 doi:10.20944/preprints201804.0066.v1

Cybercrime and Risks for Cyber Physical Systems: A Review

2018

[1]Abel Yeboah-Ofori
Computer Science Department
University of Ghana
Ayeboah-ofori@gtuc.edu.gh

[2]Dr. Jamal-Deen Abdulai
Computer Science Department
University of Ghana
jabduli@ug.edu.gh

[3]Dr. Ferdinand Katsriku
Computer Science Department
University of Ghana
fkatsriku@ug.edu.gh

Abstract

Cyber Physical Systems (CPS) is the integration of computation and physical process that makes a complete system such as the physical components, networked systems, embedded computers and software and linking together of devices and sensors for information sharing. Cyber Physical Systems are Smart Systems that comprises of the merging and integration of Industry Control Systems, Critical Infrastructures, Internet of Things (IoT) and Embedded Systems. Major industries such as the Chemical and Industrial Plants, Aviation Systems, National Grid, the Stock Exchange, Military Systems, and others depends heavily on these Cyber Physical Systems for financial and economic growth. The benefits of CPS nationally and globally are in the areas of Manufacturing, Energy, Transport, Healthcare and Communication. Cyber Physical Systems incorporates Physical systems, Digital systems and Human elements on network infrastructures to provide interactive systems. However, these three key components the Physical systems, Digital systems and Human elements may have inherent threats and vulnerabilities on them that may run the risk of being compromise, exploited, attacked or hacked. Cybercriminals in their quest to bring down these systems and may cause disruption of services either for fame, revenge, political motive, economic war, cyber terrorism and cyber war. The study seeks to review the risks that are associated with these three key components Physical systems, Digital systems and Human elements. The study considered four main risk mitigation goals for this purpose, and these are Business Value, Organizational Requirements, Threat Agent and Impact based on the review results. We used Analytical Hierarchical Process (AHP) to determine the relative importance of these goals that contributes to developing cybercrime and rich in CPS. For the results, the prioritized goals are then used to assess the risks using a semi-quantitative approach to determine the net threat level.

Keywords: Cyber Physical Systems, Cybercrime, Risk Mitigation, Risk Management, Industrial Control Systems.

1.0 Introduction

Studies have shown the economic and societal impact of Cyber Physical Systems (CPS) and how its infrastructures and applications has brought about economic benefits nationally and globally in the areas of Transport, Energy, Healthcare, Manufacturing and Communication. Cyber Physical Systems is the integration and configuration of computation, networking and physical processing systems that are embedded together and uses computer, sensors, actuators and network monitors to control processes that affect computations. [27]. CPS technology integrates the dynamics of analysis and design, modeling, abstractions of physical processes with those of the software and network topologies and provides a (smart grid) system infrastructure. Cybercrimes are crimes committed using computers and the internet. Cybercrime can be initiated from any were in the world on Network Control Systems (NCS) and Supervisory Control and Data Acquisition (SCADA) systems and know no boundaries. [10]. Major industries such as the National Grid, Stock Exchange, Aviation Systems, Military, Chemical Plants and others depends heavily on these cyber physical systems for financial and economic growth. They are autonomous systems that makes decision in real time using agents and requires real time availability of

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

information. However, these Cyber Physical Systems have vulnerabilities imbedded in them which may run the risk of being exploited by cybercriminals in their quest to bring down the system and cause disruption for fame, revenge, political motivate, economic war, cyber terrorism and cyber war. Stuxnet attack [10]. Duqu malware [9]. These perpetrators can initiate zero day attacks, evil maid attack, Denial of service attack, resonance attacks and malware, ransomware, spoofing, rootkit, and botnet attacks. The study considered four main mitigation goals for this purpose and these are Business Value, Organizational Requirements, Threat Agent and Impact Vectors based. The review results will be used to determine the relative importance of these goals using Analytic Hierarch Process (AHP). [35], [19]. The prioritized goals are then used to assess the risks using a semi-quantitative approach to determine the net threat level. The reason for considering the goals for risk assessment is that risk is define as a negation of a mitigation goal [19]. The study reviews CPS as three entities as: merging Physical systems, Digital systems and Human elements. Organizations that run their businesses using CPS platforms has certain goals or objectives that they want to achieve with the mitigation decision and risks certainly obstruct through these goals. The study considered two real mitigation use case to determine the relative importance of the goals and compare the results.

The structured of the paper is as follows: section 1 looks at background CPS risk and taxonomy of cybercrime. Section 2 outlines the overview of the search methodology for the state of the art review on, cyber physical systems, risk mitigation, cybercrime. Section 3 provides details of the findings and synthesis from the start of the art review. Section 4: provides details about the discussions, analysis. Section 5 discusses the risk mitigations goals, relative importance, net results, risk management and limitations. Section 6 presents the conclusions and recommendations.

2.0 Research Methodology for the State of The Art

The state of the art review combines a Systematic Literature Review (SLR) using journals and articles to understand the recent trend of risks on Cyber Physical Systems. The SLR will be based on a clearly formulated research and identify relevant studies, appraise their quality, synthesize and summaries the evidence by use of explicit methodology. The research methodology will conduct a literature review and consolidate the analysis from the review.

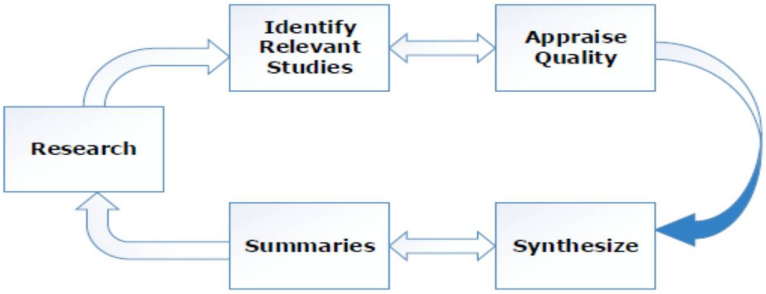

Figure 1. Research Methodology Process

The systematically identification and combination of these two techniques will assist the researchers to identify available evidence on cyber physical system risks from both academic and industry works. The study will adopt three main review steps, i.e. Planning, Conducting and Documenting. [24], [6] as shown in figure 2 below.

2.1 Step 1: Planning

With the initial step, we plan the research by identifying the necessity of literature, research questions, and relevant methods for the review. As stated previously, risk in CPS are critical, as it is one of the challengers of using the cyber space. There have been research work done in the areas of risk on CPS and risk mitigation practices in cybercrime. However, there are no study that identifies, analyze and compares all these works in an evolving threat landscape on CPS. Such study is necessary to identify the trend of research, research gap and

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

future directions so that CPS risk management can effectively supports organizations using cyber physical systems and the cyberspace.

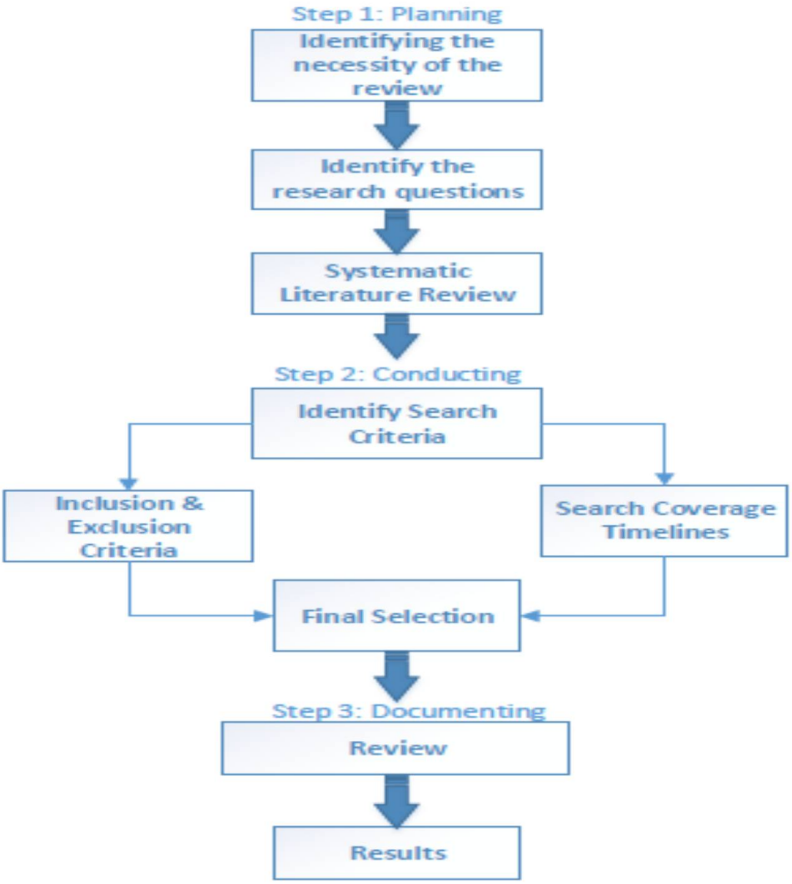

Figure 2. An Overview of Research Methodology for Review

Research Questions	Justification
RQ1: What are the various concepts, threat landscapes, attacks vectors necessary to develop and monitor cyber risks on Cyber Physical Systems	The Purpose is to obtain in-depth understanding of the threats and vulnerabilities and attacks existing in the cyber environment
RQ2: What are the various internal and external threats parameters needed to build threat models?	The purpose is to identify the key risks mitigation processes from all dimensions on CPS
RQ3: What is the state of existing research and future directions on CPS risk mitigation?	The review aims to understand the advancement of research practice of risk mitigations on CPS

Table 1. Research Questions for Review

2.2 Step 2. Conducting

The second step concerns mainly with the final selection of the studies for the review by the step 3. The study aims to identify literatures that deal with cybercrime threats, vulnerabilities and the attacks that can be initiated from anywhere on the cyber physical systems. The following keywords were used as search criteria: Cyber Physical System, Cybercrime, CPS Risk Mitigation, Risk mitigation and Risk Management

The study will use search engines from sources such as Google Scholar, IEEE Xplore, Elsivier, ACM Digital Library and Science Direct to extract the literature. Literatures relating to social commentary and expert opinions are to identify the practitioners view relating to the threats, vulnerabilities, attacks, impacts, and existing industry practices that used to mitigate CPS risks.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

The selected papers for the research were mostly from CPS risk, security related journals, and articles published from 2002 to date, as the CPS research domain is recent and are evolving rapidly. We selected the cybercrime related and legal frameworks journal from 1998 to date. The initial search identified 48 papers from the sites and 24 times from industry related sources. After reviewing the title and abstract, we observed that most of the works consider CPS design, CPS security and cyber risks and very few on CPS business risks. We carefully considered the final selection based on inclusion and exclusion criteria as shown in table 2 and table 3.

The inclusion criteria emphasizes on coverage of the area, timelines of solutions, and overall quality. We placed particular emphasis on selected literatures to ensure if they cover identified areas from well-known sites. Finally, we selected a total of 36 journals, publications and practitioners for review.

