Using a Systems-Theoretic Approach to Analyze Cyber Attacks on Cyber-Physical Systems

by

David Whyte

Submitted to the System Design and Management Program
on January 18, 2017, in partial fulfillment of the
requirements for the degree of
Master of Science in Engineering and Management

Abstract

With increased Internet connectivity and the advent of the industrial Internet, cyber-physical systems are increasingly being targeted by cyber attacks. Unlike, cyber attacks on IT networks, successfully compromising a cyber-physical environment takes considerably more time, motivation, expertise, and operational costs to the adversary.

This thesis explores how a systems-theoretic approach, the Systems-Theoretic Accident Model and Processes (STAMP), can be used by an organization to complement intelligence-driven models of intrusion analysis to provide both additional insight and prioritize defensive countermeasures in order to guard against cyber-physical attacks and compromises.

Specifically, in this thesis we analyze two *real-world* use cases of well publicized cyber-physical attacks using traditional intelligence-driven models of intrusion analysis as well as apply the Causal Analysis based on STAMP (CAST) model on one of the use cases. The STAMP/CAST based analysis afforded us deeper insights into the system causal factors that led to the successful compromise. In turn, this allowed for the generation of specific recommendations to safeguard the cyber-physical systems within the network in order to increase the overall organizational security posture. This included a recommendation to modify the existing organizational structure (i.e., the addition of a Security Operations Centre function) such that clearly defined security roles and responsibilities could be effectively implemented thus significantly improving an organization's ability to respond to cyber attacks.

Thesis Supervisor: Dr. Abel Sanchez
Title: Research Scientist, Massachusetts Institute of Technology

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgments

I would like to express my sincere gratitude to my thesis advisor Dr. Abel Sanchez. I truly appreciated our discussions and your guidance during the thesis process as well as throughout my participation in the Massachusetts Institute of Technology (MIT) Systems Design and Management (SDM) Masters program. To Professor John Williams, thank-you for your support in my research as well as your endorsement for my inclusion into the Lockheed Martin-MIT Fellowship program through the MIT Energy Initiative (MITEI).

On that note, I also wish to thank Lockheed Martin for allowing me to participate in the Lockheed Martin-MIT Fellowship, and in particular Ambrose Kam. He, along with Greg Falco, gave me both valuable feedback and ongoing support for my research. I extend thanks to my SDM cohort with whom I spent many hours and very late nights together working on a multitude of seemingly never-ending opportunity sets. A special thanks to Pallavi, Nissia, Drew, Richard, and Jillian – your support, friendship, and encouragement while on campus made this journey not only interesting but possible.

Last but not least, I am very grateful for the steadfast support and patience of my family. To my wife Michelle and children Carter and Kylie, I can't thank-you enough for allowing me to take this journey and now we can start making up for lost time.

THIS PAGE INTENTIONALLY LEFT BLANK

Contents

THIS PAGE INTENTIONALLY LEFT BLANK

List of Figures

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 1

Introduction

1.1 The Current Cyber Threat Environment

Recent high profile breaches have shown that even Fortune 500 companies with well funded security capabilities and state-of-the-art commercial security products are not able to block intrusion attempts from sophisticated threat actors colloquially referred to as advanced persistent threats (APT). At one time sophisticated targeted intrusions were the exclusive domain of nation states as they possessed the necessary motivation, resources, and technical talent required to penetrate well defended networks. However, this is no longer the case: (1) sophisticated exploit tools/software frameworks are widely promulgated on the Internet at no or low cost thus removing the requirement of high technical skill as an entry barrier, (2) crimeware as a service (CaaS) utilizes state of the art attack tools/techniques available for hire (e.g., Vawtrak financial malware [68]), and (3) outsourcing of vulnerability research means that *zero-day exploits*[1] are commoditized and available for sale. For instance, there are firms that exist today whose business model it is to find vulnerabilities and develop zero-day exploits for popular software products (e.g., Zerodium [69], Exodus Intelligence [20], Revuln [54]). In fact, a zero-day exploit against the latest version of Apple iOS was reportedly available for 1M USD [69].

[1]Exploits that have been discovered in hardware or software which have not been disclosed to the vendor or public and thus there are no detection signatures or software patches available.

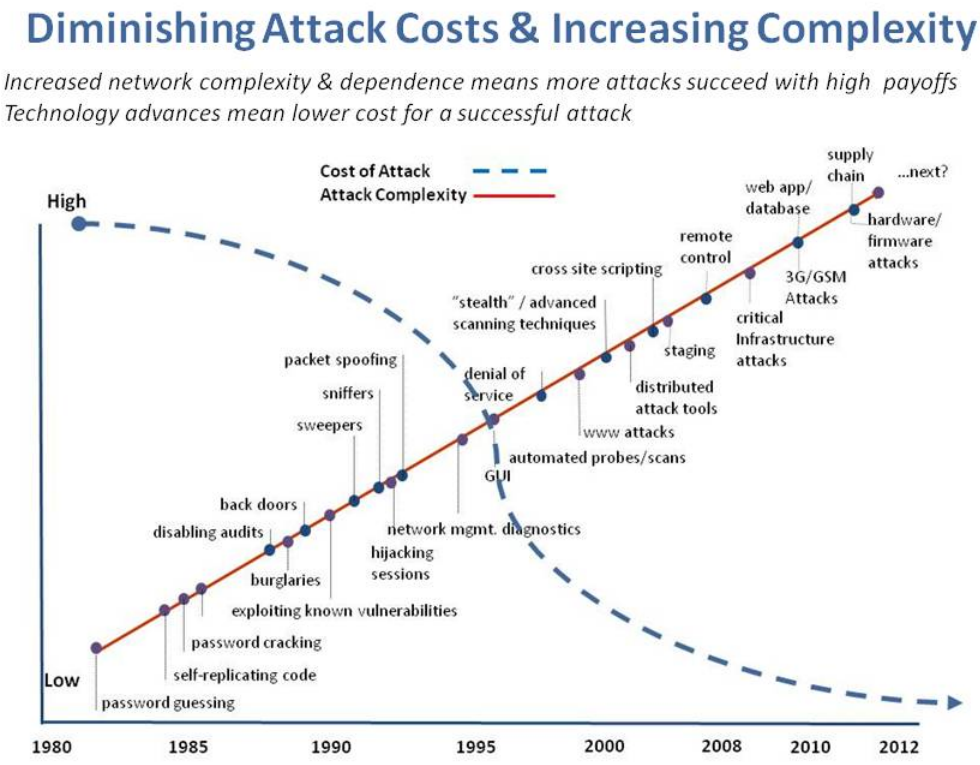

Figure 1-1: Diminishing Attack Costs and Increasing Complexity [29].

In fact, well-financed criminal enterprises with modest budgets can purchase, configure, and automate malware detection test suites comprised of the latest anti-virus software, personal security products (PSPs), and firewalls. As networks become more complex more attacks tend to succeed with a higher potential payout for the attacker (see Figure 1-1).

To rise to the challenge, we must expect that the adversary has a copy of the commercial product(s) we have employed to defend our networks for their own in-house malware testing and are adapting their capabilities to defeat our defensive countermeasures. Accordingly, the cyber threat landscape has become blurred and is outpacing our ability to adequately quantify the threat. The new reality we currently face is that sophisticated attack tools, exploits, and vulnerability knowledge are all becoming democratized. This cyber threat *tradecraft* is no longer the exclusive domain of nation states (i.e., APT) thus it is more appropriate to think of this new

class of threats as the effective persistent threat (EPT).

In order to deal with the current state of the cyber threat landscape, a network defender can adjust their security posture to take into consideration the following approaches:

1. **Tractable network defence postures focus on understanding the interaction/correlation of both internal and external network behaviours**. Modelling the Internet at an enterprise network edge in order to detect malicious activity in isolation is not a tractable security approach. Recent cyber-threats have shown that even state-of-the-art commercial security products are not sufficient to block intrusion attempts from sophisticated threat actors (i.e., APT).
2. **Detection techniques must have the necessary fidelity to enable non-human-in-the-loop automated defences**. Current intrusion detection approaches are flawed because they focus on incoming network traffic looking for malicious behaviour. The issue with this approach is that the volume, velocity, and variety of Internet traffic are all increasing at an exponential rate and thus the current externally-focused defensive strategies are bound to fail. Couple this with the fact that novel intrusions can exploit publicly unknown vulnerabilities (i.e., zero-day exploits) and thus have no observable a priori pattern. More effort is needed to exploit the temporal advantage enjoyed by the network defender (e.g., observation of subtle changes in the network using network/host baselines over time) to develop techniques to observe abnormal lateral networks movements and command and control (C2C) patterns within the enterprise network.
3. **The threat landscape has outpaced our quantification of the threat**. Sophisticated exploits are becoming democratized while sophisticated threat actors are becoming interested in low value information and compute resources. We must address the negative causal link between false positives and false negatives (i.e., the fidelity of detection has to improve to a point where sophisticated automated defensive actions are the norm). Generating an incident report or requiring an analyst to investigate a suspected intrusion attempt is akin to ad-

miring the problem. Although the initial suspected infected system may be identified and remediated, other systems inside the network may now also be compromised (e.g., lateral adversarial movements in the network to establish persistence). This time to action must be minimized by identifying and eliminating (where possible) human-in-the-loop decisions/bottlenecks/transforms. The work force is finite; acceleration of the analytic workflow needs to be leveraged by using systems/processes that are both scalable and repeatable.

4. **Traditional threat risk assessments (TRAs) are broken**. Standard TRA methodologies typically underestimate the threat and, although the process serves to indicate some measure of due diligence has been taken to assess the network security posture, it can amount to a form of security theatre. As previously mentioned, recent high-profile attacks have shown us that: sophisticated adversaries are interested in *low value information*, sophisticated exploit tools/frameworks are widely promulgated at no or low cost, thus removing the requirement of high technical skill as a barrier to entry, and outsourcing of vulnerabilities research means that zero-day exploits are commoditized and available for sale. A state-of-the-art network defence posture must borrow from an attacker's playbook and invoke a *weird machine* paradigm, for example, a heterogeneous deployment of commercial products or non-standard security product deployments to enable a non-standard and thus best of breed detection approach.

1.2 The Current Cyber Threat Environment for Cyber-Physical Systems

As Internet connectivity for cyber-physical systems continues to increase, so to does the risk of targeted cyber attacks[2]. The critical infrastructure that underpins our

[2] "Cyber-Physical Systems or "smart" systems are co-engineered interacting networks of physical and computational components. These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas "[33].

society from electric and water utilities, manufacturers, oil and gas operators often referred to as Industrial Control Systems (i.e., ICS), use complex engineering software systems such as SCADA (i.e., Supervisory Control and Data Acquisition) to operate their equipment. The automation of industrial networks has grown steadily over the last few decades. This automation has been tightly coupled with increased connectivity and depth of Information Technology (IT) penetration with the Internet. Unfortunately, ICS systems were never designed with IT security in mind and thus critical infrastructure such as the electric grid is now vulnerable to cyber attack. In fact, efforts to make the electric grid *greener* is actually increasing the exposure of the electric grid to attack since devices such as smart meters, wind farms, and solar panels add system complexity whilst serving as unprotected portals that offer yet another opportunity for exploitation that can lead to unauthorized breaches.

Recent high profile cyber attacks against ICS networks such as Stuxnet [72], the Saudi Aramco self-replicating virus attack [11], the 2008 BTC pipeline explosion in Turkey [55], and the BSI report of massive damage to a German Steel Mill [73] all highlight the fact that digital attacks are bridging from the virtual world to cause major physical damage. In fact, a number of high profile cyber-physical attacks have occurred over the years as revealed in Figure 1-2.

Despite the fact that these ICS/SCADA networks operate our most vital infrastructures, they are often running on obsolete IT equipment due to the 10-15 year lifecycle of these cyber-physical systems. Many critical operations and processes are being run from management consoles that use unsupported legacy IT (e.g., Windows XP/2000). To exacerbate matters, these networks are now being connected to the Internet (directly or indirectly through corporate networks) and are now being exposed to a wide range of cyber threats that are not traditionally monitored by IT staff and existing cyber security technologies. In fact, a recent study (i.e, project SHINE) has shown that over 2.5M ICS systems are connected directly to the Internet [51]. Figure 1-3 shows a map of the world with a representation of all of the ICS systems that have been located as part of this research project.

A recent report funded by the Energy Department and published by the National

Figure 1-2: Cyber-Physcial Attacks - Selected Historical Incidents [45, 42].

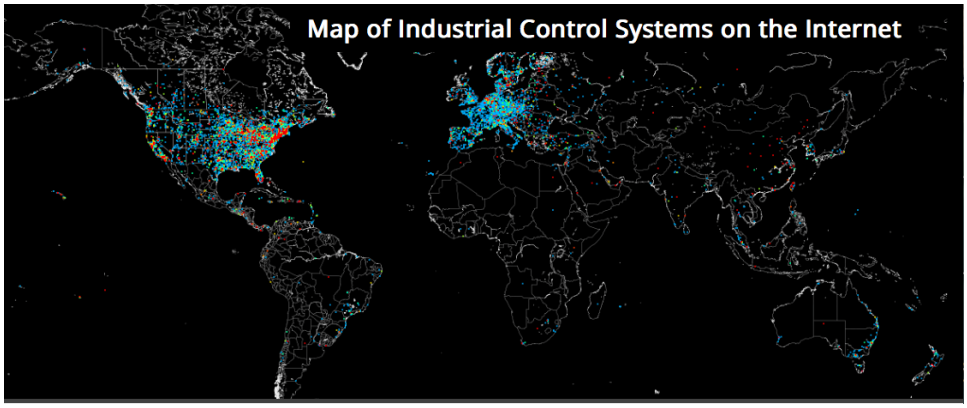

Figure 1-3: World Map of Internet Connected ICS Systems [60].

Electric Sector Cybersecurity Organization Resource, was composed of a group of industry and academic experts focused on improving cyber security practices for the power grid [17]. The report highlighted more than forty ways that nation states or a determined hacker could bypass network countermeasures and gain control of the electric power distribution system. In the past, the IT and Operational Technology (OT) networks that compose the smart grid were physically separate and managed in isolation. The IT network was typically associated with the corporate front-office systems and the OT network was associated with the back-end ICS and deployed systems in the field. Now, IT and OT networks have converged creating complex cyber-physical systems connected to the Internet which allows for increased operational efficiency, rapid connectivity, and cost savings. Unfortunately, this increased convergence has opened new threat vectors for malicious actors that, for the most part, are not being adequately addressed by the organizations and companies that rely on cyber-physical systems.

In Fiscal Year 2015, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) received and responded to 295 incidents reported by asset owners and industry partners [58]. Figure 1-4 shows the breakdown of the reported incidents by sector and the infection vectors respectively used in the incidents.

Of note, the most used infection vector is spear-phishing which involves the victim opening and interacting (i.e., through following an embedded link or opening a malicious file attachment) with a malicious email. This highlights an interesting issue for OT networks. That is, it appears the preferred means to gain access to the OT networks are through vulnerabilities that can be exploited in the IT network. In fact, there have been predictions that by 2020, IT security will be responsible for 25% of physical incidents in ICS environments [65].

Additionally, in 2015, the Dell Security Report revealed that reported SCADA attack incidents have gone from 91,676 in January 2012 to 163,228 in January 2013 and 675,186 in January 2014 [16]. This represents more than a two-fold increase from 2013 to 2014. Figure 1-5 reveals what specific attack methods Dell has observed being utilized by threat actors. In terms of the vulnerabilities available for exploit,

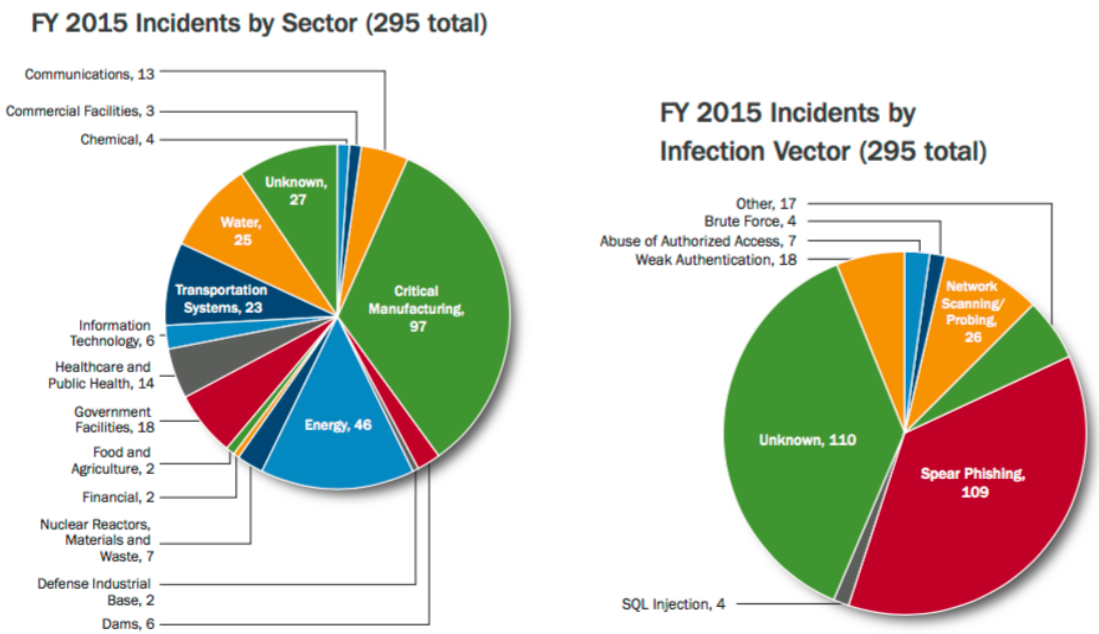

Figure 1-4: ICS Incidents by Sector and Infection Vector [58].

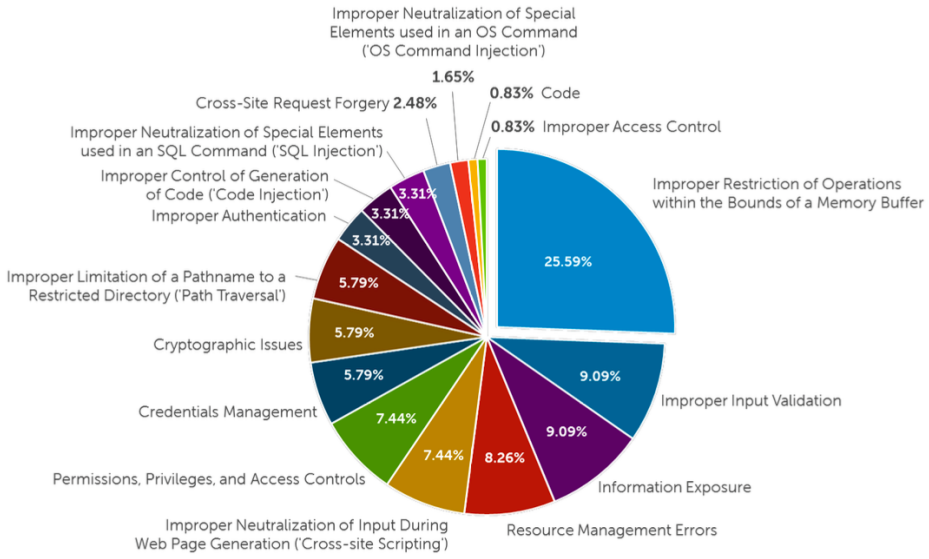

Figure 1-5: SCADA Attack Methods [16].

the Recorded Future Threat Intelligence Report claims that the NIST CVE database contains over 91,500 SCADA/ICS related vulnerabilities [24]. Figure 1-6 shows the mapping of ICS exploits to specific vendors and products.

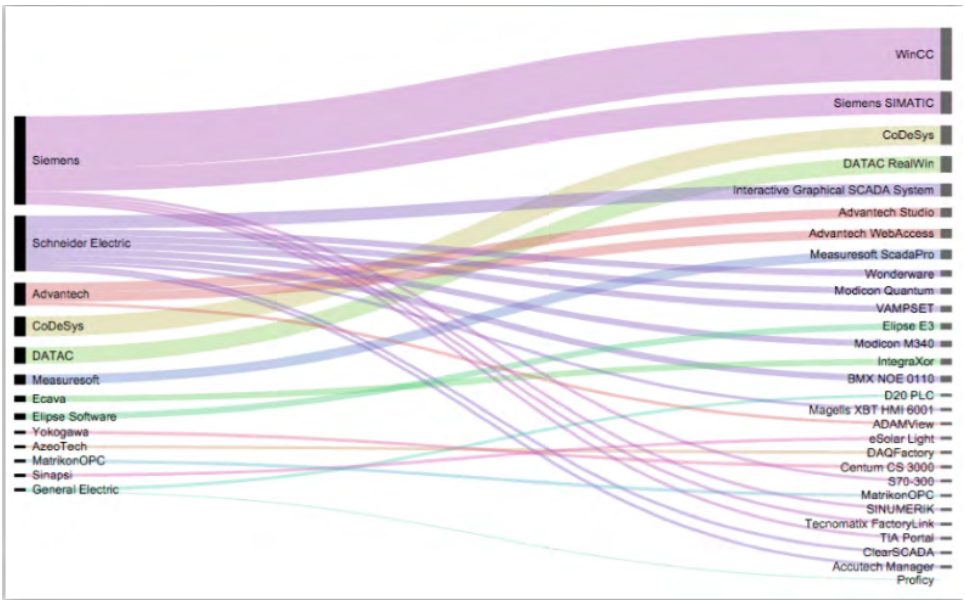

Figure 1-6: ICS Exploits by Vendors and Products [24].

