Proceedings of the 53rd Hawaii International Conference on System Sciences | 2020

The Role of Consequences in Securing Cyber-Physical Systems

Wm. Arthur Conklin
University of Houston
waconklin@uh.edu

Abstract

The importance of cybersecurity of cyber-physical systems is increasing across the wide spectrum of critical infrastructure systems and resulting in governmental attention to methods of reducing risks. Although these systems use computers to manage the communication and control of the processes, the systems are distinctly different from IT systems in business. Securing these cyber-physical systems require a different approach and set of tools. There are some unique characteristics of the physical systems under control that can be used to help mitigate risks associated with control system failures. This paper examines how security measures need to take a wider approach than just application of IT controls to a new environment if one is interested in truly managing the risk of these systems.

1. Introduction

Cyber-physical systems are systems where computers control physical processes. These systems exist in manufacturing, industrial settings, transportation, and a wide range of applications where computers are used to control actual real-world processes[1]. What makes these systems different from standard IT systems is that these systems control physical processes directly. This makes the risk equation different because of the impact associated with the physical system[2]. Because many of our critical infrastructures have an operational technology based cyber component, securing them has become an issue of importance to government, at national and local levels.

The challenge of applying security practices to cyber-physical systems lies in their structural differences from standard IT systems. These differences have resulted in the application of computers and networking being labeled as operational technology (OT) to distinguish it from standard IT. There are a host of differences between computer systems used in operational technology versus information technology. OT systems can have lifetimes in decades, and updates and changes are exceedingly rare. OT computer systems become integrated into the physical processes that they control, and changes are time consuming and expensive. From a security perspective, they have completely different risk profiles from an IT system[2]. One of the principal differences in IT and OT systems lies in their security policies. The security policy of an IT system is defined around the data and the principles of confidentiality, integrity and availability. For OT systems, the security policy is defined around safe and resilient operations. The implications of these differences are significant and can be seen throughout how the systems are designed, built and operated.

There are many unique challenges associated with OT systems that can complicate efforts to apply standard cybersecurity practices. There are also some unique characteristics that can be used to enhance overall system security. Because of their connection to actual physical processes, risk can be expressed in terms of consequences to a physical system, and the losses can be significantly more complicated and dangerous than simple data losses.

This paper examines the unique characteristics of cyber-physical systems, OT, and their associated risk issues. It does so through a lens that will assist in the development of appropriate and applicable risk mitigation standards and policies that can be employed by regulatory bodies to these unique systems. The objective of this paper is to highlight some of the key differences between IT and OT systems that can be employed to assist in proper security postures. The physical consequences of the system under control offers some unique perspectives in managing security risk in these systems. Understanding and using the unique differences in OT systems is important when developing policies and regulations to manage cybersecurity risk across these critical systems.

The term critical infrastructure is widely used in industry and government and is defined as systems

URI: https://hdl.handle.net/10125/63982
978-0-9981331-3-3

"whose incapacity or destruction would have a debilitating impact on our defense and economic security"[3].

This paper begins with an examination of OT systems and their unique characteristics. In section 3 it examines methods of examining cybersecurity risk in OT systems. Section 4 shows how these methods can be applied to OT systems, using their unique characteristics to improve risk postures. Section 5 examines how cybersecurity is actually practiced in OT systems, contrasting this with the more commonly understood practices employed in IT system. The paper concludes with conclusions and next steps.

2. System Characteristics

IT and OT systems, while using many of the same components are substantially different in configuration and use. Initially OT systems were networked using proprietary protocols and private communication paths. While IT systems were designed to increase in value through greater connectivity, OT systems thrived via isolation[4]. Three major changes have occurred over the past couple of decades that have driven change in OT system architectures. The first two act as partners in crime, TCP/IP networking flourishes and becomes ubiquitous at the same time businesses realize the value in real-time use of operational data. These changes resulted in many OT systems adopting TCP/IP for networking and the connection of OT and IT networks. The third point is the use of wireless networking to reduce networking connection costs. While these changes have brought about a convergence of IT and OT networks, there is still a significant difference in the two networks when examined from a risk or security point of view.