2.2.1 Inclusion Criteria

Inclusion Criteria	Justification
IC1 **(Coverage, Quality):** Works that focus on the risk, threat and vulnerabilities and impact in cyber physical systems	The search is interested in identifying what critical threats and vulnerabilities exist and the possible solutions there are for mitigating these cybercrimes.
IC2 **(Coverage, Timelines of the Solution)** Studies that considers cyber physical system security, risks management, techniques and tools for mitigation.	Such works provide concrete solutions on how to review, analysis and control the cyber risk critical infrastructures.
IC3 **(Timelines of Solutions):** Industry practice for mitigating risks.	The study emphasis on timely practice as it provides a realistic view of how risks are controlled by the industries using critical infrastructure.

Table 2. Inclusion Criteria

2.2.2 Exclusion Criteria

Exclusion Criteria	Justification
EC1: Works that do not clearly focus on risk, mitigating, management relating to cyber physical systems.	The main goal of the study is to identify the CPS risks. Therefore, the interest is not in other studies that does not emphasis on risk management or risk mitigation process in the domain.
EC2: Works that do not consider CPS risk mitigation process or tools.	CPS risk is a critical area for many domains. But the study is only interested in works that is explicitly considered from risk perspective.
EC3: Those from thesis and books chapters.	The study mainly consider conference and journal papers from literature reviews industry practices and articles, industry presentations, blogs, ISP websites, and white papers.

Table 3. Exclusion Criteria

2.2.3 Step 3. Documentation

This phase is the final step of the review. Here we split selected papers into five main categories based on the focus of the review, i.e.

- CPS taxonomy, CPS attacks, Threats and vulnerabilities and risk management;
- Risk and Controls;
- Laws and Legislative Framework;
- Impact: Financial, socio-economic and business assets;

Table 3 shows the main areas that take into consideration the individual category and summarizes the papers based on the category. We present the review of the selected articles, research trend and future directions as follows:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

Category	Main Areas	Papers
CPS risk management, attacks taxonomy, Cyber-attacks, Threats and vulnerabilities and	Mitigation processes, Definitions and categories of CPS, Diversities of attacks, threats, vulnerabilities that exist on CPS infrastructures.	Humayed et al. (2017), Al Faruque et al (2010). Lee & Seshia (2011), Alvaro Et al. (2010). Wan et.al (2015). Lewis (2002). Leyden (2017. Lupus (2014) Kayode et al. (2014), NIST 2014).
Risk and Controls in Cyber Physical Systems	Typical Risk assessment processes, areas technical and non-technical	Lee, 2012, Shoukry et al. (2013); Verma & Chundri (2016). Al Faruque et al (2010), Gollmann (2013) GSMA (2014). Falliere et al. (2011). Chien et al. (2012). Alvaro Et al. (2010), ITU (2012), Gordon et al. (2003),
Laws and Legislative Frameworks	The various laws and legal frameworks that exist in various countries	Zeviar-Geese (1998), Weber (2003) Marion (2010), ITU (2012), NIST (2014), Zappa(2014), Jubb (2015)
Impact: Financial, socio-economic, business assets and Insurance	Primary impact on CPS critical infrastructures and data assets, trade secrets. Human vulnerabilities that impacts on procedural security that causes financial losses, insurance and economic impact	Gapgemini (2015), Zappa (2014), Anderson et al. (2012), NIST (2014) WEF (2013),

Table 4. Categories, Main Areas and Papers from the Selected Areas

3.0 Review of the State of the Art

This section reviews the selected papers and articles from the previous section for the state of the art review.

3.1 CPS Risk Management, Taxonomy, Attacks, Threats, Vulnerabilities

3.1.1 CPS Risk Management Framework

Managing cyber physical systems risk is a challenging task for industry adoption. Risk is the probability of an attack initiated or something bad happening to the critical infrastructures system such as the process failure, component or application failure. This section includes works that considers critical cyber physical system areas. [17], proposed a unified framework that consist of three orthogonal coordinates namely: (1) from the security perspective, the authors followed the well-known taxonomy of threats, vulnerabilities, attacks and controls. (2) from the CPS components perspective, the authors focused on cyber, physical and cyber-physical components: (3) from the CPS systems perspective, the authors explored general CPS features as well as the representative systems such as smart grids, medical CPS and smart cars.

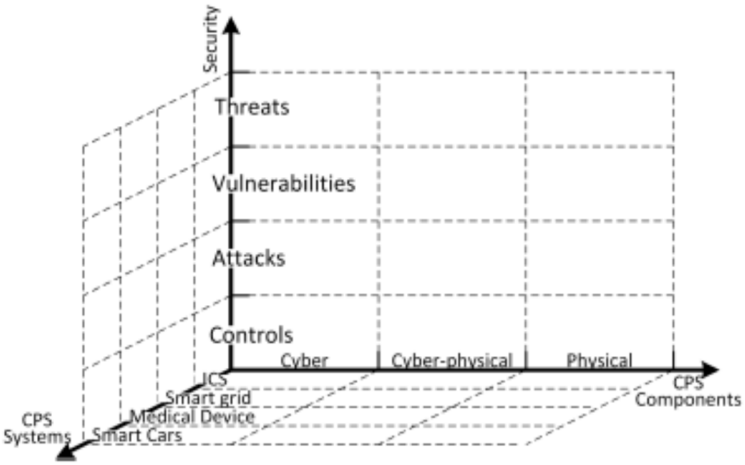

Figure 3. CPS Security Framework with Three Orthogonal Coordinates. [17]

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

The model was both abstract to capture the general interactions of a CPS application and specific to capture any details when needed. Their aim was to build a model that is abstract enough to be applicable to various heterogeneous CPS applications and to gain a modular view of the tightly coupled CPS components. The abstract decoupling will make it possible to gain a systematic understanding of CPS security and to tighten the potential sources of attacks and protection measures. However, the framework is generic and lacks specificity in detection of cybercrimes risks on CPS. The paper did not address the issues of social engineering risk from physical security perspective. [46], proposed a framework for design of secure control systems for CPS whilst taking into account properties of the underlining computations and communication platforms. The authors considered security as part of the completed CPS design process, from the start in the new design method. They addressed design flow in a holistic way to ensure secure CPS and provide an insight into new requirements on the platform-aware design of control components, design methodologies and architectures posed by CPS design. The authors discussed a multi-disciplinary modeling, simulation, tools, and software synthesis challenges for CPS. [2], proposed a security aware model based on design in methods to assess the security of CPS within four types of architecture level attacks. The group exploits the observations by identifying and fixing problems at early stage of the system development is economically beneficial. The UCI group proposed a design automation process model and tool to formulate and resolve security problems before the system is developed. They modelled a cyber-security attacks and countermeasures functionality using a novel security-aware functional modeling language implemented in the commercial design automation tool that uses simulations to validate cybersecurity vulnerabilities at system level. The functional existing models include cyber and Physical functions and how they interact with each other through energy, material, and signal flows which carries real physical and cyber properties such as mechanical, electrical, thermal energy and data. However. The existing functional models naturally leak information that the attacker may exploit through the signal flows in the cyber domain or the energy flows in the physical systems. The proposed security-aware functional models provide the means to both analyze the effect of security attacks functions on the system and refine the design using cyber security counter measures.

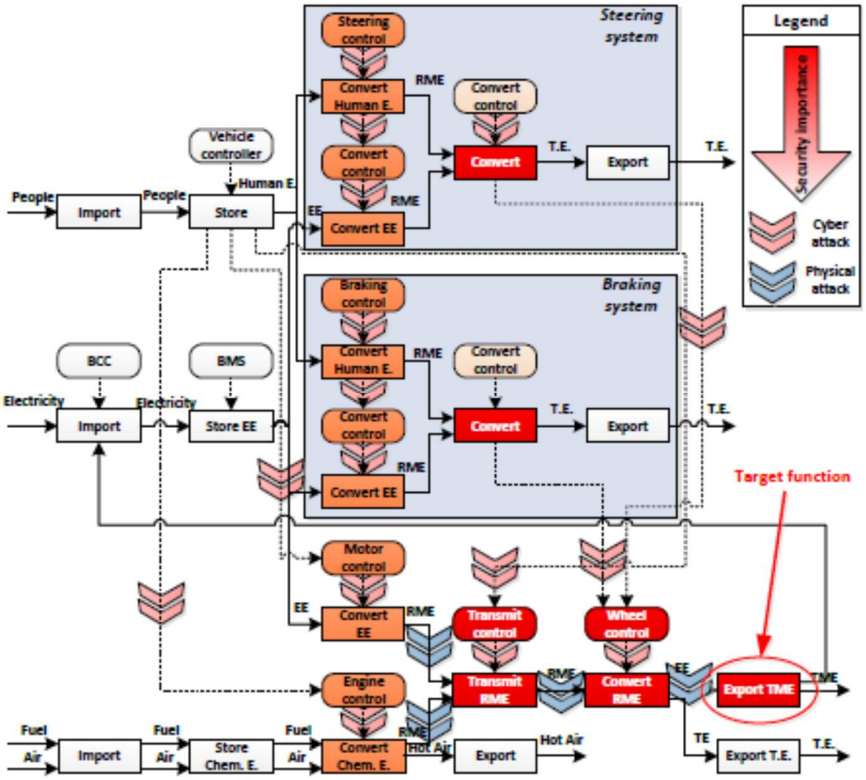

Figure 4. Security Aware Functional Level Model of Automotive. UCI Group. [2]

The blue arrows in the above model flow represents the cyber-attack vectors, while the red arrows represent the physical attack vectors. The purpose of the analysis is to quantify the effects of these attacks to the Export TME Function that maps to the velocity of the car. They simulated the model and analyzed the impact of the attack at the system-level in order for the researches to evaluate the security level of the function, and to identify the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

functions that are vulnerable to attacks. [28], reassess the risks of cyber threat on national critical infrastructures and highlights the set of issues that relates to cyber-terrorism and cyber-attacks on critical infrastructures. The author posits that the premise of cyber terrorism is that as national infrastructures become more dependent on computer networks for their organizational requirements and operations so are new vulnerabilities. Secondly, the author examined cyber-attacks against a backdrop of routine infrastructure failures. There are extensive case studies and data on power outages, flight delays, infrastructure failures, and communications disruptions we can analyze to the documented routine failures to mitigate risks. Thirdly, the author measured the dependences of infrastructures on computer networks and the redundancy already present in the system. The author also stated that for the case of cyber-terrorism, we must consider the use of cyber-weapons in the context of the political goals and motivations of terrorist and whether cyber-weapons are likely to achieve these goals. Attacks on industrial and mechanical plants such as the Stuxnet attack. [10], and Duqu malware, [9]. attacks on SCADA systems shows how vulnerable the systems are and therefore the need to ensure cyber risks mitigations are carried out on these industrial applications.

