120th ASEE Annual Conference & Exposition
FRANKLY, WE DO GIVE A D*MN
June 23-26, 2013

Paper ID #7587

Security Analysis of CPS: Understanding Current Concerns as a Foundation for Future Design

Mr. Francis N Mensah, College of Engineering and Technology, Brigham Young University

Francis Mensah received a Bachelor of Science degree in Electrical/ Electronics Engineering from Kwame Nkrumah University of Science and Technology in May 2006. He is currently getting a Masters Degree in Information Technology at Brigham Young University with an emphasis in computer networking and security. He also has a special interest in Cyber-Physical Systems. During his leisure time, Francis enjoys playing the piano and listening to classical music.

Prof. Richard G. Helps, Brigham Young University

Richard Helps is an associate professor in the Information Technology Program at BYU. He has research interests in embedded systems, human-computer interaction and curriculum design. He is a member off ASEE, IEEE, IEEE-CS, ACM-SIGITE and an ABET PEV for Information Technology.

Security Analysis of CPS: Understanding Current Concerns as a Foundation for Future Design

Abstract

Cyber-Physical Systems (CPS) or Embedded Systems are now so wide-spread that we see applications in almost every aspect of our everyday activities. Application fields include industrial process control, health care, transportation, financial transaction systems, building security systems, home electronics, and automobiles, among others. The "Physical" aspect of CPS indicates that these systems interact mainly with the physical world and thus can significantly impact human and environmental safety as well as large physical infrastructure systems. CPS failure can therefore have catastrophic consequences. It is thus very important that CPS operate in a safe, reliable and secure manner. While these systems have seen a lot of technological improvements resulting in increased functionality, the issue of security has been a low priority in their design, thus exposing them to several security threats. If we are to benefit fully from the many applications of CPS then security needs to take a central role in their design. The challenges of security design for CPS are aggravated by the lack of standardization in hardware, operating systems, networking and the diverse physical environment. Addressing such challenges needs a strong collaboration between those skilled in CPS component design as well as those skilled in security and other aspects of these complex systems.

This study includes an analysis of the available literature and design practices in several CPS application fields, with an emphasis on design for security. The Information Technology community has a rich background in security analysis, although not generally applied to CPS design. Thus a security analysis methodology for CPS was developed from recognized security analysis techniques for conventional computing. Assets, security threats and risks are analyzed relative to a CPS environment. Current security solutions are presented and compared. We discuss evolutionary changes of CPS leading to their growing importance within computing disciplines and their increasing role in large, heterogeneous distributed systems. Finally the integrative nature of CPS design is discussed and the role of Information Technology as a major contributor to CPS design for security is emphasized.

1.0 Introduction

As computing technology has grown and continues to grow in sophistication, there has also been the increasing desire to have these technologies employed in almost every aspect of human life and activity. One of such applications is the incorporation of computing and communication technologies into the control of physical processes. Systems used to accomplish such functionality are referred as Cyber Physical Systems (CPS). These systems are also known as Embedded Systems because of the manner of their deployment – usually as an integral part of a system that interacts with the physical environment. Cyber Physical Systems are currently used

in the control and supervision of processes that are critical to human lives and the national economy including water treatment and distribution, electricity generation and distribution, transportation, communication systems, financial transaction systems, building management systems among others. Other less critical but important applications includes home entertainment systems and compact mobile platforms, such as smartphones, tablets and similar devices.

Historically Cyber Physical Systems used proprietary hardware, communication protocols and operating systems to accomplish their control designs. These systems were usually deployed in homogenous environments or in other words they hardly had to interact with and/or depend on other systems to perform their functions. The well-recognized concept of 'Air Gap' suggested that the systems were isolated and had no communication with the external world of networks. To gain access into these systems required physical access and a very detailed knowledge of the platform and the protocols that were implemented in them. Thus security was a matter of securing the system from unauthorized physical access and the use of proprietary software and protocols which did not allow for third party manipulations [1,2].

With recent advancement in computing and communication technologies CPS have gradually evolved from isolated systems with proprietary protocols and operating systems to systems that use standard computing protocols like TCP/IP and operating systems like Microsoft Windows and Linux. It is now common to find CPS being applied in heterogeneous applications where several different kinds of systems interact to perform a function. While this evolution has brought added capabilities and functionalities and low cost implementations, security has often been an omitted from the design.