2.1 IT System Characteristics

IT systems have been defined by the types of data they handle in an organization. It is tough to find a business that does not have some from of IT, for information has become key to most if not all businesses. From things such as email, to web, to data storage, business management, inventory management, manufacturing execution systems, and more – data drives the modern enterprise. And when the data stops, in many cases, so does the business as illustrated by the plague of ransomware in the past few years[5, 6].

2.2 OT System Characteristics

Historically, OT systems had little resemblance to traditional IT systems in business. OT systems are specific purpose systems, not general purpose like IT. OT systems were isolated systems, using isolated networks, running proprietary protocols using specialized hardware and software. Many OT components were in physically secured areas and they were not connected to IT networks or systems

While the computers used in operational technology networks are many times the same type of PC, using the same operating systems (sometimes older versions) as found in most business networks, they live in a completely different environment. These differences stem from a couple of key differences between IT and OT networks. The first major difference is that OT networks support a host of additional connected devices that are not computers running standard OS's, but rather are special purpose devices such as programmable logic controllers (PLCs), remote terminal unites (RTUs), and human machine interfaces (HMIs). These devices form the backbone of the connection between the computers and networks, and the physical devices under control. These devices were also designed and created long before security was a primary concern and designed for resilience and 100% availability. As such, they as a general rule do not use forms of authentication, encryption, or other endpoint security functionality. This provides an interesting security issue as there is no ability to manage access control to these devices. So even if it can be invoked on the computer running the specialized software, access control cannot extend to the physical devices that are being controlled.

The lack of defined users via access control mechanisms throughout an OT system makes security controls such as defined in NIST SP800-53 meaningless. Without the elements of confidentiality, integrity and availability, the entire basis of the security control structure falls apart. That is not to imply that the controls are not useful, for they can be, but it definitely changes how, when, and where they can be employed. This issue goes directly to the hear of the difference in IT security postures which support an IT security policy and OT security efforts to support the OT security policy. Because of the differences in policy objectives between the two, these implementation differences are not drastic as one would immediately suspect.

The network architectures employed in OT networks stands in stark contrast to that of IT. In IT networks, the basic idea is to have as flat a network as possible, with as few impediments to traffic as

possible, and let the Internet Protocol stack manage the traffic. This is fine when the objective is to let everything talk to everything, and in many IT networks the breadth of network conversations is significant. In OT networks, there are a limited number of specific communication channels employed. PLC's talk to HMIs and historians, HMI's talk to PLC's and historians, but PLC's don't talk to another PLC. Typically, only one protocol is used locally, so the variety of traffic; FTP, HTTP, email, etc., is not seen on the OT network. This reduction in traffic is essential given the nature of OT message timings, and failure to segregate traffic and OT system isolation failures have led to disasters[7].

Another major difference between IT and OT systems is in their design philosophy. While IT systems are all about the data, OT systems are all about operating safely and with resilience[4]. IT systems have been advancing on a technology driven curve for the past 30+ years, with refresh lifecycles of 3 to 5 years. New OS's, new processors, new software, a PC that is 5 years old is considered ancient in the IT environment. OT systems were designed and built for 20 to 30-year lifecycles. This means it is not uncommon to find older versions of hardware and software still in service in OT systems. Because of the nature of the physical processes under OT system control, change is not a good thing, and neither is downtime. These systems can run for years without rebooting or being taken down for maintenance. This makes things like patching a challenge. Any change to a system, either by upgrade or patch, must undergo a thorough examination to ensure it does not cause unintended consequences to a system's overall operation.

