Recommended Practice:

Creating Cyber Forensics Plans for Control Systems

August 2008

Homeland Security

Control Systems Security Program

National Cyber Security Division

Recommended Practice:
Creating Cyber Forensics Plans for Control Systems

Mark Fabro, Lofty Perch, Inc.
Eric Cornelius, Idaho National Laboratory

August 2008

DHS National Cyber Security Division
Control Systems Security Program

ABSTRACT

Cyber forensics has been in the popular mainstream for some time, and has matured into an information-technology capability that is very common among modern information security programs. The goal of cyber forensics is to support the elements of troubleshooting, monitoring, recovery, and the protection of sensitive data. Moreover, in the event of a crime being committed, cyber forensics is also the approach to collecting, analyzing, and archiving data as evidence in a court of law. Although scalable to many information technology domains, especially modern corporate architectures, cyber forensics can be challenging when being applied to non-traditional environments, which are not comprised of current information technologies or are designed with technologies that do not provide adequate data storage or audit capabilities. In addition, further complexity is introduced if the environments are designed using proprietary solutions and protocols, thus limiting the ease of which modern forensic methods can be utilized.

The legacy nature and somewhat diverse or disparate component aspects of control systems environments can often prohibit the smooth translation of modern forensics analysis into the control systems domain. Compounded by a wide variety of proprietary technologies and protocols, as well as critical system technologies with no capability to store significant amounts of event information, the task of creating a ubiquitous and unified strategy for technical cyber forensics on a control systems device or computing resource is far from trivial. To date, no direction regarding cyber forensics as it relates to control systems has been produced other than what might be privately available from commercial vendors. Current materials have been designed to support event recreation (event-based), and although important, these requirements do not always satisfy the needs associated with incident response or forensics that are driven by cyber incidents.

To address these issues and to accommodate for the diversity in both system and architecture types, a framework based in recommended practices to address forensics in the control systems domain is required. This framework must be fully flexible to allow for deployment into any control systems environment regardless of technologies used. Moreover, the framework and practices must provide for direction on the integration of modern network security technologies with traditionally closed systems, the result being a true defense-in-depth strategy for control systems architectures.

This document takes the traditional concepts of cyber forensics and forensics engineering and provides direction regarding augmentation for control systems operational environments. The goal is to provide guidance to the reader with specifics relating to the complexity of cyber forensics for control systems, guidance to allow organizations to create a self-sustaining cyber forensics program, and guidance to support the maintenance and evolution of such programs. As the current control systems cyber security community of interest is without any specific direction on how to proceed with forensics in control systems environments, this information product is intended to be a first step. Overall, this document provides the reader insight into some of the more important issues that should be addressed in augmenting a cyber forensics plan so it can be effectively applied to a control systems environment.

EXECUTIVE SUMMARY

Cyber forensics has been in the popular mainstream for some time, and has matured into an information-technology capability that is common among modern information security programs. Although scalable to many information technology domains, especially modern corporate architectures, developing a cyber forensics program can be a challenging task when being applied to non-traditional environments, such as control systems. Modern IT networks, through data exchange mechanisms, data storage devices, and general computing components provide a good foundation for creating a landscape used to support effective cyber forensics. However, modern control systems environments are not easily configurable to accommodate forensics programs. Nonstandard protocols, legacy architectures that can be several decades old, and irregular or extinct proprietary technologies can all combine to make the creation and operation of a cyber forensics program anything but a smooth and easy process.

This document takes the traditional concepts of cyber forensics and provides direction regarding augmentation for control systems operational environments. The goal is to provide guidance to the reader with specifics relating to the complexity of cyber forensics for control systems, guidance to allow organizations to create a self-sustaining cyber forensics program for their control systems environments, and guidance to support the maintenance and evolution of such programs.

This document is organized into three major sections:

Section 1, Traditional Forensics and Challenges to Control Systems

Section 2, Creating a Cyber Forensics Program for Control Systems Environments

Section 3, Activating and Sustaining a Cyber Forensics Program.

The document addresses the issues encountered in developing and maintaining a cyber forensics plan for control systems environments. This recommended practice supports forensic practitioners in creating a control systems forensics plan, and assumes evidentiary data collection and preservation using forensic best practices. The goal of this recommended practice is not to re-invent proven methods, but to leverage them in the best possible way. As such, the material in this recommended practice provides users with the appropriate foundation to allow these best practices to be effective in a control systems domain.

ACKNOWLEDGEMENT

This document was developed for the U.S. Department of Homeland Security (DHS) to provide guidance for creating a cyber forensics program for a control systems environment. The author team consisted of subject matter expertise from Lofty Perch, Inc. (Mark Fabro) and Idaho National Laboratory (Eric Cornelius).

For additional information or comments, please send inquires to the DHS Control Systems Security Program at cssp@dhs.gov.

CONTENTS

FIGURES

TABLES

ACRONYMS

ANSI	American National Standards Institute
CD	compact disc
CPU	central processing unit
CS	control system
CS^2SAT	Control Systems Cyber Security Self Assessment Tool
CSIM	Control Systems Incident Manager
CSSP	Control Systems Security Program
CSSS	Control Systems Security Specialist
DCS	Distributed Control Systems
DHS	Department of Homeland Security
DVD	Digital Video Disc
DVD-ROM	DVD Read Only Memory
EWS	Engineering Work Station
FW	Firewall
GPS	global positioning system
HMI	human-machine interface
I/O	input/output
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IPS	Intrusion Prevention System
IR	incident response
ISA	Instrumentation, Systems, and Automation Society (f. Instrument Society of America)
IT	information technology
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OEM	original equipment manufacturer
OS	operating system
PCS	Process Control Systems
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
RW	rewritable
SCADA	Supervisory Control and Data Acquisition
SLA	Service/Security Level Agreement
SNMP	Simple Network Message Protocol
TCB	trusted computing base

Recommended Practice
Improving Cyber Forensics Plans for Control Systems

KEYWORDS

Control Systems, Forensics, Event Correlation, System Recovery, Incident Logging, Incident Auditing, Cyber Security, Control Systems Networks, Incident Response

INTRODUCTION

In the control systems domain, where the overarching security principles of confidentiality, integrity, and availability often default to only availability and integrity (usually in that order of importance), technologies associated with system resiliency often displace security-specific activities. Currently, contemporary cyber security systems often need extensive aftermarket calibration to be truly effective inside control systems domains. Additionally, the overhead associated with fine-tuning these complex devices (in the presence of unique and proprietary solutions) often contributes to their absence. Like security technologies, cyber security activities and capabilities also need to be fine-tuned to accommodate for the uniqueness and nuances associated with control systems.

As a core component to incident response capabilities, cyber forensics provides for the collection, examination, analysis, and reporting of incident data. In most cases, the proper collection and analysis of incident data supports investigations, uncovers illegal activities, and develops better-defined security countermeasures. Through the implementation of data exchange mechanisms, data storage devices, and sophisticated general computing components, modern networks provide a good foundation for creating a landscape used to support effective cyber forensics. Modern control systems environments, on the other hand, are not as easily configured to accommodate forensics programs. Nonstandard protocols and legacy architectures, which can be several decades old, combined with irregular or extinct proprietary technologies can make the creation and operation of a cyber forensics program anything but a smooth and easy process.

Building on the common elements of standardized forensics processes, such as those related to the collection, examination, analysis, and reporting of event data, this paper will provide the reader with a foundation to enhance and/or create a cyber forensics program for control systems environments. Due to the diversity and disparate nature of technologies, platforms, and owner/operator deployments, this document will provide the necessary elements to create a flexible framework, rather than those that support specific technologies.

This document is divided into three major sections:

- Section 1, Traditional Forensics and Challenges to Control Systems
- Section 2, Creating a Cyber Forensics Program for Control Systems Environments
- Section 3, Activating and Sustaining a Cyber Forensics Program.

Section 1 addresses traditional forensics components and emphasizes the critical elements in developing a cyber forensics capability for control systems environments. Additionally, Section 1 provides the reader with insight into the complexities and difficulties associated with building such a capability. These core components are then mapped to specific challenges in control systems to provide the reader with insight allowing for the development of a solution that can be customized to their specific environment.

Section 2 addresses general components of the cyber forensic program and the elements that need developing to ensure a viable and robust plan is usable by managers and users alike. In contrast to traditional cyber forensics plans, this section also includes requirements and suggestions related to control systems personnel, control systems operations, and business operations. This ensures the requirements associated with the forensics program are applicable to the particular control systems environment. This section introduces the reader to a cyber forensic framework that is tunable to any control systems environment while still maintaining the fundamentals of an effective cyber forensic program.

Section 3 addresses activation of the cyber forensics program for control systems, and provides insights that allow organizations to sustain their program and ensure its applicability to the architecture for which it was developed. In addition, this section highlights techniques for integrating the forensics capability into incident response, as well as ensuring the forensics plan is part of the decision process as it relates to making changes in the overall information architecture.

AUDIENCE AND SCOPE

This document is for managers and security professionals responsible for developing, deploying, and improving the cyber security posture of control systems domains. Although designed to be flexible enough for system operators and engineers to read and use, this document's intended use is by those that are deploying cyber security incident response and/or forensics programs within control systems environments. It is not designed to replace a sector-specific approach to creating a cyber forensics program, but rather provide guidance as it relates to control systems specific issues. It may be found most appropriate by either those that have experience in deploying cyber forensics programs in modern information technology (IT) domains and who are beginning to address the issues related to deploying cyber forensic strategies for control systems architectures, or by control systems network professionals requiring guidance on creating a cyber forensics capability for their systems. The scope of the material is not technically demanding and can help provide a foundation for creating or augmenting existing information resource protection and recovery initiatives.

Although it may be required that a forensic examination of an incident on a control systems device is intended to ascertain if criminal activity has occurred, the methodologies used for the correct collection of digital data (although fairly ubiquitous across most domains) require modifications to accommodate for control systems uniqueness. As such, the scope of this recommended practice will be limited to those concepts that can impede the smooth preparation and development of a cyber forensics program for control systems. Additionally, this document provides insight as to what the Owner/Operator community can do to prepare proactively for a forensics investigation in support of an incident response capability. Although this document discusses content regarding collection, handling, and analysis of control systems data, material as it relates to the detailed methodologies involved in collection, handling, and reporting of evidentiary data will be excluded from this document, and it is assumed that evidentiary data will be collected and preserved using forensic best practices. The goal of this recommended practice is not to re-invent proven methods, but to leverage them in the best possible way. As such, the material in this document will provide users with the appropriate foundation to allow for implementing its recommendations effectively in a control systems domain.

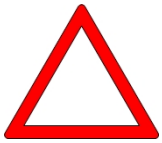
In the interest of brevity, and assuming the general readership will have experience with some IT security aspects, any standards for cyber security that are discussed are presented at a non-technical level (i.e., high level). This document does not try to provide justification as to why an organization would want to develop a forensics program, but rather it provides guidance to those that wish to augment a proven IT forensic process for their control systems domain. However, the authors recognize that within several critical infrastructure sectors, such as electricity (generation and transmission), cyber incident response and forensics plans are required.[a] Furthermore, the authors stress that the citation of any particular document is not to sway the reader's opinion in favor of the practices of any one sector, but to demonstrate the activities of that sector regarding cyber forensics.

The current landscape of terminologies associated with critical infrastructure and control systems operations can lead to unforeseen complexity. In this document, the term "control systems" will refer to technologies that are often defined as Supervisory Control and Data Acquisition (SCADA), Process Control Systems (PCS), Distributed Control Systems (DCS), or any combination thereof. The authors are not intending to discredit or avoid recognizing the often-clear differentiators in these environments. It is intended that the nomenclature used with the recommendations herein is broad enough to be applied in any of these domains.

a. For example NERC CIP cyber security guidelines required by the FERC Order 706 (see References)

To highlight some of the more important points in cyber forensics for control systems, these icons are occasionally used.

This symbol is used to identify ancillary informational points that may be of particular interest to readers developing a cyber forensics program for control systems.



This symbol is used to identify cautionary points that should be considered carefully when developing a cyber forensics program for control systems.

BACKGROUND

While the field of cyber forensics has been in the popular mainstream for some time, cyber forensics as applied to control systems is immature. With increasing computational capability and interoperability coming to previously isolated networks, the necessity for cyber forensics in control systems is becoming quite clear. In addition, the qualitative differences between corporate networks and control systems networks often highlight why security countermeasures are not easily deployable in control systems.

Control systems have considerable requirements related to (in order of priority) availability, data integrity, and confidentiality. As opposed to corporate domains, where the priorities reverse, cyber security activities in control systems networks require accommodating for systems that cannot readily be taken offline, may not be quickly modernized, and may not be able to facilitate adequate logging and audit functions. These elements are, of course, vital to a forensic program's success. Although all shortcomings that may be present in control systems (from a cyber security perspective) may be overcome by budget allocations and spending, many organizations find the cost of incorporating cyber security functionality into control systems technology quite high. Thus, being able to create effective security programs (such as forensics) for control systems involves reusing existing methodologies and practices, such as those designed for corporate domains. The requirement then becomes understanding what changes or augmentations to these proven capabilities are required to allow applicability to control systems networks.

The term "forensics" often relates to "the post-incident collection and analysis of data obtained from devices." Due to the unique and uncommon nature of control systems technologies, there is often inadequate information collected from these countermeasures following a cyber attack or incident. In some cases, where the owner/operators are cognizant of these shortcomings in commercial security products, tailored signatures and detection capabilities specific to control systems operations are created and appended to the security devices. However, because the nature of control systems operations can require deterministic and real-time data exchanges, it is often the case that these enhancements either prove useless or inhibit the actual productivity of the systems. Additionally, these enhancements are often deployed as a defensive activity only and are not extended to support any forensic function in the organization.