3.1.2 Cyber Physical System Taxonomy

Academics and researchers have used the term Cyber Physical Systems, Industry Control Systems, Critical Infrastructures and Embedded Systems interchangeable in their research papers and publications. Although there are similarities, cyber physical systems have recently been introduced as the linking together of the theses systems, networks, internet, software's and the physical systems and processes. However, there are slight differences in them in terms of compositions, concurrencies and computational applications. The following are taxonomies of the CPS systems:

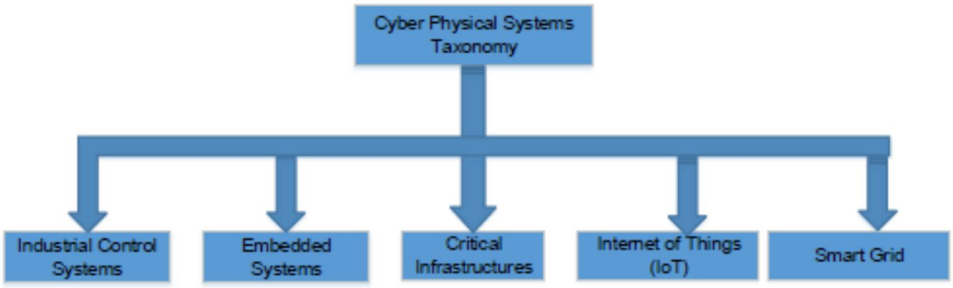

Figure 5. Cyber Physical System Taxonomy

3.1.3 Cyber Physical Systems (CPS)

Cyber Physical Systems (CPS) is an integration of the computation and physical process that makes a complete system such as the physical components, networked systems, embedded computers and software and the linking together of devices and sensors for information sharing [3].

- **Industry Control Systems (ICS)/Control Systems (CS)**
  Industrial Control systems are control systems used to enhance the control, monitoring and production in different industries such as nuclear plants, water and sewage systems and irrigations. ICS includes technologies such as Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DSC) that are at the core of business operations in manufacturing, chemical processing, oil and gas production and other industries [11]. Applications includes railroad switches, SCADA monitors and programmable logic control (PLC), a microprocessor be designed to operate continuously in hostile environment [17].

  Embedded Systems
  Embedded systems however, are mainly the software systems where codes are the executed on networks monitors and controls and usually with feedback loops where physical processes affects computations. These systems includes real time constraints and efficiency requirements like automobile, equipment, fabrication manufacturing equipment's and telecommunication networks [13].

- **Critical Infrastructures:**

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

Critical infrastructures are national system that when compromised will have a serious effect on the national economy and includes physical systems, networks and assets that are considered vital to its economic assets. These infrastructures include railroad systems, air traffic control systems, power grids, pharmaceutical, chemical, national health, and banking data centers. Other critical infrastructures includes shopping malls, dams, communication systems and defense systems.

- **Internet of Things (IoT)**

Internet of Things (IoT) referred to as the use of intelligent connected devices and systems to leverage data gathered by embedded sensors and actuators in machines and other physical objects. [15]. IoT can provide solutions that may improve decision-makings, and improve productivity for organizations and improve energy efficiency, security, health, education and many other aspects of daily lives.

- **Smart Grid**

The Advance Meter-Reading Infrastructure (AMI) system is an electricity transmission system that provide advance energy monitoring and recording, sophisticated tariff or rate program, data collection and load management command and control capacities. The AMI is a two-way communication system that can reach every device in a distributions space. It allows utilities to balance supply, demand and capacity making smarter, more efficient, grid pushing aspects of grid and control out of endpoints of delivery. For instance, the electricity company of Ghana (ECG) may use smart meters for reading digital meters and has a diagnostics port and a wireless adaptor embedded on the digital devices that interact with the meters data for billing and diagnostics. The meter reader takes the data and all the reading from various areas and send them onto the utility companies (GRIDCo) distribution center were the control system is situated.

- **AMI Components Vulnerable Spots**

The AMI network component includes, Access Point: that is within the AMI system that performs high volume collections or aggregation and transport capabilities [36]. The AMI Header-End is the back office system that controls the Advance Metering Infrastructure. The Backhaul Gateway is the communication between the access point and the backhaul network. The Backhaul Network is the high capacity mesh network to the LAN. The back haul side relays the traffic from router to router wireless until it reaches a gateway. The Firewall or DMZ a piece of computer software of hardware intended to prevent authorized access to system software or data. On the packet filtering firewalls, it is possible to slip attacks through this type of firewall as it examines packet individually and not together. The stateful packet inspection firewall uses a state table to keep track of the connection states and allows traffic through as part of a new or already established connections. Deep packet inspection firewall examines the contents and makes a judgement as to whether the package shipped based on its contents. NIC is the AMI side of the network interface card within the Smart Meter. The relay is the sub-system of the AMI system that typically relays or routes the data using radio signals between the meters and the access points.

3.2 Cyber Physical Systems (CPS) Attacks

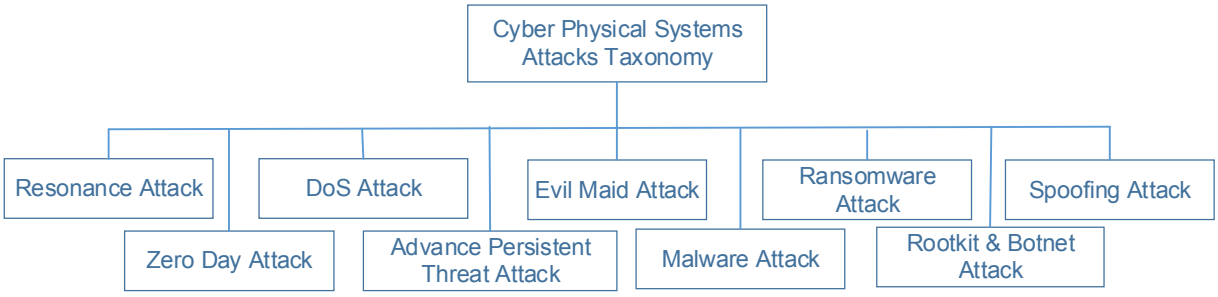

Figure 6. Cyber Physical Systems (CPS) Attacks Taxonomy

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

Cyber Physical Systems have been at the core of national critical infrastructures and major industrial control systems for years now. [10], and so are the attacks scenarios increasing as these control systems become the backbone of every economy. Various Attack scenarios that can be initiate on CPS include:

3.2.1 Zero Day Attacks

A zero day attack is an attack that exploits a system on the same day that the vulnerability is identified. Hence the number on days are zero between the time of the vulnerability is discovered and the first attack. [43], reported that the Elderwwod Project used a seemingly unlimited number on zero day attacks exploits on supply chain manufacturing systems. The report went on to say that the attack was initiated by a large organization that is supported by a nation state.

3.2.2 Evil Maid Attack

An evil-maid attack is a security exploit that targets a computing device that has been unattended to or shut down and left unattended. Here the evil maid who are mostly internal staff called (Corporate Spy) or (Industrial Espionage)attacker boot the system with a boot loader or USB drive installs a key logger and then capture encryption keys then uses it when the victims is off.

3.2.3 Resonance Attack

Resonance Attack is an attack that the perpetrator compromises some sensors or controllers that forces the physical system to oscillate at its resonant frequency. Alvaro (2010). For instances, the attacker compromise the real time of the health systems and make it provide wrong information. The actuators will not able to pick up the correct signals from the sensors.

3.2.4 Denial of Service Attack (DoS)

DoS attack is a cyber-attack that the perpetrator interrupts the network in an unauthorized manner, disrupts services and denies authorized users from having access to the network resource affecting the control systems performance. On a Wireless Network Control Systems, a perpetrator could cause optimal jamming attack which maximizes the linear quadratic Gaussian control in plants to affect the control system performance. [52].

3.2.5 Malware Attack

Malicious worm is a software program that propagates a network system and exploit vulnerabilities holes such as virus and Trojans. Stuxnet attack [10]. A malware designed to target five Iranian Critical Infrastructures an Organizations suspected to be Uranium enrichment Infrastructures. The worm initially spreads discriminately, and have a highly sophisticated malware payload designed to target Siemens Supervisory Control and Data Acquisition (SCADA) systems configured to control and monitor specific industrial processes.

3.2.6 Ransomware

A malicious software virus designed to stop a system from functioning completely by encrypting the data and sending a message to the owner to pay a ransom amount before the data will be release. Consequences are that they cause financial loss, puts human health at risk and industrial sabotage Wannacry attack [20]. Infected 230,000 computers in over 150 countries with NHS, Spanish Phone Company Telefonica, German State Railways and others. [42], Petya ransomware spread rapidly through network systems that use MS windows operating systems infected and subverts the Programmable Logic Control (PLC) on the industrial systems. [20].

3.2.7 Non-Invasive Sensor Spoofing Attack on ABS

Spoofing attack is a technique used to gain authorized access to a system by sending a signal to a system indicating that a message is coming through such as Network system, ARP, DNS and IPs. In the automobile industry, Non-invasive spoofing can be initiated on the network and the embedded system by a malicious attacker by modifying the physical system around the analog speed sensors on the ABS and inject arbitrary measurements to the ABS speed control system and cause danger and life threating situation to automobiles. [39], non-invasive spoofing attack when initiated on the anti-braking systems (ABS) will exploit the ABS speed sensor by disrupting the magnetic field around it. This tempers the output of the sensor and hence the speed value on the car. Using a thin electromagnetic actuator kept near the sensor, the magnetic field of the actuator will disrupts the sensor and prevent the ABS from function properly. [45].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

3.3 Cyber Physical System Threats

A threat is anything that has a potential to cause a harm and securing Cyber physical systems from threats comes with its own challenges. Here we identify the threats that has a potential to cause general threats and then look at specific threats to CPS. Potential threats when not identified and mitigated can cause a lot of damage and disruptions to the public, health, transport systems, and loss of data to organizations. [3].

3.3.1 CPS General Threat.

We identified five potential sources that a perpetrator can pose a threat. These are: source, target, motive, attack vectors and potential consequences. [17].

1. Threat source falls in three categories:
   - Social engineering or Adversarial threat are those that pose malicious intents from individuals, groups, organizations or states/nations to cause panic, fear and chaos.
   - Unexpected threat or accidental threat are threats that happen accidentally or through legitimate CPS components. System faults that lead to failures and down times.
   - Environmental threats are those that include natural disasters such as floods and earthquakes, human caused disasters such as fire explosions, and failure of supporting infrastructures such as power outages or telecommunications loss.
2. Target: Targets CPS applications and their components or users such as servers, network and sensors.
3. Motives: CPS attackers usually have one or more reasons to launch an attack. Their motives are normally economic, APT spying, terroristic, political or cyberwar.
4. Attack vector: A threat might perform one type of attack or more of a mechanism for a successful attack such as interception, interruption, modification and fabrication.
5. Consequences: Impact of the damage caused by the compromise of the CPS security triad confidentiality, Integrity and availability, reputation, cyber industrial espionage.