The result of this increased activity is that there is certainly more awareness among cyber-physical system owners that the threat from cyber attack is both real and increasing. As shown in Figure 1-7, in 2016, approximately 24% of respondents perceived the threat of cyber attack to be severe/critical which is greater than a 15% increase when compared with the survey results from 2015 [25].

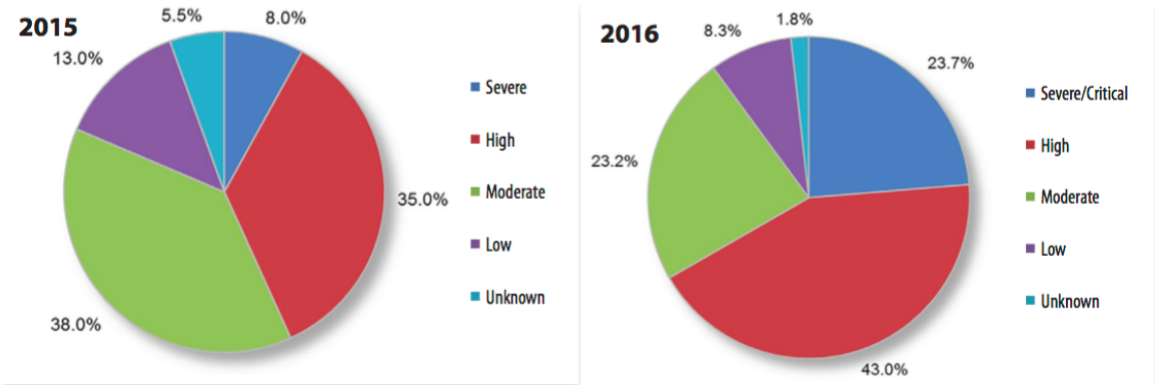

Figure 1-7: Comparison of 2015 and 2016 Perceived Levels of Threat to Control Systems [25].

1.3 Using Systems Thinking to Address the Threat of Cyber Attack to Cyber-Physical Systems

In the following thesis we will analyze two case studies of successful cyber attacks against cyber-physical systems. Furthermore, we will utilize three currently used state-of-the-art cyber attack specific models (i.e., the Cyber Kill Chain®, the ICS Cyber Kill Chain, and the Diamond Model of Intrusion Analysis) in order to more completely understand how the attacks occurred. Although these models (and the respective variants) are very useful in understanding how cyber attacks occur, they do have their weaknesses. Namely, in order to address cyber attacks one must go beyond simply understanding the underlying technology and the environment it operates within.

Cyber attacks involve both technology and people and thus should be viewed from a socio-technical point of view. That is, there are a number of non-technical issues and risks that contribute to the overall conditions that can enable the right conditions for a successful cyber attack. In this thesis, our hypothesis is that these models can both benefit and be significantly complemented by the application of the Systems-Theoretic Accident Model and Processes (STAMP) model (i.e., Causal Analysis based on STAMP (CAST)) to reveal additional insight and expose the root cause of system weaknesses that can aid the network defender in understanding how the breaches occcured.

1.4 Thesis Structure

This thesis is organized into six chapters. Chapter 1 serves as the introduction to the topic and gives the overall structure of the thesis. Chapter 2 contains a literature review covering a number of topics including the Cyber Kill Chain®, the ICS Cyber Kill Chain, the Diamond Model of Intrusion Analysis, STAMP/CAST, and Fault Tree Analysis. Chapter 3 contains two case studies that reveal: (1) potential vulnerabilities of Internet connected cyber-physical systems that can be exploited by a determined

attacker and, (2) a step-by-step analysis of how these attacks occur using the Cyber Kill Chain®, the ICS Cyber Kill Chain, and finally the Diamond Model of Intrusion Analysis. In, Chapter 4 we perform a STAMP/CAST analysis on one of the case studies presented in Chapter 3 with an augmented view on the proximate chain of events through the use of both the the Diamond Model of Intrusion Analysis and the Cyber Kill Chain®. In chapter 5 we extend the recommendations from the STAMP/CAST analysis in Chapter 4 to illustrate how a modified organizational structure (i.e., the addition of a Security Operations Centre function) with clearly defined security roles and responsibilities could improve organizational responses to cyber attacks. Finally we present our conclusions in Chapter 6.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 2

Literature Review

2.1 Cyber Kill Chain®

The Cyber Kill Chain® was developed by researchers at Lockheed Martin to address a perceived gap in traditionally focused incident response methodology [28]. Specifically,

> "A kill chain is a systematic process to target and engage an adversary to create desired effects" [28, pp. 4].

The kill chain concept has been expanded in the digital frontier to address intrusion or computer attack activity. The central tenant to a kill chain is that it is an end-to-end process and any interruption of a particular phase will affect the entire process. Namely, by definition, traditional approaches to tracking computer system intrusions presupposes a successful intrusion. This does not reflect the current cyber threat environment in which very sophisticated adversaries can conduct both multi-year and multi-pronged (i.e., a multitude of exploit vectors) attack campaigns in order to achieve their objectives. Their contention is that if network defenders do not learn from more advanced attacks and adapt then their respective detection and defensive postures, it puts them at both a tactical and strategic disadvantage. They believe that a defensive posture that leverages an *intelligence feedback loop* will allow a network defender to achieve a state of information superiority that will enable them to decrease

the likelihood of an adversary successfully achieving their respective goals.

One way to achieve this feedback loop is to deconstruct the phases of an intrusion in order to map both indicators of compromise (IoCs) and defensive techniques/capabilities to each respective phase. IoCs are used to describe the specific attributes of an intrusion and can be broken into three types [28]:

- **Atomic**: these indicators pertain to artefacts that cannot be broken into smaller components and on their own possess meaningful context about the observed intrusion e.g., IP addresses, domain names.
- **Computed**: these indicators are classified as being computed or derived from the intrusion or incident e.g., a hash computed from a file.
- **Behavioural**: these indicators are typically collections of atomic and behavioural indicators often augmented with combinatorial logic and/or regular expressions.

In their model, an aggressor (or adversary) must develop a method to enter into a trusted environment in order to establish a presence and take actions towards some intent or objective they would like to accomplish in the network (e.g., data theft). In terms of an intrusion kill chain they define it as containing the following phases [28]:

- **Step 1: Reconnaissance**. The attacker obtains information about the structure of the network, personnel, and assets that compose the network.
- **Step 2: Weaponization**. The attacker uses an exploit to create a malicious payload that will exploit an observed vulnerability in the target network/system.
- **Step 3: Delivery**. The attacker sends delivers the malicious payload (e.g., via email, web).
- **Step 4: Exploitation**. The exploit is executed on the victim system and the attacker gains access.
- **Step 5: Installation**. Installing malware on the victim system. This phase can take weeks or months as it may involve expanding access, gaining persistence, and performing internal reconnaissance within the victim network.

- **Step 6: Command and control**. The attacker creates a communication (i.e., command and control channel (C2C)) in order to maintain access to the compromised devices.
- **Step 7: Action on objectives**. The attacker performs the tasks they need to achieve their desired goals in the target network. This step can take weeks or months.

These phases are illustrated in Figure 2-1.

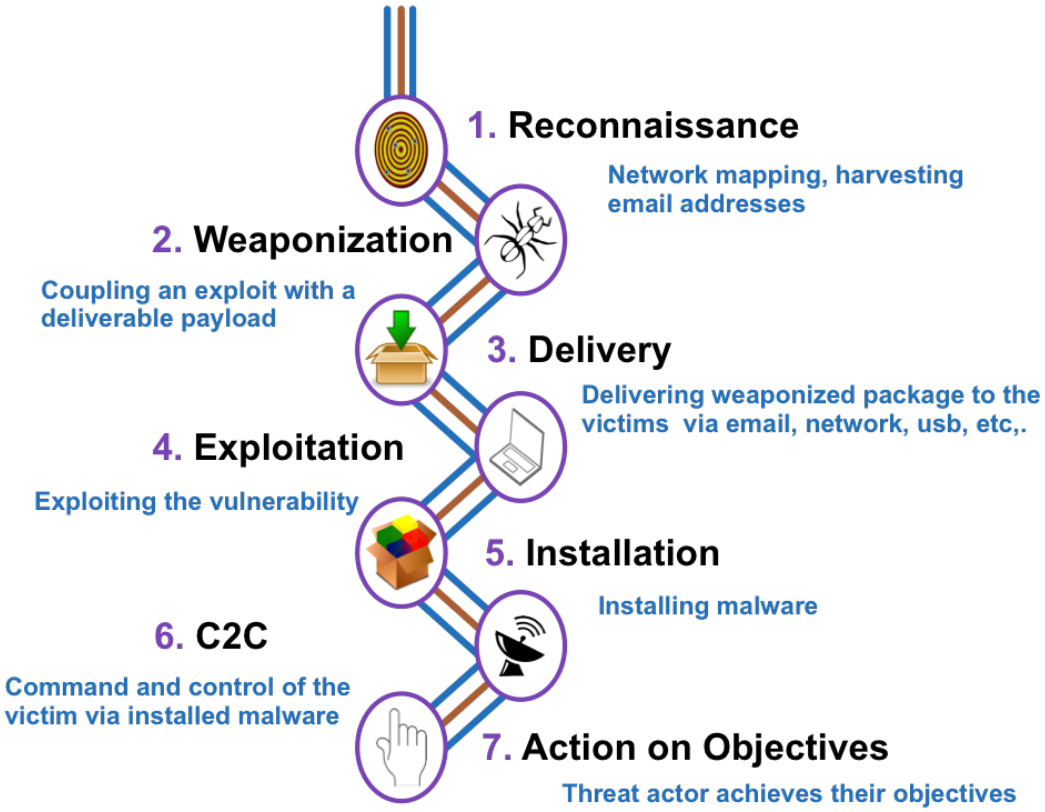

Figure 2-1: Cyber Kill Chain®.

One use of the Cyber Kill Chain® is that it can become an actionable blueprint for a defender to map their respective defences against the discrete kill chain phases. Figure 2-2 reveals a course of action matrix using the actions of detect, deny, disrupt, degrade, deceive, and destroy as outlined in the DoD information operations (IO) doctrine [48].

Application of the matrix is as follows, if we select a phase i.e., reconnaissance, we

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Figure 2-2: Course of Action Matrix [48].

see that we can detect probing attempts at our web server infrastructure by utilizing web analytics to learn about connect attempts (successes and failures) as well as the IP addresses of unique visitors. We can deny reconnaissance attempts by ensuring good firewall rules are in place to restrict access to the network to only allow access to those systems and services we wish to publicly expose.

The Cyber Kill Chain® also offers us a method to perform intrusion reconstruction which we have utilized to analyze our case studies in this thesis. Once an understanding of the adversary is gained by studying their methods, defenders can start to move up the kill chain (i.e., before an exploit is successful) in order to implement defensive courses of action across the kill chain. Adversaries tend to employ similar exploits or reuse C2C infrastructure across victims in order to achieve some sort of economy of scale. Accordingly, defenders can constantly collect information about the adversaries tools and tactics in order to make better defensive decisions.

Finally, at the strategic level, analyzing multiple intrusions over time and mapping them to the Cyber Kill Chain® will allow for the identification of common methods and IoCs. This process can serve to both recognize and link seemingly disparate intrusion attempts into a broader attack campaign that can be then, in some instances, attributed to a single attacker or adversary.

2.2 ICS Cyber Kill Chain

The ICS Cyber Kill Chain was developed by Assante et al. [10] in order to adapt the Cyber Kill Chain® framework [28] to model attacks on industrial control systems. They assert that attacks against ICS systems are different than attacks against IT networks in that the attackers intent, sophistication, capabilities, and familiarization with ICS systems and associated automated processes are indicative of more protracted attack campaigns instead of single opportunistic incidents. Specifically, attacks that can cause significant impact against cyber-physical systems require that the attacker needs to become very familiar not only with the processes being automated but the safety controls engineered into the overall systems themselves in order to cause the desired affects on the system (e.g., circumvent or disable safety mechanisms). Thus, unlike attempting to penetrate an IT network, the specific architecture of the OT network as well as the configuration parameters of the underlying components requires that an attacker have extensive knowledge to be able to impact them both in a predictable and meaningful way [28]. Figure 2-3 reveals the first stage in the ICS Cyber Kill Chain.

The attacker uses this stage to gain initial access to the target network. The authors refer to this as the *cyber intrusion* stage. In this stage, the IT network is used as a means to interact with the victim's network in order to gain access to the OT network. This is typically accomplished by some sort of malware being installed in the network that allows both lateral movement within the network as well as the establishment of a C2C channel. The entire process (i.e., phases) is described in Section 2.1. Once Stage 1 is complete, Stage 2 begins. Figure 2-4 shows the respective phases within stage 2 of the ICS Cyber Kill Chain.

This stage is referred to as the *management and enablement* stage [10] as it represents the necessary groundwork in order to launch a sophisticated ICS attack. ICS Cyber Kill Chain - Stage 2 phases are as follows [10]:

- **Step 1: Develop**. The attacker develops and tunes an attack that is specifically constructed for the victim's ICS implementation.

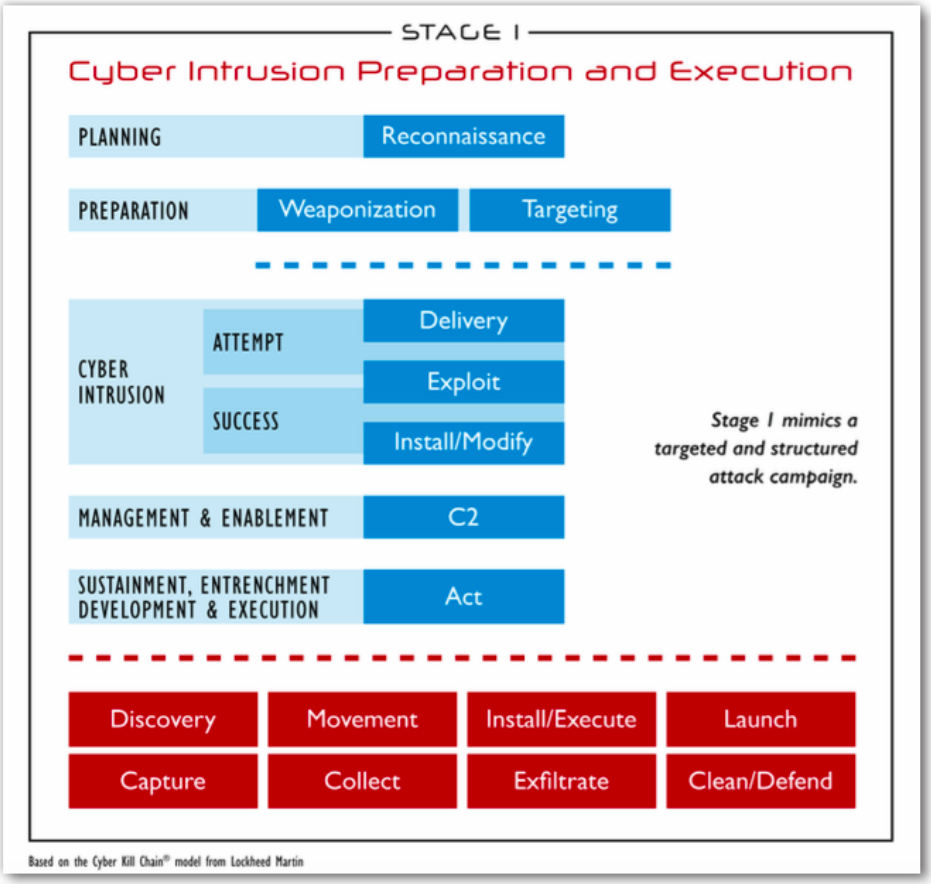

Figure 2-3: ICS Cyber Kill Chain - Stage 1 [10].

- **Step 2: Test**. The attacker makes use of similar or identical ICS software/hardware components outside of the victim's network in order to test their respective actions and/or any modifications they wish to make in the victim's network.
- **Step 3: Deliver**. The attacker delivers the capability by using the access gained in Stage 1 of the attack.
- **Step 4: Install/Modify**. The attacker installs new software or modifies existing system functionality within the environment in order to achieve their desired end state.
- **Step 5: Execute ICS Attack**. The attack is launched.

Unlike traditional attacks on IT networks, compromises on OT networks take considerably more time, motivation, expertise, and cost to successfully execute. It follows that an ICS network would have many more layers (both logical and physical)

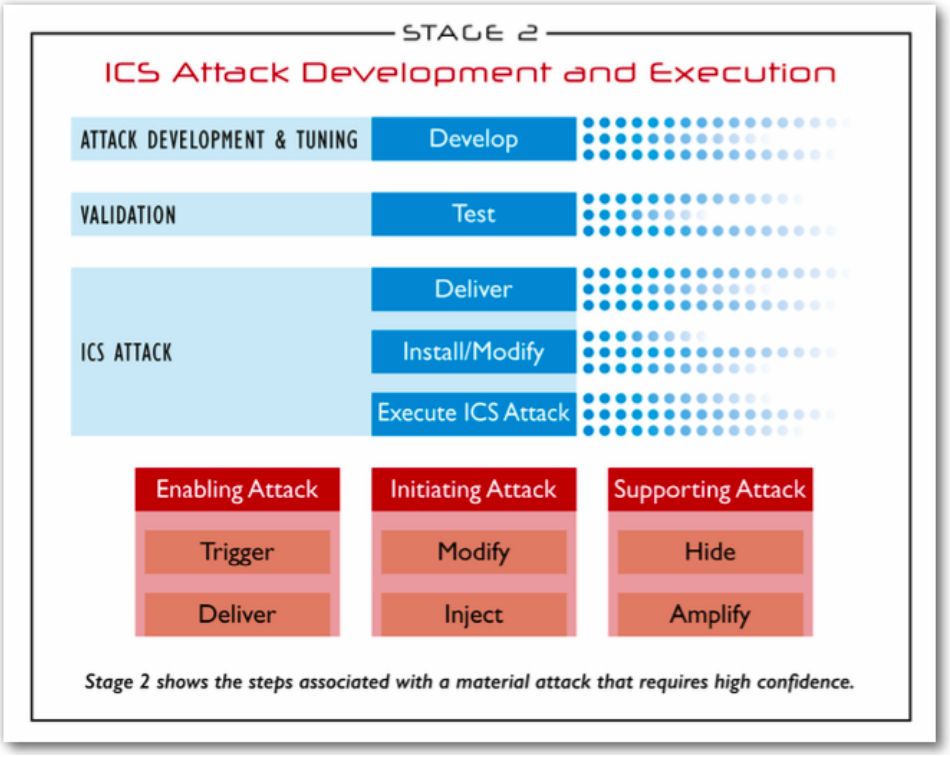

Figure 2-4: ICS Cyber Kill Chain - Stage 2 [10].

that an attacker would have to penetrate and thus there is more opportunity for a defender to detect the malicious activity. However, as mentioned in the previous section, in order to gain increased operational efficiency, rapid connectivity, and cost savings, IT and OT networks are being merged thus opening new exploit vectors for malicious actors. Specifically, directly connecting the OT network to the Internet significantly undermines the security posture of even the most well designed ICS architecture as these environments traditionally were designed with safety (typically physical) not security in mind [74].

2.3 Diamond Model of Intrusion Analysis

The Diamond Model of Intrusion Analysis [12] describes how an adversary uses a capability in an infrastructure against a victim. These activities can be regarded as atomic events that can further be broken down into features. As additional information about the attack is discovered through analysis or new information, new vertices

(i.e., events) can be populated or existing ones refined and updated. Analysts *pivot* across the edges that join vertices in order to learn more about the intrusion as well as explore new hypothesis. An adversary executes a series of events within a set

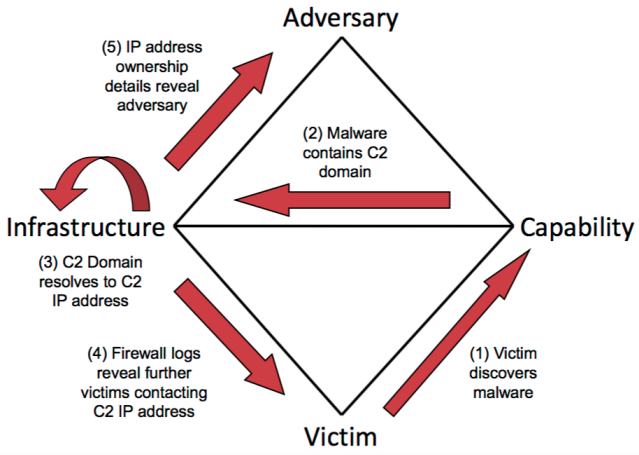

Figure 2-5: Diamond Model - Analytic Pivot [12].

of ordered phases in which each event must be executed successfully in order for the overall objective to be achieved. An *activity thread* is thus defined as:

> "...a directed phase-ordered graph where each vertex is an event and the arcs (i.e., directed edges)..." [12, pp. 30].

Each arc in turn is labeled with attributes including analytic confidence, whether the path is necessary or optional (denoted by AND or OR respectively), whether the analyst regards the arc as actual or hypothesized, and finally a description about the information or resource the preceding event provides that is required for the next event to occur. The vertical threads and any horizontal linkages between them denote the *end-to-end* intrusion activity of the adversary. The threads are organized vertically thus each activity thread is specific to a victim adversary pair. Activity threads are useful to complement the analysis undertaken to construct an attack graph.

> "An Attack Graph is a general formalism used to model security vulnerabilities of a system and all possible sequences of exploits which an intruder can use to achieve a specific goal" [43, pp. 1].