OT networks are also different when looked at from a signal timing perspective. OT messages are typically time sensitive and networks are designed to ensure there is sufficient bandwidth to ensure timely communications. While this seems trivial, realize that many OT networks can extend over large distances, in the case of pipelines, thousands of kilometers. Network connectivity across the entire reach of an OT network is also a challenge, as the standard high bandwidth IT networks in business do not necessarily extend well in widespread and industrial environments. Many OT systems were hardwired RS-232 systems before networking replaced these communication channels and the message sequencing versus bandwidth issues were measured and designed into the systems. Today's networking protocols make those decisions a thing of the past, but there are still communication implications when missing even a single message can become an issue.

An example can be seen in something as simple as the addition of a new switch on the network, with new devices. Even if the network has sufficient bandwidth to ensure no loss of current signals, the simple act of the network reconfiguring it's spanning tree protocol, an automatic function, can result in a 45 second to one minute traffic delay. To an IT network, this is rarely a problem. But in that time in an operational system, many critical messages may be lost in an OT network, resulting in the system being shut down by safety systems because they believe the network to be non-responsive.

There is much talk of convergence of OT and IT networks, and if by convergence, one is referring to connections, then, yes, they are being cross connected. But when convergence means operations, then the answer is clearly no, the two systems are operated completely differently[8]. Simply put, the differences between IT and OT make security functions a completely different world.

3. Cybersecurity Risk Analysis for OT Systems

Functional cybersecurity is an exercise in risk management. One of the foundational elements is risk analysis, an examination of the sources and impacts of the various risk factors to an enterprise. There are a variety of tools and methodologies used to perform these analysis tasks, and each has strengths and weaknesses.

In IT systems, risk is typically examined with respect to the CIA model; confidentiality, integrity, and availability, and in the end is centered around data-specific issues. In OT systems, the assessment of risk includes physical effects; damage to people, process, and the environment. These result in profoundly different methods of assessment and outcomes. For OT systems, an analysis of potential physical damage to the facility, the system output, persons, and the environment needs to be considered.

An analysis of the drivers of risk can be done in several different methods. The simple method of quantitative risk analysis from probability and impact is one method, examining the cybersecurity kill chain another and bow tie analysis is yet a third. Each of these has a useful role to play in how we measure and manage IT risks, and each can be employed in OT systems.

OT systems have an additional element that can be leveraged in controlling risk, and those are the specific physical properties of the system under control. Physical systems have limitations that can be used to mitigate risk in the event of control issues from the OT side of the system. The use of

engineering design in the form of consequence centered engineering can provide significant risk reductions in a system.

3.1 Quantitative Risk Measurement

One of the standard quantitative measures used to determine overall risk in cybersecurity is represented by the equation:

Risk = Likelihood of an adverse event
× Impact of the adverse event [9]

The two key factors are the likelihood of something happening and the impact if it does. These factors can be used in a variety of forms, both quantitative and qualitative to determine risk postures. They can also be done in aggregate, or as a series of individual independent elements. This methodology has its roots in how insurance losses can be calculated actuarily, but it has some significant limitations. First, it has scaling issues with complexities. As systems can be comprised of subsystems, and the number of elements increase, determining all of the individual risks becomes an algebraic solution of a bookkeeping nightmare. While the summations can be easy, both is serial and parallel forms, the determination of all of the individual factors grows beyond the ability to track. The second major issue is that the events we are protecting against are not necessarily independent. If a hacker achieves access using a specific method against one of your machines, it is a solid bet it will happen again against other machines in your network.

So, while this is a good method of determining the risk associated with losing assets, it is not a proactive method of analyzing all of the individual risks to determine overall composite risks.

3.2 Cybersecurity Kill Chain

The process of a Cyber Kill Chain was developed by Lockheed Martin to analyze the steps attackers use against systems to assist defenders in determining defense strategies[10]. The kill chain concept is similar to the lifecycle analysis of an organism in biology, where a system is observed across its lifecycle, and then at appropriate points the system can be attacked. This analysis of lifecycle weaknesses relies upon a consistent pattern of events across the lifecycle of an object or system. Cybersecurity related attacks tend to follow a known pattern of sequential steps and this information can be used to determine the best place in the lifecycle of an attack to mount a defense.

