer, 2010.

[30] C. D. Wickens et al., *An Introduction to Human Factors Engineering,* 2nd ed. Upper Saddle River, NJ: Prentice Hall, ch. 16,18 pp. 433-434, 474.

[31] D.I. Gertman, "Human factors and data fusion as part of control systems resilience," *Human System Interactions, 2009. HSI '09. 2nd Conference on,* May 2009, pp.642,647, 21-23.

[32] K. Kent et al., *Guide fo Integrating Forensic Techniques into Incident Response,* 1st ed., National Institute of Standards and Technology, 2006.

[33] E. Sitnikova et al., "The Power of Hands-On Exercises in SCADA Cyber Security Education," *Information Processing, IFIP International Federation for,* 2013, 83-94.

[34] C.R.J. Horbury and M.S. Wright, "Multi-skilling: research implications on control room operations," *Human Interfaces in Control Rooms, Cockpits and Command Centers, 2001. People in Control. The Second International Conference on (IEE Conf. Publ. No. 481),* 2001, pp.141,146.

[35] R. Hunt and J. Slay, "The Design of Real-Time Adaptive Forensically Sound Secure Critical Infrastructure," *Network and System Security (NSS), 2010 4th International Conference on,* Sept. 2010, pp.328,333, 1-3 doi: 10.1109/NSS.2010.38

[36] L. Spitzner, "The String: My Fascination with Honeypots," *Honeypots: Tracking Hackers,* Boston, MA: Pearson Education, 2003, ch. 1., pp. 23.

[37] J. A. Jacko, *The Human-Computer Interaction Handbook*, 3rd ed. Boca Raton, FL: CRC Press, 2012.

[38] B. Bruegge and A. H. Dutoit, "Software Life Cycle," Object Oriented Software Engineering, 3rd ed. Upper Saddle River, NJ: Prentice Hall, 2009, ch. 15, pp. 640.

Appendix A

Glossary of Terms

Term	Description
Alarm	A device or function that signals the existence of an abnormal condition by making an audible or visible discrete change, or both, so as to attract attention to that condition [2].
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system [2].
Authorization	The right or a permission that is granted to a system entity to access a system resource [2].
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [2].
Control Server	A server that hosts the supervisory control system, typically a commercially available application for DCS or SCADA system [2].
Controlled Variable	The variable that the control system attempts to keep at the set point value. The set point may be constant or variable [2].
Data Historian	A centralized database supporting data analysis using statistical process control techniques [2].
Dead (Offline) Analysis	Allows the investigator to try different techniques of analysis on a system image, without compromising data integrity
Denial-of-Service	The prevention of authorized access to a system resource or the delaying of system operations and functions [2].
Distributed Control System	In a control system, refers to control achieved by intelligence that is distributed about the process to be controlled, rather than by a centrally located single unit [2].
Disturbance	An undesired change in a variable being applied to a system that tends to adversely affect the value of a controlled variable [2].
Enterprise	An organization that coordinates the operation of one or more processing sites [2].
Field Site	A subsystem that is identified by physical, geographical, or logical segmentation within the ICS. A field site may contain RTUs, PLCs, actuators, sensors, HMIs, and associated communications [2].
Forensics	The process of applying scientific methods to collect and analyze data and information that can be used as evidence [18].
Hacktavism	Cyber incidents motivated by an activist base
Honeypot	A virtual or physical machine that mimics others devices on the network to act as a lure for intruders
Human Machine Interface	The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software [2].
Image	A copy of some device

Term	Description
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidents may be intentional or unintentional [2].
Industrial Control System	An automated group of machine equipment, generally run by a central or shared control paradigm
Information Technology	Common computer networks
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity [2].
Input/Output	A general term for the equipment that is used to communicate with a computer as well as the data involved in the communications [2].
Intelligent Electronic Device	Any device incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g., electronic multifunction meters, digital relays, controllers) [2].
Intrusion Detection System	A security service that monitors and analyzes network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner [2].
Local Area Network	A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network [2].
Malware	Malicious software
Manipulated Variable	In a process that is intended to regulate some condition, a quantity or a condition that the control alters to initiate a change in the value of the regulated condition [2].
Master Terminal Unit	The device that acts as the master in a SCADA system [2].
Network Capture	Recording traffic packets from the network.
Operator	An ICS Employee who interacts with the system to maintain process completion.
Process Control System	Akin to an industrial control system, but generally smaller.
Process Engineer	Akin to an operator, but with more specific knowledge about the process and how it is best completed. Helps to design/implement process control schemes in some designs.
Programmable Logic Controller	A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing [2].

Term	Description
Protocols	A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems [2].
Remote Terminal Unit	A computer with radio interfacing used in remote situations where communications via wire is unavailable. Usually used to communicate with remote field equipment. PLCs with radio communication capabilities are also used in place of RTUs [2].
Resilience	The ability of a system to recover from an incident.
Security Information Event Management (SIEM)	A format for storing information securely
Set Point	An input variable that sets the desired value of the controlled variable. This variable may be manually set, automatically set, or programmed [2].
Supervisory Control and Data Acquisition	A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated [2].
System Engineer	An engineer in charge of designing and developing an ICS.
Wireless Area Network	A group of computers and other devices dispersed over a relatively limited area and connected by a wireless communications link that enables any device to interact with any other on the network [2].