Specifically, attack graphs are used to both identify and enumerate the paths an adversary can take to achieve an objective (i.e., they are exhaustive in nature) while an activity thread defines the actual path the adversary has taken. In many cases, an adversary will demonstrate a preference in the types of activities they perform in order to successfully compromise a victim that will be dictated by the tactics, techniques, and procedures (TTPs) they employ. This is defined as an adversary process [12]. In fact, adversary processes are not typically exclusive to an adversary victim pair but generally encompass the standard intrusion operating procedures or *modus operandi* of a threat actor. Finally, sets of events and activity threads associated by similarities in their features or processes can be categorized and weighed by confidence into an *activity group*. The following six steps are required to create an activity group [12]:

- **Define the Problem**: this is the particular problem trying to be solved by the model.
- **Feature Selection**: event features as well as adversary processes are collected in order to classify and cluster the respective data points.
- **Create**: an activity group is created from the set of events and threads.
- **Grow**: continue to classify events as they are discovered into the model.
- **Analysis**: continual analysis of the activity groups.
- **Redefine:** redefine activity groups as required due to new and/or additional information and events.

The formation of activity groups is typically undertaken to identify a common adversary through the identification and clustering of similar TTPs.

2.4 Fault Tree Analysis (FTA)

> "Fault Tree Analysis (FTA) is a tool for analyzing, visually displaying and evaluating failure paths in a system, thereby providing a mechanism for effective system level risk evaluations" [18, pp. 1].

Specifically, FTA aims to uncover the root cause of a hazard event which can be

overlooked by non-deterministic approaches. FTA was originally developed in 1962 at Bell Laboratories in order to evaluate to evaluate the Minuteman I Intercontinental Ballistic Missile (ICBM) Launch Control System [1]. The fundamental concept of FTA is that a visual diagram and logic model is used to articulate the failure behaviour of a physical system. The visual diagram provides a step-wise decomposition of the system interconnections that allows for deeper qualitative and quantitative analysis in order to uncover the root cause of failure. FTA utilizes a backward looking deductive-based analysis in order to decompose an event (i.e., hazard) into the underlying causes. A hazard is defined by Leveson as,

> "A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss)" [37, pp. 467].

Accordingly, it uses both Boolean algebra and probability theory to implement a series of simple rules thus providing a mechanism for analyzing complex systems. The root node of a fault tree specifies the hazard event under consideration and analysis. FTA is used in order to exhaustively identify the and prioritize the causes of a failure thus uncovering weaknesses in the system. The model serves to provide a repeatable process in order to more fully analyze the event. FTA is a type of Chain-of-Events model that is used to understand the logic that leads to an undesired state. FTA suffers the same limitation that other traditional hazard analysis techniques suffer from in that they do not work well for both human and system design errors [18].

2.5 Systems-Theoretic Accident Model and Processes (STAMP)

Systems-Theoretic Accident Model and Processes (STAMP) is a type of accident model based on systems theory developed by Nancy Leveson [37]. Unlike traditional reliability theory, the STAMP model of accident causation asserts that safety is simply an emergent property that arises when system components interact within a larger

system boundary. Thus, safety is viewed as a control problem [39]. That is, there are a number of safety constraints that manifest themselves not only as physical or technical in nature but also human, organizational, and social that will either enforce (or degrade) the intrinsic safety property of the underlying system. In this paradigm, accidents happen when safety constraints are violated which results in unanticipated and unbounded interactions within the system. That is, the system finds itself in a *hazardous* state due to the inadequate system controls.

This systems-theoretic approach recognizes that accidents often involve very complex and dynamic processes that cannot be adequately modelled by temporally-focused failure event chains. Accordingly, the goal for this model is to allow for more complex relationships to be analyzed (e.g., feedback, control loops, indirect relationships) in order to explore more thoroughly why events occurred. Figure 2-6 shows a typical control loop where a controller obtains process information via feedback from measured variables provided by sensors. The sensors use this information to set control variables that will be provided by actuators to keep the process operating within predefined set points.

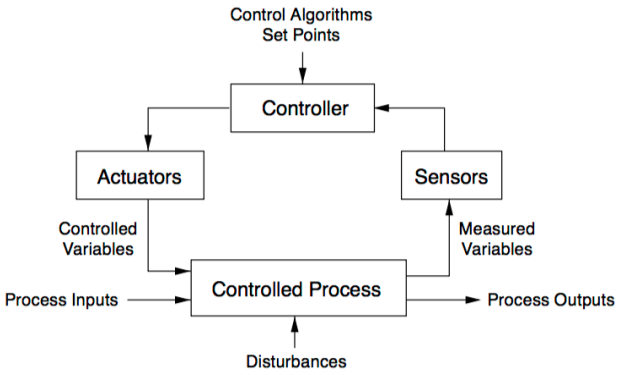

Figure 2-6: Control Loop [37].

Central to this model is the concept of a hierarchical safety control structure which serves to enforce safety constraints in an effort to prevent accidents [38]. In this context, systems are viewed as hierarchal structures where a higher level imposes constraints over the level that is directly below it. Thus, the constraints at a higher level control the behaviour at a lower level and together this should serve provide the

overall enforcement of safety on the entire system.

Leveson et al. offer the four following conditions that must be met in order to have control over a system [39]:

- **Goal Condition**: the controller must have a goal or set of goals in order to maintain safe system operation.
- **Action Condition**: the controller must be able to affect the state of the system in order to keep the process operating within the predefined limits.
- **Model Condition**: the controller must be or contain a workable model of the system.
- **Observability Condition**: the controller must be able to determine the state of the information about the process state provided by feedback.

Accordingly [39, pp. 4],

> Using systems theory, accidents can be understood in terms of failure to adequately satisfy these four conditions: (1) hazards and the safety constraints to prevent them are not identified and provided to the controllers (goal condition); (2) the controllers are not able to effectively maintain the safety constraints or they do not make appropriate or effective control actions for some reason, perhaps because of inadequate coordination among multiple controllers (action condition); (3) the process models used by the automation or human controllers (usually called mental models in the case of humans) become inconsistent with the process and with each other (model condition); and (4) the controller is unable to ascertain the state of the system and update the process models because feedback is missing or inadequate (observability condition).

2.6 Casual Analyst based on STAMP (CAST)

CAST Causal Analysis based on STAMP is a technique that can be used to attempt to fully understand why an accident occurred [37]. This process moves away from a

purely technical focus to a much broader analysis of the entire socio-technical system. The goal of this method is to resist the temptation to assign blame by shifting the focus to why the accident occurred in order to prevent similar losses in the future. Thus, the central tenant to this analysis is that the technique focuses on the question *why* rather than *what* happened. Accordingly, the entire safety control structure is considered in its entirety to locate not only component weaknesses but also the knock-on effects of weaknesses as they affect other components and the entire system as a whole. This shift from simply assigning blame to individuals to understanding the operational environment is a subtle but important distinction. That is, we must assume that people were doing reasonable things but given the complexities and uncertainties in the operational environment unexpected events occur. Therefore, we must dig deeper into the overall root causes [49]. Thus the CAST method strives to uncover weaknesses in the safety control structure that allowed the loss to occur. In order to accomplish this, hindsight bias must be minimized to determine why people behaved the way they did with only the information they had at the time[3].

The steps for STAMP/CAST analysis are defined by Leveson as follows [37, pp. 350]:

1. Identify the system(s) and hazard(s) associated with the accident or incident.
2. Identify the system safety constraints and system requirements associated with that hazard.
3. Document the safety control structure in place to control the hazard and ensure compliance with the safety constraints.
4. Determine the proximate events leading to the accident or incident.
5. Analyze the loss at a physical level. Identify the contributions of each of the following: physical and operational controls, dysfunctional interactions, and communication and coordination flaws. This is done to determine why the physical controls were ineffective in preventing the hazard.
6. Moving up the levels of the safety control structure determining how and why

[3]The perception of the nature of an event after it has happened [44].

each level contributed to the inadequate control at the current level. This includes, but is not limited to, human decisions, flawed control actions, flaws in the process models, and any required information that was not available.

7. Identify and analyze the overall communication and/or coordination failures or anomalies that contributed to the loss.
8. Determine the dynamics and changes in the system and safety control structures that related to the accident or incident, as well as any weakening of the safety control structure over time.
9. Generate recommendations.

Chapter 3

Cyber-Physical System Attack Case Studies

In this chapter we will explore two case studies that serve as illustrative examples of cyber-physical attacks. The first case study involves the compromise and subsequent shut-down of a significant section of a country's energy grid while the second case study reveals a sophisticated multi-vector attack campaign used to perform wide-scale compromise of ICS systems.

Specifically we will:

1. give a high-level overview of the two respective compromises in terms of the TTPs employed by the threat actors.
2. use both Cyber Kill Chain Model® [28] as well as the ICS Cyber Kill Chain, as described in [10] to both map and analyze the intrusion activity.
3. use the Diamond Model of Intrusion Analysis [12] to further analyze the attacks.

3.1 Ukraine Power Grid Attack TTPs - Overview

3.1.1 Ukraine Power Grid Attack Exploit Vectors

On December 23, 2015, the Ukraine power grid experienced a significant disruption. Six Oblenergos (i.e., an oblenergo is defined as a vertically integrated company that

generates, distributes, transmits, and supplies electricity [8]) were simultaneously targeted with a sophisticated cyber attack [67]. While three of the Oblenergos managed to thwart the attack, three of the Oblenergos located in Kyiv, Prykarpattia, and Chernivtsi respectively, experienced unauthorized access to their systems that caused unscheduled and unauthorized circuit breaker activity (i.e., opening and closing) resulting in power disruption [71]. To give an indication of the scale of the attack, in the Prykarpattya Oblenergo alone, a number of substations were taken offline resulting in 103 cities experiencing a blackout condition while another 186 were partially affected [50]. In total, it is estimated that approximately 225,000 customers lost power during this particular incident [36].

In terms of impact on the energy grid, power was lost for six hours with an associated 130 MW load loss [47]. In order to restore power, technicians had to physically be sent to the effected substations in order to switch the substation from automatic (i.e., digital) control to manual control [14, 47]. Exacerbating the situation was the simultaneous launch of a telephony denial of service attack (TDoS) that prevented communications between both power operators and their respective customers. Our following analysis will now focus on one victim, Kyivoblenergo, although the TTPs and intrusion patterns were widely reported to be identical for all other affected oblenergos [71].

Post intrusion analysis reveals this attack all started as a result of a successful phishing attack [71, 36]. Specifically, it is believed that Microsoft Office documents (i.e., Excel and Word) embedded with malware (i.e., BlackEnergy3 [59] were used in the phishing attack [57]. The attack specifically made use of an Object Linking and Embedding (OLE) vulnerability in Microsoft Office (CVE-2014-4114) [31]. A screenshot of the infected document is revealed in Figure 3-1.

Figure 3-2 reveals a high-level overview of the attack in terms of five distinct phases. Namely, exploit, establish foothold, lateral movement, positioning, and execute:

1. **Phase 1 - Exploit**: an attack vector is utilized in order to exploit a system and gain access to the network. In this case it was a phishing attack containing

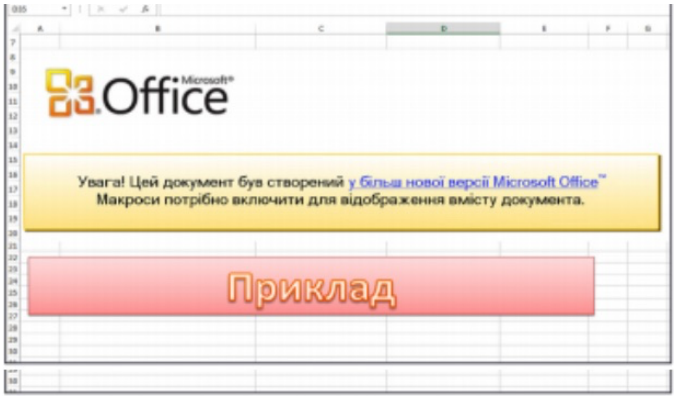

Figure 3-1: Microsoft Word Install Screen.

a malicious attachment. Phishing attacks are still an effective intrusion method —13% of people, on average, will click on a malicious link or an attachment in a phishing email [66].

2. **Phase 2 - Establish Foothold**: Malware is installed in the network (BlackEnergy3) and command and control channels (C2C) are initiated.
   (a) Malware is typically installed in two stages: (1) a malicious program/file called a dropper (first stage) is designed to gain access and install the malware, and (2) the actual payload or malware that is to be installed on the victim system establishing a *backdoor*.
   (b) A backdoor typically allows for an attacker to maintain unauthorized covert C2C with the infected systems.
3. **Phase 3 - Lateral Movement**: The threat actor attempts to compromise other systems in the network in order to maintain persistence.
   (a) Additional accounts and systems are compromised within the network (i.e., this is regarded as *lateral* movement) in order to maintain access.
   (b) Making use of BlackEnergy3 capabilities such as keyloggers, password stealers, network scans, and screenshot stealers.
   (c) VPN credentials are harvested.
   (d) Reconnaissance against the OT is undertaken to identify overall structure and network design.

(e) Access to OT network is undertaken.

4. **Phase 4 - Positioning**: Business processes are observed.

   (a) Business processes are observed over time — custom malware is installed.

   (b) Keyloggers were installed to capture all key strokes and data entry on infected systems.

   (c) Advanced Digital Sciences Center (ADSC) operations shutdown at substations were captured.

   (d) `KillDisk` utility installed on key servers/workstations.

   (e) Custom firmware was installed on Ethernet-to-serial devices Server disconnects were scheduled on uninterruptible power supplies (UPS) via the UPS remote management interface.

5. **Phase 5 - Execute**: The attack is executed.

   (a) Operator workstations were taken over using harvested credentials and malicious software.

   (b) Malicious remote operation of the breakers via virtual private network (VPN) were undertaken to remotely cut power.

   (c) Systems were wiped by executing the `KillDisk` malware at the conclusion of the attack.

   (d) Serial-to-Ethernet devices at substations inoperable by corrupting their firmware.

   (e) A TDoS is launched on the Oblenergo call centre.

3.1.2 Ukraine Power Grid Attack - Overview of Malware

BlackEnergy malware has evolved significantly over time. Reports about BlackEnergy malware were first reported in 2007 by Arbor Networks [46]. BlackEnergy started as an HTTP-based botnet used primarily by the Russian hacker underground for DDoS attacks utilizing a simple communications grammar. The use of HTTP was a departure from most botnets at the time as the vast majority of botnets used IRC to

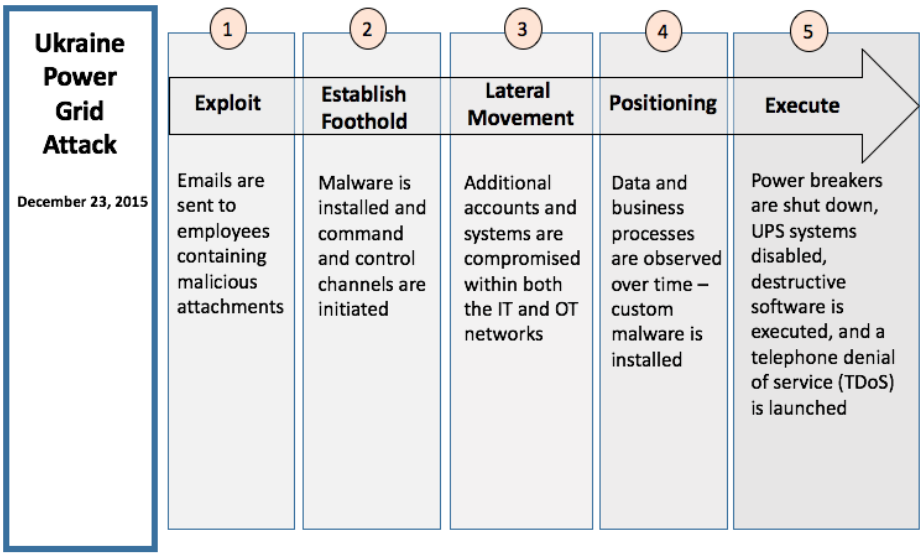

Figure 3-2: Ukraine Power Grid Attack: Intrusion Phases.

communicate.

In 2010, another version of BlackEnergy was released (BlackEnergy2) [62]. The malware experienced a complete code rewrite that made use of a modular architecture making it very easy to repurpose the botnet for spam, fraud, or Distributed Denial of Service (DDoS) attacks. Additionally, the modular architecture allowed for plugins (software updates) with various capabilities that could be downloaded from C2C servers. In this version, a plugin with a `kill` command was available that could destroy the victim's filesystem.

In 2014, BlackEnergy3 first appeared in the *wild*[4]. The changes made to this version were much smaller involving simplifications to the codebase as well as new functionality in specific plugins. One particular plugin that was found to be used in the campaign was called `si` which has colloquially been referred to as steal information. The `si` module will attempt to gather the following information or execute commands and send them to the C2C server [34]:

BlackEnergy3 malware:

1. System configuration information (gathered via `systeminfo.exe`)

[4]In this context *wild* refers to the malware being seen in the public domain.

2. Operating system version
3. Escalate account privileges
4. Current/Up/Idle time
5. Installed apps (gathered from uninstall program registry)
6. Process list (gathered via `tasklist.exe`)
7. Network connections (gathered via `netstat.exe`)
8. Routing tables (gathered via `route.exe`)
9. Traceroute and Ping information to Google (gathered via `tracert.exe` and `ping.exe`)
10. Registered mail, browser, and instant messaging clients (gathered via client registry)
11. Stored username and passwords in web browsers
12. Remote Desktop connectivity
13. Perform data collection e.g., OLE Process Control (OPC) scanner[5]

3.2 Energetic Bear Attack Campaign TTPs Overview

Since the end of 2010, a determined group of threat actors has launched a sophisticated cyber attack campaign targeting a variety of sectors including energy, manufacturing, pharmaceutical, and information technology [35]. A number of cyber threat intelligence vendors in the commercial security community are tracking this activity which is known by a variety of cover names. This includes, Crouching Yeti (Kaspersky [52]), Dragonfly (Symantec [64]), and Energetic Bear (CrowdStrike [15]. The individuals (suspected APT) behind this cyber attack campaign exhibited considerable skill, patience, and deliberate intent in achieving their objectives which appears to be industrial espionage. Henceforth, we will refer to the activity associated with this cyber-attack campaign as Energetic Bear.

Energetic Bear is an interesting case study as it reveals the skill, patience, resourcefulness, and continual tradecraft improvement a determined adversary will go

[5]OPC is a series of standards and specifications for industrial communications [23].

to in order to achieve their objectives. The TTPs changed over time in what can best be described as a series of attacks but an attack campaign against a variety of targets that make use of ICS. Network defenders often subscribe to a defence in depth security posture in order to mitigate IT security risks. This campaign has been described as an *offence in depth* [26].

Specifically, the attack vectors used by the threat actor shifted over time to include: (1) spear phishing, (2) a watering hole attack, and (3) the use of trojanized software updates. We will now describe these types of attacks in detail.

3.2.1 Energetic Bear Attack Campaign Exploit Vectors

The first attack vector used by the threat actor included a spear phishing campaign. An email containing a PDF attachment with a malicious payload (i.e., malware) was sent to at least seven different companies between February 11th and June 19th, 2013 [53]. The targets were executives and senior employees of the companies. Accordingly, the subject lines of the email to entice the recipient to open them were administrative in nature including *The account* and *Settlement of a delivery problem.* In this phase, the exploit used by the threat actor was a PDF/SWF exploit (CVE-2011-0611 [6]) that allowed for the compromise and eventual installation of the Havex trojan [35]. Figure 3-3 show the steps necessary to execute a successful phishing attack.

The second attack vector was a watering hole attack. Watering hole attacks make use of websites that the intended targets are likely to visit which are in fact compromised in order to deliver malicious iFrames[6] which will unwittingly redirect the victim to a malicious server that hosts an exploit kit. Once the infected site is visited, the exploit kit will attempt to install a remote access Trojan (RAT). Figure 3-4 shows the steps in a typical watering hole attack. This attack ran for approximately 11 months from May 2013 until April 2014 [35]. In one instance, the attack used a compromised web site belonging to a law firm that works with energy companies to serve malicious iFrames to redirect them to the attackers sites that used the LightsOut

[6]An iFrame is an inline HTML frame that can embed another HTML object/document into the current HTML document

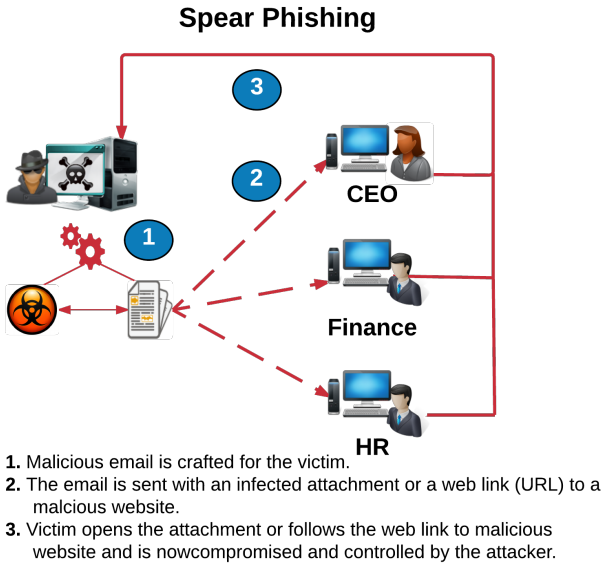

Figure 3-3: Exploit Vector: Spear Phishing Attack.

exploit kit (LOEK) to compromise their machines [21]. The LOEK checks to see whether: (1) a vulnerable version of Java is running (CVE-2013-2465) [9], (2) Internet Explorer is the browser (CVE-2012-4792)[7], and (3) if the version of Adobe Reader installed is vulnerable to an attack.