In the case of cybersecurity attacks, the stages of the Kill Chain are presented in Figure 1. The Kill Chain provides defenders a simplistic picture of a cybersecurity event as a linear process that moves consecutively through specific stages, with the objective of highlighting potential defensive activity points.[11]

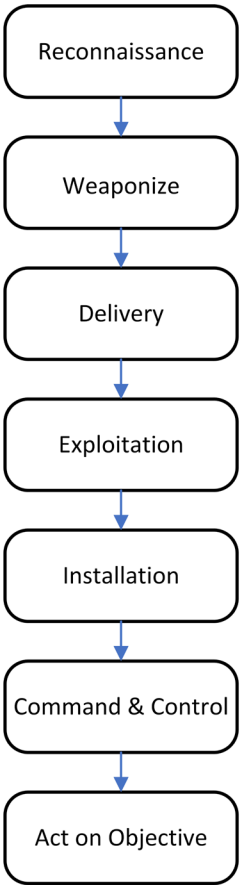

Figure 1. Cybersecurity Kill Chain [11]

The kill chain's most useful purpose is to help defenders determine where the best opportunities are for detecting attacks and defending against them. It is not necessary to interrupt all the aspects of the attacker's actions, represented as steps on the kill chain. Rather it is important to catch and stop attackers before they get to the final objective. So, while it may be difficult or impractical to attempt to stop an attacker at the earlier stages, there are points in the kill chain where activity can be observed and attacks stopped. Using multiple points and implementing a defense in depth approach can be

effective at greatly increasing the odds of catching and stopping an attack.

The cybersecurity kill chain also suffers from a scale problem in that large systems of systems, such as modern IT enterprises, this methodology has to be performed over and over at multiple locations, as attacks that are local may not be observed at a distance. This same issue can affect critical infrastructure systems, where there are many systems of systems that can be loosely connected and result in the need for repeated defensive structures. The strength of the Cyber Kill Chain methodology when employed on OT systems comes from the simplicity of the OT network, limiting the points of interaction to a few key places in the network. The network enclaving of traffic works to enhance the chance of detection of specific events associated with the kill chain, improving its utility.

When employed from an appropriate level of analysis, the cybersecurity kill chain has proven itself to be a useful tool in defending against many sophisticated attacks such as advanced persistent threats. This tool allows the concentration of detection forces where they can be most effective, and the employment of defensive controls where they can be most effective, even when these are in separate parts of the kill chain. When employed as a series of overlapping defense in depth methods, this methodology has proven very effective in combating the complex attacks faced in many systems today.

3.3 Bow Tie Risk Analysis

Bow Tie (BT) is a graphical method commonly used for process risk analysis. It combines Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) to prioritize risk management activities. [12, 13] The undesired event is the top event of the fault tree. Using the undesired event as the pivot node, BT employs FT to determine the potential causes and ET to determine the potential consequences for the undesired event. The bow tie methodology provides information both on the causes of risk, and the consequences from failures to mitigate the risks, producing a more comprehensive picture of the overall risk exposures in a system.

The bow tie analysis method is particularly good at analyzing multiple different causes and effects associated with failures, whether from a purposeful attack or merely a failure of some component. This makes the bow tie method very useful in an all hazards approach that is used in many systems, both in IT and OT to determine specific risk elements.