While efforts have, and are being made to secure these standard computing protocols and operating systems, most of these security measures have been designed to suit traditional IT application environments, which range from personal systems, through small office home office (SOHO) networks and up to large corporate networks. The security needs of CPS, however, differ from those of traditional IT applications and present unique challenges. While reliability, availability, data integrity and confidentiality are of primary concern to IT networks, human and environmental safety is paramount when considering security in CPS. Furthermore, cyber physical systems are built with performance and reliability being the primary focus. The challenges of security design for CPS are further aggravated by the lack of standardization in hardware, operating systems, networking, human computer interactions (HCI) and the diverse physical environment. Addressing such challenges needs a strong collaboration between those skilled in CPS component design as well as those skilled in security as well as designers with a strong background in systems integration other aspects of these complex systems. This collaboration is likely to bring about security solutions that are tailored specifically to applications in the CPS environment.

CPS Market Sectors

CPS security concerns vary according to vertical market sector. In fact each market sector has its own community of CPS designers, oriented to the needs and constraints of their sector. Various lists have been developed dividing up the market sectors. The list we present below evolved from parallel research into recording and classifying CPS security incidents [3].

- Utilities (electricity, water, gas)
- Health Care
- Transportation
- Aerospace
- Military
- Consumer Electronics
- Facilities Infrastructure
- Agriculture
- Physical Access Control
- Communications
- Construction Equipment

It is clear that some of these fields overlap. The purpose of listing and investigating the sectors is to attempt to address the different communities of design that, at least somewhat, develop CPS systems independently. Furthermore the risks and consequences of security breaches vary among the different sectors even if they share similar technology or security protection mechanisms.

The rest of this paper is organized as follows: Section 2 reviews the unique characteristics of CPS in comparison with conventional computing platforms and how these unique characteristics impact on security. Section 3 discusses various application fields of CPS with respect to their security requirements, challenges and current security solutions.

2.0 Constraints on the design of security solutions imposed by CPS characteristics

In discussing CPS in the context of information assurance and security, it is important to identify the differences in their requirements in contrast to the requirements of conventional computer systems (CCS). Conventional computer systems are considered to be those which include one of the well-known operating systems (Windows and Unix-derivatives), are intended for a wide range of computing services by running multiple application programs, include 802.xx network connectivity and interface with operators primarily through a keyboard, monitor and mouse.

Compared with conventional computer systems, cyber physical systems have different priorities and imply risks with a much broader scope and impact. These systems are usually behind the control of critical processes in sectors such as electric power generation and distribution, water treatment and automated highways among others. What this means is that a security breach in such a system can directly control these physical entities and therefore impact not only the system infrastructure but, even more importantly, the health and safety of humans, the

environment, and the national economy at large. Of course CPS suffer from the same vulnerabilities as conventional computer systems in addition to those peculiar to their physical interaction with the world. In this section, some of the key factors that affect the security requirements of cyber physical systems are discussed [4].

Real-Time Requirements: Cyber Physical Systems are usually used in applications where the needs for real-time responses are not negotiable. Any form of delay or jitter in real-time systems is definitely unacceptable. With this constraint a concern is immediately raised when security measures like encryption and authentication must be implemented. These measures come with some overhead that can have an adverse effect on the performance of real time systems. It is thus important to take into account this requirement when designing security solutions.

Availability Requirement: Many cyber physical systems are used in mission critical operations; as such they must always be available to perform their functions reliably. Even small amounts of downtime are just not unacceptable, and can lead to dangerous consequences. Consider, for example, medical equipment failing in the middle of a critical surgery.

Time Critical Responses: In many CPS applications, response to human interaction is critical. The ability of an operator to work with the plant (working system), especially in emergency conditions, must not be hindered by the security solutions implemented. Authentication requirements such as passwords should not interfere with human actions during emergency situations. In some nuclear plants, for example, passwords to access the control systems are written on walls. This will obviously ensure that human memory lapse does not play a role in a delayed human intervention. Of course to be in the control room also means that the user has satisfied physical security requirements.

Human-Computer Interaction Standards: Most CPS do not use a standard keyboard and mouse to interact with the system. This implies that security mechanisms like authentication need to be adapted to the custom design of the system. Entering detailed passwords through keypads is not reasonable, and in many cases CPS do not even have keypads or screens at all.

Computing Capabilities: CPS are often limited in their computing capability and memory resources. This limitation imposes a constraint when it comes to implementing security solutions that require a certain level of computing resources that is above what the CPS device can provide. For example securely encoding or decoding streamed data can be compute-intensive.

Heterogeneity: Solutions that work on platform probably won't transfer to all interacting platforms. For example the networking of scientific research instrumentation may expect standard authentication schemes, which cannot be implemented on the instruments themselves. Another example is industrial plants, which make extensive use of Programmable Logic Controllers (PLCs). The PLCs cannot easily share data and security algorithms with the supervisory computers or with the sensors and actuators that they control.