The third and perhaps the most interesting attack was the use of trojanized software downloads[7]. In this attack, trojanized software installers are modified to contain malicious code (i.e., a trojan horse) that is bundled into legitimate software download. Three different ICS suppliers had their respective websites compromised and the threat actor was able to inject malware into ICS utilities, drivers and software updates that were then accessed by targets via *unauthenticated* software downloading that required no registration [35]. In most cases the malware was injected into 32-bit and 64-bit versions of their respective drivers for the Windows and in some cases Linux operating systems. In this way, the threat actor was able to install malware into devices that were likely not susceptible to web-based watering hole or spear phishing exploit vectors.

[7]A trojan horse or trojan software is a type of malware that is often disguised as legitimate software [32].

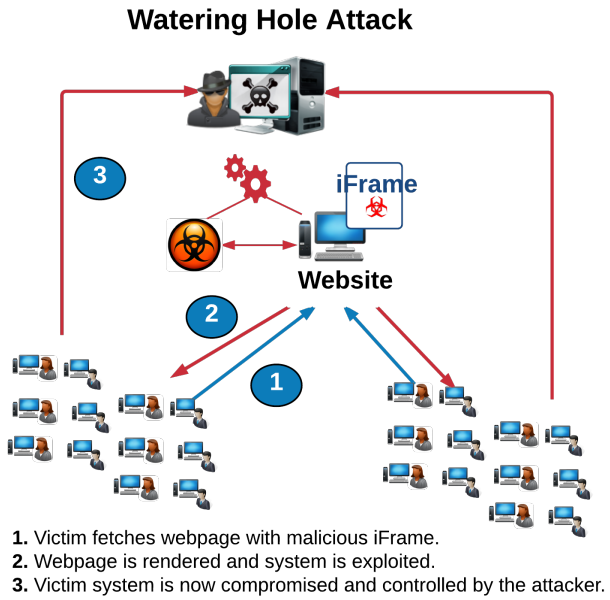

Figure 3-4: Exploit Vector: Watering Hole Attack.

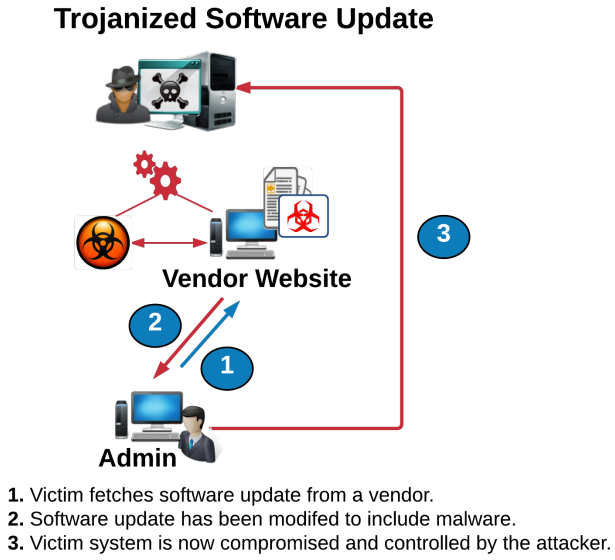

Figure 3-5: Exploit Vector: Trojanized Software Download.

3.2.2 Compromised ICS Vendors

Three ICS vendors were targeted in the Trojanized software download attack namely, eWON [1], MB Connect Line [4], and Mesa Imaging (Mesa Imaging has since been acquired by Heptagon [3])[27]. The first vendor known to have their software replaced with a trojanized version by Energetic Bear was the Swiss company MESA Imaging, who manufacture industrial grade cameras. Their cameras make use of *time of flight* (TOF) technology to render three-dimensional images. These industrial cameras are used in a number of specific sectors including robotics, healthcare, security and transportation.

eWON is a Belgian company that provides a remote maintenance service for ICS systems called `Talk2M`. In fact, two different software components were targeted in this attack [27]. The first was an application that provided Internet-based remote access (eCatcher version 4.0.0) using an application based on their `Talk2M` solution. The second application was a VPN client (eGrabit v 4.0.0) again based on their `Talk2M` solution. Of note, both these software components were made available to customers without registration, authentication or any MD5 hashes to check if the software had been tampered with [2].

Figure 3-6: Install Screens for eWON, Mesa Imaging, and MB Connect [27]

In the aftermath of the attack, eWON released the following statement,

> "The eWON commercial website `www.ewon.biz` has been attacked. A corrupted `eCatcherSetup.exe` file has been placed into the CMS (Content Management System) of `www.ewon.biz` website and eCatcher download hyperlinks have been rerouted to this corrupted file. The corrupted

> `eCatcherSetup.exe` contains a "Trojan" virus which can impact the Talk2M account access security" [19].

MB Connect Line offers a product that is similar and competitive with the eWON product line used for remote machine communications access and service. They released the following statement on their website,

> "The files `mbCHECK` (Europe), `VCOMLAN2` and `mbCONFTOOL` have been replaced with infected files. These files were available from 16th of April 2014 to 23th of April 2014 for download from our website. All of these files were infected with the known Trojan Virus Havex Rat. F-Secure informed us about this incident, after a user uploaded the infected `mbCHECK` software to their LAB portal to analyze it" [40].

Figure 3-7 reveals a high-level overview of the attack in terms of five distinct phases. Namely, exploit, establish foothold, lateral movement, positioning, and execute:

1. **Phase 1 - Exploit**: An attack vector is utilized (in this case it was a trojanized download attack) in order to exploit a system and gain access to the network. The threat actor compromised a number of vendor sites replacing legitimate software update packages with malicious (i.e., trojanized) software they believed would be downloaded by the *true* or intended victims.
2. **Phase 2 - Establish Foothold**: Malware is installed in the network (Havex Trojan) and C2C channels are initiated.
   (a) Malware is typically installed in two stages: (1) a malicious program/file called a dropper (first stage) designed to gain access and install the malware code, and (2) the actual payload or malware that is to be installed on the victim system establishing a *backdoor*.
   (b) A backdoor typically allows for an attacker to maintain unauthorized covert C2C with the infected systems.
3. **Phase 3 - Lateral Movement**: The threat actor attempts to compromise other systems in the network in order to maintain persistence.

   (a) Additional accounts and systems are compromised within the network (i.e., this is regarded as *lateral* movement).
   (b) Making use of Havex malware capabilities such as keyloggers, password/contact stealers, and undertaking network scans.
   (c) Reconnaissance against the OT is undertaken to identify overall structure and network design and access sensitive production information.

4. **Phase 4 - Positioning**: Business processes are observed and exfiltrated.
   (a) Business processes are observed over time — custom malware is installed in order to exfiltrate data.
   (b) Keyloggers were installed to capture all key strokes and data entry on infected systems.
   (c) The internal network is scanned to locate and identify ICS devices.
5. **Phase 5 - Execute**: The attack is executed.
   (a) Sensitive and proprietary production information is taken from the victim network.

3.2.3 Energetic Bear Attack Campaign - Overview of Malware

The threat actors behind Energetic Bear campaign used malware consisting of three different types of remote access Trojans (RATs) in their campaign: (1) Havex, (2) Karagany, and (3) Sysmain. The Havex RAT was the most widely used malware in the Energetic Bear campaign [35]. As with most RATs, the prime objective of this collection of malware was to maintain persistence on the target once installed, communicate to C2C servers, install additional software modules, and perform tasks for the threat actors. The three variants of malware used in the attack and the associated functionality is as follows [35, 52]:

1. Havex malware

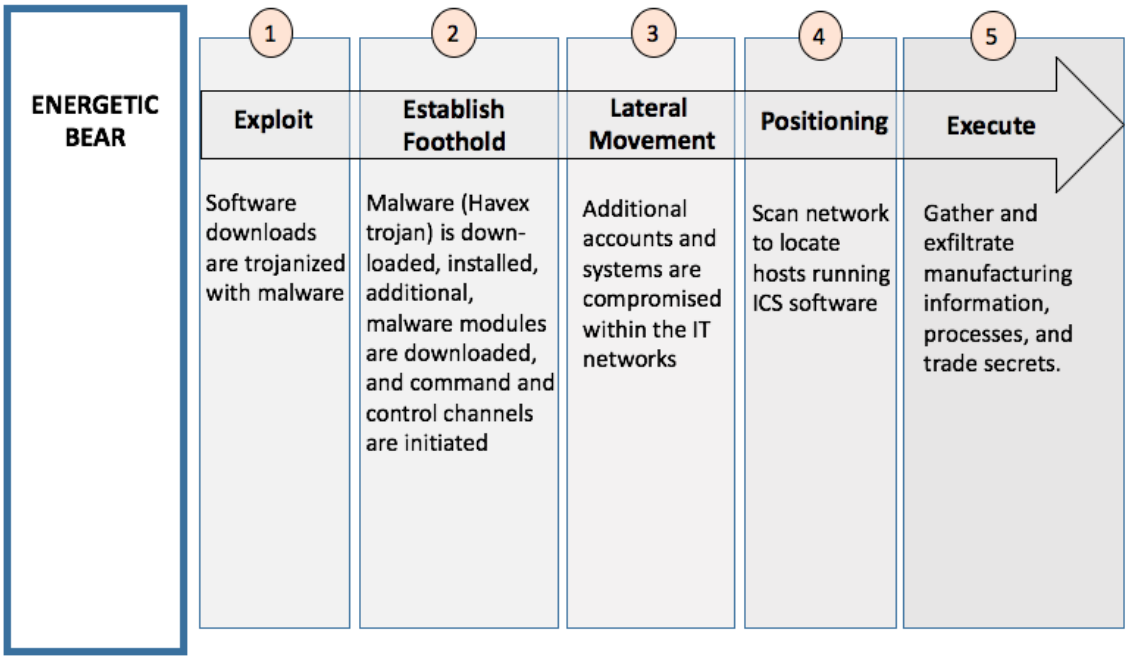

Figure 3-7: Energectic Bear Malware (Havex): Intrusion Phases.

(a) Ability to establish a C2C channel

(b) Victim identification, enumeration, and enrolment

(c) Install additional software modules to update malware functionality

(d) Perform network scanning to identify both IT and OT systems

(e) Contacts and password stealer

(f) Perform data collection e.g., OPC scanner

2. Karagany malware:

(a) Ability to establish a C2C channel

(b) File upload, download, and execution

(c) Self-updating capabilities

(d) Monitors software in order to extract basic authentication credentials sent over unencrypted HTTP sessions

(e) Take screenshots on the victim systems

(f) List files with specific names or extensions

3. Sysmain malware:

(a) Execute shell commands

(b) Ability to establish a C2C channel

(c) Launch executables and libraries (e.g., additional software modules)

(d) Examine the victim's file system

(e) Collect arbitrary files on the computer

(f) Registry key modification to remove evidence of infection

(g) Change the hard coded public key used for asymmetric encryption

The Havex malware was the most widely used during the attack campaign that infected as many as 2,470 victims with multiple versions of the malware [52]. It appears that this attack, unlike other ICS attacks [14, 73], was created in order to undertake espionage. Specifically, the main goal of these attacks appears to be for the purposes of counterfeiting technology or competitive intelligence rather than destruction of the industrial control systems it infected. Activities such as the identification and theft of proprietary recipes, production batch sequence steps, network and device information were undertaken in order to determine sensitive proprietary information such as manufacturing plant volumes and capabilities [35].

3.3 Cyber Kill Chain® Analysis

The Cyber Kill Chain® is used to enhance visibility into an attack and enrich an analyst's understanding and defensive decision-making processes in response to the TTPs used by the adversary. The ICS Cyber Kill Chain, as described in [10, 36] is an enhancement of the Cyber Kill Chain® that recognizes that ICS-custom cyber attacks require significant knowledge of the processes being automated as well as the specific physical system(s) being targeted including software configuration, and overall cyber-physical system architectural design.

3.3.1 Ukraine Power Grid Attack ICS Cyber Kill Chain Analysis

Tables 3.1 and 3.2 respectively reveal the specific adversary activities for the Ukraine Power Grid Attack broken out into the phases of the ICS Cyber Kill Chain.

Table 3.1: Ukraine Power Grid Attack ICS Cyber Kill Chain - Stage 1

Phase	**Description**
Reconnaissance	Although there were no observed (detected) reconnaissance activities observed prior to the attack(s), the level of coordination needed to penetrate both the number of Oblenergos as well as specific substations within the individual entities suggest a targeted versus opportunistic attack.
Weaponization	In this instance it is believed that Microsoft Office documents (i.e., Excel and Word) embedded with BlackEnergy3 malware were used for a phishing attack [57]. The attack specifically made use of an Object Linking and Embedding (OLE) vulnerability in Microsoft Office (CVE-2014-4114) see Figure 3-1 [31]. In fact, this type of attack vector was used in a wide-scale attack campaign against organizations located in Ukraine including those in the energy sector [13].
Delivery	Email with malware embedded in attachments were sent to the target organizations.
Exploitation	The malicious email and accompanying attachments were opened whereupon popups appeared that asked for the user to enable Office macros.
Installation	The user(s) enabled the macros and the malware was installed.
Command and Control	Once the malware was installed, a number of command and control servers were contacted on the Internet.
Action on Objectives	Internal reconnaissance inside the network to: (1) map the internal network structure, (2) identify ICS systems, and (3) compromise additional systems in order to maintain persistence. User credentials are harvested in order to gain unauthorized access to additional systems.

Table 3.2: Ukraine Power Grid Attack ICS Cyber Kill Chain - Stage 2

Phase	**Description**
Develop	Understand how to operate the distribution management systems (DMS) in the target environments, understand operator-focused processes, and develop custom firmware for the serial-to-ethernet devices.
Test	Given the success the adversary had executing the attack campaign, it is highly probable that testing of their respective capabilities (e.g., modified firmware) occurred before the attack [36].
Deliver	The adversary used the IT/OT access gained in Stage 1 via VPN accesses in order to deliver themselves into the target environment.
Install/Modify	Install modified `KillDisk` across the environment. Install modified firmware against serial-to-ethernet devices at substations. Schedule disconnects for the UPS system.
Exploitation	Using HMIs in the SCADA environment, breakers were opened, malicious firmware was uploaded/activated, and a TDoS was performed in order to stop customers from notifying the operators how extensive the outage had become.

3.3.2 Energetic Bear Attack Campaign Cyber Kill Chain® Analysis

As described in Section 3.2.3, the Havex malware contained an OPC scanner that was used to do reconnaissance in the internal network looking for ICS/SCADA systems. OPC is an interoperability standard that allows interaction between HMI/SCADA systems using the Windows operating system or other ICS applications and process control hardware [23]. Variants of the Havex malware were used to gather system information and data stored on a compromised client or server using the OPC standard [30]. The malware did not directly impact the performance of ICS systems nor is there any evidence that it installed itself on mission-critical ICS hosts [35]. Specifically, the unauthorized access was restricted to the IT network including those computer sys-

tems that interacted with the OT network (i.e., SCADA and ICS systems) and not the ICS components directly. Accordingly, these attacks can be modelled using the traditional Cyber Kill Chain®, instead of the ICS Cyber Kill Chain, as described in [10, 36]. We now focus our analysis on one of the attack vectors in the campaign i.e., the trojanized software download attack.

Table 3.3: Cyber Kill Chain® Energetic Bear Attack Campaign

Phase	**Description**
Reconnaissance	Specific websites were targeted for compromise based on the intended (true) victims.
Weaponization	Legitimate software update bundles for ICS related systems are modified and repackaged with malware (i.e., trojan malware).
Delivery	Victim visits vendor's website and downloads trojanized software updates.
Exploitation	Software updates are opened executed on the target devices of the *true* victims.
Installation	Trojanized software is installed on the system.
Command and Control	Once the malware was installed, a number of command and control servers were contacted on the Internet.
Action on Objectives	Internal reconnaissance is undertaken inside the network to: (1) map the internal network structure, (2) identify ICS systems, and (3) compromise additional systems in order to maintain persistence. Information gathering activities are started to understand proprietary business processes.

3.4 Diamond Model of Intrusion Analysis

As outlined in Section 2.3 the Diamond Model of Intrusion Analysis [12] describes how an adversary uses a capability in an infrastructure against a victim. Specifically, an adversary executes a series of events within a set of ordered phases in which each event must be executed successfully in order for the overall objective to be achieved. Recall, that an *activity thread* is

> ...a directed phase-ordered graph where each vertex is an event and the arcs (i.e., directed edges)..." [12, pp. 30].

In the following sections we will analyze both the Ukraine Power Grid Attack and the Energetic Bear Attack Campaign using the Diamond Model of Intrusion Analysis. We will expose: (1) adversary processes for instance, in Figure 3-8, events 1 to 5 inclusive show a successful phishing attack that culminates with the victim communicating with the adversary's C2C node as well as, (2) sets of events and activity threads associated by similarities in their features or processes that we subsequently categorize into *activity groups* i.e., specifically in the Diamond Model of Intrusion Analysis of the Ukraine Power Grid Attack use case.

3.4.1 Ukraine Power Grid Attack - Diamond Model of Intrusion Analysis

Figure 3-8 shows the Ukraine power grid attack analyzed using the Diamond Model of Intrusion Analysis. We have chosen to generate an activity group based on: (1) the victim (Kyivoblenergo), (2) infrastructure (C2C nodes), and (3) capability used by the threat actor (specific variant of BlackEnergy3). We have used the Diamond Model of Intrusion Analysis to consider the overall attack as an activity group that is partitioned into adversary processes (see Figure 3-8). The adversary processes that compose the activity group include:

1. **IT Network Compromise**: gain access to the IT network in order to compromise the OT network.
2. **OT Network Compromise**: gain access to the OT network and perform follow-on actions for the planned attack.
3. **Power Outage**: execute the power outage.
4. **Disable Hardware**: execute attack on both computer systems (`KillDisk`) and power system hardware using malicious software (modified serial-to-ethernet firmware).
5. **Digital Lock-out**: remove legitimate administrator access from IT systems.

6. **Analog Lock-out**: execute a TDoS attack.

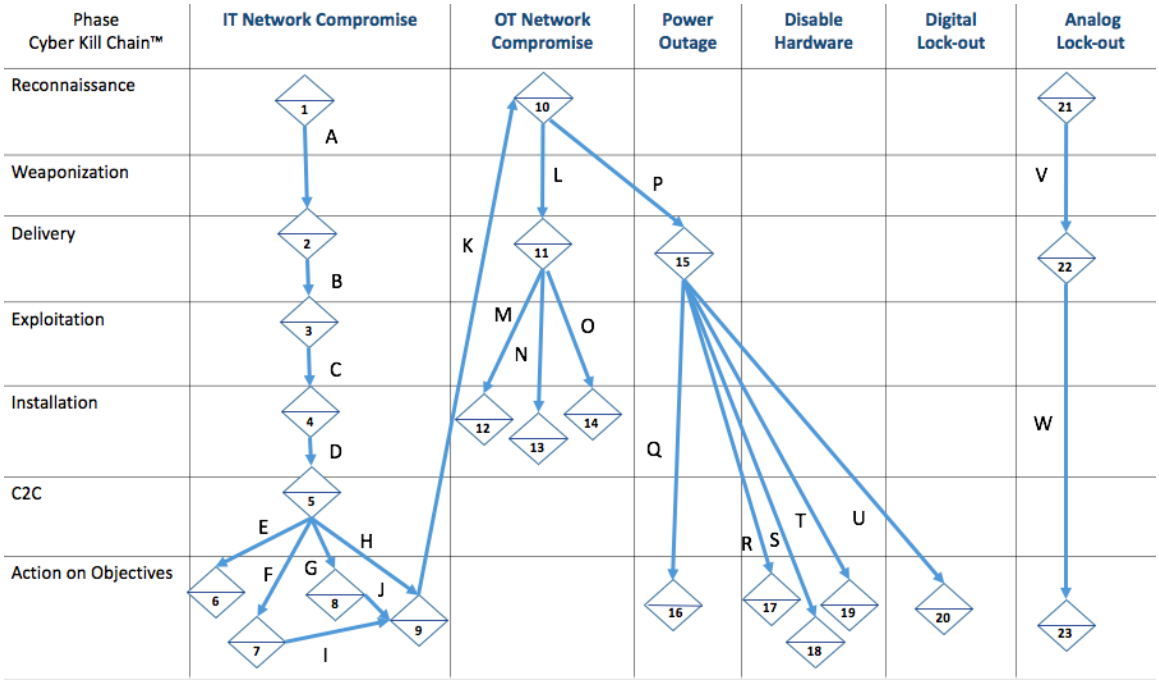

Figure 3-8: Diamond Model Activity Group Partitioned into Adversary Processes.

Figure 3-9 shows an example of the level of detail that can be attributed to the specific events (i.e., diamond number 4) within the activity group. Furthermore, the atomic events in the activity group are categorized using the phases of the Cyber Kill Chain® (i.e., left-most column of Figure 3-8).

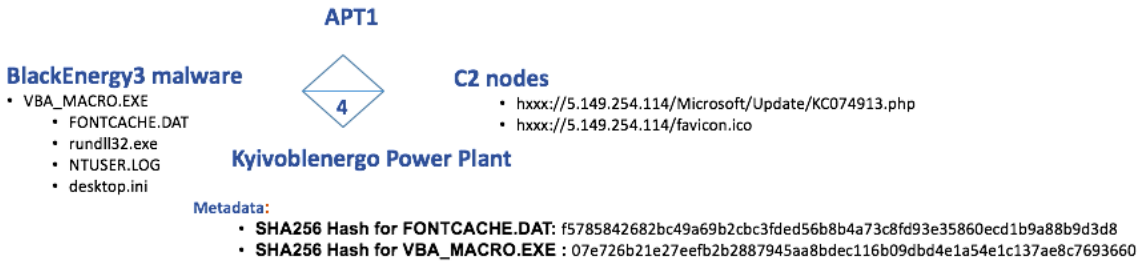

Figure 3-9: Sample Diamond Analysis - IoCs taken from [59].