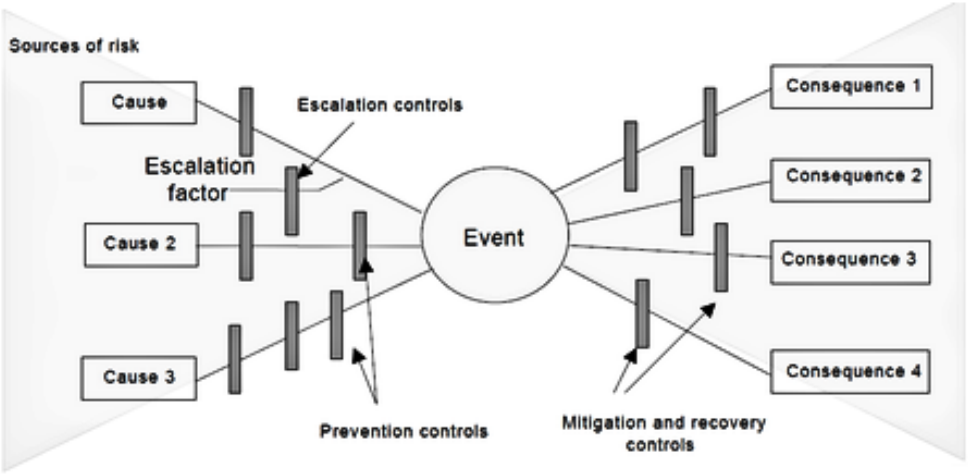

Figure 2. Simplified Bow Tie Analysis

A sample graphical depiction of BT analysis is shown in Figure 2.

This simplified model shows that controls can be placed on left hand side to address the fault tree items that can lead to the undesired event. These controls can be against specific root causes, or against factors that can escalate the situation.

Should the undesired event occur, then the consequences of the event are modeled using event

trees to illustrate the various risks and potential mitigation or recovery controls. Putting these all to work in the form of a ransomware infection example will help clarify the processes involved. For ransomware, the undesired event is a ransomware infection. The outcome of this infection can be minor – the loss of a few files and inconvenience, or it could result in the loss of the whole business if all data is lost, or somewhere between these two extremes. The causes of the ransomware infection can be many, from simple phishing attacks, to watering hole attacks, to advanced attacks, although not infinite, a great many ways to initiate a ransomware attack exist. This can make the total size of the detailed fault tree very difficult to manage. If a multilayer approach is used, many of the individual initial elements can combine into common elements, making the defensive approach more manageable with later application of controls after the combination of sources occurs.

In the case of ransomware, if it occurs (the central event), multiple consequences can occur, across the range already described. A series of mitigation and recovery tools, such as parallel systems, backups, and network isolations can be employed to prevent the spread and subsequent damage from the attack.

Again, as in the previous models, the scalability of the bow tie model is challenging as system complexity increases and the number of threats increase. Although the calculus of managing the data can be done with Bayesian networks [13], this method rapidly becomes challenging with the myriad of risks associated with modern computer systems.

All of these risk models work well to an intended level of complexity and are useful for managing risk at high levels. None of them are useful against individual threats to individual components on a system with hundreds of threats against hundreds of interconnected components. The math, while as accurate as the inputs, becomes meaningless with respect to being an actionable component in the management of the system.

4. Application of Risk Management to CPS

The application of risk management to cyber-physical systems is not new or novel. These systems are engineered systems and have used methods such as fault trees and failure mode effect analysis to manage failures for decades. One of the major differences between IT and OT networks is the level of risk driven control exerted over changes in the systems.

In IT networks, there are varying level of change control mechanisms used, but at the end of the day, the network, its components, and software elements are updated and changed on a fairly regular basis. This has become standard practice and is a security best practice. The patching of known flaws and the updating of software is a routine task. Similar is the employment of security controls such as antivirus/antimalware programs, access control mechanisms including two factor methods for high risk systems, and controls such as backups to restore data when lost or damaged.