3.3.2 CPS Specific threat

To be able to ensure that CPS risks are assessed for proper mitigation, we explore the potential threat to the CPSs four applications using the proposed threat models. The study will highlight the threat that are specific to each applications with respect to the five factors: source, target, motive, attack vector and consequence.

3.3.3 Threat against Industrial Control Systems

- **Criminal attackers (motive) is to cause APT attack:** Attacker could penetrate the system becomes familiar with the system (sources) could exploit wireless capabilities (vector) to remotely control an ICS application and possibly disrupt its operations (consequences).
- **Financially Motivated Customers (Motive):** A capable customer (Source) aiming to reduces utility bill and tariff might be able to hack into the physical equipment or inject false data (vector) to misinform the utility (target) causing it to loss financially (consequence).
- **Politically Motivated Espionage:** Intelligence agencies (source) might perform reconnaissance operations targeting a nations critical infrastructures (target) through spreading malware (vector) resulting in confidentiality violations of critical data (consequences).
- **Politically Motivated Cyber warfare**: (motive) a hostile nation (source) could initiate a cyber war against another nation (target) by remotely attacking it critical infrastructures e.g., nuclear plants and gas pipelines by spreading malwares or accessing field devices (vectors) resulting in a plants shutdown, sabotaging components, or environmental pollutions (consequences).
- **Physical Threats:** An attacker (source) could spoof a sensor that measures the temperatures of a particular environment (target) by applying the heat or cold to it (vector) resulting in sending a misleading false measurement to the control center (Consequence). [3].

3.3.4 Threats against Smart Grids

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

The smart grid also referred to as power grid are for electricity generation, transmission and distribution to industries and homes. At the industrial level, it provides enhanced emission control, global load balancing, smart generations and energy savings. Whiles at local consumer's level, it provides the users better control of their energy usage that is economical and environmentally friendly. [17], Cyber attackers with political motives may target these critical national (smart grid) infrastructures and attack the core level where power application where energy is generated, transmission and distribution take place or can target the supporting infrastructure where intelligent components where controlling and monitoring takes place**.**

3.3.5 Sensor Attacks on Health Care Systems

The author [30], proposes a chart that depicts a bedside–sensor data from healthcare settings by plotting two charts that reveals active sensors and compromised sensors. The first chart, each dotted line represents an event when the health of the patient has been at risk. The second chart depicts three compromised sensors. The attacker can cancel all three points and mask the events indicating that should this attack happens the consequences could be fatal.

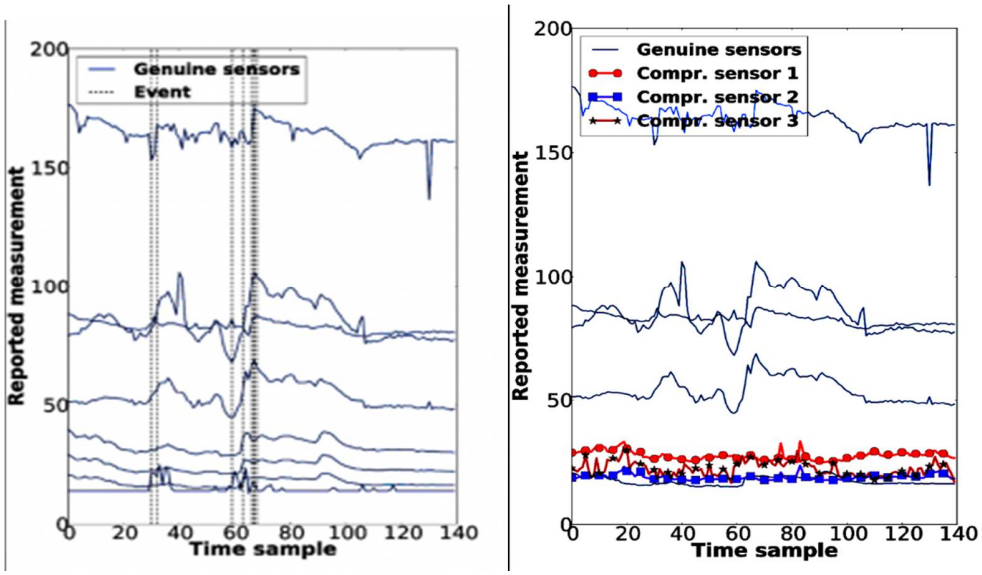

Figure 7. Sensor Attacks on Health care Systems. [30]

3.4 CPS Risk and Controls

For us to have a risk on these CPS in a given situation, we need to have both the probable threats and vulnerabilities that when exploited, could cause major disruptions. The paper looks at cyber risk and controls in the various cyber-attacks and risks that may exist on the CPS infrastructure and the identifying threats and vulnerabilities. [2]. proposes the need to change the way we reason about controls in CPS, and to start designing attack resilient control schemes and architectures capable of dealing with cyber physical attacks on the environment of the controller such as the sensors, actuators and communication media. Recent attacks on control components of CPS have clearly revealed that relying exclusively on cyber security techniques for securing CPS is insufficient. The author's goal was to develop tools and techniques to ensure that CPS maintain a degree of control even when the system is under cyber and or physical attack.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

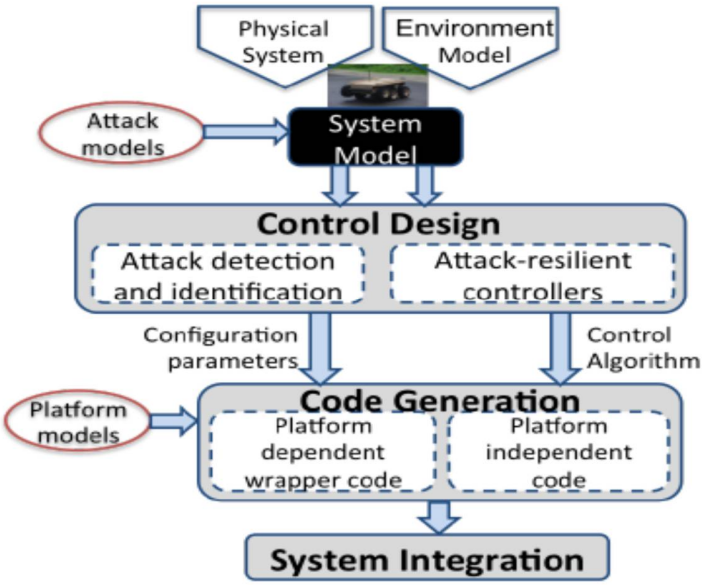

Figure 8. Proposed Framework Design for Secure Control of CPS. [2]

The authors proposed additional security awareness to the control systems to recover the information about the state of the controlled process despite the attacks. The above figure was an approach to build attack resilient control systems is by combining secure detection and attack identification with added logical redundancy in system design.

[26], proposed a cyber physical systems concept map and incorporated cyber security features into the taxonomy as core requirements in building trust as the over aching goal. The authors proposed four key cyber security features namely Resilience, Privacy, Malicious Attacks and Intrusion Detection as part of the CPS development. They classified resilience as the ability of a material to absorb energy when it is deformed. In the context of unexpected inputs, subsystems failures, or environmental conditions or inputs that are outside the specified range. They indicated that fault tolerance, fault detection and adaptation are all techniques that ensure resilience. In the context of CPS, privacy is the problem of protecting information about humans from unauthorized access by other humans or machines. All network systems face the risk of malicious attacks and as CPS systems become more open, so does the vulnerable spots. There are risks due to incomplete trust in suppliers and the possibility of accidental introduction of malicious codes such as back doors, Trojan and virus. The authors considered intrusion and technologies that can bring to bear including embedded vision, motion detection, tracking human detection and face recognition. The timing models include enabling detections of timing anomalies that can reveal intrusions.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

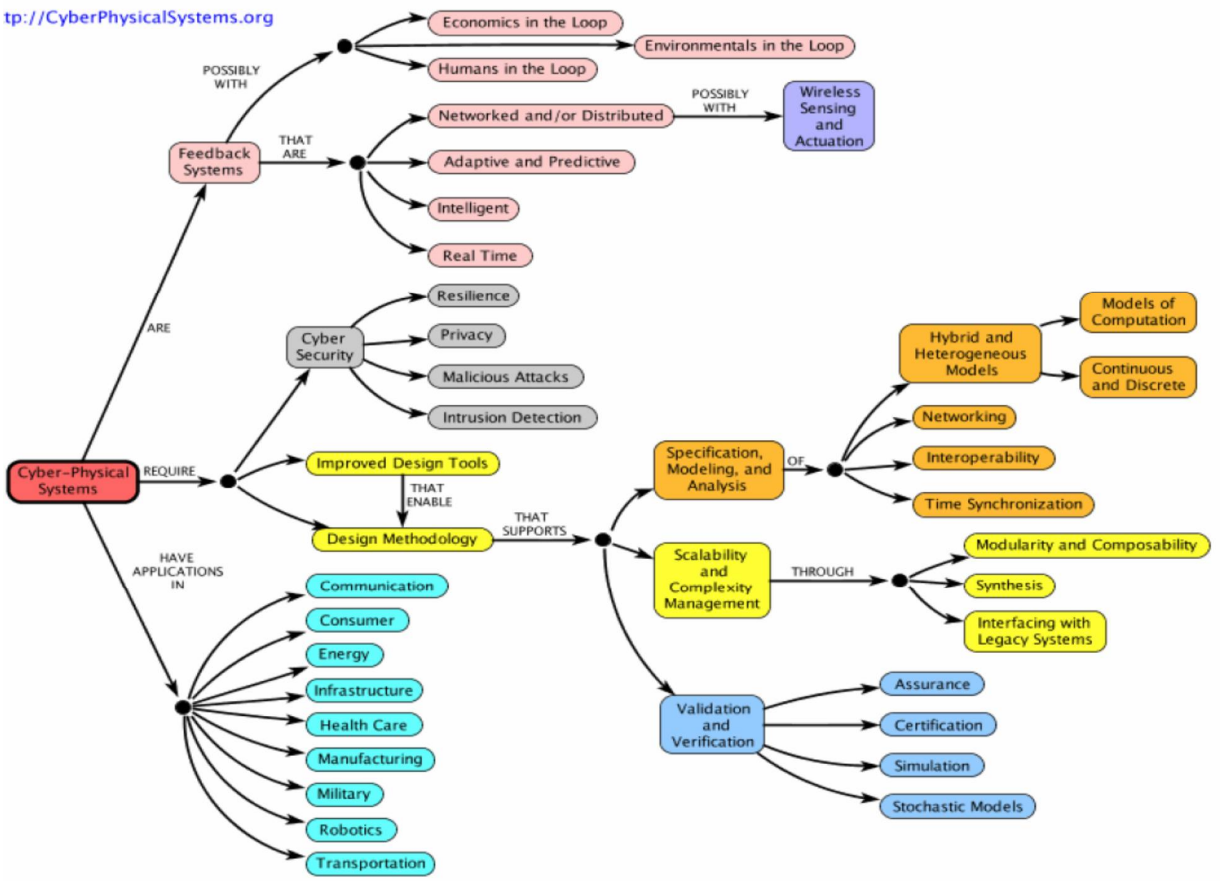

Figure 9. CPS Concept Map. [26]

[39], devised a robust output- feedback controller that is resilient to an attack to the scheduling of packets in a network control system. The authors studied the extent to which an adversary can attack a cyber physical system by tampering with the temporal characteristics of the network in a packet scheduling attack, leading to time varying delays and more importantly by changing the order in which packets are derived. The authors showed that such an attack could destabilize the network system if the controller was not design to be robust with respect to an adversary scheduling of messages. The authors proposed a controller that uses a received packet up to the current time, to be robust to such attacks and provide maximum control for CPS systems under network packet scheduling attacks.