Table 3.4 shows the Activity Thread Event Descriptions for the activity group while Table 3.5 shows the Activity Thread Arc Descriptions.

Event #	Verified	Description
1	Hypothesis	Adversary conducts open source intelligence.
2	Actual	Adversary sends a spear-phishing email with a trojanized attachment to employees from `info@ukrenergo.energy.gov.ua`.
3	Actual	One or more employees opens the malicious attachment executing the enclosed exploit allowing for unauthorized code execution (BlackEnergy3).
4	Actual	Malware is installed – BlackEnergy3.
5	Actual	C2C nodes are established.
6	Hypothesis	Lateral movement in the network to gain access to the active directories, create/harvest account credentials, maintain presence, keylogging, password grabs, and screenshots are taken.
7	Actual	Harvest valid VPN credentials.
8	Hypothesis	Learn business processes, ADSC operations and identify ICS networks.
9	Actual	Use VPN credentials to access ICS network.
10	Hypothesis	Scan ICS network to gain knowledge of both IT and OT networks and discovery of field devices, such as serial-to-Ethernet devices.
11	Actual	Access ICS dispatch servers and workstations using stolen credentials.
12	Actual	Upload and install `KillDisk` software on key workstations/servers and RTUs.
13	Actual	Schedule disconnects for server Uninterruptible Power.
14	Actual	Upload and install firmware to Serial-to-Ethernet devices.
15	Actual	Use VPN credentials to log into ICS network.
16	Actual	Turn off breakers using compromised HMIs in the ICS environment and cause a power outage.
17	Actual	`KillDisk` wiping of workstations, servers, and an RTU.
18	Actual	Windows-based human-machine interfaces (HMIs) embedded in remote terminal units overwritten with `KillDIsk`.
19	Actual	Render serial-to Ethernet substations inoperative.
20	Actual	Lock system administrators out of their respective accounts.
21	Hypothesis	Power plant call centre numbers are gathered.

Continued on the next page

Table 3.4 – continued from previous page

Event #	Verified	Description
22	Hypothesis	A war dialling application is used to make numerous calls to the call centres.
23	Actual	Telephone denial of service (TDoS) is executed.

Table 3.4: Activity Thread Event Descriptions: Ukraine Power Grid Attack.

Arc	Confidence	And/Or	Hypothesis/Actual	Provides
A	High	AND	Hypothesis	Provides a targeted list of email addresses for the phishing attack.
B	High	AND	Actual	[None]
C	High	AND	Actual	[None]
D	High	AND	Actual	[None]
E	High	AND	Actual	[None]
F	High	AND	Actual	[None]
G	High	AND	Actual	[None]
H	High	AND	Actual	[None]
I	High	AND	Actual	Provides VPN Credentials.
J	High	AND	Actual	IP addresses of ICS systems.
K	High	AND	Actual	Provides VPN Credentials.
L	High	AND	Actual	IP addresses of ICS systems.
M	High	AND	Actual	[None]
N	High	AND	Actual	[None]
O	High	AND	Actual	IP addresses of ICS systems.
P	High	AND	Actual	[None]
Q	High	AND	Actual	[None]

Continued on the next page

Table 3.5 – continued from previous page

Arc	Confidence	And/Orl	Hypothesis/Actual	Provides
R	High	AND	Actual	[None]
S	HIgh	AND	Actual	[None]
T	High	AND	Actual	[None]
U	High	AND	Actual	[None]
V	High	AND	Actual	Provides call centre phone numbers.
W	High	AND	Actual	[None]

Table 3.5: Activity Thread Arc Descriptions: Ukraine Power Grid Attack.

To complete our analysis, the Ukraine Power Grid Attack involved a multi-stage and determined attack against a cyber-physical system that is best modelled using the ICS Cyber Kill Chain. Thus, in order to complete the mapping between the Diamond Model of Intrusion Analysis and the ICS Cyber Kill Chain, Stage 2 of the ICS Cyber Kill Chain is revealed in Figure 3-10. Within the diagram, there are a series of dashed diamonds specifically in the develop and test phases. These dashes indicate that these activities most likely took place within a space under the attackers control (e.g., lab) and thus are unobservable to the network defender (i.e., therefore we consider these to be hypothesized activities).

3.4.2 Energetic Bear Attack Campaign - Diamond Model of Intrusion Analysis

Table 3.6 shows the Activity Thread Event Descriptions as a result of our analysis while Table 3.7 shows the Activity Thread Arc Descriptions. Finally, Figure 3-11 shows the Energetic Bear attack trojanized software download attack analyzed using the Diamond Model of Intrusion Analysis.

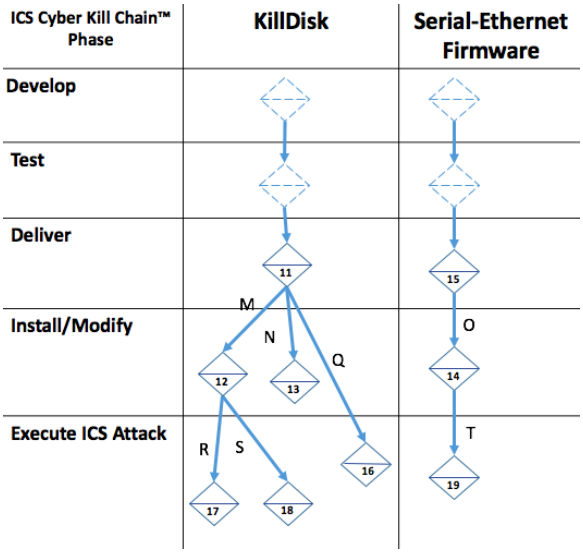

Figure 3-10: Diamond Model of Intrusion Analysis - ICS Cyber Kill Chain - Stage 2

Event #	Verified	Description
1	Hypothesis	A spear phishing campaign is used to conduct an information gathering exercise to determine the ICS vendors used by the victims.
2	Actual	Adversary compromises an ICS vendor's website in order to inject malicious code into a legitimate software update (i.e., trojanized software update).
3	Actual	Victim downloads trojanized software update.
4	Actual	Victim installs trojanized software update - Havex.
5	Actual	Malware C2C nodes are established.
6	Actual	Malware software modules are installed.
7	Hypothesis	Lateral movement the network to gain access to the active directories, create/harvest contact information, maintain presence, keylogging, and password grabs.
8	Hypothesis	Scan OPC network to locate hosts running SCADA software.
9	Hypothesis	Gather and exfiltrate intelligence about business information, proprietary processes, and manufacturing plant volumes and capabilities.

Continued on the next page

Table 3.6 – continued from previous page

Event #	Verified	Description

Table 3.6: Activity Thread Event Descriptions: Trojanized Software Download Attack.

Arc	Confidence	And/Or	Hypothesis/Actual	Provides
A	High	AND	Hypothesis	A list of ICS vendor websites used by the victims.
B	High	AND	Actual	[None]
C	High	AND	Actual	[None]
D	High	AND	Actual	[None]
E	High	AND	Actual	[None]
F	High	AND	Actual	[None]
G	High	AND	Actual	[None]
H	High	AND	Actual	[None]

Table 3.7: Activity Thread Arc Descriptions: Trojanized Software Download Attack.

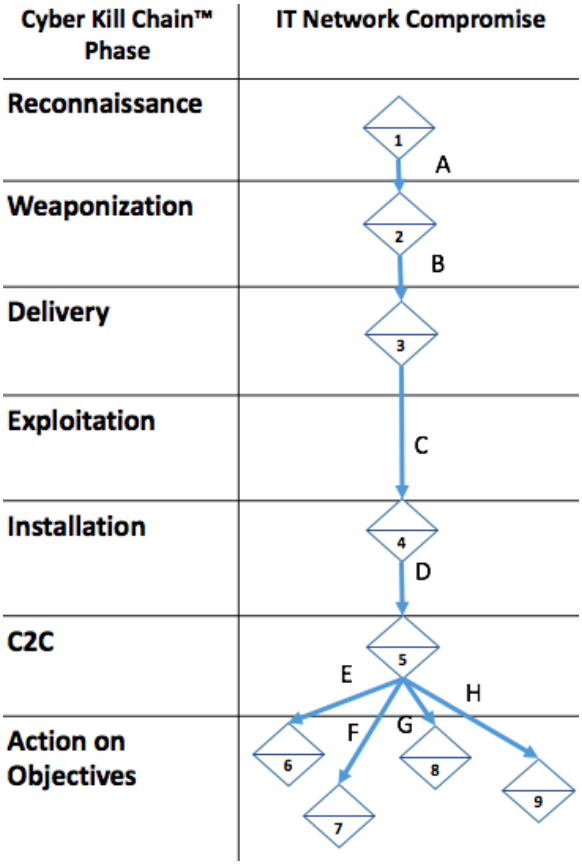

Figure 3-11: Cyber Kill Chain® Trojanized Software Download Attack.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 4

STAMP/CAST Analysis of the Energetic Bear Attack Campaign - Trojanized Software Download

In order to explore how systems theory and systems thinking can assist on how to deal with the threat of cyber attacks in cyber-physical systems, we will undertake Leveson's STAMP/CAST [37] analysis using our understanding of the Energetic Bear campaign gained from the examination in Section 3.2 as a reference. Recall from Section 3.2.1 that there were three sets of victims caused by three different exploit vectors. Specifically, these were firms that were compromised during a phishing attack, some that were exploited using drive-by download techniques (watering hole attack), and those that downloaded malicious software updates (i.e., trojanized) from compromised vendor sites.

In reality, any one of the three attack scenarios would have made good candidates for our STAMP/CAST analysis. However, we selected the trojanized software update attack as it allowed us to examine not only the security procedures involving software and the overall IT product life cycle (i.e., patching) but also the requirement for security-focused operational monitoring of the network. Thus, our focus will be on the attack from the point of view of a company attempting to download and install a (unbeknownst to them) malicious software update.

Specifically, our scenario will involve: (1) the analysis of a cyber attack involving a victim downloading trojanized software from a *trusted* website, (2) we will make use of a fictitious medium-sized firm in the energy sector[8] that makes use of industrial control systems as part of their production chain, and (3) this fictitious company will be loosely based on an actual client of one of sites infected with trojanized software updates [5] as described in Section 3.2.1.

Overview of STAMP/CAST. As described in section 2.6 the steps for STAMP/CAST analysis defined by Leveson are as follows [37, pp. 350]:

1. Identify the system(s) and hazard(s) associated with the accident or incident.
2. Identify the system safety constraints and system requirements associated with that hazard.
3. Document the safety control structure in place to control the hazard and ensure compliance with the safety constraints.
4. Determine the proximate events leading to the accident or incident.
5. Analyze the loss at a physical level. Identify the contributions of each of the following: physical and operational controls, dysfunctional interactions, and communication and coordination flaws. This is done to determine why the physical controls were ineffective in preventing the hazard.
6. Moving up the levels of the safety control structure determining how and why each level contributed to the inadequate control at the current level. This includes, but is not limited to, human decisions, flawed control actions, flaws in the process models, and any required information that was not available.
7. Identify and analyze the overall communication and/or coordination failures or anomalies that contributed to the loss.
8. Determine the dynamics and changes in the system and safety control structures that related to the accident or incident, as well as any weakening of the safety control structure over time.
9. Generate recommendations.

[8]Victim identities in all the Energetic Bear reports were protected so we do not know the actual identity of the firms that downloaded and installed the trojanized software.

In the following sections we will discuss each of these steps in detail using our case study as the subset of analysis.

4.1 Systems and Hazards Identification

In our case study, malicious threat actors were able to carefully install malware into vendor sites that they knew their targets would download and install in their networks. In order for this type of attack to be successful, a number of cyber security gaps had to have existed that reveal deviations from industry best practice in the victim network that: (1) allowed malicious software to be installed, and (2) *ex-post* malware installation there were no mechanisms or processes in place to identify compromised or anomalous system behaviour.

In this section, we will identify and analyze the specific system (i.e., a specific component) in the overall hierarchical system safety structure where the systemic failures manifested themselves to allow malware to be installed in the network. We will also identify the system hazards associated with the incident.

System. New software updates are a necessary and integral part of any software system's overall product life cycle, proper functioning, and overall security posture. In this scenario, malicious software was downloaded from a vendor's site and installed by the IT and OT engineers into the corporate network. This resulted in the compromise of not only the system with the software update but subsequent systems within the network as the threat actors attempted to expand access within the network by identifying and compromising additional vulnerable systems.

To understand how malicious software could be downloaded by the IT/OT staff as well as remain undetected post installation, we will examine the **Servers and Services** component (see Figure 4-2) that is responsible for coordinating all operational aspects of the the hardware and software on both the corporate and industrial networks.

Hazard. The hazard that is being avoided is that the IT and OT systems within the network must **avoid both unauthorized and untrusted software instal-**

lations. In this case, malware that infected the system(s) in the network were downloaded and installed by authorized IT personnel that assumed (i.e., trusted) the vendor's software updates and processes were secure.

4.2 System Safety Constraints and System Requirements

1. The software update process must guard against the installation of modified and malicious software (i.e., malware).
2. Adequate security processes need to be in place to identify and prevent: (1) *ex-ante*: malware from being installed, and (2) *ex-post*: quickly identify and contain systems that have been infected with malware.

4.3 Hierarchical System Safety Control Structure

4.3.1 Overview

The hierarchical control structure for this company can best examined by considering two main functionally discrete but interrelated areas namely, the IT and OT domains. Specifically, both the IT and OT domains are comprised of the Management and Operations layers respectively. These two functional areas, in turn, all reside under the auspices of the Systems Management layer. We will now discuss the safety control structures for the system as well as the feedback mechanisms to gauge both the effectiveness of the controls as well as the ability of the overall system to adapt to changes in the environment (i.e. in this case resilience to cyber attacks).

4.3.2 Hierarchical Control Structures

The three firms that were the initial victims of the Energetic Bear trojanized software update attacks (i.e., Mesa Imaging, MB Connect, and eWon) had a number of attributes in common. Specifically, they were small companies (i.e., according

to Linkedin they all ranged in size from 11 to 50 employees), they were targeted not for access to their company assets per se but the access they would afford to the *true targets* i.e., the much bigger companies that were their customers. In this regard, the compromised companies allowed a trust relationship to be exploited in order for a malicious third party to gain unauthorized access to their customer networks. Accordingly, we examined a number of companies that were the customers of these initial three victims focusing on the energy sector (i.e., oil and gas). Although there have been various reports of hundreds of companies compromised as a result of downloading the trojanized software update none were publicly named [53, 64, 35]. Accordingly, after looking at the typical profile of victim companies [53] we created, based loosely on our observations, what we believed to be a typical management, operational, and production environment of a compromised company.

Company's Hierarchal Control Structure. The legend shown in Figure 4-1 (best viewed in colour) identifies the meaning of the various symbols, and lines in Figure 4-2. Specifically, a grey box denotes the components. The numbers represent the naming taxonomy of the control and feedback flows for a component which forms a loop. The physical process is delineated by a dashed blue oval. Grey arrows denote the interactions amongst components an upward arrow represents feedback whilst a downward arrow denotes control flows. The entire system boundary is represented by a dashed red lines. The system in this case represents the company that has been the victim of a cyber attack (i.e., downloading trojanized software) for which we are performing a CAST analysis.

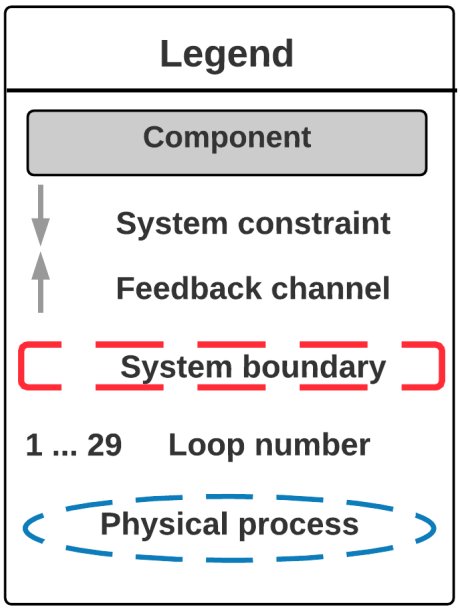

Figure 4-1: Legend

The physical processes is the starting point for the CAST analysis. In our scenario, the physical process we will analyze is found at the **Servers and Services** component that provides hardware (e.g., compute and storage) and software services to: (1) the IT operations component and (2) the workstations and consoles component within the OT environment. Recall that the management consoles within the OT environment that have the necessary HMI interfaces to control, and monitor the physical systems are typically windows OS based and rely on external software updates for proper functioning of both the operating systems and installed applications. This software update process will be analyzed in detail in section 4.6.2.1. We will now discuss the hierarchal system safety control structure in detail as illustrated in Figure 4-2. A summary of the system components associated controls and feedback is contained in Table 4.1.

Starting at the Servers and Services component we see that it interacts with both with the IT Operations component (loop # 19) and the Workstations and Consoles component (loop # 24). Specifically, the IT Operations component provides control to the Servers and Services component in terms of levying system requirements and administration services (including software updates or patching) while the Servers and Services component provides feedback in terms of providing data storage, software, compute resources, authentication, and logs to the IT Operations component. That is, in order to run the daily operations requests for servers must be provisioned and maintained, identification and authentication services must be provided (e.g., active directory, LDAP), and software must be both installed and updated. A subset of these same services are also provided to the Workstation and Consoles component as feedback which is falls under the OT Operations area. In turn, the Workstations and Consoles component also provides control in terms of day-to-day administration as well as system requirements.

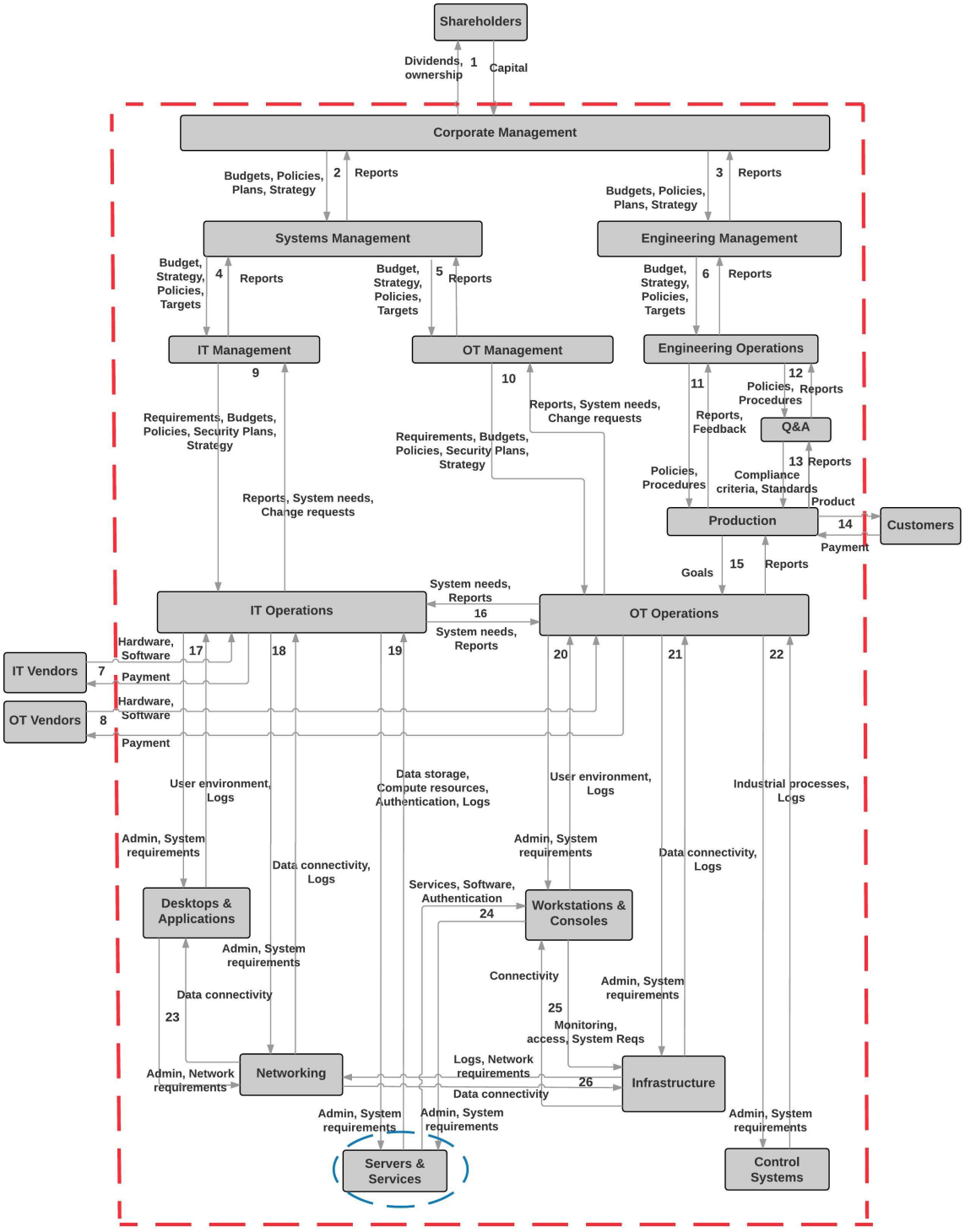

Figure 4-2: Hierarchical Control Structure.