Figure 1 is a basic control systems security reference architecture[b] that illustrates the concept of the control systems forensics domain in relation to traditional IT domains. This reference architecture simply provides a basic framework for illustrative purposes, and is not representative of any architecture other than a notional one.

b. See Control Systems Cyber Security: Defense in Depth Strategies, http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf.

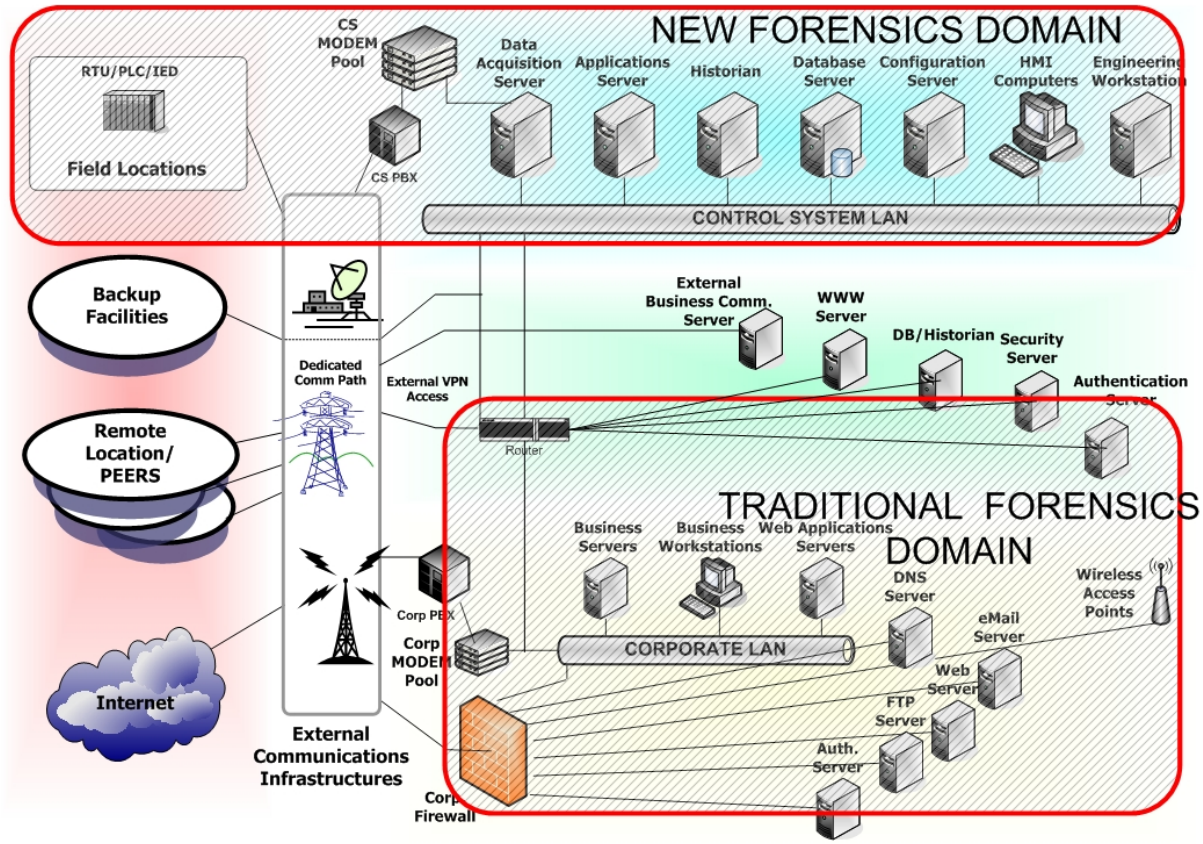


Figure 1. Control systems forensics domain and CSSP reference architecture.[c]

There are additional challenges with forensics analysis for control systems. The field devices that are used within control systems architectures, perhaps the terminus of a cyber incident resulting in physical consequences, often have no inherent capability for detailed logging. Furthermore, it has been found that on devices where extensive logging is supported the feature is often disabled, or the devices lack sufficient capacity to store enough data to allow analysts to meet forensics requirements.[d] Lastly, the diversity of the control systems technologies in use today also poses significant problems. Owner/operator staff often does not have the skill sets to collect, examine, or analyze command and control traffic. Instead, owners of the control systems (and devices) rely upon vendor/integrator staff for support. This in itself can precipitate delays in incident analysis and resolution, as understanding of detailed device operations and logging capabilities are often left until it is too late or completed "after-the-fact." Although systems can be configured to alarm operators in a timely fashion, the interpretation of the data and the correlation to an incident remain dependent upon the end user's technical skill level. Indeed, countermeasures can be instituted for any and all of these issues, but the cost associated with making such changes to the controls systems operational domain is generally too high in both time and testing, and requires significant amount of time and effort by the owner/operator.

c. The diagram is notional in nature and does not account for all possible architectures. As an example, it is not uncommon for modems to be connected directly into applications servers as well as PLCs, especially in legacy environments.

d. Readers should be aware that in some sectors, such as energy/electric, specific audit requirements demand that event data is stored at some point in the system. Although this data storage may not be fully viable to an incident, investigation, transaction, and event data are available in some form within the information domain.

Overall, the challenges impacting effective forensics in control systems can be summarized as:

- Many traditional device and control systems technologies do not provide for the collection of effective data that could be used for post-incident security analysis.[e] Those systems that do have such capability are often in operation mode without such capability active.
- Current cyber-forensic methodologies are not always fully extensible to traditional control systems architectures.
- For the architectures that do use modern cyber-centric security procedures and technologies (Firewalls [FW], Intrusion Detection Systems [IDS], Intrusion Prevention Systems, [IPS], etc.), the unification of forensic data collected by these systems cannot always be effectively correlated with device and control systems logging data.
- Post-incident analysis is often dependent on vendor involvement, and any proactive understanding of device logging is often not required by the end user or incorporated into a defense-in-depth strategy.

To address these issues at the appropriate level, guidance for developing a control systems forensic program is required. This guidance must be fully flexible to allow for deployment into any control systems environment regardless of technologies used. Moreover, the guidance must provide for direction on the integration of modern network security technologies with traditionally closed systems, the result being a true defense-in-depth strategy for control systems architectures. This strategy will be a combination of technical, managerial, and operational issues that provide for a structured approach that, when the aggregate is finished, gives a flexible but strong security posture.

This document introduces some of the more essential cyber security activities that are important for the development of a control systems cyber forensic program. Figure 2 illustrates the major components that will contribute to helping create an organizational cyber forensics plan for control systems domain.

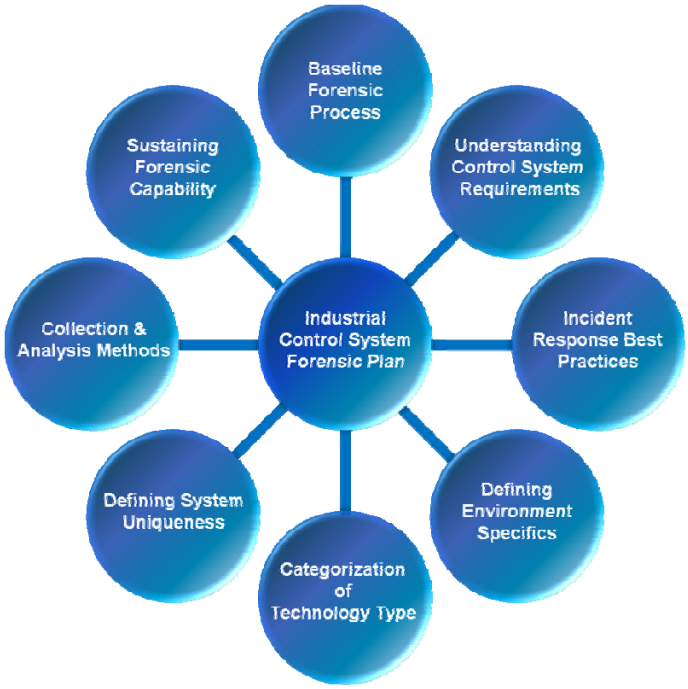


Figure 2. Forensic plan components.

e. Requirements from NERC demand that event data is stored in some fashion, usually for the purpose of event recreation. The data may not help in a forensics investigation, but readers should be aware that such requirements do exist.

1. TRADITIONAL FORENSICS AND CHALLENGES TO CONTROL SYSTEMS

To understand some of the issues associated with creating a cyber forensics program for control systems, it is pertinent to review the core components of standard cyber forensics programs and discuss them in terms of the irregularities associated with control systems. Generally, the definition of cyber forensics is:

> "…the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data." [f]

For this recommended practice document, the forensics process considered will be comprised of the three core areas of *collection*, *analysis*, *and reporting*. Although cyber forensics is a mature domain, an organization will need to tailor traditional forensics components to control systems environments to overcome specific challenges, as described below. However, prior to understanding how these core areas are implemented in a control systems environment, it is important to understand the differences between traditional IT domains and control systems architectures. Having a solid understanding of some of these major differences will help expedite the understanding of what components are necessary in a cyber forensics plan that will be unique to control systems architectures.

To accommodate for some of the technological uniqueness within control systems, especially those that may prevent effective collection of critical non-persistent or volatile data, in-depth reviews of existing data analysis capabilities (followed by the reinterpretation of that capability to fit into a forensics schema) are required. In many cases, this may simply require the inclusion of a secondary piece of appropriate technology into the networking environment to introduce capabilities to support collection. As with other aspects related to architecture modifications, this technology will have to meet approved deployment (and costing) guidelines, and should not introduce any operational risk to the control systems domain.

Methodologies regarding cyber forensics usually include the removal of impacted information resources from the environment. Although this is usually done following complete system backups and integrity verification of the acquired data, the nature of control systems does not always accommodate for such procedures. In many cases, the impacted technology is simply not replaceable due to cost or lack of available technology. Moreover, the impacted equipment may have such an integral role to business operations that it cannot be taken offline. For the forensics investigator, these aspects alone can severely impede effective analysis activities. While a control systems environment may not be able to come off-line, inherent troubleshooting capabilities for production systems maintenance should provide some useful data.

1.1 Challenges with Collection

As cyber forensics is closely tied to incident response, some response program elements can contribute to the complexity of using traditional forensic activities in the control systems domain. A simple example is artifact and data collection. Effective cyber forensics requires that a response team collect data in a manner that involves identifying, recording or copying, and labeling material from a variety of different data sources throughout the information architecture. A response team must also collect such data in a timely manner. In most modern control systems environments there will be

f. NIST SP 800-86, "Guide to Integrating Forensics Techniques into Incident Response," http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

technologies in place that can provide some of these minimum requirements. However, some of the core system support/control technologies (those that would be targets for an attacker) simply cannot and do not allow for effective data collection by a cyber forensics analyst. Because the capability for embedded data logging and security detection is vendor provided, the owner/operator cost associated with creating the capability is often quite high. Other collection methods, such as those associated with network and host-based detection and logging, will introduce a cost that could be high depending on the nature, size, and criticality of the control systems network.[g]

For the investigator of a cyber forensics incident to understand the nature and severity of the occurrence, he or she will need to have access to and obtain event specific information from as many sources as possible. Record types, such as those associated with audits, authentication, authorization, and general system activities become critical in executing a successful forensics investigation. The practice of merging all source data from across the enterprise is a common strategy to investigators, and fusion of these data sources is a process that has been documented at many times and in many different ways.

Effective forensics collection in any environment requires addressing several challenges such as volatile memory, poor administrative functions, absent or inadequate logging, and general cultural limitations. In control systems environments, there are additional challenges including:

- Automation. The key information resources in the control systems domain will be created and deployed to handle data in such a way that the implementation of a data retention scheme is neither cost effective nor a requirement.
- Volatility of Data. The data within the process and state information is deleted, removed, or overwritten at a rate that makes collection on some devices unviable or impossible.[h] Although after-market solutions can be architected, they are often too cost prohibitive to implement.
- Data Mingling. The total information sample that is resident in the investigated system is comprised of both data related to incident activity (possibly malicious) and data that is unrelated to the incident. Moreover, due to the limited memory storage of the system (see above) these data types are often indistinguishable. Although it is not a unique problem to control systems, this can be attributed to inadequate labeling and is in itself a function of the control systems (vendor supplied) technology.

Research has shown that the most valuable asset to an attacker may be those that influence the control or behavior of the system endpoints (including field devices).[i] Thus, it becomes important to consider the capabilities of control systems information resources in terms of data retention, and how that data can support an investigation. If the control technology is simple or older in nature (i.e., legacy or no longer supported), they often have no inherent capability for detailed logging. Without after-market modifications or costly system enhancements, these factors can make the collection of incident-specific information very difficult if not impossible.

---

g. Initiatives are in place to for federal, state, local asset owners, and regulators to obtain a common control systems security understanding using these procurement guidelines to help ensure that security is integrated into control systems. http://www.msisac.org/scada/documents/4march08scadaprocure.pdf.

h. Within some safety systems, high-speed data recorders have been used for many years. This type of recording activity will maintain the data that is often overwritten within system components and can be used for analysis and event recreation.

i. The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems, http://www.threatmind.net/papers/SCADA-Attack-Trees-IISW.pdf.

Data volatility and non-persistence can also contribute to the complexities associated with harvesting meaningful data from an information resource. As listed in order of decreasing volatility, the volatile components are[j]:

- Registers, cache
- Routing table, arp cache, process table, kernel statistics, memory
- Temporary file systems
- Disk
- Remote logging and monitoring data that is relevant to the system in question
- Physical configuration, network topology
- Archival media.