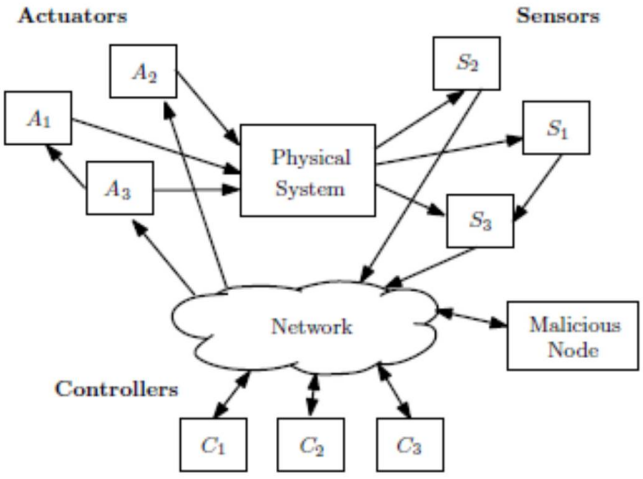

Figure 10. A typical Networked CPS system with Adversary Attack on the Shared Network. [39]

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

In a typical CPS system, the multiple sensors transmit information to the controllers through a shared communications channel and the controllers transmit the control packets to the actuators connected to the physical systems. [39], [45]. Data packets are scheduled for transmission and they must arrive at their destination node before a certain allowed deadline. An attack on the scheduling algorithm will lead to time-varying delays and more importantly can lead to a change in the order that packets are received. [23], proposed a formal model for risk management in cybercrime control systems. The framework recommended three steps namely, Risk Assessment, Risk Mitigation and Evaluation. The risk assessment step involves classification of cyber asset, identify threat, identify vulnerabilities and analyze risk. The Risk mitigation step identifies options, choose an option and implement. Then the Evaluation step looks at the technical improvement, Behavioral or organizational improvement. The mathematical techniques used stem from probabilistic theory, set theory and stochastic process theory. However, the framework does not include evolving threats and vulnerabilities such as Advance Persistent Threats (ATP) that deal with cybercrimes such as Intellectual property theft, spear phishing, Identity theft, ransomware and malwares. The risk level function does not link to any value that makes it difficult to differentiate between high, medium and low risk. [29]. proposed framework built around an established international standard for vulnerability disclosure, ISO/IEC29147-2014. The aim of the method is to provide faster and more efficient triage on reports of security flaws consistent with what NCSC describe as Active Cyber Defense. The framework is to identify and resolve vulnerabilities across three public facing systems used in UK Public Sector organizations. However, the framework is generic and applicable to any risk context. The model is not conducive for evolving cybercrime threads on cyber physical systems. [14], proposed a three-step approach to cyber-incidence risk management framework to manage the risk rising from cyber incidents. The steps include assess risk, reduce risk to acceptable level and maintain risk at acceptable level. Step 1 is to access their computer systems and determine the level IT security in terms of risk exposure and potential lose. Step 2 reduce risk of security through technology preventive measures and breaches and use insurance. Then step 3 is to maintain risk at an acceptable level. However. The framework did not look at identifying emerging threats and vulnerabilities such as resonance attacks, malwares and APTs that are evolving and the loopholes that they can exploit which are difficult to detect and quantify. [50], posits that the European Cyber Security Strategy was a propose framework for a directive on the security of networks and information that imposes obligations on Member States in relation to three key areas namely Prevention, Management and Response to cyber risks and incidents. The proposed framework directive will create a mechanism for collaborations between member states and establish security requirements for market operations and public authorities. However, the framework did not include emerging and developing economies that have now become the hub for cybercrimes and cyber threats. It also failed to include small-scale businesses that used as baits to target major organizations and industry control systems. [21], looks at the evolving risk, controls in cybercrime environment, proposed a response strategy and solutions to the threat of cybercrime especially for developing economies. ITU posits that the risk associated with weak protection measures could in fact affect developing nations more extremely. The Global Cybersecurity Agenda has seven main strategic goals, build on five areas: (1) legal measures; (2) Technical and Procedural Measures; (3) Organizational Structures; (4) Capacity Building; and 5) International Cooperation. The study theorize that developing countries need to integrate protection measures into the rollout of the internet from the beginning though this might raise the cost of internet. However, the development of cybercrime protection and technical measures to mitigate risk and promote proper cybercrime legislation is important for both the developed and developing nations. The recognition of the developing nations as potent and potential cybercriminal has become imperative and bringing them together with the developed and the emerging countries under one legal umbrella is vital.

3.5 Laws and Legislative Frameworks

[47], evaluates the potential efficacy of the Council of Europe's Convention on Cybercrimes quest to address the jurisdictional issues posed by the evolution of the internet and the council's treatment of the jurisdictional conflicts underlying cybercrime regulations. Its goal was to harmonize cybercrime laws and assure the existence of procedural mechanisms to assist in the successful prosecution of cyber criminals. The study identified three jurisdictional challenges that manifest in cybercrime cases as: lack of criminal statutes, lack of procedural powers and lack of enforceable mutual assistance provision with foreign states. The convention on Cybercrime called for the criminalization of nine offences in categories. However, the convention lacks cohesion, did not factor in the risk mitigation strategies and standards that organizations must adopt and incorporate into their policies that will aid in persecuting cyber perpetrators locally and internationally. [51], propose that the development of the law of jurisdiction must address whether the laws of the state or country control a particular event in cyberspace

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

where the website is located. The law of the state or country where the internet service provider is located, by the laws of the state or country where the user is located, or perhaps by all the laws. A number of commentators have voiced the notion that cyberspace should be treated as a separate jurisdiction. In practice that has not been supported by the courts or addressed by lawmakers. The issues of dealing with cyber jurisdiction remains unsettled. These issues attest to the fact that the law has a long way to go in addressing cyber jurisdictional laws in an evolving cybercrime cases. [32], proposed a US cybersecurity framework that will provide collaboration between government and private sector to use common language to address and manage cybersecurity risks in a cost-effective way based on business needs without placing additional regulatory needs on businesses. The Model will maintain a cyber environment that encourages efficiency, innovation and economic prosperity while promoting safety, security, business confidentiality, privacy and civil liberties. The framework is to help organizations align it cybersecurity activities with its business requirements, risk tolerance and resources. The tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cyber risk [21], the ITU Global Cyber security Agenda proposed a global framework for dialogue and International Corporation to coordinate the international responses to growing challenges to cybercrime and to enhance confidence and security in the information society. To address the relevance of Cybercrime issues within the Pillars of Cybersecurity, the Global Cybersecurity Agenda has seven main strategic goals built on five working areas namely Legal, International Corporation, Organizational Structures, Capacity Building and Technical and Procedural measures. Issues relative to cybercrime plays an important role in all five pillars and among these working areas, the Legal measures focuses on how to address the legislative challenges posed by criminal activities. However, the framework did not consider the cooperation between law enforcements and ISPs as particularly essential in cybercrime investigations. The framework did not provide for the efficient cooperation that defines expectations, responsibilities and authorities but also limitations and those that ensures the right that protect users.

3.6 Impact: Financial, Socio-Economic, Business Assets & Insurance

[50], posits that SMEs are the heart of every economic growth as they make up the social fabric. However, these businesses are mostly the victims of cybercrime as they fail to deploy security policies to mitigate cyber risks and used to target CPS systems on an extranet environment. SMEs make up 99% of all businesses in the EU employing 86.8 million people, equivalent to 66% of the workforce. However, as they depend daily on the internet to facilitate their organizational requirements and work process, these businesses are the most vulnerable and victimized when it comes to cybercrime attacks. These SMEs use inexperience IT personal, hence are prone to threats and vulnerable to attacks. [1], looks at the infrastructures supporting cybercrime and proposed a framework for analyzing the cost of cybercrime. The study looked at cybercrime defense cost, direct losses and indirect losses, criminal revenue and cost to society. The report looked at the threats, monetary equivalent online loss, damage or other suffering felt by the victim as consequence of cybercrime. This includes money withdrawn from victims account, time and effort to reset account credentials and others. Indirect loss in monetary equivalent and opportunity cost imposes on society by cybercrimes payments. Loss of trust in banking online, missed business opportunity and reduced uptakes by citizens and effort to clean up and restore systems. The defense cost are the monetary equivalent of prevention efforts. However, the framework did not research further to include insurance claims, litigation issues and reputational damage. [7], estimated the global cost of cybercrime to $388 billion with direct cash cost of $114 billion including money stolen and spent on attack resolutions. However, a study in 2009 estimated the cost of stolen intellectual property and expenditures for fixing the damage from data breach to be $1 trillion. In the US, according to Ponemon Institute cybercrime has increase 22.6%, the average cost of cybercrime on 95% companies suffer 64% experienced web-based attacks, 44% experienced stolen or hijacked computing devices, and 42% on experience malicious codes attack. UK spent £27 billion per year loss to the UK economy on cybercrime. Approximately 80% or £21 million borne in companies. In Germany, the estimated cybercrime losses was 90 billion Euros in 2010. In a study conducted in five countries, Australia, France, Germany, UK and US, the cost per company arising from data breaches reached $4 million in 2010, a rise of 18% from 2009. However, these estimations did not factor in the developing countries such as Africa, looking at the global and evolving nature of cybercrime. Hence, the data is incomplete and limited. Challenges not addressed are difficulties in calculating insurance losses such as reputational damage and ransomware attacks. [48], report indicates that if businesses and government do not develop adequate defense polices quickly, the economic losses caused by cyber attackers could be up to 3000 billion dollars by 2020. The WEF highlighted the interdependences

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

of IT, introducing new vulnerabilities and flaws with unpredictable consequences. It emphasized the macroeconomic impact of IT risks in terms of growth of GDP. WEF emphasizes the delicacy of cybercrime and explained that if not address promptly, and taken into account by all stakeholders, it could lead to serious consequences. It will create a scenario in which the internet could suffer the mistrust of users, no longer be a free resource and research tool, and no longer be used for ecommerce. However the report failed to include the various threat and vulnerabilities from evolving organization landscape context, that when exploited will cause this impact.