3.0 Analysis of current security requirements in CPS application sectors

Different market sectors (discussed above) have significantly different expectations and security needs. An analysis of security for CPS must consider these differences. Bruce Schneier developed a generalized five-step procedure for security analysis [5]. This framework will be adopted and then applied in several aspects for the review of CPS security needs.

Throughout his security analysis of systems, technologies and practices Schneier asks five questions to aid in an effective security evaluation of a system. The questions he asks are as follows:

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

According to Schneier these questions, while not a design methodology for a security solution, will provide a mechanism to evaluate a proposed security solution. It will be possible to realize how ineffectual some common security solutions are, in other words how they solve the wrong problem or cause more problems than they solve. One objective of this paper is to identify current solutions for CPS both from a generic and market sector perspective and then analyze them with respect to CPS characteristics in order to assess their efficacy.

The adopted CPS analysis framework for the purpose of this paper consists of three steps. Each step answers a question on an aspect of security similar to that proposed by Schneier. The aspects of security discussed include the following:

- Assets and Risks
- Vulnerabilities
- Existing prevention and mitigation mechanisms

The application of these steps to CPS is illustrated by examples from a few market sectors.

3.1 Assets and Risks

In the context of information assurance and security an asset is the resource that is being protected from being compromised either by a deliberate act or an accident. Assets may be real property or intangible properties of the system which have real value. Modern CPS includes the assets for CCS but also includes assets derived from their characteristics discussed in section 2 above. The assets which are peculiar to CPS include a strong emphasis on concepts such as human life and safety (consider controlling of a moving vehicle or aircraft), loss of production

(as in a manufacturing industry), user satisfaction (the ability of the system to interact satisfactorily with the user), major system breakdown (such as electrical grid malfunction), decreased performance of a physical system and damage to equipment (as in the Stuxnet incident).

Protection of CPS assets includes the standard concepts of security, namely availability, integrity, confidentiality, authentication and non-repudiation. The main objective of security is to ensure the quality of an asset in a system is preserved and is free from danger, in other words, protected from adversaries [6]. Any object, person or other entity that presents a danger to an asset is known as threat. Threats can come from numerous sources including those with malicious intent such a hostile governments, terrorist and organized crime groups, cybercriminals, disgruntled employees as well as from those without malicious intent such as human errors, equipment failures and natural disasters [7]. An attack occurs when a threat takes advantage of a weakness in a system to control, damage or extort critical information. The probability of threat being able to launch a successful attack is risk that a system faces. In the following examples from selected market sectors, some CPS assets and risks will be illustrated.

Medical Sector

Health care is desirable for all levels of society and as such should be accessible to all as easily and conveniently as possible. Technology is a major enabling factor leading to an achievement of this goal in various aspects of the health sector with Cyber Physical Systems forming a bulk of these technologies. One of the emerging roles of CPS in healthcare is to provide timely medical assistance, including monitoring and even treating patients outside the confines of traditional medical establishment, such as in-home medical monitoring and treatment systems, in addition to other functions like imaging and drug dispensary. While these technologies are helping to improve the quality of life in many parts of the world it is also important to make sure that the assets involved are protected from any form of security failure.

The most prominent asset in this sector is human health and safety. Other assets include patient confidentiality and diagnostic information. The Health Insurance Portability and accountability Act (HIPAA) mandates the protection of a patient's data [8]. In addition to these assets there are also various medical system devices that are used for several operations including drug dispensary, medical imaging and image storage, remote diagnostics among others.

These assets have specific threats, some of which are specific to CPS aspects of the system. The use of CPS in medical systems to collect, exchange, store and control electronic health data rely heavily on existing computer and communication technologies. These technologies expose the medical systems to similar threats that are familiar to conventional computer systems. Some of these threats, as mentioned by Venkatasubramanian and Gupta [9] include:

1. Unauthorized access to health data

2. Deliberate alteration of health data, leading to incorrect diagnosis, treatment and ultimately fatality.
3. Deliberate generation of false alarms or suppression or real alarms raised by the system in the case of emergencies.
4. Deliberate software attacks (malware)
5. Hardware malfunction or failure leading to wrong dosage of treatment.

It is now obvious that high risk systems do not just involve obvious systems like nuclear plants but also hospitals, anesthesia systems and the practice of medicine in general [10]. Because of the value of assets involved in this sector, it is very critical to apply a thorough risk assessment and management analysis when using cyber physical systems in the medical sector. Most importantly it is necessary to use a holistic system approach when assessing the security status of such systems. It is not enough, for example, to test individual equipment and declare the system as secure. Equally important is the overall communication infrastructure of which the individual equipment forms part.