Looking at the levels of volatility, the non-persistent data associated with both registers and caches are at risk. Within the control systems environment, both registers and cache play a significant role as it pertains to both network and field devices alike, but the rate at which information is pushed to and taken from these devices does not always permit for useful incident-specific information to be collected. However, it is important to know that as the non-persistence of data that could be used by an investigator increases, (as does the reduction of possible data mingling) the overall uniqueness of the data decreases (see Figure 3).[k]

Non-persistent data may become persistent in some form. Some data that can be considered volatile due to its lifetime on a device (i.e., overwritten quickly) may become persistent in some other data store in the system. Some regulatory requirements, such as those in the energy sector, mandate the recording of all transactions and instructions leading to some device activity for maintaining, but not at the device itself.

j. RFC 3227, http://www.faqs.org/rfcs/rfc3227.html Example order of decreasing volatility for a typical system.

k. Non-persistence and volatility are important in forensics, as they each impact how accessible incident data is and how the investigator can access it.

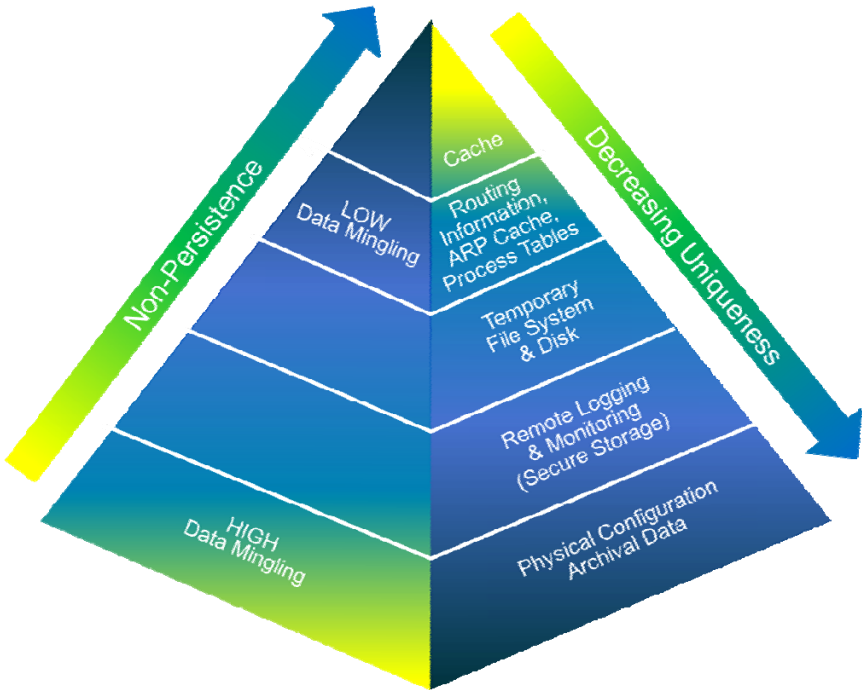


Figure 3. Non-persistence and uniqueness in data.

The diversity of the technologies used in modern control systems environments also pose significant challenges, as the ability to understand device or operational log data is often a vendor-only skill. This fact can force the efficiency of any post-incident response to be proportional to the level of vendor support, or until local investigators become appropriately learned in the technology. This in itself can precipitate delays in incident analysis and resolution, as detailed understanding by the end user regarding device operations and logging capabilities are often left until it is too late or are completed "after-the-fact." Establishing a vendor relationship and service level agreements that are capable of ensuring effective and timely forensics support is a task that is beyond the scope of this report. However, the reader is advised that such relationships with the vendor, and thus the creation of incident or forensics programs that are tailored to a specific installation, are critical to creating and maintaining an effective cyber security posture.

In some incident response plans, the standard organizational practice is to replace the impacted components from the architecture or take the resources offline. Such activities in many control systems environments are quite unrealistic, as taking equipment offline is either infeasible, too cost intensive, will have an unacceptable impact on critical infrastructure, or is simply prohibited from a business operations perspective. Because of the concerns relating to the possibility of equipment becoming unavailable may create adverse impacts on the production system, organizations have a challenge in choosing how to correct problems created by cyber incidents. Moreover, cost issues associated with control systems technology equipment can prevent the swapping in and out of impacted resources, and organizations often do not have backup devices available in quantity nor the time required to wait for the delivery of replacement technology.

To account for these and other nuances associated with control systems, the introduction of proactive monitoring and analysis capabilities are recommended. These can be considered countermeasure support functions, and can include (but are not limited to):

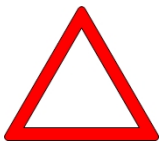
- Inclusion of real-time forensics tools for active analysis

- Embedded forensics analysis tools within the critical operational environment
- Security information management and collection systems.

1.2 Challenges in Data Analysis

One of the more obvious solutions to the forensics problem for control systems would appear to be the simple application of contemporary forensic analysis technologies to the control systems domain. However, cyber forensics tools will not function in all computing environments. Contemporary tools, such as those that examine running processes and services, automate evidence collection through precompiled scripts or programs, bit copy processes, or programs for generating checksums for complete and total image verification may not map perfectly to control systems technologies. Although some newer environments in the control systems domain will be able to benefit from these technologies, for the most part control systems and industrial automation environments will include system, platform, and software elements that are simply unable to benefit from these existing forensic tools in their native form. As a result, many forensics tools cannot be adapted to operate in many control systems computing environments. To meet this challenge, vendors of the cyber forensics tools would be required to modify their software to run in specific control systems environments, which they will not do without sufficient market demand.

The diversity of platforms upon which control systems technologies run requires due consideration. Although there is a proportion of Windows and UNIX-based environments,[l] the aftermarket modifications to these systems, combined with vendor specific or owner/operator modifications, extends the uniqueness of the systems into a type that cannot always benefit from forensic analysis tools. This relates to the issues of data collection as discussed above. Furthermore, the way in which control systems architectures create, share, and manage data is not always conducive to creating a simplified process for information extraction. Investigators working with control systems cyber incidents need to review correlations between operational information obtained from key data repositories (such as Historians) and volatile, non-persistent, and frequently overwritten state information that could be collected from field devices and other elements closer to I/O points.



Without fully understanding the extent to which forensics tools can influence control systems operations, due care must be practiced in trying to use standard forensic methods on control systems technologies. If it is not fully understood from evaluation in a test environment how the tools can impact the production system, then deployment in the production environment should be avoided.

A core component of any forensics capability is to ensure that the information that has been collected from the environment is correctly assimilated and reviewed. Being able to have only one or two data sources often limits the investigator's overall effectiveness at carrying out data analysis, so understanding how the incident may have impacted numerous resources within the domain becomes critical.

Currently, it is commonplace to find control systems architectures that are devoid of any logging or multi-source security information collection capability, as well as finding an architecture that has not utilized any add-on or aftermarket logging capability for the core control systems information resources. Within control systems architectures where firewalls and intrusion detection or other security technologies have been deployed, centralized data collection from the security resources is often not a

l. This is assumed for more modern environments. There is no question that there exists a significant number of proprietary systems that do not use Windows or UNIX operating systems as a base operating system.

part of the overarching cyber security strategy. This is not to say that administrators and architects are at fault, but rather to emphasize the fact that in order to create an effective cyber forensics capability for control systems there are some proactive strategies involving logging and data collection that need to be developed.[m]

Defense-in-depth strategies can greatly improve the cyber security posture (and forensic applicability) of a control systems environment while supporting the need for business operations.

The forensics investigator will need to draw on all types of records as well as the interaction of the record holder with other core devices in the network. However, current information technologies that have the capability to maintain these types of audit records may not necessarily be in a data exchange relationship with the devices in the control systems domain that experience a cyber incident. As such, this can limit the scope to which the forensics investigator can extend his or her investigation.

Many control systems environments are beginning to use various security-centric technologies to aid in both cyber risk reduction and conformance to industry mandates. Combining multiple log files, such as those retained by syslog, those for event recreation, and physical access logs (facility, plant) can support an investigation.

1.3 Challenges in Reporting

The complexity of many control systems environments, along with the uniqueness that is often associated with proprietary installations, drives the requirement for vendor interaction before, during, and following a cyber security incident. Historically, installations that have experienced a cyber incident will often opt to communicate directly with the vendor in an attempt to get support, insight, or some direct interaction that will allow for a deeper understanding concerning the incident. Moreover, because many of the control systems environments around the world are involved in critical infrastructure systems, the first priority during and following any incident is usually the resumption of services. In many cases, this can lead to the replacement of key devices or the overwriting of operational data, some of which could have been critical in analyzing the root cause of the incident.

Documentation is paramount to the success of forensics investigations in the control systems environment. Asset owners should take preemptive steps to identify and document any changes made to operating systems, hardware configurations, device drivers, or any other elements whose modified behavior may differ from its original equipment manufacturer's (OEM's) defaults. Furthermore, it is recommended that asset owners communicate with their vendors in order to identify and document similar changes made by the vendor. This information should be provided to the forensics investigator prior to any forensics activity. The investigator shall note the modifications and account for them accordingly. The investigator shall thoroughly document and explain his/her actions with respect to modified components and maintain compliance with proven forensics best practices.

m. See Control Systems Cyber Security: Defense in Depth Strategies, http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf.

2. CREATING A CYBER FORENSICS PROGRAM FOR CONTROL SYSTEMS ENVIRONMENTS

Within any networked environment, cyber forensics should be a capability that supports the protection of key information assets, while facilitating the collection of evidence assisting in the understanding of cause, mitigation strategies, resiliency programs, or even law enforcement activities. By definition, a cyber forensics program is designed to support a cyber incident response program, and it is the components within the incident response program that should be appropriately integrated into the fabric of the forensics capability. Before, during, and following a cyber incident, and after returning the control system to its operational state (if possible), it is the cyber forensics process that intends to discover what happened, how it happened, who did it, and what can prevent it from happening in the future. In the event that any activity related to the incident was illegal, the cyber forensics program will possibly provide evidence that is admissible in court.

As discussed above, the issues that can impede a successful forensic investigation include vendor technology, volatility of key data, and lack of extensive system-specific understanding. Although these factors are not unique to control systems per se, they combine to make the process of creating a control systems forensics program complicated at best. An effective cyber forensics program for control systems environments is contingent on a number of different variables. From a macroscopic level, a forensics policy that indicates process and procedures for forensics analysis on control systems components is paramount. In addition to this policy, specific information about existing services within the operational environment is also required.

With effective preparation mandatory for any successful response program, understanding the environment is critical. A clear understanding of the architecture in question, combined with clear documentation highlighting unique modifications, will empower the investigator, and most likely expedite analysis. For control systems environments, the development of a concise operational picture should be a straightforward task provided the critical information regarding device applications, any control systems specific security technologies, primary operator interfaces, and device control logs are accessible.

A cyber forensics program for control systems should be flexible enough to accommodate for the appropriate response based upon the significance or extent of a given incident. To accommodate for this requirement, the cyber forensics plan should include (but not be limited to) these phases[n]:

1. Identifying system environment and uniqueness
2. Defining environment specific requirements
3. Creating capabilities for identifying, collecting, and preserving data evidence and artifacts

2.1 Identifying System Environment and Uniqueness

A requirement of any forensics capability is to ensure the response mechanism is both supportive of the incident response team and appropriately mapped to the environment in question. Due to the diversity in contemporary vendor solutions, as well as owner/operator customizations, uniqueness will play a key role in the development of a forensics plan for control systems environments. By understanding each environment and its uniqueness, investigators can properly scope, appropriately resource, appropriately

n. Other phases, such as creating capabilities for examining data and reporting results can be closely mapped to standard forensic practices, with special emphasis paid to ensuring subject matter expertise (control systems cyber security) are available to provide support. See Section 3.1 for discussion on forensics activity supporting roles.

align with business operations, and appropriately pass information to law enforcement agencies, if required.[o]

An organization looking to deploy a forensics capability for their control systems environment needs to be able to understand fully a wide range of consequences that could be associated with a cyber event. By using risk models that are functions of threat, vulnerability, and consequence, an organization can have a much more granular understanding of how a cyber incident can impact certain components and control systems operations.[p] The consequences associated with cyber incidents in a control systems environment can vary and can include:

- Loss of localized or remote control over the process
- Loss of production
- Compromise of safety
- Catastrophic cascading failures that affect critical infrastructure and can extend to peer sites and other critical infrastructure sectors
- Environmental damage
- Injury or loss of human life

To help better categorize the consequences, an initial phase in the development of a cyber forensics plan for control systems should be a review of both the theoretical and practical consequences of incidents on the system. For most medium-to-large scale enterprises (and even some smaller ones), scenario-based reviews often provide insight into the associated criticality of the information resources and devices in the control systems domain. Using any traditional model for forensics, organizations can quickly come to understand what information resources can support forensics methodologies and those that cannot.

Understanding consequence is usually within the province of an organization's risk management team, insurance underwriters, or some combination of these and other corporate resources. Recently, as a product of the Department of Homeland Security (DHS) Control Systems Security Program (CSSP), a specialized toolkit designed to help an organization understand their consequence associated with their control systems was created. The Control Systems Cyber Security Self Assessment Tool[q] (CS^2SAT) provides owners and operators a non-intrusive mechanism to understand operational risk better as it relates to the cyber security of all components within control systems architectures. The tool, which also allows users to learn more information about various cyber security standards associated with control systems, provides for the calculation of security assurance levels that can be tied to the most common consequences in which organizations are familiar. This includes physical damage, human injury and loss of life, environmental impact, and other qualitative or quantitative aspects related to an incident that impacts control systems operations. In addition, the tool provides the users with the functionality to create effective reproductions of the control systems architecture to understand the relationships between the control systems domain, the corporate domain, peer domains, and the security relationships in amongst core operational devices. Using tools such as this, along with other viable consequence analysis methodologies, can provide an organization with a much-needed proactive review of how a cyber incident can manifest in a control systems domain. The information learned in this process can help organizations have a better cognitive view of the extensiveness of incidents, as well as understand what relationships

o. Factors that can impact system environment and overall uniqueness can be very extensive, and can include mergers, acquisitions, corporate security policies, and regulatory/compliance issues.