In OT systems, the use of change control is highly controlled. Systems are rarely updated, for that would require them to be shut down and restarted. Systems such as pipelines, utility grids, refineries, chemical plants, they run 24 hours by 7 days a week by 365 days a year, and if possible, for multiple years between shutdowns. As most of these systems are actually systems of systems, there are times that individual components can be updated, changed, repaired or fixed. But change comes with a risk of will the system work the exact same way as before? In IT systems we have all heard the stories of how a specific patch caused an issue, resulting in the change control process forcing it to be backed out and the original system restored. Many times, there is a time lag between these changes, so in essence a second change corrects the first. In the case of an OT system, this “outage” can have severe physical consequences. If an IT system goes down, and data is lost, then a good backup system can restore it. In an OT system, if the system fails from an update, equipment can become damaged, people hurt, or environmental damage, none of these can be addressed via a backup strategy. This is the basis of the security policy that is focused on safety and resilience. Safety protects the system, resilience protects the output of the system.

5. OT system security

OT systems have distinctly different attack taxonomies than IT systems[14-16]. There are a wide range of reasons, but one of the most common is the attacker objective. For an OT system, the attacker objectives include such elements as loss of control, or loss of view, elements designed to separate plant operations from operator control. When examining incidents such as Stuxnet or the Ukrainian electric grid attack, these elements become clear. OT security elements are specifically designed to prevent these problems, regardless of the source, from impacting the security of the facility.

In most OT systems, there is a fall back system, the safety system, that is integrated into system

operations with one overarching objective; do not allow the system to fail to an unsafe position. These safety systems are not specifically part of the security system, they exist as a last line of defense, but the manner in which they are constructed goes to the point of using the system itself as a security mechanism.

OT systems have been designed for years using a completely different network architecture designed to provide isolation and resiliency to its component structures. This architecture, know as the Purdue architecture, defines zones and conduits that are used to control information flow and thus control across a system[17]. In OT systems, the role of network as a security control has diminished in importance as networks have become hardened to specific attack and network security is no longer in the top 20 security controls list. But in OT networks, the network is part of the system and its role in ensuring system resilience is important because the network is part of the control system and the control system is part of the overall operational system, thus network issues can become system issues. This goes beyond simple data or transport issues, but to the core of the overall system. This makes network isolation as defined in ISA-99 a key security component in the overall system.

Another key operational characteristic of the system that can lead to better security is the design of the specific components so that failure result in a safe state or at least a state that physically cannot become catastrophic. An example of this is in a water treatment plant where chemicals are added to water for potability – typically a chlorine agent to disinfect. If an unlimited supply, both in quantity and in delivery rate were available, then an attacker could command an unsafe amount of additive. But if the system is designed so that no more than a 50% increase in additive rate could ever be applied, and this level is still in the safe range, then this engineering design would never fail to an unsafe level.

Another example is the use of output filters to test output conditions before applying them to the physical system. The concept of having these filters post control system allows them to mediate outputs without influence from an external source. Many traffic lights use just such a system, so that when the logic circuits tell the lights to change patterns, this circuit then interprets the new condition to see if it is legal. Even if the PLCs tell all lights to turn green, this filter then intercepts this output, determines it is not allowed and switches the lights to a safe alternate state -typically all flashing red. It then disconnects the system from the control circuit until it is reset.

The use of these physical controls, be it a pipe size that restricts flow, a separate system to check outputs, a set of mechanical stops to prevent specific unallowed movement, these are all physical process elements that can be designed into the system to assist in the attainment of safe and resilient operation.

There are many additional OT specific security methods that are employed to fulfill the security policy mandate, but for the purposes of this paper, the key elements are the focus on the security objective differences and the use of physical process controls as part of a system solution.

6. Conclusions

IT and OT systems while sharing many similar or even identical components have dramatically different environments and operating characteristics. These are clearly summed up in the different security policies employed. While security policies are high level in nature, most OT systems have inherent physical properties that are also foundational in nature and can be used to help manage risk. This paper examined some of the differences and demonstrated why OT systems require different security mechanisms than IT systems. This is important to consider these differences when developing government regulations and standards associated with OT based critical infrastructure controls.