Consider for example a heterogeneous system such as a home-based patient wearing a medical monitoring device, which communicates through a variety of channels, including the Internet, to a hospital monitoring system, which may in turn communicate with remote medical personnel and emergency responders. The data from the monitoring device may be sniffed or modified in transmission before it gets to the hospital system. This may cause the health care professionals to miss a real problem causing a patient, whose health and immunity to disruption is already compromised by their medical condition and possibly by their treatment, to be deprived of proper medical care. This is one area where there needs to be a strong collaboration between the device engineers, integrated system designers and network and security engineers to ensure that the system functions in a secure and reliable manner.

Utilities Sector

The utilities sector is part of what is known as the critical infrastructure (CI). CI systems play a very important role in the functioning of the national economy. Examples include electric power generation and distribution, oil and gas production among others. Operations in these sectors involve a lot of interaction between the physical systems and the natural environment. Compromising these systems has impacts in several areas. Firstly the equipment itself has significant value, such as in the cyber-attack on the Iranian nuclear facilities in 2010 [11], secondly the equipment directly interacts with the environment and environmental disasters are possible, and finally the lives of thousands to millions of people can be adversely affected by compromised services. In addition compromising these systems have economic effects that can be national or even global in scale. According to the Department of Energy, the annual cost of power outages is estimated to be $25 - $180 billion. The following table shows the cost of a power outage for some selected industries that depend on electric power [12].

Table 1 (*source: Report on Workshop on Future Directions in Cyber-Physical Systems Security, January, 2010***)**

Cost of Power Outages for Selected Industries Stake Holders	
Industry/Stake Holder	**Cost of power outages (per hour)**
Brokerage	$6,480,000
Credit Card	$2,580,000
Airline Reservations	$90,000
Telephone Ticket Sales	$72,000
Cellular Communications	$41,000

Manufacturing Sector

Manufacturing plants are another major user of CPS systems. Malfunctioning systems in a factory can have immediate effects on the manufacturing equipment and the product being produced. Perhaps more seriously, malfunctions can have wider-ranging impacts as well, for example a chemical plant incident can affect the environment and human lives. An example of how bad a manufacturing plant accident can be is in the Bhopal Union Carbide chemical plant disaster in India, 1984, where deaths were numbered in the thousands [13].

CPS usage in Utility and Manufacturing Sectors

There are additional concerns in the Manufacturing and Utilities sectors that are common to both of them. The manufacturing and energy sectors represent one of the largest users of CPS. Just like other CPS sectors, the manufacturing and energy sectors have migrated to the use of modern sophisticated computer and communication technologies. It is now common to find geographically dispersed systems connected and interacting with each other. Technologies used to accomplish this architecture and functionality includes Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS). This has resulted in improved production, efficiency and reduced cost of operations. It is now possible to perform remote monitoring, debugging and maintenance. In addition performance data can easily be accessed and processed by management and other non-engineering departments.

The technologies that have been adopted by these sectors have many advantages but have also exposed the systems to various threats and possible attacks. Most of these threats and attacks are similar to threats in the medical and other CPS sectors in concept, but apply in a different context. Some of these threats and attacks are listed as follows:

1. Unauthorized access to manufacturing data. Most manufacturing industries make of proprietary control recipes to produce their products. Such information is considered to

be the intellectual property of the company and thus should not fall into the wrong hands, especially a competitor.

2. Denial of service. This this the situation where a system's operations are disrupted due to an inundation of messages sent to it. Such an attack can halt production which also leads to other cascading effects.
3. Deliberate alteration of control system algorithms or set points leading to incorrect control procedures. This situation can be potentially catastrophic if the algorithm involves safety procedures. Consider, for example, if the trip current of a circuit breaker is 100A is changed to 1000A dangerous levels of current can flow within the system.
4. Deliberate generation of false alarms or suppression or real alarms raised by the system in the case of emergencies.
5. Deliberate software attacks (malware)
6. Equipment failure leading to loss of production
7. Command Spoofing. This attack can result from an attacker generating a command that seems to come from a trusted source and sending that command to control a device in the control network.

The consequences of any of these attacks can be catastrophic and efforts must be taken to prevent or mitigate their impact.

The Smart Grid

The Smart grid extends the computational control of the normal electrical grid and attempt to predict and intelligently respond to the behavior and actions of all electric power users connected to it in order to efficiently deliver reliable, economical and sustainable electrical services [4]. Components of the smart grid include:

- Smart meters
- Communication infrastructure
- Supervisory control devices
- Central control computer systems

From a security point of view, the smart grid connects the customer's home to the power grid and to the network infrastructure of the utility service provider. Thus the conventional computing system has now been extended into the CPS realm and the complete system contains physical plant that can be impacted by IAS incidents and many more points of entry (I.E. vulnerabilities) into the system. Since by its nature a smart grid has the capability to control energy flows, it can also have serious consequences if a security failure mis-directs the energy flow.