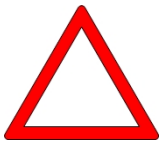
p. Department of Homeland Security, "Risk=ThreatxVulnerabilityxConsequence from the Nation Infrastructure Protection Plan," http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm.

q. CS2SAT, http://www.us-cert.gov/control_systems/pdf/CS2SAT_Trifold_Web_version_Final_062308.pdf.

among key devices need to be examined with regards to formulating a response associated with a cyber forensics investigation.

It is important for organizations to understand the extensiveness of the connections in amongst their peers' sites and partners. By looking to understand the uniqueness associated with the system, organizations developing the components for a tactical forensics plan must also take into consideration other variables such as:

- Connections to and from partner or peer locations
- Access to mechanisms used by the vendor to support control systems technology
- Access to mechanisms used by contractors to support control systems environments
- Actual relationships between cyber resources and real-world operations
- The pervasiveness of effective cyber security policies governing control systems operations
- Information exchange mechanisms within the supply chain



It is particularly interesting to note that this last point related to supply chain operations is often neglected or misunderstood. Supply chain operation networks, unfortunately, often include direct connections into the primary users of the supplied materials, but due to the trusted nature of the connections, the incident pathway can be overlooked.

By assessing the uniqueness of the control systems environment and the components within that environment, organizations can categorize their technologies and create a cohesive plan that contains flexibility for network elements that may lack logging or audit capabilities. To offset any inadequacies regarding logging and audit capability, this method also supports the granular understanding and calculation of the appropriate levels of detail that each information resource in the network is generating. In lieu of devices that are unable to store information adequately, specifics relevant to information generation and the role of the device in the network can be very helpful.

In the interest of simplicity, it may serve the organization very well to categorize their technologies into one of three areas: Modern/Common, Modern/Proprietary, and Legacy/Proprietary.

The technological differences and characteristics between devices in these three categories can be quite extensive, thus the difference in approaches to each by a forensic examiner will need to be adjusted accordingly. The concepts introduced in the following sections are provided to successfully augment proven methods, and are not intended to recreate any existing forensics investigation methodologies. The concept of categorizing technologies can greatly expedite investigators arriving at conclusions in both the collection and analysis phases. The range of currently deployed control systems technologies encompass those that are very new and deemed forensics friendly, to those that are very old and rely almost entirely on knowledge held by a small number of people. The next section explores the differences in these technologies, as well as forensics responses to each that are likely to be successful.

2.1.1 Modern/Common Technologies

Modern/Common technologies are those that are critical to a control systems operation, have modern computing capabilities, and are most likely still fully supported by the vendor. These technologies will most likely run on some sort of contemporary operating system, may have some detailed information about the operations available in the open source community, and have been continuously supported since their original deployment. This support may include patch levels, system upgrades, vendor enhancements,

or other aftermarket modifications that allows the technology to remain current as it relates to compliance with standard practices (i.e., OSI interoperability). Figure 4 illustrates some of the technologies in the control systems environment most likely to be of the Modern/Common type.

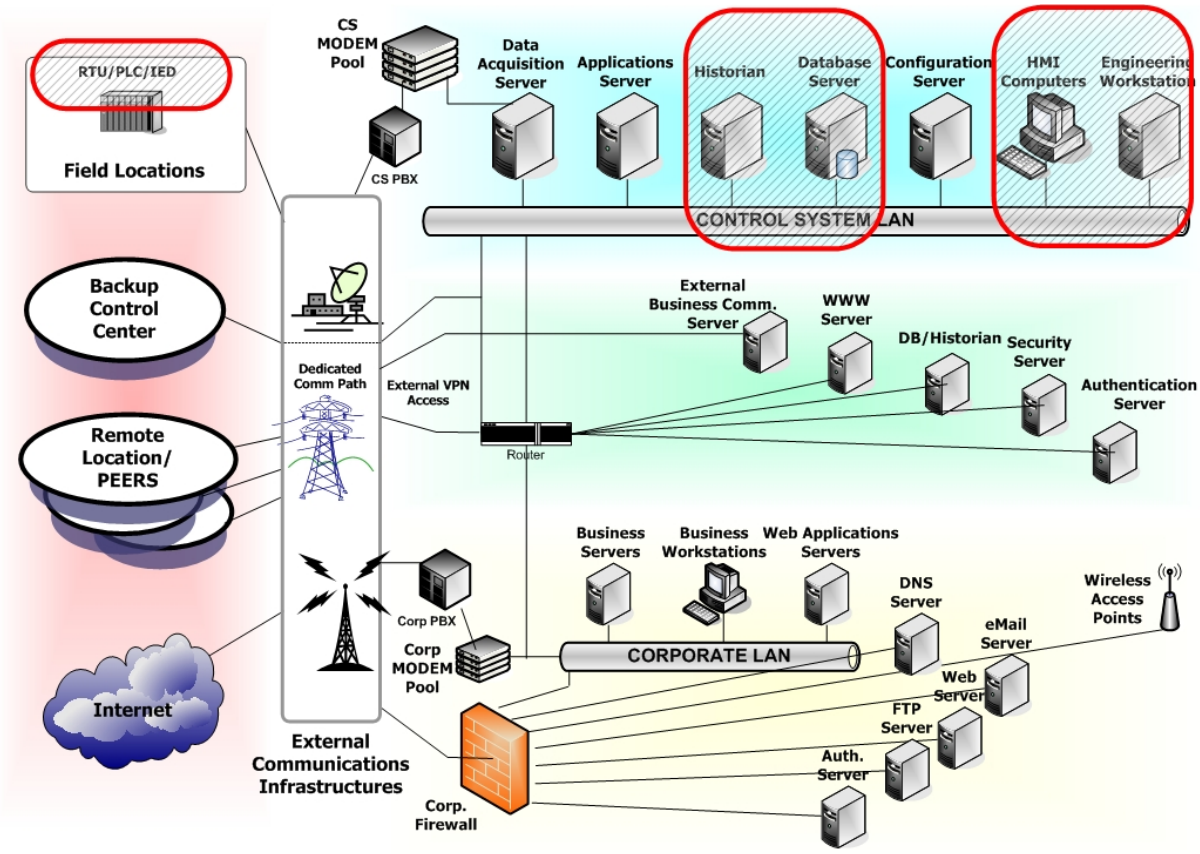


Figure 4. Example Modern/Common components.

This category of technologies inside the control systems domain will be those that would be most susceptible to modern cyber threats and vulnerabilities, while at the same time being mature enough to allow some contemporary forensic methods to be successfully performed on them. Most common technologies that fall into this category include Microsoft Windows operating systems, those systems using the UNIX platform, or another vendor specific solution that has functionality that can be investigated using standard forensics methodologies.

Table 1 below highlights several of the major features associated with these types of technologies relevant to creating a cyber forensics program.

Table 1. Modern/Common technologies and forensics compatibility.[r s]

Modern / Common Technology	Effective Audit/ Logging	Forensics Compliant	Reference Materials Available
Engineering Workstations, Databases	Yes	Most Likely Yes	Most Likely Yes
HMI	Yes	Most Likely Yes	Most Likely Yes
Field Devices (PLC, RTU, IED)	Possibly Yes Most Likely No	No	No

Section 2.3 discusses specifics relating to identification and collection of evidence from the system.

Within this category of Modern/Common technologies, technologies are found that meet the criteria to be categorized as Modern/Common, but they do not have any inherent data collection capabilities (such as local logging or audit) that could be leveraged by standard forensics methodologies. Simple examples of this could be the Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Intelligent Electronic Device (IED), or some other field-level device that is empowered to communicate through modern communications mechanisms. These devices often have available services embedded in them to enhance administration, some of which include Web services, Simple Network Message Protocol (SNMP), and diagnostic tools. These devices, categorized as modern and common, often lack the capability to provide an investigator with any data that could be useful following an incident.

By including the capability to perform a forensics investigation on an online system, the investigator is better positioned to collect critical state information that could be used to formulate a more effective response and develop a more detailed and accurate report.

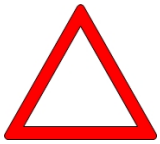
When considering Modern/Common technologies, a proactive forensics framework must therefore consider the use of live system forensics (see Section 2.3.5). Although many modern field operation devices have inherent capabilities to support granular command and control, a number of them will lose critical state information upon power cycling. Moreover, being able to provide for live analysis removes the need for the investigator to take the device offline, thus reducing interruption of the operational process. Live incident response means that the initial incident response will determine whether a complete forensic investigation is needed. In the strategy formulation phase of the incident, response determines the

r. Some functions, such as those supporting safety operations, have extensive event logging functions built in. As this paper focuses on cyber incidents, this table relates to the ability of system components to provide effective forensic data that can be utilized during standard forensic investigations.

s. In this and following tables, the term “Forensics Compliant” refers to whether or not the technology is easily investigated by contemporary forensics technologies. “Reference Materials Available” refers to the availability of open source information regarding methods associated at diagnosing failures and incidents.

most appropriate response strategy, given the circumstances of the incident. The strategy should take into consideration both technical and business factors, and should be approved by management.

In summary, the deployment of a flexible forensics framework needs to consider both live and dead (powered on versus powered off) systems analysis. On devices categorized as both Modern and Common, contemporary forensics techniques are most likely to yield favorable results. Wherever possible, the forensic examiner should employ live systems analysis to avoid disrupting the operational process, or where critical volatile information risks of being lost. As a corollary, the examiner should employ traditional dead systems analysis whenever a backup is easily available in order to obtain a greater amount of information.



Whenever possible, investigators should run offline tests within a testbed environment to ensure that possible resource taxation will not be an issue on the system as a whole.

2.1.2 Modern/Proprietary Technologies

Modern/Proprietary technologies are those that are critical to a control systems operation, have been created within the last 10 years, and are still fully supported and understood primarily by the vendor (or systems integrator). In this case, the control systems technology and information about its operation are not generally available through open-source methods. Moreover, the technology and protocols associated with command and control of the operational environment may only be known to the vendor and just partially to the owner/operator. Figure 5 illustrates some of the technologies in the control systems environment most likely to be of the Modern/Proprietary type.

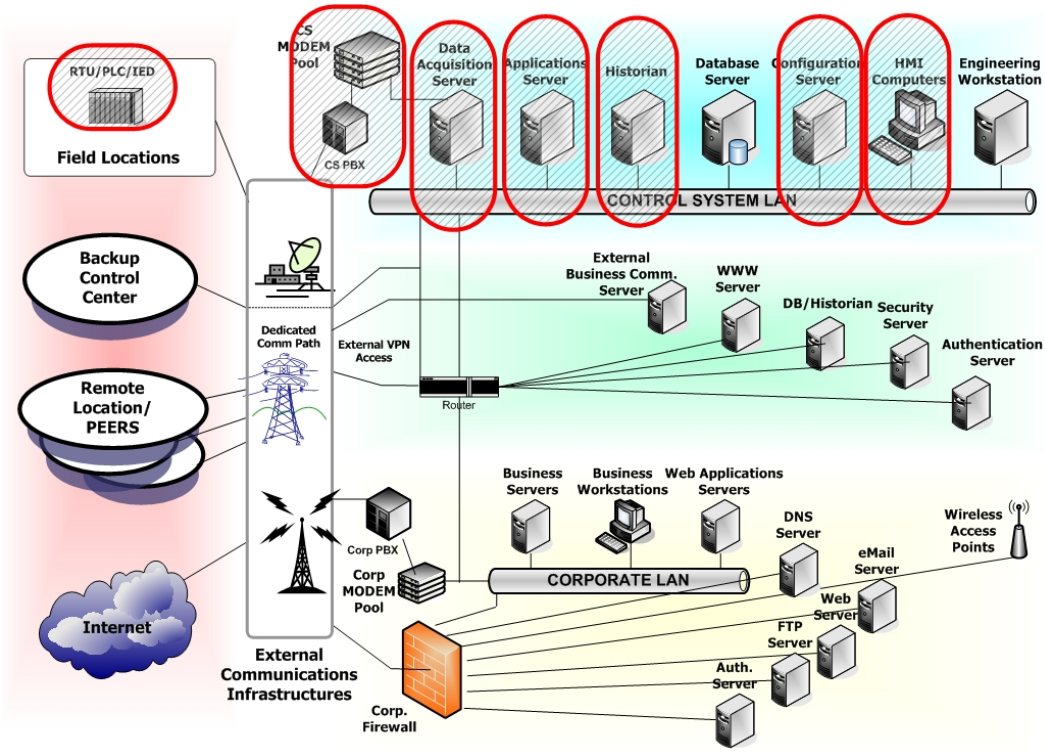


Figure 5. Example Modern/Proprietary components.

The reader should note that there is some overlap between the Modern/Common and Modern/Proprietary classifications. This is because there may (and probably will) be proprietary components residing within a Common technology (Windows, UNIX), which modify its behavior or otherwise change its default operating system (OS) functionality.

When categorizing the control system technology to be both modern but proprietary, the complexity related to executing a successful forensics investigation is increased. In an ideal world, most of the contemporary deployments for control systems would be of the previous Modern/Common type, thus allowing for effective incident handling and forensics techniques to be applied. In the previous category, it introduced complexity when the modern field device technology or operating systems did not have any inherent capability to support logging or audits. This of course will force the investigator to initiate secondary or tertiary activities to collect as much information as possible from a live system (see Section 2.3 on collection). Table 2 illustrates some of the more important aspects associated with Modern/Proprietary systems.