The Networking component is responsible for providing the backbone networking infrastructure on which the IT and OT systems interact. It connects with the Desk-

tops and Applications component (loop #23), the IT Operations component (loop #18), and the OT Infrastructure component (loop #26). The Networking component provides feedback in terms of implementing and providing data connectivity to the Desktops and Applications component as well as the OT Infrastructure component while they, in turn, provides control in terms of day-to-day system administration, system requirements and logs. Specifically, as new systems and/or applications are needed this may have impact on not only the required minimum latency in the network but also data rates.

The Networking component not only provides data connectivity but also logs to the IT Operations component as feedback. Additionally, the IT Operations component controls the Desktop and Applications component (loop #17) via administration and system requirements while it is provided feedback in terms of a user environment and logs. The IT Operations component makes use of logs collected from all relevant components in order to monitor and ensure the proper operation and functioning of the IT systems. The IT Operations component provides administration and system requirements (i.e. control) to the Networking component and has a more global view based on log inputs/aggregation on the health and status of the overall network.

On the lower left side of Figure 4-2 the OT Operations component provides a layer of control over the Work Stations & Consoles component (loop #20), the OT Infrastructure component (loop #21), and the Control Systems component (loop # 22). The OT Operations component provides control to these components by means of administration and system requirements. The Work Stations & Consoles component provides feedback to the OT Operations component by providing a user environment and logs based on the interpretation of the system requirements it has been given. The OT Infrastructure component is responsible for the physical and logical interfaces required to ensure the OT equipment is accessible to the other systems in the network that needs to interact with one another. Accordingly, we see that the OT Infrastructure component connects to both the OT Operations component and the Networking component (already discussed - loop #26). The Networking component provides feedback via connectivity services and logs to the OT Operations component

while receiving feedback in the form of administration and system requirements. The Control Systems component is responsible for the interfacing between the systems that operate the equipment that carry out physical processes. The Control Systems component provides feedback via industrial processes and logs to the OT Operations component. The Work Stations & Consoles component provides control to the OT Infrastructure component (loop #25) by providing monitoring and access while receiving feedback in the form of connectivity. That is, the physical workstations and management consoles that allow the operators to use the software to monitor the systems are provided by this component.

At the next level of control, we see that IT Operations and OT Operations (loop #16) which provides both system needs and reports to each component as control and feedback respectively. These components interact closely with one another as the smooth operation of one component relies on the other given the convergence of IT and OT systems (i.e., cyber-physical systems) that enable overall production to occur. IT and OT vendor components interact with the IT and OT Operations components respectively. Specifically, IT Vendors provide software and hardware to IT Operations (loop #7) as feedback while control is provided in the form of payment and continued orders from the IT Operations component. The same applies for OT vendors which provide software and hardware to OT Operations (loop #8). Control, again, is provided in the form of payment and continued orders. Next level up in the hierarchy is IT and OT Management components. IT Management is responsible for the setting the overall operational requirements, distributing budgets, security plans and the IT strategy (loop #9). Feedback is given from the IT Operations component in the form of reports, system needs, and change requests. In turn, OT Management is responsible for the setting the overall operational requirements, distributing budgets, security plans and the OT strategy (loop #10). Feedback is given from the OT Operations component in the form of reports, system needs, and change requests.

Next level in the hierarchy is the Production component that is responsible for the overall oversight regarding the output of the physical product manufactured by the company. It controls output by setting and promulgating goals and receives feedback

from OT Operations by way of reports (loop #15). Loop #14 represents the interaction between Production and Customers. The company produces products (control) which in turn are purchased by customers with payment (feedback). Loop#13 represents the interaction between the Q&A (quality assurance function) with the Engineering operations component. Q&A provides control in the form of compliance criteria and standards while feedback is provided from Production to Q&A in terms of quality reports.

Next level in the hierarchy is Engineering Operations component that is responsible for overseeing the overall day-to-day engineering related aspects of the production process (i.e., OT). It interacts with the Production component (loop #11) and the Q&A component (loop #12). Engineering Operations provides policies and procedures to the Production component and receives reports and feedback on production activities as feedback. In fact, the exact same control/feedback interactions happens with the Q&A component.

At the next level in the hierarchy we have the Systems management and Engineering management components. The Systems Management component is responsible for overseeing all the budget, strategy, policies and targets for both the IT management and OT management components. It exerts overall management control over the IT and OT areas within the company (loops #4 and #5 respectively). In turn, the Systems Management component receives feedback in the form of reports from the two components. Finally at the top of the hierarchal control structure is the Corporate Management Component that interacts with both Systems Management and Engineering Management via loops #2 and #3 respectively as well as shareholders (external to the system boundary) using loop #1. Corporate Management provides budgets, policies, plans, and strategies to both System Management and Engineering Management while receiving reports as feedback. Shareholders provide capital to Corporate management and receive as feedback dividends and ownership of the company. Table 4.1 contains a listing of all the interactions between the components.

Loop #	**Structure**	**Control & Feedback**
1	Shareholders ↔ Corporate Mgt	Control: Capital. Feedback: Dividends, Ownership.
2	Corporate Mgt ↔ Systems Mgt	Control: Budgets, Policies, Plans, and Strategy. Feedback: Reports.
3	Corporate Mgt ↔ Engineering Mgt	Control: Budgets, Strategy, Plans and Budget. Feedback: Reports.
4	Systems Mgt ↔ IT Mgt	Control: Budgets, Policies, Strategy, and Targets. Feedback: Reports.
5	Systems Mgt ↔ OT Mgt	Control: Budgets, Policies, Strategy, and Targets. Feedback: Reports.
6	Engineering Mgt ↔ Engineering Ops	Control: Budgets, Strategy, Policies, and Targets. Feedback: Reports.
7	IT Vendors ↔ IT Ops	Control: Payments. Feedback: Hardware, Software.
8	OT Vendors ↔ OT Ops	Control: Payments. Feedback: Hardware, Software.
9	IT Mgt ↔ IT Ops	Control: Requirements, Budgets, Policies, Security Plans, and Strategy. Feedback: Reports, System Needs.
10	OT Mgt ↔ OT Ops	Control: Requirements, Budgets, Policies, Security Plans, and Strategy. Feedback: Reports, System Needs.
11	Engineering Ops ↔ Prod	Control: Policies, Procedures. Feedback: Reports, Feedback.
12	Engineering Ops ↔ Q&A	Control: Policies, Procedures. Feedback: Reports.
13	Q&A ↔ Production	Control: Compliance criteria, Standards. Feedback: Reports.

Continued on the next page

Table 4.1 – continued from previous page

Loop #	Structure	Control & Feedback
14	Production ↔ Customer	Control: Product. Feedback: Payment.
15	Production ↔ OT Ops	Control: Goals. Feedback: Reports.
16	IT Ops ↔ OT Ops	Control: System needs, Reports. Feedback: System needs, Reports.
17	IT Ops ↔ Desktop Apps	Control: Admin, System requirements. Feedback: User environment, Logs.
18	IT Ops ↔ Networking	Control: Admin, System requirements. Feedback: Data connectivity, Logs.
19	IT Ops ↔ Servers and Services	Control: Admin, System requirements. Feedback: Data storage, Compute resources, Software, Authentication, Logs.
20	OT Ops ↔ OT Workstations & Consoles	Control: Admin, System requirements, Reports. Feedback: User environment, Logs.
21	OT Ops ↔ OT Infrastructure	Control: Admin, System requirements. Feedback: Data connectivity, Logs.
22	OT Ops ↔ Control Sys	Control: Admin, System requirements. Feedback: Industrial processes, Logs.
23	Desktop Apps ↔ Networking	Control: Admin, Network requirements. Feedback: Data connectivity.
24	OT Workstations & Consoles ↔ Servers & Services	Control: Admin, System requirements. Feedback: Services, Authentication, Software.
25	OT Workstations & Consoles ↔ OT Infrastructure	Control: Monitoring, Access, System requirements. Feedback: Connectivity.
26	Networking ↔ OT Infrastructure	Control: Logs, Network requirements. Feedback: Data connectivity.

Table 4.1: Hierarchical Control Structure.

4.4 Proximate Event Chain

We have seen through the analysis of the two case studies presented in Section 3 that attack campaigns against cyber-physical systems are typically executed in stages and may take months or even years to execute. However, when applying the STAMP/CAST methodology, the term proximate implies a relatively short time horizon (perhaps days or weeks) [37]. Accordingly, we will *loosen* the definition of proximate in line with Salim's treatment of the proximate event chain in his research,

> "Therefore, in the context of cyber-security and specifically in this thesis proximate can also mean a longer time horizon generally in the range of 1-2 years" [56, pp. 103].

We have studied the Energetic Bear Attack Campaign Trojanized Software Update attack in detail using both the Energetic Bear Attack Campaign Cyber Kill Chain® Analysis in Section 3.3.2 and the Energetic Bear Attack Campaign Diamond Model of Intrusion Analysis found in 3.4.2. Therefore, we refer the reader to these sections to understand the proximate event chain that led to the loss.

4.5 Analyzing the Physical Process

In this step, will we now analyze the physical process within our scenario that was the cause of the loss. Our analysis will focus on the physical controls that were ineffective, inadequate, or simply missing that allowed the cyber-attack to occur. Specifically, we are undertaking an exploration to understand not only the root cause but the contributing factors that transitioned the overall system state into a hazardous condition that rendered the cyber attack successful. To undertake this analysis we will consider a number of factors that includes:

> "Analyze the loss at the physical system level. Identify the contribution of each of the following to the events: physical and operational controls, physical failures, dysfunctional interactions, communication and coordi-

nation flaws, and unhandled disturbances. Determine why the physical controls in place were ineffective in preventing the hazard" [37, pp. 351].

4.5.1 Servers and Services Component

As discussed in the previous section 4.3.2, the physical process we will analyze is found at the **Servers and Services** component that provides hardware (e.g., compute and storage) and software services to: (1) the IT Operations component and (2) the workstation and console component within the OT environment. The Servers and Services component is a part of two control loops that it forms with the IT Operations component (loop # 19) and the Workstations and Consoles component (loop # 24) (see Figure 4-2). That is, in order to run the daily operations requests for servers must be provisioned and maintained, identification and authentication services must be provided (e.g., active directory, LDAP), and software must be both installed and updated. The same services are also provided to the Workstation and Consoles component as feedback which falls under the OT systems area. In turn, the Workstations and Consoles component also provides control in terms of system requirements.

4.5.1.1 Inadequate control/feedback

1. **Lack of standardized IT-focused security processes**: The compromise of the network occurred due to malware (i.e., trojanized software updates) being inserted into legitimate software updates which were subsequently downloaded and installed on internal systems. Specifically, the IT Operations component is responsible for proper maintenance and administration of the IT systems including the Servers and Services component (loop #19). During the course of normal operation, malware was introduced into the network environment due to inadequate internal processes (i.e., verification of the integrity of software *patching* updates). Additionally, the hardware and software provided by some of vendors (loops #7 and #8 respectively) was insecure which provided the

necessary conditions to allow the initial exploit vector.

2. **Lack of co-ordination between the IT and OT domains**: IT and OT Operations interact directly through control loop #16 exchanging system needs and reports. However, there was a systemic lack of internal knowledge of prevailing cyber security issues within the manufacturing/OT sector. Accordingly, following operational industry best practice within the company was not adhered too due to insufficient awareness, expertise, misinformed organizational risk tolerance.
3. **Inadequate monitoring**: Overall there was a systemic lack of non-production focused monitoring of both IT and OT systems. Specifically, the malware used in the attack had to establish C2C nodes in order to maintain contact and interact with the compromised systems in the network. That is, internal network systems with no reason to interact with the Internet were able to maintain uninterrupted and undetected contact with the malware's C2C nodes. The feedback in the form of logs from the Servers and Services component (loop #19) did not contain basic security information to enable detection of compromised systems. Furthermore, the collection and processing of security related events is a time consuming but meaningless exercise unless there is some dedicated effort for skilled security personnel to interpret and take action analyzing/investigating anomalous events.

Safety Requirements and Constraints Violated

- Unauthorized access to the OT and IT networks.

Emergency and Safety Equipment (Controls)

- Standard IT identification and authentication technology for employees to gain access to accounts (e.g., active directory, login/passwords, single-factor authentication).

Failures and Inadequate Controls

- Lack of secure software patching procedures and processes.
- Lack of security-focused monitoring.
- No segregation of IT and OT network enclaves.
- No restrictions on Internet connectivity of the OT network/systems with the Internet.
- Lack of monitoring and coordination between the IT and OT networks.
- No centralized security-focused logging and analysis area (i.e., big picture) or capability.

Physical Contextual Factors

- Log aggregation and correlation amongst systems takes both skill and technology (i.e., a SIEM).
- Expensive to test new patches (i.e, separate test infrastructure may be expensive or impractical to set-up).
- Lack of general awareness by management and staff of the risk of cyber-attack to OT networks i.e., complacency and lack of awareness.

Figure 4-3: Analyzing the Physical Process

4.6 Analysis of the Higher Levels of the Hierarchical Safety Control Structure

4.6.1 Workstations and Consoles

The Workstations and Consoles component interacts with both the IT and OT areas.

Safety-Related Responsibilities

1. Ensure that system integrity (hardware/software) of the workstations and consoles is maintained to enable proper production quality and targets.
2. Ensure system availability to meet production targets i.e., quality and output are met.

Context

1. Focus on system uptime, operational requirements and functionality.
2. IT Systems are seen only as necessary overhead to enable production.

Unsafe Decisions and Control Actions

1. Lack of use of basic IT security software (e.g., IDS, anti-virus).
2. Lack of basic IT security processes (e.g., network security policy, cyber strategy).

Process Model Flaws

1. Lack of awareness that cyber-physical systems are at risk from cyber attack using IT systems as an entry vector.
2. The belief that the value of the organization lies in the actual production chain not the information holdings and IT systems that enable production.

Figure 4-4: CAST Analysis of Workstations and Consoles

Specifically, these workstations and consoles are procured and provided by the IT area for use in the OT area. The management consoles and HMI systems will all run on hardware/software provided from the corporate IT (IT Operations) area in

order to properly control, operate, and maintain the cyber-physical systems. This component relies on the Infrastructure component for connectivity (feedback) whilst providing control in the form of the ability to monitor, maintain access to devices, and provide system requirements (loop #25). The component receives services, software, authentication services from the servers and services component (feedback) while providing administration and system requirements as control (loop #24).

4.6.2 IT Operations

Next level up in the control structure is the IT Operations, which is responsible for the proper and secure deployment, provisioning, and operation of all IT related systems. IT Operations provides the basic information technology assets and infrastructure to the organization. This includes networking services, desktops and applications, as well as servers and services. IT functions include basic network connectivity, data storage, compute resources, user environments, and authentication services. This area develops all standard IT operating procedures and policies to ensure IT systems are secure and available to enable production and business functions. Additionally, IT systems are monitored for not only system health (uptime and hardware/software) issues but also for signs of unauthorized access and/or system compromise.

4.6.2.1 Inadequate control/feedback

Monitoring of networks: the malware made use of OPC scanning modules to undertake reconnaissance inside the network to locate ICS systems and map the overall IT/OT topology. Potential victims were identified and malware was installed in order to maintain persistence in the network. Once this was achieved, intelligence gathering began that included the collection and exfiltration of network/system information (e.g., passwords, contacts, network topology) as well as proprietary manufacturing information (e.g., production schedules, manufacturing specifications). As noted in the Cyber Kill Chain®, the threat actor will maintain control of the compromised systems as well as receive information via a two-way communication channel i.e., via

C2C channel. Even the most basic network monitoring should have been able to pick up anomalous activity that would have prompted some sort of investigation.

This is due to the fact that, in contrast to conventional IT environments, automation networks (OT networks) offer a unique and arguably more-manageable problem space from a security point of view [41]:

1. ICS/SCADA networks have a constrained threat surface because of the limited number of installed applications and running services.
2. They are static by design and any system and/or configuration changes follow well-documented procedures that often includes extensive testing before operational deployment.
3. Network communications should be predictable (i.e., deterministic) due to the fact they are dominated by machine-to-machine exchanges that only use a limited set of protocols and steady polling rates.

Poor patch management procedures: any software updates should be done in a secure manner by verifying the integrity of the software being introduced into the environment [61]. Additionally, new patches should be tested to ensure they work as expected and that there are no unintended or adverse interactions within the application, device, and network. The firms that were infected with the trojanized software update did not have the proper patch management framework in place.

Security operations: as discussed, basic network security monitoring should have been sufficient to detect the malware operating inside of the network. However the process of monitoring networks and/or devices, undertaking log collection, as well as the implementation of security policies is not sufficient if there is no dedicated effort to analyze, interpret, and follow-up on this information. A dedicated security operations area is needed to ensure that, at a minimum, security processes and procedures are adhered to as well as obvious signs of suspicious or unauthorized activity is detected and acted upon. This dedicated security operations function does not have to be an actual operations area but could be achieved through a matrixed effort as the organization may not have sufficient staff (e.g., small or medium sized business)

to have a dedicated security person. The important point is that there are defined security functions that are assigned to a responsible person or area for execution.

Safety-Related Responsibilities

1. Develop and communicate specific security processes including software/hardware patching.
2. Develop and communicate policies/processes for system monitoring (i.e., security).
3. Ensure compliance with patching and monitoring policies.
4. Ensure that measures are implemented for protecting information assets and information infrastructure from cyber attack.
5. Detect unauthorized access and/or system behaviour that could indicate a compromise (operational security monitoring).

Context

1. No dedicated role or area to conduct cyber security functions i.e. operational security monitoring.

Unsafe Decisions and Control Actions

1. Unsafe software patching processes.
2. Lack of focus on cyber-attack detection skill to detect compromises and remediate unauthorized system accesses.
3. No dedicated cyber security role to ensure adequate monitoring.
4. Lack of proper network segmentation and zoning to prevent OT system from directly communicating with the Internet.

Process Model Flaws

1. Inadequate or incorrect process/checklists for maintaining cyber security infrastructure and monitoring.
2. No dedicated cyber security role to ensure process improvement.

Figure 4-5: CAST Analysis of IT Operations

4.6.3 OT Operations

The OT Operations component is responsible for the proper and secure deployment, provisioning, and operation of all OT related systems.

Safety-Related Responsibilities

1. Develop and communicate specific security processes including firmware/hardware patching.
2. Develop and communicate policies/processes for system monitoring (e.g., status and security).
3. Ensure compliance with patching and monitoring policies.
4. Ensure that measures are implemented for protecting OT assets and OT dependent infrastructure from cyber attack.
5. Detect unauthorized access and/or system behaviour that could indicate a compromise (operational security monitoring).

Context

1. No strategy to collect or baseline monitoring information to facilitate cyber security functions i.e., operational security monitoring.

Unsafe Decisions and Control Actions

1. Unsafe software patching processes (including firmware).
2. Lack of focus on detecting system abnormalities.
3. Lack of proper network segmentation and zoning to prevent OT systems from directly communicating with the Internet.

Process Model Flaws

1. Inadequate or incorrect process/checklists for maintaining OT monitoring.
2. No dedicated champion to ensure ongoing monitoring process improvements.

Figure 4-6: CAST Analysis of OT Operations

This area develops all standard OT operating procedures and policies to ensure OT

systems are secure and available to enable production. OT systems are monitored for system health (uptime and hardware/software/firmware) issues as well as additional telemetry information to facilitate in correlation/fusion with IT systems events in order to baseline activity to identify possible signs of unauthorized access and/or system compromise. OT Systems provides the basic operational technology assets and infrastructure to the organization. It includes all ICS systems in the manufacturing zone that interact with the IT management or corporate network zone.

4.6.4 IT/OT Vendors

The IT and OT vendors are responsible for supplying goods and services to the organization (e.g., software). Supply chain security has to deal with a security program in place at both the vendor and client sites in order to ensure supply chain breaches do not occur. This will involve both technical and non-technical measures to mitigate the potential risks introduced as a result of trusted suppliers that may have extensive access too or inadvertently introduce untrusted products into the environment.

4.6.4.1 Inadequate control/feedback

Lack of Cyber security practices: legitimate software updates for customers were made available for download on the company website. In order for a threat actor to be able to insert malicious code into the software update, a compromise of the vendor network/site had to occur a priori. That is, unauthorized access to the vendor network was achieved so that malware could be left in the downloadable code/software update repository in order to infect the *true* victims. This would indicate that lack of adherence to cyber security best practices that not only resulted in adverse consequences for the system/network owner but also their unwitting customers.

Insecure software deployment strategies: one method for a system owner to verify the integrity of a downloaded software update before installing them is through the use of cryptographic checksums [61]. By not providing cryptographic checksums for their customers, there was no ability to verify that the software being downloaded

had not been tampered with.

Safety-Related Responsibilities

1. Ensure the integrity of software and hardware available for purchase by customers.
2. Provide mechanisms for the attestation of software updates to ensure they were not tampered with (e.g., cryptographic checksums).
3. Ensure that the digital interaction with the public and customers is secure.

Context

1. The software life cycle focused on a development model that providing functionality with little or no though about securing the supply chain as part of the value proposition.
2. Customers did not ask or require methods to ensure secure software downloads.

Unsafe Decisions and Control Actions

1. Providing software updates (patches) without the mechanism to verify the integrity of the provided software.
2. Inadequate focus on the overall IT security of the organization that allowed the software updates to be tampered with.