3.2 Vulnerabilities

As discussed above, CPS are used in a wide variety of market sectors ranging from critical operations to home consumer devices. Each of these sectors exists as a vertical market, with each

having its own special needs and requirements. In spite of this specialization of functions and requirements in each of these sectors, there is significant overlap and commonality in the underlying technologies that are used to achieve the various functionalities in the sectors. Most CPS sectors, for example, make use of standard networking and communication protocols like Ethernet and TCP/IP as well as standard computing platforms like Embedded Windows, Embedded Linux and Microcontrollers. Because of these common underlying technologies, the vulnerabilities that expose the systems in the various CPS sectors to attacks are also similar.

For example industrial control systems comprise a set of technologies that are employed in several CPS application sectors including power generation and distribution, medical systems, manufacturing, transportation control systems and so on. According to NIST SP 800-82 [7] an Industrial Control Systems (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. Because of the wide spread use of ICS in several sectors of CPS, they will form the focus of discussion in this section. Because of the commonality of these technologies the discussion can also extended to others technologies use in CPS.

ICS, like most other technologies, have taken advantage of advanced computer and communication technologies to greatly improve their functionality and efficiency. Their designs (both platforms and protocols), however, has mainly been focused on allowing data to be exchanged and getting the work done. For as long as they work they are good. This has often been the goal of control engineers, for example. Cyber security was historically not considered as a major part of the design of these systems. CPS Security design was less important when security was mainly a matter of physical security, using air-gapped systems and unknown proprietary protocols (security by obscurity). This is not the case today.

The transition to standard network protocols and operating systems and hardware has made ICS, and for that matter CPS, just as vulnerable to cyber-attacks as conventional computer systems. Several researchers and analysts have discussed vulnerabilities of CPS systems. Some of these discussions are presented as follows:

According to NIST SP800-82 [7] ICS vulnerabilities can be categorized under two broad criteria, Platform and Network vulnerabilities. These categories can be summarized as follows.

- **Platform Vulnerabilities**: These are vulnerabilities that are introduced due to flaws, misconfigurations or poor maintenance of hardware, operating systems and application software.
- **Network Vulnerabilities**: These vulnerabilities occur from misconfigurations and/or poor administration of network connections in the control network. This is especially so when creating connections with other networks such as the Internet.

The categories [7] are focused primarily on the ICS application. The discussion of ICS vulnerabilities can, however, be extended to other CPS applications since the vulnerabilities are usually based on the underlying technologies which are common to most CPS. The following list identifies key vulnerabilities that should be considered by designers and analysts [4]:

1. **Communication Protocols**: Communication in ICS the past were done primarily through the use of non-routable serial protocols including Modbus, Profibus, and Foundation Fieldbus among others. These protocols were not designed with security in mind. For example, there are no means of authentication and so devices can accept connections from any other device that seeks to communication with them. However, because these protocols are not routable, an attacker will have to be physically connected to the network in order to have access to the devices. With the transition from these non-routable protocols to routable protocols like TCP/IP, ICS have become susceptible to the weaknesses that are already present in these protocols. It is now possible for an attacker to gain access from any other network to gain access to the system and with the lack of security mechanisms like authentication the system can be easily compromised.
2. **Standard Operating Systems and Applications**: Most ICS have migrated to the use of standard operating system platforms like Windows and Linux as well as common applications like VNC, MS-SQL and so on. Most of these platforms and software already have vulnerabilities associated with them. The vendors of the platforms periodically release patches to take care of the identified vulnerabilities. The nature of operation of most CPS is, however, such that the application of patches can greatly interfere with their normal operations. To make matters worse, some Vendors even prohibit the application of patches or the use of third party security solutions. The exposes the CPS system to several forms of attack in the wild.
3. **Interconnectivity of ICS**: Unlike in the past, CPS networks are commonly interconnected with corporate network systems. It is also normal to allow the remote administration of devices from outside of its local network. This often means that public network infrastructure is used, including the Internet and several technologies offered by telecommunication companies. This exposes the network to various potential attacks from these publicly accessible networks
4. **Inappropriate and Insecure Connections**: Several ICS come with modems to allow for remote diagnostics, maintenance and monitoring. Most times, these access links are not protected with strong authentication and encryptions mechanisms. As a result, the CPS network can be easily compromised.