Table 2. Modern/Proprietary technologies and forensics compatibility.

Modern / Proprietary Technology	Effective Audit/ Logging	Forensics Compliant	Reference Materials Available
Engineering Workstations, Databases, Historian	Unknown	Unknown	No
HMI, Data Acquisition, Application Server	Possibly Yes	Possibly Yes Most Likely No	No
Field Devices (PLC, RTU, IED), Modem/Remote Comms	Probably No	No	No

When the modern control system contains a high level of unique and proprietary technology, the investigator or team of investigators will require significant in-depth information concerning the vendor solution. In such circumstances, forensics investigation (not to mention incident response) can be impeded. Although the investigator may be able to use contemporary imaging and collection methods on some of the supporting technology and the environment, without a clear and concise understanding of how the proprietary technology is working in the operational environment, the investigator risks the possibility of misinterpreting the data. It could be assumed that, over time, the investigator may come to learn the internals of the proprietary technology, but it makes sense that the time required to do so would push the timelines associated with the investigation into the realm of the impractical.[t] When the data has been stored and is available for event recreation, the investigator does not need to know any internals. However, for a cyber incident, the data retained for event recreation may be insufficient for forensic purposes.

t. There may also be evidentiary admissibility issues in such discovery without appropriate vendor support.

When categorizing the devices in question as both Modern/Proprietary, the forensic investigator is encouraged to perform contemporary dead (offline) analysis wherever possible. Performing a dead analysis will allow the investigator to try many different techniques on an image of the system without risking a compromise of the data's integrity. If the system in question cannot be taken offline, the investigator is encouraged to perform a contemporary live analysis. However, the investigator is cautioned to be fully aware of the potential ramifications these techniques can have on production systems. Unless the investigator has adequate knowledge of the proprietary technology in question, it is highly recommended to only perform a passive analysis. Furthermore, interaction with the vendor is encouraged when examining proprietary technologies.

In summary, as the organization develops a forensics methodology using consequence-based analysis, the Modern/Proprietary type of environment is at risk due to possible excessively slow responses in correcting the impact on network components. This type of environment is also plagued with the problems associated with restoration, the replacement of technology, and most likely a concurrent need to have continuous operations. Issues associated with collecting evidence from these types of environments are discussed in detail in Section 2.3.

2.1.3 Legacy/Proprietary Technologies

Legacy/Proprietary technologies are those that are critical to a control systems operation, may have been deployed more than 10 years ago, and have moderate computing capabilities (compared to modern systems). Moreover, they may or may not be supported be the vendor and are in most cases only understood (in-depth) by the vendor. The possibility that the vendor no longer has the requisite knowledge due to the age of the system further compounds this situation. As such, situations can arise when the owner of the system has key knowledge of the system (or at least how to maintain it) as the vendor no longer exists.

Obviously, from a cyber security perspective, environments that are rich with these types of technologies will be the most difficult to address when creating a cyber forensic program. Moreover, the development of such a program is usually cost intensive. Difficulties can arise, when operators have limited or non-existent vendor relationships, and all support comes from "in-house" expertise. This is not to say that the owner or operator cannot begin to lay the foundation for a forensics framework in these types of environments, but to understand the capabilities that can contribute to a forensics program the vendor will need to be involved.

Figure 6 illustrates some of the technologies in the control system environment most likely to be of the Legacy/Proprietary type.

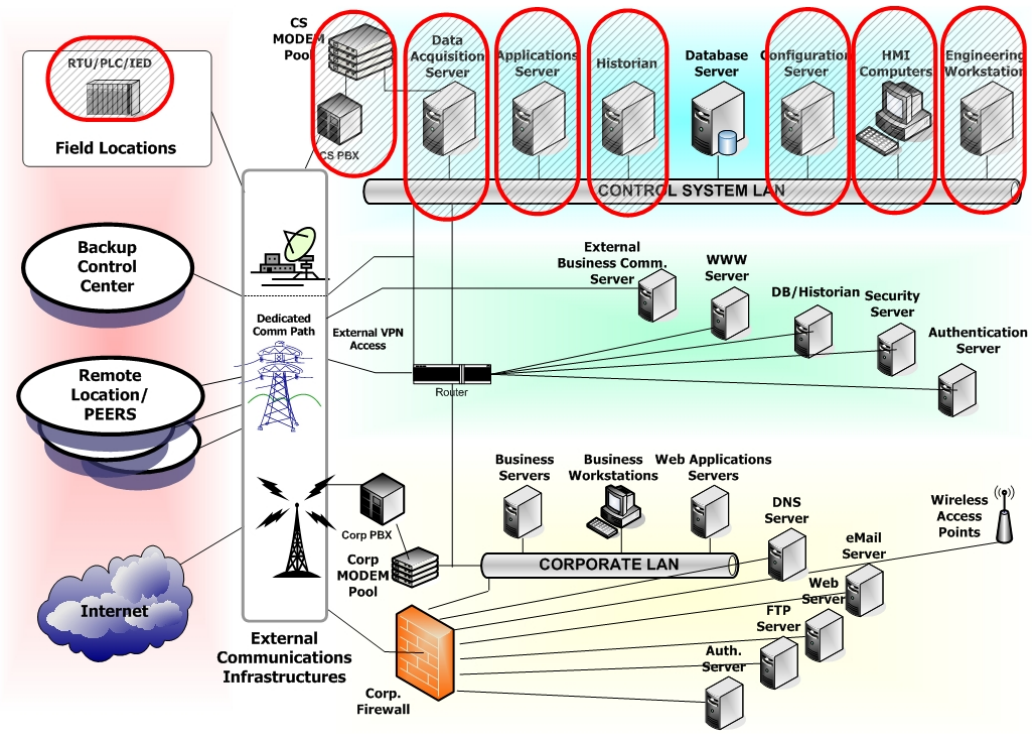


Figure 6. Example Legacy/Proprietary components.[u]

The assumption that the vendor is available to support these types of technology environments could often be false. In many instances, where the systems are beyond 20 years old, not only are the technology and the command-and-control protocols no longer supported, but the physical elements, such as field devices, are no longer being manufactured or are no longer available on the open market. Thus, developing a cyber forensics program that will assist an organization to understand what information can be harvested from these devices becomes exceptionally difficult.

In these circumstances, the expertise required to support cyber forensics investigation will probably be within the province of one or two veteran engineers or systems administrators who have a very rich experience and history with the system in question. Undoubtedly, investigators operating in these types of architectures should not have high expectations for being able to collect detailed incident information or artifacts. As a system's age approaches 20 years or beyond, historical analysis has shown that undoubtedly these aged technologies do not have the capability to support an extensive forensics investigation. In many cases, all that can be done is to draw on the network-based communications (if indeed a network is involved) and try and extrapolate specific information as to how the incident occurred. In addition, using process system reports, trending graphs, and snapshots of system activity (event logs) over time can provide valuable data points. Table 3 illustrates some of the more important aspects associated with Legacy/Proprietary systems.

u. The diagram is notional in nature and does not account for all possible architectures. As an example, it is not uncommon for modems to be connected directly into applications servers as well as PLCs, especially in legacy environments.

Solutions that utilize third-party log monitoring can in many cases help with log data analysis. In some cases, the usage of these tools can help with investigative analysis.

Table 3. Legacy/Proprietary technologies and forensics compatibility.

Legacy Proprietary Technology	Effective Audit/ Logging	Forensics Compliant	Reference Materials Available
Engineering Workstations, Databases, Historian	No	No	No
HMI, Data Acquisition, Application Server	Most Likely No	No	No
Field Devices (PLC, RTU, IED), Modem/Remote Comms	No	No	No

2.2 Defining Environment Specific Requirements

To define environment specific requirements effectively, preplanning for forensics activities must take into consideration the analysis of possible consequences associated with a cyber incident in the control systems domain. Regardless of the domain of interest, understanding the overall consequences associated with an incident is critical to understanding what incident response activities are required as well as how to apply a focused forensics investigation. Naturally, each environment will be unique. Although there will be some commonalities in vendor technology, field technology, and command-and-control support technologies, it is assumed that no two forensics investigations will be identical.

Considering the entire information infrastructure, not just the control systems environment, is vital to developing a proactive cyber security stance. This stance will help shape the cyber forensics program for the control systems domain as it allows relationships to be formed between the control systems domain and the other domains from which activity (malicious or other) can be sourced. Previous work completed by the DHS CSSP and ANSI/ISA has produced concepts related to security "zoning" that allows an organization to consider attack pathways and security countermeasure requirements based on location of the information resource.[v][w]

Issues addressed in developing the forensics capability should map closely to those associated with what is done for the control systems incident response (IR) plan. In the same way that the IR plan is predefined, vetted, and mapped to the actual assets in the operational domain, so must the forensics effort

v. See Control Systems Cyber Security: Defense in Depth Strategies, http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf.

w. See ANSI/ISA-TR99.00.1 Security Technologies for Manufacturing and Control Systems.

be tuned. In doing so, several key considerations can help ensure the forensics plan is adept at supporting both the IR plan and the needs of the business.

2.2.1 Impacts of Vendor Solutions on the Operating System

When reviewing the classifications of types of systems from the previous section, it becomes clear that a variety of operating systems support control systems operations. With each major information resource within a control system being dependent on the core operating system, it becomes very important to understand what the impact of software and operations technology can have on this base operating system. Although the type and age of operating systems will vary, a successful forensics program will need to consider how the operating system is handling information as it relates to audits and transaction, as well as any changes made to inherent logging and audit mechanisms. Should the investigator be in a position to utilize existing capabilities of a forensics toolkit, as well as being a position to apply proven forensic methodologies, some factors remain that should be considered.

Although there may be the occasional installation that utilizes software that only requires minimal interaction with the base operating system, a majority of control systems, regardless of their classification, will have customized operating systems running the control systems domain or applications that reside on contemporary operating systems. In its simplest form, these operating systems would be Windows, UNIX, or some variant of the UNIX platform. For the forensics investigator, working with these systems is often very straightforward. Harvesting the core data files, collecting the necessary evidence relevant transactions and audit, or in deployments that are more modern, it is easy to harvest current state information as relates to processes and connections. However, when the control systems solution is developed to reside on top of the core operating system, and significant changes have been made to the file structure (to accommodate for the control systems applications) some complexities can arise insofar as data analysis. More often than not, these complexities are associated with the security and authentication of operations.

Contemporary access control to these systems is often role-based, allowing an organization to provide some significant granularity as it relates to having control of how operators, developers, and engineers gain access to the system components. It is not unusual to have a solution that allows for the development of access policies that only permit certain roles to execute certain tasks. Although many of the contemporary solutions take advantage of underlying authentication mechanisms, the way in which the solution ties that authentication into the actual management of the control systems may introduce new logging mechanisms or at the very least, a secondary transaction log that may be unknown to the investigator. In these cases, using lockout mechanisms ensures that unauthorized users cannot have access to the system while confining authorized users to operations related to their role.

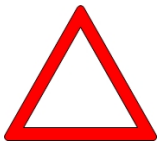
In addition to the standard access control mechanism for an information resource in the operational domain, it is also very possible that the solution is using security mechanisms that are extensible to how set points and device behavior is managed. It is becoming common for vendors to create technologies that extended the native operating system authorization mechanism into the realm of databases, alarms, or engineering activities, all of which can influence the behavior of a system. Simple examples include replacing traditional startup executables in Windows-based environments with other customized executables that meet the needs of the industrial process. It is not uncommon for owner/operators to use these technologies in such a way that the authentication and authorization associated with gaining access to the system is different from the authentication and authorization associated with making modifications to the system (i.e., set points). That said, the traditional mechanisms inside the operating systems that investigators may be familiar with may not only be modified in a manner that is unique to the solution, but may actually be divided among several areas in the system. To support audit and transaction regulations, or some other sector specific mandates, the functionality to provide additional levels of

auditing, monitoring and access control in critical systems may not be as simple as using the base operating systems security functionality.

For those entities that require authentication or authorization for each modification that is to be made in the control system domain, the concept of "change point verification" may very well introduce the need for the instantiation of unique audit trails. This information can include such detailed information as reason codes, overrides, decision approval codes or other information that could be closely tied to an incident source or incident occurrence. In some solutions, the security extends from the localized user out to nodes and points-of-presence in the control system domain.

Clearly, this information is extremely pertinent to the investigator during evidence collection or incident support, and could reside on any of the primary resources found in the control systems environment (human-machine interface [HMI], engineering workstation [EWS], Historian, etc.). Of course, the more proprietary in nature the solution is the more reliance the investigator will have on input from the developers and the vendor of the solution.

During a forensics investigation, the investigator may find the largest concentration of modifications to the OS will be in the HMI.



An investigation harvesting evidence from core components that augment base operating systems should only be done with a full understanding of how the OS has been changed. In addition, any auditing activity needs be carefully tested and deployed to assess for any taxation on system resources.

2.2.2 Data mingling Consideration

During the development phase of the cyber forensics program, organizations need to pay special attention to what information to harvest, collect, and analyze in the event of an incident. Realizing that the operators and administrators should recognize a good portion of the information in the control systems environment, being able to understand quickly the types of data, and the relationships of the data in the domain can be very valuable to an investigation that is occurring offline or in real time. Traditional control systems environments were not necessarily developed with the foresight that they would be impacted by a cyber incident. The data that moves in and among devices within a command and control environment was not necessarily predicted to be at risk due to a compromise of availability or integrity. Considering that in many control systems environments the data is exchanged at a very rapid pace, or sensor/indicator information from field devices is often collected and overwritten hundreds of times a second, there is an inherent problem in isolating incident-related traffic from non-incident related traffic. The co-mingling of data within a control systems environment will often make the investigator's task (as well as the incident response task) challenging.