4.0 Analysis and Discussions of CPS

We discuss the findings of the start of the art review and synthesis the results of the various literatures. The study reveals that most of the existing literatures justify the need and relevance of considering cybercrime risk mitigating from the context of cyber physical systems. The results also identified a list of critical CPS threats and vulnerabilities, associated factors and mitigation goals that impacts on the physical systems, the digital systems and the human elements. The study reveals several observations for future directions necessary to mitigate cybercrime from CPS context. The study have reviewed CPS risk from these three entities as merging the Physical systems, Digital systems and Human elements. These elements may have different cyber-attacks inherent in them that can be initiated from anywhere in the world and when that happens the impact may affect not just one of the element but all the three elements depending on the nature of the cyber-attack. We discusses the elements as follows:

The physical systems include the infrastructures that communicate and interact with the real world and provide feedbacks. These includes the computers, monitors, wired and wireless networks, IPS, air control centers and military command centers. The digital systems are the software programs, embedded systems, computational programs such as the (PLCs) and the SCADA systems that functions as intelligent agents that send and receive instructions from the physical and human elements. The human elements are the components such as the sensors and actuators that connect components to the physical systems. The human elements requires transparent interfaces that uses existing electrophysiological signals such as electroencephalography (EEG), electrocardiography (ECG) and electromyography (EMG), which measures electrical signals emitted by the brains, heart and skeletal muscles, respectively. [38]. Sensors are used to monitor the respiratory rates, pulse oximetry and skin resistance and can provide a more comprehensive view of the whole body.

Several research studies from journals and industry papers focus on CPS design methodologies and CPS security. However, none of them was considered mainly from cybercrime on cyber physical, cyber digital and from human elements as their key objectives for CPS risk management.

Cyber Physical Systems Risk Management		
Author	**Date**	**Literature Proposed**
Humayed et al.	2017	generic framework, lacks capability to detect the diversities of attacks, threats, vulnerabilities
Lewis	2002	Cyber security features resilience, privacy and intrusion detections as part of the CPS development.
Al Faraque et al.	2010	modelled attacks and countermeasure functionality using a novel security-aware functional modeling
Kayode et al.	2014	risk assessment and evaluation framework to manage risk and calculates impact using probabilistic theory
Lee & Seshia	2011	generic framework, lacks capability to detect the diversities of attacks, threats, vulnerabilities
Anderson et al.	2012	Looks at the infrastructures supporting cybercrime and proposed a framework mitigating and analyzing
Lee	2012	concept map and incorporated cyber security features into the taxonomy as core requirements in building trust

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

Alvaro et al.	2010	generic framework, lacks capability to detect the diversities of attacks, threats, vulnerabilities
Leyden	2017	Framework built around an established international standard for vulnerability disclosure
NIST	2014	cyber-risk framework designed to align cybersecurity activities with business requirements and risk tolerance
Risk and Controls in CPS		
Authors	**Date**	**Literature Proposed**
Lee	2012	Intrusion detect such as embedded vision, motion detection, tracking human detection and face recognition.
Shoukry et al.	2013	controller that uses a received packet up to the current time, to be robust attacks and provide maximum control
Verma & Chundri	2016	an electromagnetic actuator kept near the sensor that will disrupts the sensor and prevent the ABS from function properly
Al Faraque et al.	2010	Security-aware functional models to analyze the effect of security attacks functions and provide security counter measures.
Gollmann	2013	software codes that when executed on networks monitors, will provide controls feedback loops on physical processes
GSMA	2014	studies considered risks controls from technical and non-technical areas in the CPS system design
Symantec	2012	considered zero day attacks and risks controls from technical and non-technical areas on CPD design
Falliere et al.	2011	targets ICSs specialized assembly like on PLCs. considered risks controls from technical and non-technical areas on CPS
Chien et al.	2012	Adopt APT attack method and gather intelligence from victims ICSs. risks controls from technical and non-technical
Alvaro et al.	2010	studies considered risks controls from technical and non-technical areas in the CPS system design
ITU	2012	Looks at risk associated with weak protection measures that could affect developing nations more extremely.
Laws and Legislative Frameworks		
Authors	**Date**	**Literature Proposed**
Webber	2003	Evaluates the jurisdictional conflicts regulations and the potential efficacy of the CoE Convention on cybercrimes mission
Zeviar-Geese	1998	Identifies lack of jurisdictional law that addresses whether cyberspace is controlled by country where ISP or user is located
ITU	2012	Identifies global framework to coordinate international responses to growing challenges to cybercrime.
Zappa	2014	legal challenges that exist on deep web and the inability to track, cyber criminals and the illegal activities as the cyberspace
Marion	2010	Identifies the CoE Convention and treaty on Cybercrime and analyzed it laws for societal benefits.
Impact: Financial, Socio-Economic, Business Assets and Insurance		
Authors	**Date**	**Literature Proposed**
Zappa	2014	identify SMEs use of extranet with major organizations causing human vulnerabilities and impacts on procedural security

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

WEF	2013	indicates the economic losses caused by cyber attackers could be up to 3000 billion dollars by 2020
NIST	2014	identifies the additional regulatory needs for businesses to address and manage cybersecurity risks in a cost-effective way
Capgemini	2015	Identifies amount stolen or spent on cyber-attack as huge including the resolutions and global cost of cybercrime.
Anderson et al.	2012	Looks at the infrastructures supporting cybercrime and proposed a framework for analyzing the cost of cybercrime.

Table 5. CPS Risk Mitigation Goals Reviewed

4.1 CPS Risk Management

The study considered CPS Risk management challenges from the various design methodologies as well as the threats and vulnerabilities. The reviewed designed methodologies and frameworks emphasized mainly on cybercrime risks. [17], [2], [17], [3], [28], studies considered risk mitigation processes but frameworks were generic and lacks the capability to detect the diversities of attacks, threats, vulnerabilities that exist on CPS infrastructures. [23], Identifies risk assessment, risk mitigation and evaluation framework to manage cyber risk and calculates the risk impact using probabilistic theory and stochastic process methods. However, the framework is not applicable to any risk context and does not include evolving threats and vulnerabilities such as Advance Persistent Threats (ATP). [29], proposed framework built around an established international standard for vulnerability disclosure, ISO/IEC29147-2014. However, the framework is generic and applicable to any CPS risk context. [32], identifies cyber-risk framework designed to align cybersecurity activities with business requirements, risk tolerance and CPS resources. [1], looks at the infrastructures supporting cybercrime and proposed a framework for analyzing the cost of cybercrime. However, there are no considerations for insurance claims, litigation issues and reputational damage.

4.2 Risk and Controls in CPS

[26], [39], [45], [2], [13], [15], [43], [10], [9], [3], studies considered risks controls from technical and non-technical areas in the CPS system design. [26], proposed cyber security features as resilience, privacy, malicious attacks and intrusion detections as part of the CPS development. However, the model failed to identify the physical, digital and the human elements. [21], looks at risk associated with weak protection measures could in fact affect developing nations more extremely.

4.3 Laws and Legislative Frameworks

Legal issues relative to cybercrime measures focuses on how to address the legislative challenges posed by criminal activities. The study identified three jurisdictional challenges that manifest in cybercrime cases as: lack of criminal profiling, lack of procedural powers and lack international cooperation. [47], evaluates the jurisdictional conflicts underlying cybercrime regulations and the potential efficacy of the Council of Europe's Convention on Cybercrimes mission to address the jurisdictional issues and offences against confidentiality, integrity and availability. [51], identifies the lack of development of the law of jurisdiction that address whether a particular event in cyberspace is controlled by the laws of the country where the ISP or the user is located. However, CoE did not factor in the CPS risk mitigation strategies and standards that must be adopted and incorporate into organizational policies. [21], Identifies global framework to coordinate international responses to growing challenges to cybercrime. [50], observed the legal challenges that exist on the deep web and the inability to track, cyber criminals and the illegal activities as the cyberspace. [31], identifies the CoE Convention treaty on Cybercrime and analyzed it laws for societal benefits.

4.4 Impact: Financial, Socio-Economic, Business Assets and Insurance

We discuss the primarily impact of financial, socio-economic, business assets and lack of insurance on CPS critical infrastructures and control systems, data assets and trade secrets. The financial benefits of cyber criminals are unquantifiable as they use advance persistent threat methods to gain access to victims systems [50], identify SMEs use of extranet with major organizations causing human vulnerabilities and impacts on procedural security. [48], indicates the economic losses caused by cyber attackers could be up to 3000 billion dollars by 2020. However, the estimations did not factor in the developing economies such as Africa. [32], identifies the additional

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

regulatory needs for businesses to address and manage cybersecurity risks in a cost-effective way. [50], highlight the lack of security controls in SMEs as they make up 99% of all businesses in the EU and poses APT attacks to CPS systems. [7], identifies the amount of money stolen or spent on cyber-attack as huge including the resolutions global cost of cybercrime.

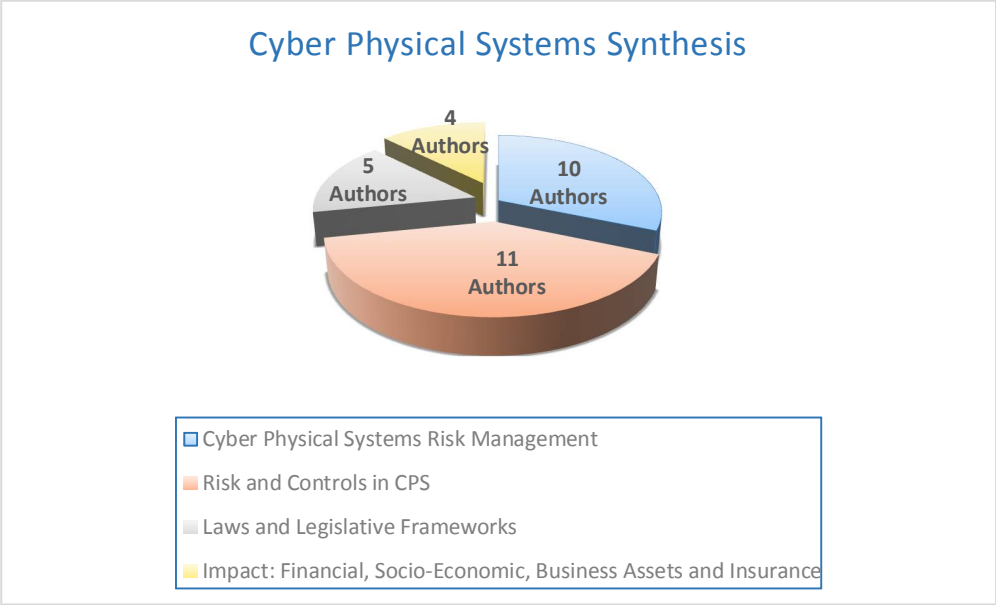

Figure 11. Cyber Physical Systems Synthesis

5.0 Cybercrime and Risk Mitigation in CPS

The study adopts a risk mitigation method based on the reviews of the state of the art and observations. We use CPS cyber-attack vectors to determine the risk levels as impediments of the mitigation goals. To determine their relative importance, we prioritize the goals using the Analytical Hierarchical Process (AHP). [35], [19]. The concept includes intangible and tangibles and how much more one element dominates another in term of relative importance with respect to a given attribute. We quantify the attributes to be the cyber-attack risk vectors that needs mitigating to ensure the CPS systems are secure.