3.3 Existing Prevention and Mitigation mechanisms

Security mechanisms for CPS fall under three main categories namely proactive, reactive and design models, as proposed by Cardenas, Amin, and Sastry [14]. Proactive mechanisms are those that take measures to prevent the possibility of an attack while reactive mechanisms are the security measures taken when an attack is already in progress. Most of the current solutions in

CPS security are based on adapting CCS mechanisms to work for CPS. Typical security measures adapted to CPS are discussed below. This is followed by a discussion of CPS-specific mitigation measures. The adapted standard mechanisms work to the extent that CPS systems overlap conventional systems; the difficulties that arise due to the distinctive nature of CPS make some of these mechanisms less effective.

Crypto-Systems

Crypto-systems comprise various mechanisms used to ensure IAS properties such as integrity, confidentiality, authentication and non-repudiation through the use of cryptographic techniques. The use of cryptography can be seen as a proactive way of preventing cyber-attacks. For example, through the use of crypto-systems, an access control system can be set up to ensure that only authorized devices or users can access a system. Several technologies and protocols are currently available for the implementation of crypto-systems in CPS, examples of which include Public Key Infrastructure (PKI), Message authentication codes (MAC), Kerberos, Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Internet Protocol Security among others [15].

Intrusion Detection Systems

A security approach often employed in CCS networks, and described by Knapp [16], is the defense in depth mechanism. In this approach the components of the network are categorized into zones according to their functionality. All traffic into and out of the zone is then forced through one or more known network connections that can be monitored and controlled. There are one or more security devices that are placed in line with these connections. These network connections and security devices form part of what is known as an electronic security perimeter [16]. An example of a perimeter security device is a network based intrusion detection system (NIDS). The function of an NIDS is to closely examine the network traffic that is allowed into the perimeter in order to detect malicious traffic. NIDS operate either by comparing network traffic with a set of attack signatures or by detecting anomalies in traffic pattern. Several CPS networks especially those used in ICS use this approach to detect malicious attempts to gain access to the network.

In addition to NIDS there are also host based IDS (HIDS) which are installed on a single device to monitor network traffic and application activity. The operation of HIDS may also be signature based or anomaly based. There is on-going research into using IDS for CPS network security with the main objective of improving the ability of IDS to detect and stop CPS cyber-attacks. One such project by Digital Bond Inc. involved the development of attack signatures for the Modbus/TCP protocol [17].

Firewalls

Firewalls are devices that are used to allow certain types of network traffic to pass through the network perimeter or a host device. Interconnectivity of systems works through the use of network services that operate on TCP or UDP ports. Sometimes a component of a CPS may be designed to operate on certain ports; however, not all of them will be used for a particular application. A firewall can in this case be used to deny all traffic that operates on the unused ports. This is important because unused ports can be used as an entry point into a network or device. Some advanced firewalls can also control the direction of flow of traffic as well as allowing or denying traffic based on application layer contents.

Data Diode

A data diode is a special form of a firewall. It allows for a one way network connections either at the perimeter or on the host device. A data diode is often a physically restricted connection that uses only one fiber optic strand from a transmit/receive pair [16]. By using only one strand it is impossible for communication to flow in the opposite direction.

VPN

Oftentimes it becomes necessary to perform remote monitoring of a device in a CPS network. This requires some form of remote access. In systems such as ICS, modems are sometimes used to achieve this. Modems are however not a very secure mechanism since an attacker can use methods such as
"war dialing" to gain unauthorized access into the network. Virtual Private Networks provide a security channel through which a remote device can gain access into a network.

Software Patches

Application software is seldom flawless when it is released onto the market. As time goes on vulnerabilities are discovered in software that can make the system susceptible to cyber-attacks. The usual practice, whenever a vulnerability is discovered, is that the authors work release a patch to repair the vulnerability. Thus to ensure that a device is safe it is important to keep all patches are up to date.

It can be concluded from the previous discussion that several efforts have gone into the development of security solutions for CPS. These security solutions, however, do not sufficiently articulate what is new and fundamentally different in CPS compared to CCS [8]. There are some challenges that arise when these security solutions are applied to CPS. In this section some of these challenges are discussed.