Although the impacts of data mingling cannot be fully understood until there is a requirement to ascertain the source in consequence of an incident, proactive measures in terms of isolating or understanding the behavior of the most critical resources within a control systems domain can aid in quicker problem resolution. Many organizations will undoubtedly have a problem in trying to isolate or prioritize critical information resources inside their operational environment. However, using consequence-based analysis, as well as understanding how to collect key audit and transaction data, organizations may be better positioned to extrapolate evidence related to a cyber incident.

2.3 Identification and Collection of Data

Assuming the investigator has been able to classify the type of environment to be evaluated, the identification and collection of evidence from key information sources can be started. Accordingly, the forensics investigator should be able to ascertain which components of the architecture can be assessed using contemporary forensic technologies versus those that may not. The forensics guidelines and best practices as they apply to contemporary technologies (i.e., where they have been proven effective before) are beyond the scope of this report, so this section will focus on the identification and collection of pertinent forensics evidence within a control systems environment that will need special attention and methods.

The basic framework for any investigation, as it pertains to the identification and collection of digital evidence (whether it is in the control systems environment or not) will have several core components or elements that must be adhered to by any investigator. To ensure the investigator has a concise and effective framework for executing a forensics program in a control systems environment, the following traditional forensics elements will be examined and the uniqueness of a control systems environment and the impacts on these elements will be discussed. These elements are:

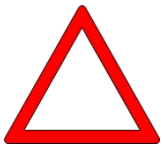
- Reference clock system
- Activity logs and transaction logs
- Other sources of data
- General system failures
- Real time forensics
- Device integrity monitoring
- Enhanced all-source logging and auditing

2.3.1 Reference Clock System

As in any forensics investigation, an analyst must be able to establish a context of time when evaluating collected data. In control systems environments, being able to establish a reference time source is paramount to success not only for incident investigations, but also for business operations. Unlike transactions in the corporate or modern business environment, activity and transactions within control systems environments are often required to occur in milliseconds. Combined with extensive use of volatile memory and small storage capacity, investigators looking to align incidents and consequences effectively within a control systems environment will need a very specific clock reference. Should the investigation reach the legal domain, the time stamping and mapping of activities from a temporal perspective will be critical to success. As most users and administrators of control systems environments will know, a very quick and simple modification to the control data in the operational environment can have devastating consequences, and such modifications are quick to manifest at input/output (I/O) points (impacting how a device behaves).

Prior to the investigation of event data or the collection of any forensics evidence, the investigator is advised to obtain a reference clock or timing source within the control systems domain. Fortunately, due to the way that many modern (and even some older) control systems environments are established, synchronized timing within the operations is normally addressed. Thus, the investigator may be fortunate and have access to an already pre-existing, functionally centralized time function synchronized to all

elements in the control systems domain.[x] It is advised that the investigator, prior to commencing investigation, works closely with control systems network administrators and engineers to confirm the centralized clocking mechanism is trustworthy, and determines the extent to which it influences timing on the other network components. In addition, to compensate for the possibility of there being multiple centralized clock mechanisms for each of the control systems (and IT functions within a control systems domain), the forensics investigator is strongly advised to ascertain if more than one clocks exist. If so, it is imperative to determine if theses clocks are synchronized and which Network Time Protocol (NTP) server each system is statically set to resolve to.[y]



Many organizations use global positioning system (GPS) clocks to ensure ubiquitous time across the domain. However, it is not uncommon that network latency can introduce considerable time differences in amongst devices. Network Time Protocol (NTP) can be used to estimate and account for this latency, and some organizations incorporate both methods. Caution is advised, because NTP can permit for network spoofing attacks, causing severe discrepancies in timing and time stamping.

2.3.2 Activity Logs and Transaction Logs

No matter what kind of environment a forensics investigation is being done in, access to activity logs and transaction logs are critical to the success of the investigation. Historically, in the IT domain, activity and transaction logs and their associated granularity has been a function of the initial audit requirements as set forth by network developers and security policy administrators. Unfortunately, the traditional approach to activity and transaction logging in a control systems domain is often only created to support production and troubleshooting, and as such is often lacking the granularity required by an exhaustive forensics or incident investigation.

However, due to the business reporting and production requirements seen in many control systems deployments, activity logs and transaction logs relating to control systems domains are usually very closely tied. In many cases, the control systems environment under forensic investigation will have some significant impact on critical infrastructure and/or the health and well-being of human lives, and will thus have to adhere to regulatory requirements. Moreover, the control systems environment will usually have a significant impact on the viability of business operations. As such, regardless of the age of the environment, control systems are engineered in such a way that transactions and activity are often monitored very closely. Undoubtedly, the age of the system will reflect how useable the available logs are, and the investigator will need to have some success in ascertaining core control systems elements that may possibly align the classification types for the previous section.

Understanding the role of technologies within the control systems domain will play a part in helping the investigator to ascertain the specific role (if any) a particular information resource played in a cyber incident. Identifying the connectivity of resources within the control systems domain as well as the connectivity resources have to other domains, also helps define plausible attack vectors and assist the investigator in post-incident analysis. The aforementioned reference architecture (see Figure 1 in Background), shows that technology components could very well be involved in the transferring of critical data and critical operations information into demilitarized zones or directly into corporate environments. Technologies in the control systems environment should be regarded as highly critical to

x. “Centralized time function” refers to a master time source in the system being investigated, not a centralized system in terms of geography. Also, investigators should be aware that the timing mechanism for the control domain may itself have been impacted by the cyber incident and thus should be deemed unreliable.

y. Creating effective clocking mechanisms for forensics investigations is beyond the scope of this report.

the success of a forensics investigation. Although specific vendors may have provided the operational software on the systems, the underlying network communications capability provides not only vital communications to the control systems domain, but possibly exploitable pathways for attackers.

This approach empowers the investigator to be able to expedite the investigation as it pertains to whether or not it can be determined which systems have been impacted. If the impacted systems are identified, OS logs and transaction logs directly relevant to control systems elements can be collected and investigated using OS-centric guidelines that are widely available. If the incident response activity is unable to define any specifics effectively as to the incident location (and as such specific platforms or technologies) it forces the investigator to identify all possible audit logs and transaction activity logs, thus creating a very extensive collection profile. Clearly, without an effective incident response capability for an operator's control systems environment, this latter scenario would probably be prevalent.

To assist the reader in understanding where evidence could be collected in the control systems environment, as well as help them understand plausible unique relationships in the control systems environment, several key components are considered from the reference architecture. In the interest of brevity, it is assumed that the investigator has been able to ascertain the environment classification of the control systems domain.

2.3.2.1 Modern/Common Control Systems Technologies

Engineering Workstations, Database, Historian

Figure 4 above illustrates the example reference architecture citing sample Modern/Common components. From this diagram, the engineering workstation, database, and data historian components need to be cited in a forensics investigation. The technologies associated with these three elements will almost certainly have some sort of well-known, if not widely used, computing support mechanism, which is used by both control systems environments and non-control systems environments alike. As is the case in many control systems domains, the devices could be running either the Windows or any of the UNIX platform environments. In addition, these control systems components may be comprised of a combination of these elements.

Apart from for the vendor-supplied applications that may reside on these core operating systems, the capabilities associated with activity and transaction logging may be straightforward. Except for extreme volatile memory, such as registers and cache, the information from these resources may be obtainable using traditional forensics methodologies. In addition, investigators are reminded that in many environments non-persistent data on one resource may become persistent in another resource. What becomes important to the investigator, should the system still be running, is to obtain as much information about the state of the processes within the system as well as the concurrent communications and connections to core components inside the commanding control domain (i.e., those to the field devices).

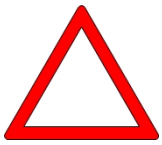
Assuming that these key elements are critical to the control systems operation, and like many organizations, no secondary backups are available, it is assumed that the systems cannot be taken offline for forensics analysis. In many cases, this would be the recommended approach, because if these technologies are involved in the actual attack or are a key component in the cyber incident, the current state, process, and connection status can greatly empower the forensics investigator. Due to the real-time requirements for control systems operations, having the opportunity to acquire real-time information about incident activity is critical. In these cases, the proactive incorporation of real-time forensics aids may prove very useful to the investigator.

HMI

The criticality of the HMI in the control systems environment cannot be overstated. As the primary point for all command and control activity within the control systems environment, the HMI will demand special attention in a forensics investigation. Common/Modern deployments of the HMI allows the investigators significant leeway in trying to understand what, if any, elements of the incident impacted the production environment. Although consideration must be given for some vendor-specific software applications that are tied uniquely to the control process, it is often the case that the underlying functions of the core operating system will allow for forensics analysis.

However, like all elements in the domain, attention must be paid to the volatility of the different types of information available from this resource. In lieu of any vendor interaction upon the immediate evidence collection activity, the investigator will need to consider a number of elements that may impact the using of standard forensic methods.

Of concern to the investigator is the possibility that the version of the HMI software may have required initial hardening of the operating system (kernel) or use a standard "build" that removed non-essential services and/or files from the base operating system. To that end, some of the more common features and capabilities associated with transaction monitoring, alarm and event logging, or diagnostics may be modified or absent all together. Although the core drives and resident data could be harvested for offline investigative analysis, key data stores and file structures may be so different that a vital evidence collection may be impossible. Furthermore, without in-depth understanding of how the HMI is executing the command and control function in the environment; the investigator may be unable to locate pertinent evidence that is in the HMI data stores.



Investigators are reminded that if the HMI has extensive customized applications that augment the core OS kernel, there is an elevated risk of data mingling that will cause the investigator problems in trying to isolate key incident-specific data.

Field Devices (PLC, RTU, and IED)

Although many of the technologies associated with field level operations may not have any inherent activity or transaction logs, consideration must be given to the communication tied to field devices. Within the control systems environment there are communication elements within the control systems' domain that have activity and transaction logging enabled tie to field devices. Although the investigator should not neglect field-level technologies or other devices that may not have extensive logging, they should understand the relationships between field devices and other command and control elements in the domain.

Traditional forensics analysis tends to look specifically at points of presence in network architecture that has experienced a cyber incident. Because of the uniqueness of the control systems environment, the investigator needs to understand the relationships associated with all the information assets in the evaluated domain. In any control systems investigation, regardless of the age or uniqueness of the environment, collecting information from field devices will be a difficult task. These devices also tend to operate within very specific data exchange confines, and the rate at which they collect, exchange, and overwrite data often leads to the inadvertent removal of critical need-to-know forensics information. However, before the concept of data forensics was in the mainstream IT community, many of the devices that were built for resiliency and fault correction often contained a capability to help in quick restoration of services.

Whether or not a field device is on or off, or available for either online or offline investigation, until the extent of the incident is fully understood, the investigator may have no insight as to what the best method might be. When it comes to field devices, many elements give rise to added complexity in the investigation. If a field device is available for offline investigation, it is unknown (prior to analysis) whether such a situation is an advantage or a disadvantage to the forensics investigator. In addition, as may most often be the case, the field technology will not necessarily be made available due to the requirement that must remain operational to supporting real-time operations. However, if the system is available for analysis, the investigator may have some opportunities, depending on the classification of the device. All of these factors can contribute to making each investigation, unique. However, some common practices can be used in all cases.

If the impacted field devices belong to this category, chances are there is some useable capability within the field device that supports forensics investigation. Investigators need to understand that historically the deployment of these field devices is often very specific as it pertains to business operations and the requirements of the control systems. The specific configuration of these devices should be readily available to any investigator assuming that the configuration files have been kept, maintained, and stored in a relatively secure environment. From the previous section, not only should the configurations and any logic operations associated with the devices be readily available, any proactive security actions such as hashing, checksums, or integrity verification should be used to allow the investigator to cross-reference findings and ascertain if any tampering has been done.[z]

If the control system is online, the investigator is reminded of both the order of volatility of the data, as presented in Section 1.1.[aa] If the incident response team has been able to verify that the incident is perhaps still ongoing or the control system is back to a normal operating state, the forensics investigator has the opportunity to recognize other useful files and information in the field device environment. This often becomes a matter of urgency because this volatile system information, which includes running processes, current connection states, and memory content, can often be deleted, overwritten, or destroyed instantly. Due to this concern, it is recommended that wherever possible that the incident response team collect volatile information available from the field devices.

Significant computing horsepower can outfit some modern field devices, and a live forensics investigation may be able to obtain critical incident information on a running system that would be lost if the system was shut down or rebooted. This includes:

- The device date and time
- Current active processes
- Current running processes.

In addition to having access to field device configuration files for analysis, modern networked field technologies (whether online or offline) should be able to provide information similar to their common enterprise network counterparts that may include open ports, applications associated with open ports, and network connections. Although this type of information may not be available on all of these types of devices, the control systems vendor community is producing field systems with such capabilities at a rapid rate. In the same way that an attacker may be able to leverage both the network functionality and device capability of the elements within a control systems environment, the forensics investigator should be able to use those same types of technologies to aid in an investigation. When embedded services are

z. This method is effective for the detection of modifications after the technology has been deployed into operation, but cannot detect if the firmware had been tampered by the vendor (i.e., insider attack during production or external attack on vendor production systems).

aa. The issue of non-persistence is also critical, as the longevity of the data on a particular device also impact investigation.

available on the devices, such as Web or network management tools, the investigator should have an opportunity to harvest current state information relevant to those services.