When examining the levers one has to control with respect to securing critical infrastructure elements that are built with cyber-physical systems it is of utmost importance not to fall into the trap of thinking these are just another IT system. OT systems have different capabilities and limitations than IT systems, both on a component level and on a system level. Attempting to regulate security using rules and objectives from a different domain will result is less than optimal outcomes. Early attempts in the regulation of cybersecurity in the electric sector led to rules that any network connected device must use an antivirus solution or have a written exception report. This led to many technical feasibility exception reports for routers and switches, as these are network connected devices, and although they never could run an antivirus solution, the rules didn't care.

Meaningful security solutions can be had for the cyber-physical systems that comprise the critical infrastructure systems of our society. Regulations can be made that help in the proper securing of this important asset. What is important is that the regulations be drafted for the OT systems in a manner that is befitting them, not an IT system. Mandating

that all communications be encrypted end to end with a specific level of user level authentication may make sense in IT systems, but in the majority of OT systems these elements are not even possible.

7. Future work

This paper examined some key differences between IT and OT systems when it comes to cybersecurity. There is a whole new class of systems, built around the Internet of Things concept, where the scale of number of devices becomes incredibly large and possibly over the entire globe. These systems, whether called the Internet of Things (IOT) or the Industrial Internet of Things (IIOT) will have different security objectives and methods because they too will be different than either IT or OT systems. Regulating these systems will need to be done through the lens of their capabilities and limitations, and not done as we are doing either IT or OT systems.

8. References

[1] E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress, 2014.

[2] R. J. E. Piggin and Technology, "Industrial systems: cyber-security's new battlefront [Information Technology Operational Technology]," vol. 9, no. 8, pp. 70-74, 2014.

[3] J. Ellis, D. Fisher, T. Longstaff, L. Pesante, and R. Pethia, "Report to the President's Commission on Critical Infrastructure Protection," Carnegie Mellon University Software Engineering Institute, 1997. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a324232.pdf

[4] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, A. J. N. I. o. S. Hahn, and Technology, "NIST special publication 800-82, revision 2: Guide to industrial control systems (ICS) security," 2014.

[5] A. Greenberg, "The untold story of notpetya, the most devastating cyberattack in history. Wired, 22 August, 2018," ed, 2018.

[6] B. A. S. Al-rimy, M. A. Maarof, S. Z. M. J. C. Shaid, and Security, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions," vol. 74, pp. 144-166, 2018.

[7] S. Ismail, E. Sitnikova, and J. Slay, "Towards developing scada systems security measures for critical infrastructures against cyber-terrorist attacks," in *IFIP International Information Security Conference*, 2014: Springer, pp. 242-249.

[8] G. Murray, M. N. Johnstone, and C. Valli, "The convergence of IT and OT in critical infrastructure," 2017.

[9] (2012). *SP 800-30 r1 Guide for Conducting Risk Assessments*.

[10] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research,* vol. 1, no. 1, p. 80, 2011.

[11] T. Yadav and A. M. Rao, "Technical aspects of cyber kill chain," in *International Symposium on Security in Computing and Communication*, 2015: Springer, pp. 438-452.

[12] K. Mokhtari, J. Ren, C. Roberts, and J. Wang, "Application of a generic bow-tie based risk analysis framework on risk management of sea ports and offshore terminals," *Journal of hazardous materials,* vol. 192, no. 2, pp. 465-475, 2011.

[13] N. Khakzad, F. Khan, and P. Amyotte, "Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network," *Process Safety and Environmental Protection,* vol. 91, no. 1-2, pp. 46-53, 2013, doi: doi.org/10.1016/j.ssci.2013.01.022.

[14] (2015). *SP 800–82 revision 2 Guide to Industrial Control Systems (ICS) security*.

[15] B. Miller and D. C. Rowe, "A survey SCADA of and critical infrastructure incidents," *RIIT,* vol. 12, pp. 51-56, 2012.

[16] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *2011 International conference on internet of things and 4th international conference on cyber, physical and social computing*, 2011: IEEE, pp. 380-388.

[17] *ANSI/ISA–99.00.01–2007*, ANSI/ISA, 2007.