Overview of Challenges that is CPS-Specific

Because of the requirements and characteristics of CPS, many of the security solutions that are used to protect conventional IT systems cannot be used or have very little effect in CPS. The largest CPS user of CCS security technologies is ICS mainly because of the nature of their operations as well as their level of sophistication. Even with their level of sophistication there are challenges with the implementation of some security solutions. With other CPS technologies which are not as sophisticated as ICS, the situation is even worse. One reason for this is the resources that are demanded by these security solutions. The use of public key infrastructure, for example, demands several computing resources like processing power that may not be readily available to most CPS systems. Another situation is where the security solution has not been adequately adapted to the protocols commonly used in CPS. For example, intrusion detection and prevention systems (IDS and IPS) products used in ICS are effective in detecting and preventing well known Internet based attacks, but until recently they have not addressed ICS protocol attacks. Some ICS and other third party vendors are beginning to develop and incorporate attack signatures for various ICS protocols. Digitalbond and Tofino, for example, are ICS security vendors that have developed such products [18,17].

Application of software patches and updates

CPS are not as friendly to application of software patches as compared to CCS. Application of patches and updates usually require the system to be restarted in order to take effect. This is usually not acceptable in CPS especially in ICS. Some security patches may even violate the certification of control systems [8]. Applying patches to medical systems may require re-certification of the devices for use on humans, an expensive and time-consuming effort.

CPS with non-standard operating systems

Most firewalls, for example, have been designed to run on standard operating systems like Windows and Linux or on dedicated hardware. Many CPS, however, make use of non-standard operating systems. This presents a challenge when applying a firewall solution to the device.

Delays in execution of real-time systems

When additional network devices like IDS are placed in line with network traffic, there is also the introduction of network latency that can affect the execution of real time commands and responses. This is because the IDS need to inspect and process the packets in the traffic before passing them on.

The security challenges identified above suggest that a different approach is needed when implementing security solutions for CPS. In addition to the fact that these existing solutions are traditionally designed for CCS which makes them not sufficiently adequate for CPS, they only consider defending the cyber portion of CPS. The physical component is largely left out. Just as

in CPS, the computing component is used to effect control in the physical world; changes in the physical state of the CPS's environment also have an effect on the computing component. It is thus important to use an integrated approach, comprising both cyber and physical aspects, when designing security solutions for CPS [19].

In addition, consider that an attacker has already gained access in to the system. In this situation the attacker is able to issue legitimate commands to control the physical components. This situation demands that the system is able to monitor its physical state in order to detect and stop such an attack. Though specific controls do not exist yet for such scenarios, there is research going on these areas. This is discussed in the next section.

4.0 Future of CPS security

Research into CPS systems is proceeding in several directions. For example, there is research into the theoretical underpinnings of the discipline, noting that current computing research foundations do not cover the problems of CPS [20]. An aspect of this increasing interest in CPS is research into the holistic systems design aspects of CPS, meaning consideration of the design of the complete system, including the users, the physical systems, the ancillary concerns (such as IAS concerns) in addition to the CPS devices themselves.

An analysis by Neuman [21] stresses the need to pay attention to the hard problems rather than applying ad hoc solutions which is the situation currently. According to him security for CPS needs to be considered in an integrative manner (from a system perspective) and not as a separate solution.

There is a need for design models addressing this integrative view of CPS design. Many researchers are calling for the need to fully consider a comprehensive modeling of the physical environment component [22,23,24,25]. Furthermore there are different communities of design in the different market sectors cited above. It is the contention of this analysis that there is significant commonality between the design needs of the different sectors and that analysis of existing models of design can reveal these commonalities, as well as the important and distinctive differences.

The call for CPS security design to incorporate both cyber and physical mechanisms means that there needs to be a new look at the disciplines that are involved with CPS design. This problem is too big for isolated developers. Traditionally computer science has been involved in the development of the computing components. Engineering skills are valuable in developing the complex sensor, actuator and real-time control aspects of these systems. With the CPS being interconnected and security needs being considered, another discipline is needed, namely Information Technology (IT). The IT discipline is needed to bridge the gap between the computer science and electrical engineering. IT professionals have specific skills in the areas of system integration, networking, and security that can be extremely valuable in this domain. IT professionals will need to interact with computer science and electrical engineering, as well as

consider market sector issues and user issues, and then design a security solution that considers all stakeholders.

5.0 Conclusion

The importance of CPS to computing in general is growing exponentially. Rajkumar et al.[26] suggest that computing and communication will soon be embedded in all types of objects and elements in the physical environment. It is important that we consider the security needs due to the critical nature of operations of these devices.

As discussed above much of the research and development in this field has come from two directions. The first is an ad-hoc adding of security features to evolving CPS designs, which did not previously have them. The second is an evolution of existing security approaches from CCS into the CPS world. While both of these approaches are valuable, neither of them sufficiently addresses the complete problem space.