5.1 CPS Risk Mitigation Goals

We compare the CPS risk mitigations goals qualitatively and quantitatively and follow the analytical hierarchical process to determine the relative importance. We compare the risk mitigation these against these four goals: Business Value, Organizational Requirements, Threat Agent and Impact Vectors based on the review results.

- **Business Value:** This includes the organizational assets, market value, customer base, collaborations, business partners, market stance, directions and system infrastructures.
- **Organizational Requirements:** Includes the activities and operational requirements need for successful implementation of the business objectives such as service delivery, policies and procedures, service level agreements, roles and responsibilities.
- **Threat Agent:** This goal identifies all the nature of threat, vulnerabilities and attacks. The threats includes phishing, spear phishing, cross-site scripting attack, session high jacking attacks and SQL injections. The vulnerabilities includes spots that the attacker can exploit such as the web servers, firewalls, DMZ, and IDS/IPS. Attacks vectors includes resonance, malware, ransomware, spyware, Advance Persistent Threat (ATP) and DoS attack that can be initiated in the threat landscape.
- **Impact Vectors:** This function considers all the probable consequences of the cyber-attacks listed as the threat agents on the CPS. These in includes loss of revenue, reputation, expertise, assets, profit, customers, market stance and collapse of business.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

5.2 Risk Mitigation Results

The study adopts a semi-quantitative risk assessment method to determine the risk level due to the invisibility nature of cybercrime. Using a complete quantitative method to determine the risk probability values will be a challenging for the risk management.

The Semi-quantitative risk assessment approach will assist in determining relative importance of implementing the countermeasures to protect the CPS assets and the cost of alternatives. We calculate the net risk value expected based on the threat vectors of a particular attack on a system with the frequency of occurrence within a period to the estimate the number of times a threat exploited would be successful on a vulnerability. Therefore, the risk assessment follows a semi-quantitative method to calculate the new risk values.

5.2 Relative Importance of the Risk Mitigation Goals

The study follows the AHP to determine the relative importance of the net risk mitigation calculation depending on the relative importance of the mitigation goals. [35], [19], based on an organizational context, each goal's relative importance level is compared with other goals. We adopt the AHP scales of the 1-9 as shown in table. Where 1 indicates extremely low risk in terms of the importance to a threat or an attack and 9 indicates extremely high risk in terms of its importance should a cyber-attack actually occurs on the CPS compared to another goal. Ones the importance levels of each goal is obtained compared to another, the Comparative Matrix (CM) levels are normalized to identify the relative weight of each goal. We adopt the AHP formula to determine the consistency ratio as shown in equation to check the consistency levels. The weighted value should sum up to (1). However, if the consistency ration is more than 10 then the assumptions for the relative importance are inconsistent and need to redefine the values.

Let:
CR: Consistency Ratio
CV: Consistency Vector
RV: Random Consistency Vector
CM: Comparison Matrix Value

Relative Importance of Risk Mitigation Goals
BV: Business Value
OR: Organization Requirements
TA: Threat Agent
IV: Impact Vectors

5.4 Risk Mitigation Goals

The relative importance of the net risk mitigation calculation depends on the relative importance

Relative Importance Levels	Probability	Explanations
1	Extremely Low	Acceptable mitigation of two goals that contribute equally
3	Low	Moderate mitigation or slightly in favour of a goal over the other
5	Medium	Strongly mitigation goal that favour one goal over the other
7	High	Very strong mitigation goal that its dominance demonstrates practice
9	Extremely High	Extremely high evidence of favouring one mitigation goal over the other is clear
2, 4, 6, 8.		Intermediary values that determines oscillations between mitigations vectors

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

Table 6. Net Risk Relative Importance

	Comparative Matrix Values			
	BV	**OR**	**TA**	**IV**
BV	**9**	**7**	**5**	**9**
OR	**7**	**1**	**7**	**5**
CM_i TA	**5**	**3**	**1**	**9**
IV	**9**	**2**	**3**	**1**

Table 7. Comparative Matrix

$$(CR) = \frac{CI}{RI} \quad \text{---------- (1)}$$

Step 2: Net Risk Mitigation Calculations

The net risk mitigation calculations depends on the associated threat agents (TA). The threat agents are the causes of risks factors that we need to determine the threat level to estimate the outcome of its probability and impact of the overall risk as shown in table 2.We use subjective judgment depending on individual perception to determine the probability and impact values due to the invincibility nature of cybercrimes; we consider these rules below [19], to support our estimations:

- Rule 1: Risk impact to depend on the affected mitigation goal: If a risk affects important mitigation goals such as impact on CPS business value and organization requirements, then the impact is deem as high.
- Rule 2: If the risk factor may be at least partial, beyond the control of a user organization and mainly posed by the CPS, the overall risk impact can be higher.
- Rule 3: Individual judgment is always useful for net risk calculation. However, individual perception should be closely mapped with reality; otherwise, we may overestimate or underestimate the risk value.

Net Risk Results

The net risk level is the summation of the risk level importance of the affected migration goal as shown in equation below. We determine the risk level and relative importance accurately through their influence to the risk mitigation goals. We use the same approach to determine the risk value, probability and impact.

Let,

Ri: Value of Risk
ri: Individual risk factor value
ri1……riN: N influence risk factor of a risk Ri.
P(ri): Probability of risk factor ri….
Probability scales = low/unlikely (less than 0.30), medium/likely (0.30-0.49), high/critical risk (0.49--0.59), extremely/certainly high (above 0.60)
I: Impact of overall risk Ri
Impact scales = low(less than 0.30) medium (0.30--0.49) high (0.49--0.59) extremely high (above 0.60)
Rnet: Net risk of Ri
Rw: Relative weight of the affected mitigation goal [BV, OR, TA, IV] by Ri.
Risk level scales: low risk (less than 0.30), medium (0.30--0.49) critical risk (0.49--0.59), highly critical risks (above 0.60)

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 April 2018 doi:10.20944/preprints201804.0066.v1

ri=P(ri) x I……..(2)

Ri= $\frac{1}{N}$ **∑{ri1, ri2, ri3……,rin}……..(3)**

Rnet = ∑ Rw x Ri……..(4)

Determining Risk Levels

Saaty [35], posits that decisions involve many intangibles and tangibles that need to trade off. To do that, we measured the decisions alongside tangibles and evaluated the measurements to determine how well they serve the objectives of the decision. We adopt the pairwise comparisons method to determine which risk level has a greater risk impact and requires mitigation. We determine that from the formulae above as:

Low risk of (less than 0.30) TA has minimal impact on BV and implies that it is recommended to develop a corrective measure and contingency plan to mitigate the risk such as formulation Policies, Educating users, regular updates and constant monitoring of the threat.

Medium risk (between 0.30-0.49) TA is considered moderate and needs constant monitoring and as it may never happen such a Zero day attack bit when it does the consequences may cost system failure and financial impact. Regular Backups.

High risk (between 0.49-0.59) OR process needs to be evaluated to mitigate TA and implies the risk has an adverse effect on the CPS and corrective actions are required and a contingency plan should be developed if necessary to mitigate the risk. Developed a plan for the execution of the control measures within a specific period. These includes cyber-attacks such as DoS Attack, APT, spoofing, evil-maid attack. The risk mitigation process includes having counter measures in place such as regular backups, regular updates, insurance, training and awareness workshops and adoption of cloud services.

Extremely High risk (above 0.60) TA could impact on BV with high impact factor on IV and implies the identified control measures on the CPS for the risk mitigation are require to be implemented immediately with a contingency plan. The risk level is highly critical where the probability of the risk event and its impact are high or one is medium and another high. This could cause financial loss, economic, trust and reputation damage to the organization. The counter measures are required for such attacks resonance attacks, ransomware attack and malware attack that may sabotage the systems.

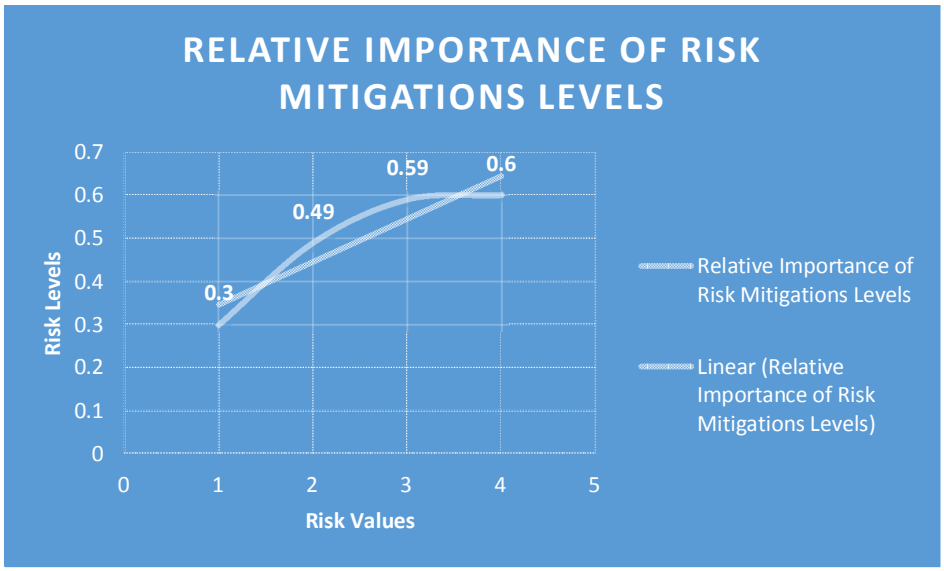

Figure 12. Relative Importance of Risk Mitigation Goals

Limitations

We should emphasis that due to varying organizational requirements, the risk management method may not adopted in the paper may not respond well to your business processes. The estimate of the variances determines the relative importance of the risk mitigations goals. Further research is required to determine the relative importance of the CPS risk management considering the changing threat landscapes...

6.0 Conclusion and Recommendations

We review the various Cyber Physical System taxonomies, the cybercrime threats that can be initiated and vulnerabilities that the attacker can exploit. Our state of the art was focus on four risk mitigation goals for this purpose, and these are Business Value, Organizational Requirements, Threat Agent and Impact based on the review results. The study reviewed the risks that are associated with the Physical systems components, Digital systems components and Human elements. We review CPS management frameworks. CPS controls, CPS legal frameworks and the CPS financial, socio-economic and business impact. We determined the relative importance of the risk mitigation goals using AHP and semi quantitative methods to priorities the risks and the threat levels. The study revealed that CPS attacks are imminent looking at the evolving nature of cybercrimes. For instance threat vectors that an attacker may deploy on power plant smart grid may be different to that of sensor attack on health care systems or automobile ABS. Therefore, to mitigate CPS risks, it is important to provide a risk management framework that is able to support organizational goals and objectives.