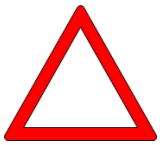
Note that regardless of the classification type of the field device technology, at some level the vendor should be involved in the investigation. Extending this ensures the Service or Security Level Agreements (SLA) with the vendor include verbiage for support during forensic investigations. Although the vendor does not need to be advised of the investigation specifics, or be the recipient of any acquired information, the vendor can certainly provide direction as it relates to logging, transaction activity, embedded service functionality, or how the field devices store, handle, and write to volatile memory space.

The forensics plan should call for a detailed investigation of the process logic internal to the field devices. Of particular importance is the historical administrative record that may indicate subtle changes to the logic made to accommodate changes in the physical system. [bb]

2.3.2.2 Modern/Proprietary Control Systems Technologies

Engineering Workstations, Database, and Historians

Engineering workstations, databases, and historians within the control systems architecture may have similar capabilities to those defined in the modern/common classification. Legacy equipment and technologies (10+ years old) still make up approximately 70% of the existing technology throughout all critical infrastructures. Being able to accurately pinpoint capabilities within these technologies is difficult due to the incredibly diverse landscape contributed by numerous vendors, independent developers, and an organization specializing in the customize nature of control systems technologies. For the most part, however, contemporary forensics should be able to work on these information resources as the importance of these resources running smoothly and effectively is critical to system operations. This leads to the assumption that these workstations, databases, and historians will not only use modern networking technology, but will also be mature in terms of their computing horsepower.



When dealing with modern but proprietary control systems technologies, especially those dedicated to the command and control function in an operational environment, interaction with the vendor prior to the investigation is strongly recommended. Although it may be obvious what file systems are in use, it is not uncommon for standard file systems to be modified by the vendor to accommodate unique control capabilities. These modifications can impact the functionality of both the forensics investigator's tools as well as any inherent operating system specific auditing functions, leading to poor evidence collection or added complexity due to data mangling.

HMI, Acquisition Servers, and Application Servers

Inside the operational domain, categorized as modern and proprietary, the investigator can expect that the services that support the HMI, Acquisition, and Application servers (as well as others) could be unique in terms of vendor's specifications. In this classification of data, the operating system modifications that could be vendor specific include:

- Kernel integrity that is driver independent

bb. The reader can review the official Taum Sauk incident report, highlighting some detailed information about the modifications made inside the vice logic to accommodate for subtle changes in how water levels were being recorded. www.ferc.gov/industries/hydropower/safety/projects/taum-sauk.asp

- Fault tolerance that automatically kills jobs
- Real-time reallocation of memory space

Such modifications can work both for and against an investigator; depending on whether or not the system is online (alive) or offline (dead), the activity of these modifications needs to be fully understood. A simple example would be in a situation where fault tolerance has overridden the need for a supporting system process, which was truncated by malicious activity. The vendor's solution to kill the process instantaneously removes any evidence that could be used by the investigator. Although most of the proprietary influence could very well be on the HMI, it is not unusual for vendors to push proprietary solutions into the acquisition or application servers as well.

Modern/Proprietary Field Devices

Field devices under this category may have some inherent technology or capability that can aid a forensics investigation, but it may be substantially less than in the Modern/Common category. As industry moves into this category, the dependence on input from the vendor will grow. It is also important to note that many of the proactive strategies associated with understanding the integrity of the core files in these devices can still be used effectively.

This report is directed to those environments that have network-based communications and are open. However, some vendor solutions for field devices are proprietary in nature. They are often deployed using a network address schema provided by the vendor. Therefore, a good investigation will need to know the entire architecture including how the system is addressed. For organizations that use proprietary field devices, there is a good chance that these modern (but proprietary) devices may very well have some sort of embedded vendor-specific security mechanism. If this is true, the investigator should be alert to the fact that there will be a relationship between the activity at the field devices and the commanding control equipment somewhere else in the network.

2.3.2.3 Legacy/Proprietary Control Systems Technologies

Engineering Workstations, Database, Historian

As the age of the system approaches 20 years or more, the architectures under analysis will have been developed with data integrity and availability surpassing all needs for what would be deemed as system "security." The audit functions related to the engineering workstations or primitive databases will most likely be non-receptive to modern forensic techniques.

HMI, Configuration Servers, Application, and Acquisition Servers

An HMI that is considered Legacy will be running on a proprietary system or, if it is not, it will be running on an operating system that is no longer supported by the original vendor, or the operating system may no longer be in business. In some, technologies that are 15 years old will no longer be viable or supported by many vendors. If the solution is actually Legacy but Common (meaning it is utilizing a once widely available and supported platform), there may actually be a small window of opportunity for forensics activity. However, a live investigation in real time would to try to collect pertinent state information related to the process. Systems of this categorization may also be comprised of both network and serial-based communications, the latter of which may offer no opportunity for any cyber forensics.

Legacy/Proprietary Field Devices and Modems

Field devices under this category will most likely be without any inherent technology or capability that can aid a forensics investigation. To support after-incident analysis on this type of equipment will require a functional understanding from the vendor. Furthermore, the systems capabilities will be tailored

to providing for immediate recovery than to collecting log data for analysis. The dependence on input from the vendor will be beneficial and unless trained in the actual device technology, the investigator will most likely be unable to obtain any viable incident evidence. Such restrictions (as alluded to in previous sections) will also limit the feasibility of any proactive strategies associated with understanding the integrity of the core files in these devices.

From a networking perspective, legacy and proprietary field device structures will most certainly be based on serial connections. For those installations that are trying to migrate to modern networking infrastructures, protocol servers will augment serial-based connections to the field devices, subtly translating between proprietary port serial-based communications and Ethernet-based mechanisms or even wireless. For the most part, however, the information available from field devices in these types of architectures will be able to provide little or no information beyond the vendor-specific fault tables in the devices. The rapid sampling and data overwrite rates for these devices, in combination with the often-trivial amount of memory inside them, combines to make a very difficult situation for the forensic investigator. These issues are of course compounded by the fact that if there is indeed some sort of incident it may interrupt the capability of the field device to work properly. Normal operations usually demand the instantaneous reboot or the swapping out of the device so that process operations can continue.

As the age of the system increases, it becomes more probable that the original vendor responsible for the development of the technology is either no longer in business, the contracts have expired, or there is simply no information about the device available. This drives demand for "community-level" support, and as such, peer networks can become one of the few remaining support mechanisms.

When faced with the challenge of working with legacy and proprietary field devices, whether or not the devices are available online or offline, the vendor should be contacted and an experienced engineer should be made available to support the investigation.

2.3.3 Other Sources of Data

Other sources of data for use as evidence associated with control systems environments are those categorized as sources found in any information architecture. In general, the information, as it relates to the I/O appropriate to all hardware or data mechanisms and the environment, should be considered other sources of evidence. Moreover, collecting evidence from these sources follows standardized methods of evidence collection that should be part of any standard forensics plan. The devices and media in this sense are no different in the control systems domain than they would be in any other IT architecture. Sources that can include other evidence that would be related to a cyber incident within a control systems domain should be include and not limited to:

- Floppy drives including Zip© and Jaz© drives (where appropriate)
- Removable media drives for CD/DVD/DVD-ROM/RW
- Handheld devices, personal digital assistants, or operation-specific handheld computers
- Unauthorized hardware including modems, USB devices, and keystroke loggers

The forensics capability within an organization should assist the incident response capability. Table 4 illustrates key artifact that should be collected by the Incident Response Capability that can empower a forensic investigation.

Table 4. Sample of possible artifacts and relevant forensic information.

Artifact	Information Provided
Process Commencement & Initialization	Information about program specific times & users; can be used to ascertain process activity initiated by unauthorized users
Resident Memory Usage	Often done only in real time, memory usage can provide insight into rogue programs and other malicious activity
Alarms (Unauthorized Attempts, Unauthorized File Access)	History of login attempts, file access, state changes. Can be used in tandem with error log file analysis
System Halt/System Shutdown/ System Reboot	Provides information regarding process termination, shutdown, interruption, & who initiated activity. Often can disclose activity associated with attacker access to bootup/shutdown files
Process & Resource Utilization	Provides information as to what processes are running & the affiliated resources to run that process. Can provide insight into unauthorized applications or concurrent attack vectors
CPU Activity	Provides CPU activity. Can be mapped (using timer/clock) to specific activities
Overall Disk Potential & Capacity Usage	Direct review can provide insight into malicious code or activity in specific disk sectors. Information can also be provided on how the disk was used

2.3.4 General System Failures

When an operating system or application, such as an HMI, crashes or fails in the control systems environment, it should not render the control systems in any type of insecure state. During the standard development and design phase, control systems are generally designed to fail "safe" and not incur damage to the system. However, as new and more powerful systems are introduced into the control systems landscape, the need for recovery of the system with full integrity is required.

The recording of system failures and event-based incidents are often required for event recreation activities. This data can be of particular importance during the initial steps of an investigation.

When reviewing modern cyber attack vectors, one of the key components of attack includes the forced failure and rebooting of a compromised system, which allows any malicious code to impact the function of the information resource attacked. Thus, as part of the cyber forensics plan that addresses how systems will fail and recover (which may span several components), the investigator should assume that the design and maintenance phases of the system development lifecycle may have been used to incorporate safeguards as they relate to recovery. Although such methodologies may be vendor specific, the inherent capability to restore system functionality as soon as possible will probably be within most control systems technologies regardless of their classification.

In general, how a control systems component's operating system responds to a type of failure can be of value to the user/operator, and an understanding of what failures mean can contribute to an overall better understanding of cyber security in the control systems domain. Moreover, an effective cyber forensics plan that includes training, response, and management practices reduces system downtime and increase overall security posture.

System failures may be categorized as:

- System reboot
- Emergency system restart
- System cold start

A system reboot takes place after the system shuts itself down (or is forced to shutdown) in a controlled manner in response to a trusted computing base (TCB) failure. Also, if the system finds inconsistent object data structures in its environment or if there is not enough space in some critical tables to perform key tasking, a system reboot may take place. The reboot often releases resources and returns the control systems component to a more stable and safer state.

Emergency system restarts often occur after a system failure happens in an uncontrolled manner. The cause of these restarts may be anything from a core operation failing to work or a lower-privileged user process attempting to access memory segments that are restricted. The system may see this as an insecure activity that it cannot properly recover without rebooting. When this happens, the system enters a maintenance mode and recovers from the actions taken and then is brought back online in a consistent and stable state.

A system cold start takes place when an unexpected activity occurs and the regular recovery procedure cannot recover the system to a more consistent state. The system and user objects may remain in an inconsistent state while the control systems attempts to recover. The control systems user or administrator may require intervention to restore the system.

From a forensics perspective, having the capability to monitor key file structures for integrity as well as functionality is advantageous. Moreover, for systems with a high level of observed "uptime," unscheduled restarts could be indicative of a serious security issue. The importance of being able to recognize and understand system faults is critical to forensics investigation in the control systems domain. The cyber forensics plan should have instruction and guidance on how these incidents are observed and reported, and can be deployed as new operational reporting standards or augmentations to existing operator reporting practices. In either case, cyber security applicability to traditional recovery may help contribute to a positive cyber security culture being developed and will support the overall reliability of the control systems information architecture. Like all failures and reboots, the cause should be investigated as required because there may be security issues requiring immediate attention.

Modern control systems domains have redundancy built in, with backup networks and key resources mirrored to accommodate for any catastrophic failure. Often, in the case of networked infrastructures, facilities have secondary ready-to-go systems, known as "hot standbys," that are resident online information and control systems assets ready to come online in the event of primary system failure. The key to operations (and cyber security) is ensuring that these secondary systems are fully compliant with current configurations and, if needed, can become operational with the exact same configuration and system upgrades as the primary system. Therefore, if an event requiring a switchover to the redundant system is required, operation can and will be maintained as if the main system was still online. Unfortunately, many organizations do not ensure that key secondary systems are upgraded and configured to the same cyber security requirements. There have been instances where secondary systems have been

vulnerable, and as such, ensuring secondary systems are secured prior to deployment becomes important.[cc]

Being able to have an effective history of system faults can aid investigators in pinpointing abnormal system activity and cross-reference with other obtainable information such as time of day, operator actions, and device activity.

2.3.5 Real-time Forensics

When considering how vital the components within a control systems environment are, in terms of business functionality and mission criticality, it may likely be the case that the forensics investigator will complete investigations in real time (live incident response). Clearly, these types of investigations are much more complex than in situations where the impacted technology can be taken offline (dead) and analyzed in a proper investigative environment.[dd] Of course, leaving the system online increases the overall system exposure to the attacker and could allow for an extend period of adversarial control. In the control systems domain, the replacement of technologies with back-up or secondary technologies may just provide for attack propagation (due to identical technology). To ensure proactively that a forensics investigation on a control system can indeed have a positive impact after a cyber incident, the forensic toolkit used by the investigator should include the capability to do a real-time investigation.

The success of real-time forensics and control systems is going to vary appropriately with the nature of the system investigated. Of course, newer systems that use contemporary computing technologies may be more adept at handling real-time forensics analysis. However, some older technologies, perhaps as old as 25 or 30 years, may be beyond the capability of the investigator and the capabilities within the forensics toolkit. Still, the cost associated with doing a forensics investigation where the system has been proactively prepared versus the investigation on a system that has not been prepared ahead of time will always be significantly less. For the control systems domain that can accommodate modern-day real-time forensic technologies, it is highly recommended that organizations make use of contemporary tools to allow this.

Currently, many widely available tools can aid a forensic examiner while performing a live analysis. Many of these tools perform tasks such as process monitoring and analysis, and can be installed to a system preemptively to an incident. The advantage of having these tools[ee] pre-installed is that the examiner will not have to compromise any volatile state data by performing an install after a cyber event has occurred.