Process Model Flaws

1. Inadequate general knowledge of prevailing security issues (i.e., threat environment) within the OT industry.
2. Inadequate knowledge about the threat of supply chain attacks.

Figure 4-7: CAST Analysis of IT/OT Vendors

4.6.5 IT Management

Next level up in the control structure is the IT Management, which is responsible for the management of all IT related systems. It is also the area charged with developing

the overall IT security polices of the organization as an extension of the overall IT/OT security strategy and principles as imposed by Systems Management. IT Management is also responsible for ensuring overall compliance of any adhered to IT standards and principles as outlined in the overall IT/OT security strategy.

Safety-Related Responsibilities

1. Develop and promulgate overall IT security policies.
2. Provide adequate resources for security monitoring functions.
3. Ensure that IT standards are enforced.
4. Ensure compliance with IT security policies.
5. Conduct security posture assessments (SPA) as required.
6. Ensure any subsequent audit recommendations as a result of the SPA are followed-up/resolved.

Context

1. Focus on overall production capability (i.e., system health and uptime) not on security.
2. Inadequate or lack of security policies.

Unsafe Decisions and Control Actions

1. Inadequate or lack of IT/OT security strategy policies.
2. Cyber-safety corporate culture not properly cultivated by management.

Process Model Flaws

1. Inadequate understanding of cyber-physical security issues.
2. General lack of awareness of the risk posed by overall threat of cyber-physical attacks.

Figure 4-8: CAST Analysis of IT Management

4.6.6 OT Management

The OT Management component is responsible for the management of all OT related systems. It is also the area charged with developing the overall OT security polices of the organization as an extension of the overall IT/OT security strategy and principles as imposed by Systems Management. OT Management is also responsible for ensuring overall compliance of any adhered to OT standards and principles as outlined in the overall IT/OT security strategy.

Safety-Related Responsibilities

1. Develop and promulgate overall OT deployment policies
2. Provide adequate resources for OT device monitoring functions.
3. Ensure that OT standards are enforced.
4. Ensure compliance with OT deployment (including security) policies.

Context

1. Focus on overall production capability (i.e., system health and uptime) not safe or expected interactions with IT systems.

Unsafe Decisions and Control Actions

1. Inadequate or lack of IT/OT security strategy policies.
2. Cyber-safety corporate culture not properly cultivated by management.

Process Model Flaws

1. Inadequate understanding of cyber-physical security issues.
2. General lack of awareness of the risk posed by overall threat of cyber-physical attacks.

Figure 4-9: CAST Analysis of OT Management

4.6.7 Engineering Management

Engineering management is responsible for the overall operations and production output for the organization. This includes developing and promulgating a production strategy and associated safety principles.

Safety-Related Responsibilities

1. Develop and promulgate production strategy and associated safety principles.
2. Ensure overall compliance with production strategy and safety principles.
3. Identify production quality assurance program targets and goals.

Context

1. Lack of awareness of the threat of cyber-attack to cyber-physical systems.
2. Lack of maturity of IT/OT cyber security standards as well as advice/guidance on best practices.
3. Cyber security seen as unnecessary due to lack of understanding about the threat environment and associated risk and it is considered an expensive and unnecessary cost.

Unsafe Decisions and Control Actions

1. Inadequate consideration of IT/OT security strategy and principles in production strategy and principles.
2. Cyber-safety corporate culture not a priority.

Process Model Flaws

1. Inadequate senior management attention and appreciation of the overall risk posed by the threat of cyber-physical attacks to production processes.

Figure 4-10: CAST Analysis of Engineering Management

4.6.8 Systems Management

Systems management is responsible for the overall management of all IT and OT systems. This includes the development and promulgation of overall IT/OT strategy and principles for the organization including a cohesive IT/OT security strategy.

Safety-Related Responsibilities

1. Develop and promulgate overall IT/OT strategy and principles for the organization including a cohesive IT/OT security strategy.
2. Ensure overall compliance with IT/OT security strategy and principles.
3. Periodically sponsor a security posture assessment (audit) of IT/OT systems.

Context

1. Lack of awareness of the threat of cyber-attack to cyber-physical systems.
2. Lack of maturity of IT/OT cyber security standards as well as advice/guidance on best practices.
3. Cyber security seen as unnecessary due to lack of understanding about the threat environment and associated risk and it is considered an expensive and unnecessary cost.

Unsafe Decisions and Control Actions

1. Inadequate or lack of IT/OT security strategy and principles.
2. Cyber-safety corporate culture not a priority.

Process Model Flaws

1. Lack of clear cyber security vision and strategy.
2. Inadequate senior management attention and appreciation of the overall risk posed by the threat of cyber-physical attacks.

Figure 4-11: CAST Analysis of Systems Management

4.6.9 Corporate Management

The Corporate management component is the highest level of management in the company i.e., headquarters.

Safety-Related Responsibilities

1. Ensure organizations business needs are met by the technology choices.
2. Ensure that industry best practice procedures are in place to protect company assets including adherence to any regulatory requirements.
3. Ensure the proper balance of resources are allocated to protect company assets including adherence to any regulatory requirements.

Context

1. No requirement or plan to have dedicated cyber (IT) security role or function.
2. Constant pressure to keep costs in check while focusing on business needs and production output.
3. Most cyber security related standards are voluntary and can be both burdensome and easily misinterpreted or use in IT/OT network to secure a cyber-physical network.

Unsafe Decisions and Control Actions

1. Cyber security safety and awareness culture non-existent.
2. Lack of clear guidance given on the priority (or lack thereof) of cyber security risks to IT/OT networks.
3. Priority given to internal cost savings instead of adequately resourcing the IT departments.

Process Model Flaws

1. Inadequate knowledge of prevailing cyber security issues within the manufacturing/OT sector
2. Inadequate communication of priorities with respect to IT/OT security

Figure 4-12: CAST Analysis of Corporate Management

This component is responsible for all oversight and governance activities within the organization. It interacts directly with the IT and OT management components exerting overall control and gathering feedback from the entire system. Ultimately it is responsible to the shareholders that provide control in the form of capital investment and gain feedback through shares and ownership.

4.7 Coordination and Communication

1. The personnel working in IT and OT Operations components lacked the necessary expertise and did not have the proper focus in order to understand and implement internal processes/technology to enable compliance with industry best practices for IT/cyber security. Coordination amongst the two areas was in place in order to have a consolidated view on safe operations with respect to physical/production matters but not for *digital* security thus exposing a weakness in the communications of loop #16. Furthermore, IT Management (loop #9) as well as the OT Management component (loop #10) are responsible for promulgating the expected security posture guidelines into the respective operational areas. General lack of understanding of the true nature of cyber threat, as it relates to the company, meant that minimum IT security guidelines were weak as well as any associated communications around this topic.
2. There was a disconnect between the expectations of the operational areas and vendors when it comes to secure patching/software updates. Specifically, loops #7 and #8 are concerned with the flow of hardware and software as products to the IT and OT Operations components respectively.

    (a) Most vendors provide an authentication mechanism to validate that the software update available for download has not been tampered with. Typically, this would involve some sort of cryptographic checksum, Pretty Good Privacy (PGP) signatures, and/or digital signatures [61]. In this way, once a software update is downloaded, it can be checked to determine if any modifications or tampering of the software has occurred. Had these

measures been in place, and the associated proper internal processes been followed, the malicious software updates may have been detected.

3. The threat of cyber attack to cyber-physical systems is both well documented and well publicized. As shown in Figure 1-2 we saw that there have been many instances of compromises of cyber-physcial systems resulting in adverse effects. Perhaps one of the most well-publicized is the Stuxnet worm that was used to sabotage the Iranian nuclear program [70]. This sophisticated attack attracted world attention and became an exemplar for the risks associated with cyber attacks to cyber-physical systems. Despite this, very little attention from senior level management (loops #9 and #10) was given to the prospect of a cyber attack on the OT networks. Accordingly, the organizational security policies including security monitoring lacked both focus and rigour that allowed for the attacks to succeed and go undetected.

4.8 Dynamics and Migration to a High-Risk State

In this section, we will explore how the system migrated to a high-risk state over time.

Increased Automation and Business Intelligence Requirements: Until recently, it was industry best practice to physically separate the corporate or IT network from the OT or operational networks through an *air-gap*. That is, no physical connectivity existed between the two network segments so it was this physical isolation between them that was relied upon to provide an overall layer of security. The overarching principle is that a physical gap can stop both unauthorized access and malware infection. There were no associated hardware or software security controls built into the products and proprietary protocols (e.g., Modbus, Pro bus, Ethernet/IP)[9]. However, the demand for Near Real Time (NRT) access to data for metrics, business process improvement, remote connectivity, and ease of system ad-

[9]The Stuxnet worm proved that even air-gapped networks can be penetrated by a determined adversary as it is believed that malware-infected removable media (USB key) was able to inject malware into an non-Internet connected network segment [70].

ministration has shifted many organizations to favour increased connectivity between the corporate (i.e., Internet connected) and production networks with little though about the increased security risks.

In fact, expert testimony from Sean McGurk, former Director, National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security included the observation,

> "In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network. On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network" [63, pp. 52].

Accordingly, the networks that cyber-physical systems currently operate on are starting to resemble traditional IT networks. The wide-scale adoption of open networking standards (e.g., TCP/IP, Ethernet) coupled with the cost savings of replacing dedicated single purpose devices with off-the-shelf commodity hardware/software has significantly decreased costs but has caused an overall increase in the risk from cyber attack. Specifically, the use of commodity software as well as the increased connectivity to the corporate network has dramatically increased the overall attack surface. Accordingly, we make the following observations about the state of most cyber-physical networks [22]:

1. **Inherent lack of security**: ICS technology has been designed for operational robustness and reliability in an isolated environment and was never designed with the security features to safely interact with exposures to non-OT networks in mind. Thus, the security model relied on both isolation and hardware/protocol obscurity as effective deterrents.
2. **Increased attack surface**: air-gapped networks, proprietary protocols, and specialized hardware/software are not a normal deployment strategy for most

modern IT/OT networks.

3. **Poor network segmentation**: standard network segmentation is used to isolate functions and services into logically separated zones in order to provide opportunities for containment, and the ability to apply a different security posture based on the perceived risks. Most IT/OT networks do not do proper network segmentation in favour of a flat network structure for ease of administration.
4. **Lack of security skills**: there is a general lack of awareness when it comes to the threat that cyber attacks pose to cyber-physical systems and thus there is a general lack of internal skills as well as interest in the burden of implementing applicable security processes and procedures.

Failure to Recognize the Increasing Risk of Cyber Attacks Against Cyber-Physical Systems: We have seen in Figure 1-2 that cyber attacks against cyber-physcial attacks are becoming more sophisticated. As these risk of cyber attack increased, management did not respond appropriately to manage these risks. Specifically, as senior management became more aware about the increasing threat from the external threat environment, more organizational focus should have been taken on securing both information and cyber-physical assets from attack. Senior management response could have ranged from the establishment of a virtual security role by leveraging existing IT personnel all the way to the creation of a dedicated and defined organization role and/or area with a prime focus on cyber security. The important principle that was missing was a conscious decision by senior management to develop an internal capability and a robust security posture to deal with cyber security incidents.

4.9 Recommendations

Based on our STAMP/CAST analysis we offer the following recommendations in order to deal with future cyber attacks and manage the associated risks more effectively.

Understand the risks: In order to build an appropriate cyber security strategy and an associated network security policy you must first understand the risks your

are trying to mitigate. A TRA is a mechanism to understand the pertinent threats, risks and assets you are trying to protect. Management did not understand the risks of cyber attacks to the cyber-physical environment. A detailed and independent review of the threat environment that considers benchmarks against peer institutions (i.e., industry sector) as well as geo-political considerations would allow for the adequate classification and prioritization of cyber security related risks. Only then can prioritization for security investments be made for a viable and workable security posture.

Regular security posture assessments: Periodic reviews of an organization's overall security posture is required to ensure that the overall security posture is commensurate with the current threat environment. Over time, changes to the network architecture, investment on new technology, unknown shadow IT and/or changes in system configuration could result in an overall insecure state of the network. Regular (and perhaps independent) reviews of the overall network are needed to ensure that the organization's security posture is commensurate with the overall threats in the environment balanced against the assets they are trying to protect.

Establish a dedicated IT security function: System and network administrators alone cannot adequately protect organizational systems and assets. In our case study, there was a failure to ensure secure software update practices were being followed as well as a implement basic security-focused cyber threat monitoring. A dedicated security function with the proper tools, processes and procedures must be in place to adequately protect a organization. Establishing a viable cyber security focused function in an organization can be a daunting task. In addition to being able to dedicate personnel to undertake the associated security tasks, these individuals will have to undergo specialized training in order to proper deal with complex security technology and tradecraft. A dedicated security function will ensure that security-related tasks are performed and reviewed, threat information is reviewed and actioned, and a risk-based overall security posture is maintained.

Impose security requirements on vendors - secure the supply chain: Any organization typically uses a network of suppliers to obtain the necessary goods and

services in order to run their respective businesses. Sophisticated attackers will use any means necessary in order to gain access to a target's network including leveraging the access and trust afforded to third-party suppliers. In fact, many third part-suppliers are *softer* targets than the intended victims. That is, some third-party vendors and suppliers may have have fewer security controls in place than host organizations,that may make them more susceptible to an initial attack. Once these trusted third-parties are breached, access can more easily be gained to the *true* target. As we have seen in our case study, a vendor could be compromised via malware that modifies source code (e.g., inserts malware/trojan) that is then distributed to organizations that downloads the software.

Accordingly, a robust software update program needs to be implemented within an organization that includes not only software patch/update verification process (e.g., cryptographic checksums) but also an assessment of a trusted third-parties supply chain security posture. Part of an evaluation process for acquiring new products could involve an assessment of the supply chain security in order to choose vendors that have good internal security practices to guard against supply chain attacks.

Chapter 5

Improving Security through a Security Operations Centre (SOC) Function

As we have seen in the previous section, the CAST/STAMP process generated a number of recommendations to help the organization analyzed in the case study to manage the risk from cyber attack. These stemmed from a number of inadequate controls and feedback within the hierarchical control structure.

Namely,

1. **Supply chain security issues**: a lack of security procedures and processes to ensure that software entering the organization had not been tampered with before software update download and installation (i.e., control loops #7 and #8).
2. **Inadequate awareness of the threat environment**: general lack of awareness of the threat of cyber attack on cyber physical systems. This involves a lack of tactical threat information (e.g., IoCs, cyber-physical specific threats) as well as strategic sector-specific threat intelligence.
3. **Lack of internal coordination between corporate and production segments**: very little cyber security information flow and feedback was passed

between the corporate (IT) and production (OT) areas as cyber security was seen as an IT-specific issue and very little emphasis in general was given to this topic (i.e., control loop #16).

4. **No dedicated security function**: perhaps one of the biggest issues that allowed the compromise to occur was the lack of a dedicated security function/area within the organization. Establishing a security focused team (whether it is staffed with dedicated resources or virtually created out of matrixing existing staff) will serve to: (1) assign responsibility and thus accountability that the basic day-to-day security functions are being performed, (2) ensure that new cyber threats are adequately dealt with from both a tactical and strategic level, and (3) assist with promoting a cyber-security aware corporate culture through outreach.

5.1 Proposed SOC Structure

One possible way to address these concerns is through formalizing a cyber security function within the organization by creating a security operations centre (SOC).

> "A SOC is a team primarily composed of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents" [75, pp. 9].

A SOC allows an organization to prioritize efforts to enhance the visibility of cyber threat information and enable a proactive vs. reactive response through monitoring, analytics and prompt detection. A SOC typically employs a suite of advanced analytic capabilities enabled by the correlation and fusion of all source information e.g., network monitoring, host telemetry information, commercial threat feeds, open source threat feeds, and system logging all in support of operational dynamic defence activities. Using our case study as an example, we propose a new system hierarchical control structure that includes a SOC function (see Figure 5-1).

We can see in this system that the addition of a new SOC component interacts with the IT and OT Operations components and as we move up the control struc-

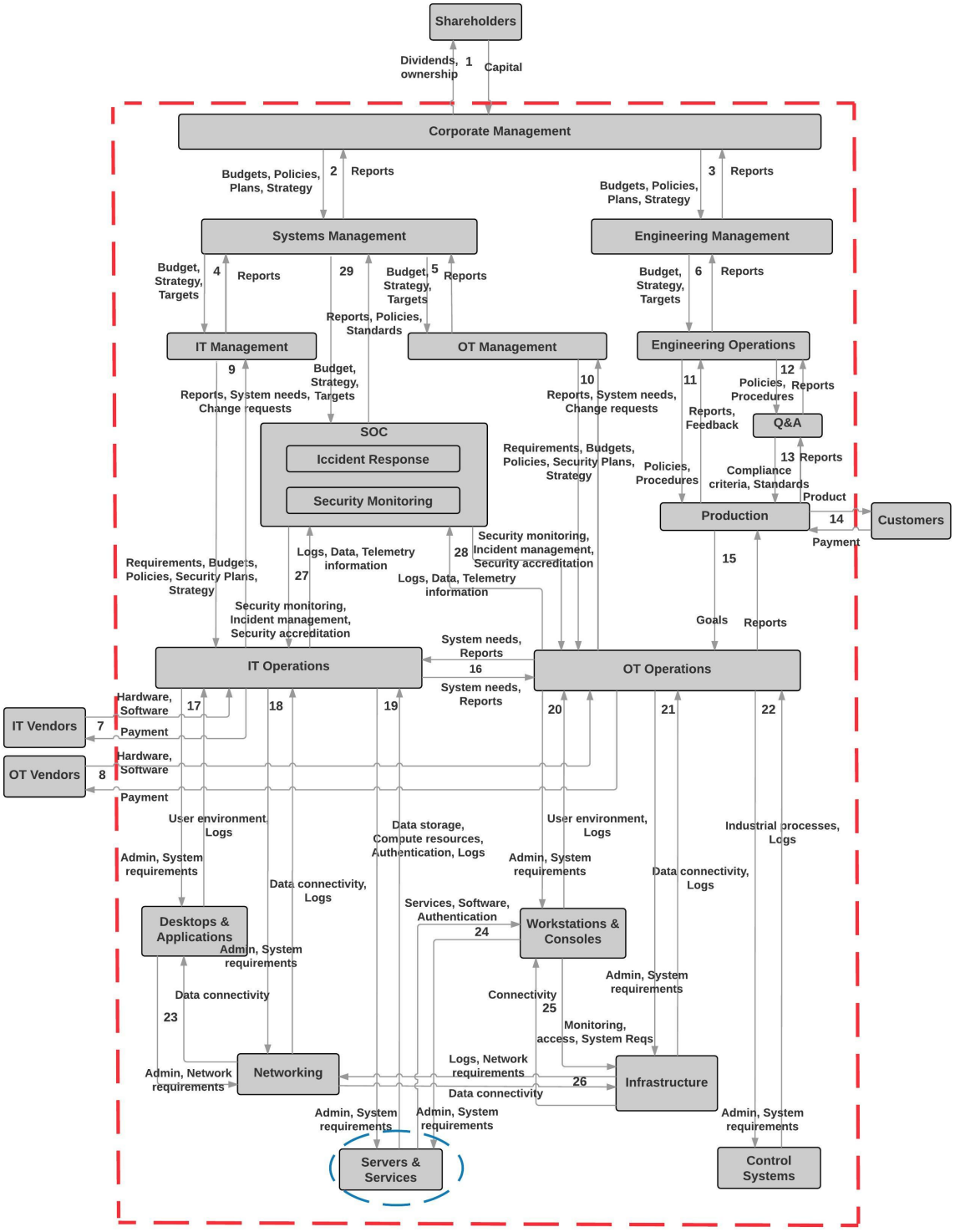

Figure 5-1: Implementing a Dedicated Cyber Security Function (SOC).

ture the Systems Management component. Specifically, the SOC component provides security monitoring, incident management, and security accreditation to the IT and

OT operations components respectively (loops #27 and #28) while getting feedback in the form of logs, data, and telemetry information. Additionally. the SOC receives budget strategy and targets from the Systems Management component while providing feedback in the form of reports, policies, and standards (loop #29).

The addition of the SOC component and the associated control loops serve to address a number of the recommendations in the previous section by: (1) improving the flow of cyber threat and IT security information, (2) ensuring more timely communication, and (3) providing additional security controls. Specifically, secure supply chain processes are promulgated by the SOC to both the IT and OT Operations areas (security accreditation via loops #27 and #28 respectively). Additionally, the SOC gives standards as part of the feedback to the Systems Management component which will include secure supply chain processes. In terms of security monitoring, these functions are provided as well as an incident response function via loops #27 and #28 respectively.

5.2 Proposed SOC Functions

It is envisioned that co-location (even virtually) of key operational staff in both the IT and OT areas within a dedicated SOC function would yield significant business benefit given the tight coupling and dependencies on shared IT infrastructure, access to highly skilled personnel, and business processes. Formalizing a security operations function within in organization allows for proactive monitoring to occur in order to detect and respond to both common and advanced cyber threats. A SOC is a team primarily composed of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents. Taking into consideration the size of an organization, the creation of a SOC can be virtual in nature and the functions assigned to existing operational staff members with the right expertise coupled with additional cyber security-specific training. As well, there are a number of outsourcing options (i.e., managed security services) that allow an organization to have an effective SOC that is simply outsourced to a managed security service.