We recommend that CPS risk management reviews must be carried out on a regular basis to prevent evil maid and zero day attacks. CPS Attacks such as advance persistent threats are very difficult to detect without proper software updates. Updates must be done on an ad hoc bases to prevent perpetrators from detecting the when it is done. We recommend that more emphasis be placed on research areas of CPS physical components, digital components and the human elements.

References

[1]. Anderson, R., Barton, C., Bohme, R., Clayton, R., Van Eeten, M. J. G. Levi, M. Moore, T. & Savage, S. 2012. Measuring the Cost of Cybercrime. Computer Laboratory, University of Cambridge. http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf

[2]. Al Farugue, M., Regazzoni, F. & Pajic, M. 2010. Design Methodologies for Securing Cyber-Physical Systems.
(Date Accessed 05-032018) http://people.duke.edu/~mp275/pubs/CODES_ISSS15.pdf

[3]. Alvaro Cardenas, A. A., Amin, S., Lin. Z., Haung, Y., Huang, C. & Sastry, S. 2011. Attacks against Process Control Systems Risk Assessment, Detection, and Responses. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, page 355-366. ACM.

[4]. Amin, S., Schwartz, G. A. & Hussain, Alefiya, A. 2013. In Quest of Benchmarking Security Risks to Cyber-Physical Systems. IEEE Network, 27(1): 19-24.

[5]. Byres, E. & Lowe, J. The Myths and Facts behind Cyber Security Risks for Industrial Control Systems. British Columbia Institute of Technology.

[6]. Brebeton, P., Kitchenham, B. A. Budgen, D., Turner, M., & Khalil M. 2007. Lessons from Applying the Systematic Literature Review Process within the Software Engineering Domain. Journal of Systems and Software. Vol. 80. No. 4, pp. 571-583.

[7]. Capgemini. Using Insurance to Mitigate Cybercrime Risk. Challenges and Recommendations for Insurers. https://www.capgemini.com/wpcontent/uploads/2017/07/Using_Insurance_to_Mitigate_Cybercrime_Risk.pdf

[8]. Chabukswar, R. Secure Detection in Cyberphysical Control Systems. 2014. Carnegie Mellon University. (Date13-03-18) https://pdfs.semanticscholar.org/3492/f55f9672a4f0b19f43d3061bb939295ddd29.pdf

[9]. Chien, E., Murchu, L. O. & Falliere, N. 2012. W32. Duqu. The Precursor to the Next Stuxnet. In Presented as Part of the 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats, Berkeley, CA..

[10]. Falliere, N., Murchu, L. O. & Chien, E. 2011. W32. Stuxnet Dossier. White Paper, Symantec Corp. Security Response.

[11]. FireEye Inc. 2017. Cyber Security Solutions for Critical Infrastructure and Industrial Control Systems: Non-Invasive Protection Across Operational and Information Technology Assets.

[13]. Gollman, D. 2013. Security for Cyber-Physical Systems. In Mathematical and Engineering Methods in Computer Science, pages 12-14. Springer.

[14]. Gordon, L. A., Loeb. M. P. & Sohail, T. 2003. A Framework for Using Insurance for Cyber-Risk Management. Communications of the ACM. University of Maryland. USA. https://dl.acm.org/citation.cfm?id=636774

[15]. GSMA. Connected Living 2014. Understanding the Internet of Things (IoT), (Date Assessed 10-03-2018) <https://www.gsma.com/iot/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf>

[16]. Herterich, M. Holler, M. Uebernickel, F. & Brenner, W. 2015. Understanding the Business Value: Towards a Taxonomy of Industrial Use Scenario enabled Cyber-Physical Systems in the Equipment Manufacturing Industry. International Conference on Information Management.

[17]. Humayed, A., Lin, J., Li, F. & Lou, B. 2017. Cyber Physical Systems Security – A Survey. (Assessed 25-02-2018) https://arxiv.org/pdf/1701.04525.pdf

[18]. INFORSEC Institute.2015: Duqu 2.0: The Most Sophisticated Malware Ever Seen. Exploit Development, General Analysis, Hacking Malware Analysis. (Date Accessed 15-03-2018) resources.infosecinstitute.com/duqu-2-0-the-most-sophisticated-malware-ever-seen/

[19]. Islam, S., Fenz, S., Weipi, E & Kalloniatis, C. 2016. Migration Goals and Rick Management in Cloud Computing: A Review of State of the Art and Survey Results on Practitioners. International Journal of Social Sciences and Education. IJSSE.

[20]. Controller and Audit General: 2017. Investigation: WannaCry cyber-attack and the NHS. Department of Health. National audit Office. UK

[21]. ITU, 2012. Understanding Cybercrime: Phenomena, Challenges and Legal Response. (Date Accessed 10-03-2018) Available online at: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

[22]. Jubb. J. 2015. Cybercrime: The Risks and How to Avoid It. Best Practice & Trends for Legal Professional.

[23]. Kayode, A. B. Arome, G. J. Oluwatoyin, O. & Daramola, O. A. 2014. Modelling of Risk Management Procedures for Cybercrime Control Systems. Proceedings of the World Congress on Engineering. London. UK

[24]. Kitchenham, B. & Charters, S. 2007. Guide for Performing Systematic Literature Review in Software Engineering. Keel University and University of Durham, 2007.

[25]. Krotofil, M. & Gollmann, D. 2011. Industrial Control Systems Security: What is Happening? In Industrial Information (INDIN). 11th IEEE International. Conference. Pages670-675.

[26]. Lee, E. 2012. Concept Map for Cyber Physical Systems. (Date Assessed 20-02-2018) http://CyberPhysicalSystems.org/CPSConceptMap.xml

[27]. Lee & Seshia, 2011. Introduction to Embedded Systems – A Cyber-Physical Systems Approach. cyberphysicalsystems.org/Cyber-Physical_Systems.html

[28]. Lewis, J. A. 2002. Assessing the Risks of Cyber Terrorism, Cyber War and other Cyber Threats. Center for Strategic & International Studies. CSIS. https://www.csis.org/analysis/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats

[29]. Leyden, J. 2017. UK vuln 'fessing pilot's great but who's going to give a fol? (Assessed 10-03-18) https://www.theregister.co.uk/2017/03/22/uk_gov_vuln_disclosure_pilot/

[30]. Lupus, E. & Swinscow-Hall, D. 2017. Can We Trust Cyber-Physical Systems? Institute for Security & Technology. Imperial College London

[31]. Marion, N. E. 2010. The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation. International Journal of Cyber Criminology. University of Akron, USA. Vol 4. Issue 1&2

[32]. NIST 2014. Framework for Improving Critical Infrastructure Cyber Security. National Institute of Standards and Technology. Version 1.0

[33]. NIST 2017. Framework for Improving Critical Infrastructure Cyber Security. National Institute of Standards and Technology. Ver 1.1

[34]. Pajic, M., Weimer, J., Bezzo, N., Sokolsky. O., Pappas, G. J. & Lee, I. 2016. Design and Implementation of Attack Resilient Cyber Physical Systems. IEEE Control Systems Magazine. (Date Assessed 20-02-2018) http://people.duke.edu/~mp275/pubs/pajic_csm16.pdf

[35]. Saaty, T. L. 208. Decision Making With the Analytical Hierarchical Process, International Journal of Services Science. (IJSSCI). Vol. 1, No. 1, 2008.

[36]. Sarfi, R., Green, B. D. & Simmins, J. 2011. AMI Network (AMI Head-End to/from Smart Meter). American Electrical Power Company.

[37]. Savage, K. & Spasojevic, B. 2012. Symantec. W32.Flammer. http://www.symantec.com/security_response/writeup.jsp?docid=2012-052811-0308-99

[38]. Shirner, G., Erdogmus, D. & Chowdhury, K. & Padir, T. 2013. The Future of Human-in-the-Loop Cyber-Physical Systems. IEEE. Computer Science. PA Consultants Group.

[39]. Shoukry, Y., Araujo, J., Tabuada, P., Srivastava, M. & Johansson, K. H. Minima. 2013. Control for Cyber Physical Systems under Network Packet Scheduling Attacks. Physical Science and Engineering. (Date 20-02-18) <https://people.kth.se/~araujo/publications/hicons14-shoukry.pdf>

[40]. Shoukry, Y., Martin, P., Araujo, J., Tabuada, P. & Srivastava, M. 2015. Non-invasive Spoofing Attacks For Anti-Locking Braking Systems. IACR. Springer-Verlag. 10.1007/978-3-642-40349-1_4.

[41]. Stankovic, J. A. Cyber Physical Systems and IOT. Department of Computer Science. (Accessed 10-3-2018) <http://www.seas.virginia.edu/research/pdfs/stankovic.pdf.>

[42]. Symantec, 2017. Petya Ransomware Outbreak: Here's what you need to Know. Symantec Security Response. https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper

 doi:10.20944/preprints201804.0066.v1

[43]. Symantec, 2012. The Elderwood Project: Zero Day Exploits. (Accessed. 22-3-2018) http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf

[44]. Tabuada, P. Secure State-estimation and Control of Cyber-Physical Systems. Cyber-Physical Systems Laboratory. Department of Electrical Engineering. University of California at Los Angeles. UCLA.

[45]. Verma, V. & Chundri, P. 2016. Enforcing Opacity in Cyber Physical Systems Using State Machine Models.

[46]. Wan, J., Canedo, & Al Faruque. 2015. Security-Aware Functional Modelling of Cyber-Physical Systems. 20th IEEE International Conferences on Emerging Technologies & Factory Automation. ETFA. 2015

[47]. Webber, A. M. 2003. The Council of Europe's Convention on Cybercrime. Berkeley Technology Law Journal. Volume 18. Issue 1.

[48]. WEF (2018), The Global Risk Report: https://www.weforum.org/reports/the-global-risks-report-2018

[49]. Zhu, Q. & Basar, T. 2011. Robust and Resilient Control Design for Cyber- Physical Systems with an Application to Power Systems. 5th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC). Orland, FL. USA.

[50]. Zappa, F. 2014. Cybercrime: Risks for the Economy and Enterprises at the EU and Italian Level. United Nations Interregional Crime and Justice Research Institute.

[51]. Zeviar-Geese, G. 1998. The State of the Law on Cyber jurisdiction and Cybercrime on the Internet. Gonzaga Journal of International Law, (Accessed 10-03-18) http://www.gonzagajil.org/.

[52]. Zhang, H., Cheng, P., Shi, L. & Chen, J. 2014. Optimal Denial-of-Service Attack on Scheduling Against Linear Quadratic Gaussian Control. American Control Conference (ACC). Portland, Oregon. USA.