A comprehensive security analysis and design approach needs to address the specific characteristics of CPS and the constraints imposed by the different market sectors in which it is applied. Designers, security analysts and users in these fields need to become more aware of the complex nature of this problem. Research into CPS security is on-going, as discussed above, and it is expected that the challenges so far identified will be informative thus leading to reliable, safe and secure design of CPS in the near future.

REFERENCES

1. B. M. Mckay and P. A. Engineer, “Best practices in automation security.” *Cement Industry Technical Conference, 2012 IEEE-IAS/PCA 53rd*, pp. 1 - 15, 2012.

2. N. Adam, "Workshop on Future Directions in Cyber-Physical Systems Security ", in *Report on Workshop on Future Directions in Cyber-Physical Systems Security*, January, 2010.

3. B. Miller and D. Rowe, “A survey SCADA of and critical infrastructure incidents,” in *Proceedings of the 1st Annual conference on Research in information technology - RIIT ’12*, p. 51, 2012.

4. ENISA, “Protecting Industrial Control Systems,” 2011.

5. B. Schneier, “All Security Involves Trade-offs,” in *Beyond Fear*, 2006, pp. 14 – 16.

6. M. E. Whitman and H. J. Mattord, "Introduction to Information Security," in *Principles of Information Security*, pp 8, 2011

7. K. Stouffer and K. Scarfone, “Guide to Industrial Control Systems (ICS) Security Recommendations of the National Institute of Standards and Technology,” 2011.

8. A. C. Alvaro, “Challenges for Securing Cyber Physical Systems.” in *Workshop on future directions in cyber-physical systems security*, 2009.

9. K. K. Venkatasubramanian, "Security in Pervasive Computing,” *Ph.D. dissertation*, Arizona State University, Arizona, 2009.

10. J. Wang, H. Abid, S. Lee, L. Shu, and F. Xia, “A Secured Health Care Application Architecture for Cyber-Physical Systems.” *Control Engineering and Applied Informatics*, Vol.13, No.3, pp. 101-108, 2011

11. N. Falliere, L. O. Murchu, and E. Chien, “W32 . Stuxnet Dossier version 1.4,” [Online] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, 2011.

12. N. Adam, "Workshop on Future Directions in Cyber-Physical Systems Security ", in *Report on Workshop on Future Directions in Cyber-Physical Systems Security*, January, 2010.

13. M.J. Peterson, “Bhopal Plant Disaster – Situation Summary,” Science, Technology & Society Initiative, University of Massachusetts Amherst, 2009.

14. A. Cardenas, S. Amin, and S. Sastry, “Secure Control: Towards Survivable Cyber-Physical Systems,” *The 28th International Conference on Distributed Computing Systems Workshops*, pp. 495–500, 2008.

15. Citation styles online, “Department of Homeland Security: Control Systems Communications Encryption Primer,” [Online] https://ics-cert.us-cert.gov/pdf/Encryption%20Primer%20121109.pdf (Accessed 20 November, 2012.

16. E. D. Knapp, "Establishing Secure Enclaves" in *Industrial Network Security*. 2011, pp. 166 – 167.

17. Citation styles online, "Online! Citation styles," [Online]. Available: https://www.digitalbond.com/tools/quickdraw/.

18. Tofino, “Using Tofino ™ to Control the Spread of Stuxnet Malware Using Tofino ™ to Control the Spread of Stuxnet Malware,” Application note #119, 2010.

19. T. R. Mcevoy and S. D. Wolthusen, “A Plant-Wide Industrial Process Control Security Problem,” in *Critical Infrastructure Protection (2011)*, pp. 1–19, 2011.

20. Citation styles online, “NSF Workshop.” [Online]. Available: http://varma.ece.cmu.edu/CPS/.

21. C. Neuman, “Challenges in Security for Cyber-Physical Systems.” in *Workshop on future directions in cyber-physical systems security*

22. B. A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber–Physical Systems," *Proceedings of the IEEE* , vol.100, no.1, pp.283,299, 2012

23. C. Neuman, “Challenges in Security for Cyber-Physical Systems.” in *Workshop on future directions in cyber-physical systems security*

24. S. Cheung and K. Skinner, “Using Model-based Intrusion Detection for SCADA Networks,” in *Proceedings of the SCADA Security Scientific Symposium*, pp. 1–12, 2006.

25. T. R. Mcevoy and S. D. Wolthusen, “A Plant-Wide Industrial Process Control Security Problem,” in *Critical Infrastructure Protection (2011)*, pp. 1–19, 2011.

26. R. (Raj) Rajkumar, I. Lee, L. Sha, and J. Stankovic, “Cyber-physical systems,” in *Proceedings of the 47th Design Automation Conference on - DAC ’10*, 2010, p. 731.