In terms of activities performed by the cyber team within the SOC, the following activities are typically performed to some degree with consideration to the number of assigned personnel [75]:

- **Tier 1 analyst functions**: continuously monitors alerts generated from security devices, triages the security alerts, monitors and actions threat intelligence feeds, monitors the health of security sensors and endpoints, regularly reviews the Security Incident and Event Monitoring (SIEM), and collects the data and context necessary to initiate Tier 2 analyst work.
- **Tier 2 analyst functions**: performs deep-dive incident analysis by correlating data from various sources, determines if a critical system or data set has been impacted, advises on remediation activities, provides support for new analytic methods for detecting threats.
- **Tier 3 analyst functions**: possesses in-depth knowledge on network, endpoints, indicators of compromise, threat intelligence, forensics and malware analysis. Acts as an incident hunter not waiting for escalated incidents and is also responsible for developing, tuning and implementing threat detection analytics.

Figure 5-2 reveals a typical SOC structure that describes both a set areas within the SOC as well as their constituent responsibilities. Furthermore, a logical view of the inputs (data) and outputs (functions) can be found in Figure 5-3 [75].

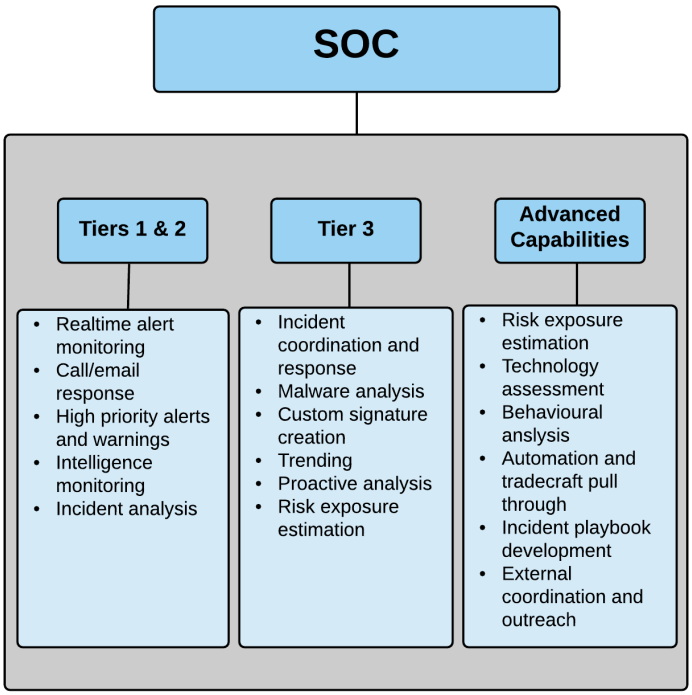

Figure 5-2: SOC Structure.

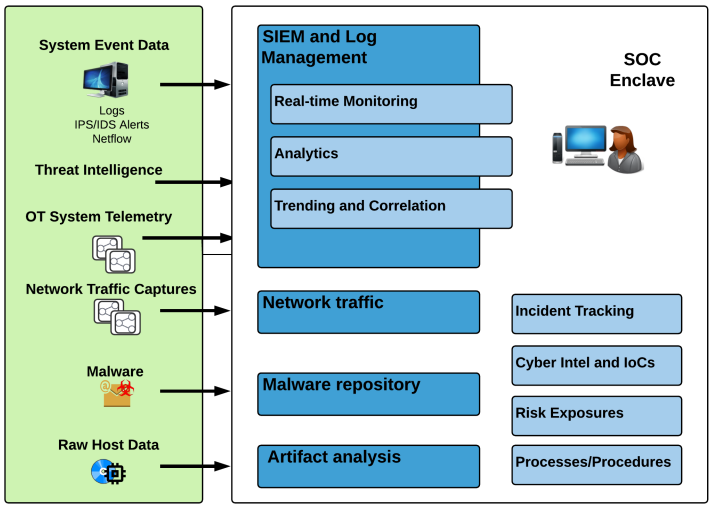

Figure 5-3: SOC Functions.

Chapter 6

Conclusions

Keeping pace with the constantly evolving cyber threat landscape is a daunting task. IT security systems and architectures, everywhere, are being driven to perform in ways they were never intended to operate. The Internet is a complex globally distributed system that was initially designed for maximizing connectivity with very little thought about security. Although any Internet connected system is potentially at risk, our use case analyses in Chapter 3 highlights the fact that cyber-physical systems are particularly vulnerable. An unintended consequence of this connectivity is that it has introduced new vulnerabilities, adversarial threats, and challenges to our society. The security, robustness, and stability of our access to electronic information and services are keystone requirements for sovereign economies.

Our discussion in Section 1.2 revealed that as the automation of industrial networks has grown steadily over the last few decades, it has increased the connectivity and depth IT penetration with the Internet. This convergence of IT/OT networks has resulted in critical infrastructure (e.g., the electric grid) becoming vulnerable to cyber attack as cyber-physical systems were never designed with IT security in mind.

In Chapter 3 we showed that cyber attacks against cyber-physical systems are inherently different than attacks against IT networks in that the attackers intent, sophistication, capabilities, and familiarization with ICS systems and associated automated processes are indicative of more protracted attack campaigns instead of single incidents. Accordingly, we used the STAMP/CAST model to complement the appli-

cation of intrusion analysis models (i.e., Diamond Model of Intrusion Analysis, the Cyber Kill Chain®, and the ICS Cyber Kill Chain) on a specific use-case in order to identify additional causal factors that revealed insights into why the attack was successful. Specifically, it revealed limitations of these intrusion analysis models in that they focus on event-based classification and correlation in order to: (1) generate actionable IoCs and/or create intelligence feedback loops, (2) increase the likelihood of detection of similar intrusion activity, and (3) provide a way to identify security posture gaps and prioritize defensive countermeasures. These NRT intelligence focused models do not purport to nor do they strive to uncover the root causes that led to a successful cyber attack. Specifically, we found the STAMP/CAST analysis uncovered a number of flaws not considered in the intrusion analysis models namely:

1. A break down in security processes and perceived responsibility for implementing these processes i.e., no dedicated IT security function led to the corporate ethos that security is a *best effort* only task.
2. Recognition that the breakdown in security processes allowed for a previously unconsidered threat vector (i.e., supply chain threat) to be used by an adversary to gain access to the network.
3. Failure of management to look outside of traditional sector-specific threat models (e.g., flawed mental models in thinking that safety issues in the physical world manifest themselves exclusively in the physical not digital world).
4. The drive for increased automation and the need for business intelligence introduced new vulnerabilities and risks not properly addressed by the organization.
5. General failure to consider the risk of cyber attack led to faulty risk and thus security related investment decisions.

Accordingly, the main contributions of this thesis are:

- The analysis of two use cases of *real world* cyber-physical attacks using three state-of-the-art intrusion analysis models.

- The use of a Systems Theory based approach (STAMP/CAST) in order to complement traditional intelligence-driven analysis models applied to cyber-physical attacks.
- The proposal of a SOC model to address inherent cyber security related process and communication weaknesses within an organization.
- The use of STAMP/CAST in order to highlight the underlying system weaknesses (i.e., non-technical socio-technical) in a typical small/medium sized manufacturing organization that could lead to a cyber-physical attack.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix A

Acronyms

- ADSC: Advanced Digital Sciences Center
- APT: Advanced Persistent Threat
- C2C: Command and Control
- CaaS: Crimeware as a Service
- CMS: Content Management System
- CPS: Cyber Physical System
- CVE: Common Vulnerability Exposure
- DDoS: Distributed Denial of Service
- DMS: Distribution Management System
- DoD: Department of Defense
- EPT: Effective Persistent Threat
- HMI: Human Machine Interface
- HTML: Hyper Text Markup Language
- HTTP: Hypertext Transport Protocol
- HQP: Highly Qualified Personnel
- ICS: Industrial Control System
- IO: Information Operations
- IoC: Indicators of Compromise
- IRC: Internet Relay Chat

- IT: Information Technology
- LOEK: LightsOut exploit kit
- LDAP: Lightweight Directory Access Protocol
- NCCIC: National Cybersecurity and Communications Integration Center
- NIST: National Institute of Standards and Technology
- NRT: Near Real Time
- OLE: Object Linking and Embedding
- OPC: Object linking and embedding for Process Control
- OT: Operational Technology
- PDF: Portable Document Format
- PGP: Pretty Good Privacy
- PSP: Personal Security Products
- RAT: Remote Access Trojan
- RTU: Remote Terminal Unit
- SCADA: Supervisory Control and Data Acquisition
- SIEM: Security Incident and Event Managment
- SOC: Security Operations Centre
- TDoS: Telephone Denial of Service
- TOF: Time of Flight
- TTP: Tactics, Techniques, and Procedures
- UPS: Uninterruptible Power Supply
- VPN: Virtual Private Network

Bibliography

[1] ewon. https://ewon.biz. [Accessed: 30, October 2016].

[2] ewon - machines can talk. https://ewon.biz. [Accessed: 21, March 2016].

[3] Heptagon. http://hptg.com/industrial/. [Accessed: 30, October 2016].

[4] Mb connect line. https://www.mbconnectline.com/en/. [Accessed: 30, October 2016].

[5] Mb connect line gmbh. https://www.mbconnectline.com/en/. [Accessed: 21, March 2016].

[6] CVE-2011-0611. Available from MITRE, CVE-ID CVE-2011-0611., April 2011. [Accessed: 30, October 2016].

[7] CVE-2012-4792. Available from MITRE, CVE-ID CVE-2012-4792., December 2012. [Accessed: 30, October 2016].

[8] Definition. http://www.liquisearch.com/what_is_oblenergo, 2012. [Accessed: 21, October 2016].

[9] CVE-2013-2465. Available from MITRE, CVE-ID CVE-2013-2465., June 2013. [Accessed: 30, October 2016].

[10] Michael Assante and Robert Lee. The industrial control system cyber kill chain. https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297, October 2015. [Accessed: 30, October 2016].

[11] Christopher Bronk and Eneken Tikk-Ringas. The cyber attack on saudi aramco. *Survival: Global Politics and Strategy April-May 2013*, 55(2):81–96, April 2013.

[12] Sergio Caltagirone, Andrew Pendergast, and Christopher Betz. The diamond model of intrusion analysis. Technical report, US Department of Defense, 2013.

[13] ICS CERT. Alert (ics-alert-14-281-01e): Ongoing sophisticated malware campaign compromising ics (update e). https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B, March 2016. [Accessed: 30, October 2016].

[14] ICS CERT. Alert (ir-alert-h-16-056-01): Cyber-attack against ukrainian critical infrastructure. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01, March 2016. [Accessed: 30, October 2016].

[15] Crowdstrike. 2013 global threat report. https://scadahacker.com/library/Documents/Threat_Intelligence/CrowdStrike-GlobalThreatReport2013.pdf, March 2013. [Accessed: 21, March 2016].

[16] Dell. 2015 dell security annual threat report. https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf, 2015. [Accessed: 2, December 2016].

[17] Electric Power Research Institute (EPRI). Electric sector failure scenarios and impact analyses national. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf, September 2013. [Accessed: 21, March 2016].

[18] Clifton A Ericson and Clifton Ll. Fault tree analysis. In *System Safety Conference, Orlando, Florida*, pages 1–9, 1999.

[19] eWon. Talk2m incident report. https://ewon.biz/news/talk2m-incident-report, January 2014. [Accessed: 30, October 2016].

[20] Exodus intelligence. https://www.exodusintel.com. [Accessed: 4, December 2016].

[21] Dennis Fisher. Energy watering hole attack used lightsout exploit kit. https://threatpost.com/energy-watering-hole-attack-used-lightsout-exploit-kit/104772/, March 2014. [Accessed: 3, November 2016].

[22] Fortinet. Securing industrial control systems with fortinet. https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/SB-Securing-Industrial-Control-Systems-with-Fortinet.pdf, 2015. [Accessed: 6, December 2016].

[23] OPC Foundation. What is opc? https://opcfoundation.org/about/what-is-opc/. [Accessed: 5, December 2016].

[24] Recorded Future. Up and to the right ics/scada vulnerabilities by the numbers. https://go.recordedfuture.com/hubfs/reports/ics-scada.pdf, 2016. [Accessed: 2, December 2016].

[25] Derek Harp and Gregory-Brown Bengt. Sans 2016 state of ics security survey. https://www.sans.org/reading-room/whitepapers/analyst/2016-state-ics-security-survey-37067, June 2016. [Accessed: 6, December 2016].

[26] Daavid Hentunen. Havex hunts for ics/scada systems. https://www.f-secure.com/weblog/archives/00002718.html, June 2014. [Accessed: 3, November 2016].

[27] Erik Hjelmvik. Full disclosure of havex trojans. http://www.netresec.com/?page=Blog&month=2014-10&post=Full-Disclosure-of-Havex-Trojans, October 2014. [Accessed: 3, November 2016].

[28] Eric M Hutchins, Michael J Cloppert, and Rohan M Amin. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1:80, 2011.

[29] ISI Information Security Incorporated. Diminishing attack costs and increasing complexity. http://infosecurityinc.net/wp-content/uploads/2011/07/Consult-Cyber-1Cyber-Threats-Diminishing-Attack-Costs-Increasing/-Complexity4.jpg. [Accessed: 2, January 2017].

[30] Swati Khandelwal. New variant of havex malware scans for opc servers at scada systems. http://thehackernews.com/2014/07/new-variant-of-havex-malware-scans-for.html, July 2014. [Accessed: 14, November 2016].

[31] Eduard Kovacs. Attackers use word docs to deliver blackenergy malware. http://www.securityweek.com/attackers-use-word-docs-deliver-blackenergy-malware, January 2016. [Accessed: 30, October 2016].

[32] Kaspersky Lab. What is a trojan virus? - definition. https://usa.kaspersky.com/internet-security-center/threats/trojans#.WFAYXHeZP_Q. [Accessed: 6, December 2016].

[33] NIST Engineering Labratory. Cyber physical systems. https://www.nist.gov/el/cyber-physical-systems. [Accessed: 26, November 2016].

[34] F-Secure Labs. Blackenergy and quedagh, the convergence of crimeware and apt attacks. https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf, 2014. [Accessed: 26, November 2016].

[35] Joel Langill. Defending against the dragonfly cyber security attacks. http://www.belden.com/docs/upload/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks.pdf, December 2014. [Accessed: 3, November 2016].

[36] Robert Lee, Michael Assante, and Tim Conway. Analysis of the cyber attack on the ukrainian power grid defense use case. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, March 2016. [Accessed: 30, October 2016].

[37] Nancy Leveson. Engineering a safer world: applying systems thinking to safety, 2012.

[38] Nancy Leveson. An stpa primer, version 1. http://sunnyday.mit.edu/STPA-Primer-v0.pdf, August 2013. [Accessed: 6, December 2016].

[39] Nancy Leveson, Mirna Daouk, Nicolas Dulac, and Karen Marais. A systems theoretic approach to safety engineering. http://sunnyday.mit.edu/accidents/external2.pdf, October 2003. [Accessed: 6, December 2016].

[40] MB Connect Line. Security incident follow-up report. https://www.mbconnectline.com/de/neuigkeiten/presse-unternehmen/detail/security-incident-follow-up-report-09192014.html, September 2014. [Accessed: 30, October 2016].

[41] A. Loschmann. Private email, 2015.

[42] Checkpoint Software Technologies LTD. Scada cyber attacks timeline. http://www.slideshare.net/erangoldstein/scada-cyber-attacks-timeline, June 2016. [Accessed: 30, October 2016].

[43] Vaibhav Mehta, Constantinos Bartzis, Haifeng Zhu, Edmund Clarke, and Jeannette Wing. Ranking attack graphs. In *International Workshop on Recent Advances in Intrusion Detection*, pages 127–144. Springer, 2006.

[44] Merriam-Webster. Definition - hindsight. https://www.merriam-webster.com/dictionary/hindsight. [Accessed: 25, November 2016].

[45] Bill Miller and Dale Rowe. A survey of scada and critical infrastructure incidents. In *SIGITE, ACM*, October. 2012. [Accessed: 30, November 2016].

[46] Jose Nazario. Blackenergy ddos bot analysis. http://atlas-public.ec2.arbor.net/docs/BlackEnergy+DDoS+Bot+Analysis.pdf, October 2007. [Accessed: 26, November 2016].

[47] Ukrainian Ministry of Energy and Coal. The work group to study the causes of

the temporary malfunction of power supply companies. http://mpe.kmu.gov.ua/minugol/control/publish/article?art_id=245082298, December 2015. [Accessed: 30, October 2016].

[48] Headquarters Department of the Army. The cyber attack on saudi aramco. *Information Operations: Doctrine, Tactics, Techniques, and Procedures*, FM 3-13, November 2003.

[49] Jose Pagliery. Stamp workshop. advanced tutorial. cast - casual analysis using system theory. http://psas.scripts.mit.edu/home/get_pdf.php?name=1-6-CAST-Guided-Exercise.pdf, April 2012. [Accessed: 12, December 2016].

[50] Jose Pagliery. Scary questions in ukraine energy grid hack. http://money.cnn.com/2016/01/18/technology/ukraine-hack-russia/, January 2016. [Accessed: 30, October 2016].

[51] Fahmida Y. Rashid. Project shine reveals magnitude of internet-connected critical control systems. http://www.securityweek.com/project-shine-reveals-magnitude-internet-connected-critical/control-systems, October 2014. [Accessed: 21, March 2016].

[52] Kaspersky Lab Global Research and Analysis Team. Energectic bear - crouching yeti. https://kasperskycontenthub.com/securelist/files/2014/07/EB-YetiJuly2014-Public.pdf, July 2014. [Accessed: 21, March 2016].

[53] Symantec Security Response. Dragonfly: Western energy companies under sabotage threat. https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat, June 2014. [Accessed: 30, October 2016].

[54] Revuln. http://revuln.com. [Accessed: 4, December 2016].

[55] Jordan Robertson and Michael Riley. Mysterious 08 turkey pipeline blast opened new cyberwar. https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar, December 2014. [Accessed: 12, December 2016].

[56] Hamid Salim. Cyber safety : a systems thinking and systems theory approach to managing cyber security risks. Master's thesis, Massachusetts Institute of Technology, Cambridge, Massachusetts, 2014. [Accessed: 30, October 2016].

[57] Securelist. Blackenergy apt attacks in ukraine employ spearphishing with word documents. https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word/documents/, January 2016. [Accessed: 30, October 2016].

[58] Homeland Security, NCCIC, and ICS-CERT. Nccic/ics-cert year in review. https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf, 2015. [Accessed: 21, November 2016].

[59] Udi Shamir. Analyzing a new variant of blackenergy 3. https://www.sentinelone.com/wp-content/uploads/2016/01/BlackEnergy3_WP_012716_1c.pdf, January 2016. [Accessed: 7, November 2016].

[60] Shodan. Map of industrial control systems on the internet. https://icsmap.shodan.io, June. [Accessed: 26, November 2016].

[61] Murugiah Souppaya and Karen Scarfone. Guide to enterprise patch management

technologies. nist special publication 800-40 revision 3. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf, July 2013. [Accessed: 3, December 2016].

[62] Threat Stop. Black energy security report. http://www.threatstop.com/sites/default/files/threatstop_blackenergy.pdf, February 2016. [Accessed: 26, November 2016].

[63] Homeland Defense Subcommitee on National Security and Foreign Operations. Cybersecurity: Assessing the immediate threat to the united states. http://oversight.house.gov/wp-content/uploads/2012/04/5-25-11-Subcommittee-on-National-Security-Homeland-Defense-and-Foreign-Operations-Hearing-Transcript.pdf, 2011. [Accessed: 5, December 2016].

[64] Dragonfly Symantec. Cyberespionage attacks against energy suppliers, version 1.21. *Mountain View, California*, 2014.

[65] Kathy Trahan. Industrial control systems: Next frontier for cyber attacks? https://www.tripwire.com/state-of-security/featured/ics-next-frontier-for-cyber-attacks/, June 2016. [Accessed: 23, November 2016].

[66] Verizon. 2016 data breach investigations report. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/, 2016. [Accessed: 30, October 2016].

[67] David Whitehead, Kevin Owens, Dennis Gammel, and Jess Smith. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. https://cdn.selinc.com/assets/Literature/Publications/TechnicalPapers/6774_UkraineCyber_DEW_20161014_Web.pdf?v=20161019-161044, October 2016. [Accessed: 30, October 2016].

[68] James Wyke. Vawtrak - international crimeware-as-a-service. https://www.sophos.com/medialibrary/PDFs/technical%20papers/sophos-vawtrak-international-crimeware-as-a-service-tpna.pdf, 2014. [Accessed: 4, December 2016].

[69] Zerodium. https://www.zerodium.com. [Accessed: 4, December 2016].

[70] K Zetter. An unprecedented look at stuxnet, the world's first digital weapon. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/, March 2014.

[71] K Zetter. Inside the cunning, unprecedented hack of ukraine's power grid. http://www.wired.com/2016/03/inside-cunning/unprecedented-hack-ukraines-power-grid/, March 2016. [Accessed: 30, October 2016].

[72] Kim Zetter. An unprecedented look at stuxnet, the world's first digital weapon. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/, November 2014. [Accessed: 30, October 2016].

[73] Kim Zetter. A cyberattack has caused confirmed physical damage for the second time ever. https://www.wired.com/2015/01/german-steel-mill-hack-destruction/, January 2015. [Accessed: 30, October 2016].

[74] Bonnie Zhu, Anthony D. Joseph, and Shankar Sastry. A taxonomy of cyber attacks on SCADA systems. In *2011 IEEE International Conference on Internet*

of Things (iThings) & 4th IEEE International Conference on Cyber, Physical and Social Computing (CPSCom), Dalian, China, October 19-22, 2011, pages 380–388, 2011.

[75] Carson Zimmerman. Ten strategies of a world-class cybersecurity operations center. `http://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf`, 2014. [Accessed: 6, December 2016].