2.3.6 Device Integrity Monitoring

One of the greatest advantages a control systems environment has in comparison to other types of IT infrastructures is that the control systems environment does not change very often or, when it does, it may

---

cc. Potential Vulnerability of Plant Computer Network to Worm Infection Notice, http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2003/in200314.pdf.

dd. This is a very difficult issue to address, as leaving the impacted system online may allow the attack to perpetuate, while failing over to back up systems may introduce the same vulnerability into the systems due to identical technology being used. In addition, disconnecting the system causes system productivity to drop to zero.

ee. It would prove prudent to use tools that are based on industry standards, and these standards should be a combination of those forming both the IT and Control System domain. In addition, taxation on system resources should be tested prior to installation on a control system machine as minor delays may not be acceptable in a control system environment that may require rapid execution of commands to end point field devices

not change very much. In addition, the data that is pervasive on the network is often very predictable, and in many cases somewhat deterministic. All of these factors can combine to ensure that the network administrators in the control systems domain have a well-structured, common operating picture as to how the system is operating and what it does when it is operating. In reviewing the control systems reference architecture, it shows that many of the vital technologies in the control systems network will have some sort of application, operating system, or logic associated with its normal function. These elements are well known by the operators, engineers, and administrators and are most likely to have copies and support backups to aid in the reconstitution of the system in the event of failure.

Many of the key elements in the control systems architecture, specifically the field devices, will have logic associated with them that does not change. Although in some network entities the state information, resident memory, connection entries, and other service data will change, some entities may have datasets in the form of firmware or logic that are not intended to be changed. This static nature of control systems provides the opportunity for the organization to take specific baseline measurements of key system internals that are not intended to change. These baseline measurements should be taken both prior to deployment and following each authorized change in order to verify a device's integrity.

A variety of different means can complete these specific measurement activities, including checksums, hashes, or some other type of quantitative measurement associated with that particular instance of data logic. A simple example would be to run a hash algorithm, such as SHA-1, on the logic found in the critical field devices. The hash associated with the field devices can be kept offline or stored in a secure read-only environment. In the event of a cyber incident considered to have played a part, simple calculation of the hash on the existing logic inside the device would provide comparison for the known hash that was previously calculated. If such an activity showed the hash as different, the investigator would immediately know that the tampering or changing of the logic within the field device was a component of the incident. Such knowledge would greatly empower the investigator, who would quickly be able to develop an information flow between the field devices and other control systems information resources. This would allow for the targeting of specific entities that may have appropriate logging or transaction information, or provide insight as to what information resources should be processed for evidence collection.

Although reloading critical configuration files is important to operations and productivity, it can have a negative impact on a forensics investigation. In addition, reloading files with inherent vulnerabilities may not always mitigate an attack or incident.

Forensics practice includes the process of hashing, which is considered one of the mandatory steps in evidence collection. Once an investigator has actually acquired hard drives or other memory devices for evidence, the investigator needs to be able to make an exact copy of the device so the original may be preserved. By using various copy mechanisms in combination with proven signature and hash methods, the investigator is able to make exact copies of the information to allow for the extraction of evidence in a manner that would be admissible in a court of law. For certain data, logic, or other operational instructions sets that are deployed to be static in nature, the use of hashing can be extended to help investigators in the event of a cyber incident.

2.3.7 Enhancing All-Source Logging and Auditing

Detailed logs are a tremendous help to a forensic examiner. The absence of these logs may result in huge time losses for the examiner as events must be discovered and then correlated on a timeline. Also mentioned was the fact that many systems with logging and audit capabilities are deployed with such features disabled. Enabling logging and auditing capabilities on field devices is greatly encouraged.

Additionally, this is a very simple task for an experienced administrator that can have far-reaching benefits (assuming there is no adverse effect on the performance of the system).

In the event that a field device lacks sufficient logging or audit capabilities, it is encouraged to log all network traffic to and from the device. Logging network traffic may aid the forensics investigator in determining a specific device's role in a cyber event. A passive network capture device can accomplish this. Most modern operating systems allow for this functionality with the installation of a software package such as Wireshark ™ or TcpDump ™.

Lastly, it is highly recommended that all audit, network, and device logs are stored securely either offline or in a read-only capacity. This is a critical step in maintaining the integrity of the logs for an examiner to utilize during an investigation as an attacker will often try to destroy or modify these logs to cover their tracks.

3. ACTIVATING AND SUSTAINING A CYBER FORENSICS PROGRAM

A cyber forensics program in any organization must be very closely tied to the incident response capability of that organization. Although this document does not extend to the recommendations and practices associated with providing evidentiary information for legal proceedings, the steps and methods suggested in this recommended practice clearly outline functionality that can be used to support incident response activities. In most cases, following the detection and correction of a cyber incident, forensics investigation will be used to ascertain the cause of the incident, as well as other fundamental attributes that can be collated to provide a full cognitive picture surrounding the cyber event.

It is clear that for executing successful forensics operations within a control systems environment, there should be some sort of pre-deployed and proactive effort to assist investigation in the event of a cyber incident. The volatility of data, the uniqueness of the technology, the proprietary components of the control systems environment, and the almost certain need to have the equipment running and available all combine to create substantial hurdles for the forensics investigator. As such, it becomes paramount to create activities for introduction prior to the cyber incident, such that following an incident response investigation the forensics program will have a pre-established starting point. It is also very important to introduce these types of solutions so that they are not intrusive, and in no way impact the business operations, stability, or the critical functionality related to the control systems environment.

3.1 Immediate Response and Incident Support

How the incident response capability operates and when the response is complete will drive the initial response associated with activating a cyber forensics program. Traditionally, a cyber forensics program will be initiated after elements, such as restoration, mitigation, and initial reporting, have been finalized by the incident response capability. For many organizations, incorporation of the forensics function into the entire IR process has worked well, especially in cases where the start of the forensic function cannot be clearly delineated. This model has proved successful in mitigating many of the issues discussed in this document, such as those related to system access, expediting technical review (to support timely restoration), and minimal impact on system resources.

In the case of developing a forensics program for control systems environments, this concept may work quite adequately, with the forensics function a contained aspect of the incident response capability, up to and including any submission of data for prosecution purposes.

The core components of cyber incident response (IR) with an embedded forensics component are:

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

Table 5 below shows the relationship between the incident response function and the forensic function when handling control systems cyber security incidents. It illustrates the primary activities with a (P) while secondary functions are illustrated with an (S). The table shows how the specific roles for a forensic support function can be embedded into an incident response capability.

Table 5. Roles matrix for incident response and forensics in control systems.

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

The forensics function inside an organization can be designed to support the incident response function, both during and after initial response phases. Those overseeing the forensics investigation will require access to all of the information obtained by the incident response team, as well as all reporting, ideas, and after action activities that have been developed. If the organization is interested in ascertaining if any legal wrongdoing has occurred, the analysis of the evidence will be critical to the organization's wish to advance with prosecution.

The collection of the evidence, as well as the adherence to appropriate chain of custody practices, will be as important in a control systems investigation as in any other cyber forensics investigation. Thus, it is recommended that the organization include members from the forensics team to be active or, at the very least, passive participants in an incident response activity. By doing this, the investigator has a much clearer understanding of the incident from discovery to remediation and can focus on the impacted elements. The team members will include:

Control Systems Incident Manager (CSIM) – This team leader will be responsible for coordinating the response with control systems personnel and those responsible entities who oversee IT operations (and security operations) with the control systems domain. The CSIM will engage for the entire response portion that involved control systems, and will being involvement after the Detection phase. Each of the core activities will be primary except for the Summary Report, with special emphasis on ensuring tactical involvement at all phases of the response. The CSIM will oversee the translation of duties and activities from the primary IR function to the Control Systems Security Specialist (CSSS), the CS Engineering

(CSE) team, and any vendor coordination that is required. The CSIM will interface directly with both the IR Director and the IR Coordinator.

Control Systems Security Specialist (CSSS) – This function will provide critical support from a security perspective, and will aid in both the recovery and mitigation phases of the incident response. The CSSS will also be involved in ascertaining what critical assets may have been impacted, and will work with control systems engineering, vendors, and other members of the incident response team as required. The CSSS will initially have secondary functions during both the Response Initiation and the Forensics Collection phases, migrating to a primary role during the latter part of the incident resolution lifecycle. The CSSS will work closely with both engineers and incident managers supporting both investigation and containment activities, and will have specific tactical activities supporting restoration, reporting, and analysis. This role will also play a significant part in the in-depth analysis of the acquired data and be very familiar with methodologies that can be used to overcome the challenges associated with data collection.

Control Systems Engineering Support – The importance of having control systems engineering support an incident response and forensics function cannot be overstated. As in most control systems, it is the engineering function that understands the control system operation better than anyone understands, and can work effectively with both the primary incident response team and the control system incident manager. Being able to have the control systems engineering capability support primary functions such as containment, recovery planning, and restoration (as well as system upgrade), will provide significant value to both incident response and forensics activity. In addition, it is the control systems engineering function that may be able to facilitate more effective liaising with the vendor community.

Due to the uniqueness of the data and the relationships amongst the information resources in the control systems domain, a team comprised of individuals that have an advanced understanding of the system should complete an analysis of collected evidence. This analysis team needs to be vetted to ensure that there is a low risk of one on the team members being actually involved in instigating, propagating, or trying to conceal the incident.

4. REFERENCES

AGA-12: Cryptographic Protection of SCADA Communications General Recommendations, http://www.aga.org/NR/rdonlyres/B797B50B-616B-46A4-9E0F-5DC877563A0F/0/0603AGAREPORT12.PDF, Web site accessed July 2008.

ANSI/ISA-TR99.00.01, *Security Technologies for Manufacturing and Control Systems*, 2007.

Braid, Matthew, "Collecting Electronic Evidence after a System Compromise," Australian Computer Emergency Response Team, December 2001.

Barrett, Neil, *Computer Forensics Jump Start: Computer Forensics Basics*, Solomon, Sybex Printing, 2005.

Cyber Security Procurement Language for Control Systems Ver. 1.8 http://www.msisac.org/scada/documents/4march08scadaprocure.pdf. Websiet accessed July 2008

Department of Energy, *21 Steps to Improve Cyber Security of SCADA Networks*, http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf, Web site accessed July 2008.

Department of Energy, *Common Vulnerabilities in Critical Infrastructure Control Systems*, http://www.oe.netl.doe.gov/docs/prepare/vulnerabilities.pdf, Web site accessed July 2008.

DHS United States Computer Emergency Readiness Team (US-CERT), http://www.us-cert.gov.

DHS Control Systems Security Program, http://www.us-cert.gov/control_systems/, Web site accessed July 2008.

Electric Power Research Institute, http://www.epri.com/, Web site accessed July 2008.

Executive Order 13231: Critical Infrastructure Protection, http://www.fas.org/irp/offdocs/eo/eo-13231.htm, Web site accessed July 2008.

Federal Energy Regulatory Commission Order 702 Final Rule www.ferc.gov/EventCalendar/Files/20071030162551-RM06-23-000.pdf, Web site accessed July 2008.

Information System Security Association, http://www.issa.org/, Web site accessed July 2008.

Information Systems Audit and Control Association, http://www.isaca.org/, Web site accessed July 2008.

Instrumentation, Systems, and Automation Society, http://www.isa.org/community/SP99, Web site accessed July 2008.

National Association of Regulatory Utility Commissioners, http://www.naruc.org/, Web site accessed July 2008.

NIST PCSRF, http://www.isd.mel.nist.gov/projects/processcontrol/, Web site accessed July 2008.

NIST 2nd Public Draft: Guide to Industrial Control Systems (ICS) Security http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.pdf. Web site accessed July 2008

NIST Special Publication SP 800-53 Revison 1 Appendix I http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf. Web site accessed July 2008

NIST Special Publication SP 800-53 Revision 1 Appendix F Augmented for Industrial Control Systems http://csrc.nist.gov/groups/SMA/fisma/ics/documents/papers/ICS-Augmentation-Appx-F-800-53-rev1_clean_22jun07.pdf. Web site accessed July 2008

North American Electric Reliability Council (NERC), http://www.nerc.com/, Web site accessed July 2008.

Partnership for Critical Infrastructure Security, http://www.pcis.org/, Web site accessed July 2008.

Presidential Decision Directive 63: Critical Infrastructure Protection, http://www.fas.org/irp/offdocs/pdd-63.htm, Web site accessed July 2008.

Process Control Systems Forum (PCSF), http://www.pcsforum.org/, Web site accessed July 2008.

RFC 3227 Guidelines for Evidence Collection and Archiving, http://www.faqs.org/rfcs/rfc3227.html Web site accessed July 2008.

Sandia National Labs Center for SCADA Security, http://www.sandia.gov/scada/home.htm, Web site accessed July 2008.

Thiagarajan, Val, Information Security Management BS 7799.2:2002 Audit Check List for SANS, 2003.

The White House, *Presidential Directive on Critical Infrastructure: Identification, Prioritization, and Protection - HSPD-7*, http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html, Web site accessed July 2008.

The White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, http://www.whitehouse.gov/pcipb/physical.html, Web site accessed July 2008.

The White House, *The National Strategy to Secure Cyberspace*, http://www.whitehouse.gov/pcipb/, Web site accessed July 2008.

Technical Support Working Group (TSWG) SCADA Security Web site, http://www.tswg.gov/subgroups/ps/infrastructure-protection/products.html#, Web site accessed July 2008.

Government of Western Australia Department of the Premier and Cabinet Office of e-Government Forensic Plan, http://www.egov.dpc.wa.gov.au/documents/forensic_plan.pdf. Web site accessed February 2008.