The Security of Cyber Physical Systems

April 13, 2016

Shannon Bolton and Nikki Pruitt

CS 470

Table of Contents

Abstract 2

Introduction 3

Background 3

What Are Cyber Physical Systems? 3

How Do Cyber Physical Systems Work? 5

How Are Cyber Physical Systems Used? 6

Cyber Physical Systems and the Internet of Things 7

Purpose 7

Scope 7

General Discussion 8

Cyber Security and Cyber Physical Systems 8

Security Objectives of Cyber Physical Systems 9

Challenges and Vulnerabilities of Cyber Physical Systems 10

Solutions for Cyber Physical Systems 11

Conclusion 12

Bibliography 13

# Abstract

In this paper, we will examine some of the security issues that stem from cyber physical systems. First, we will discuss what a cyber security system is exactly, how they are used, and how they work. Then we will analyze the different security concerns that are specific to cyber physical systems, as well as the vulnerabilities that these systems are faced with. Finally, we consider potential security solutions for cyber physical systems, and what advancements must be made in order to fully secure these systems.

# Introduction

# Background

In this section, there are three basic questions that need to be answered:

* What are cyber physical systems?
* How do cyber physical systems work?
* How are cyber physical systems used?

## What Are Cyber Physical Systems?

Cyber physical systems, or CPS, are feedback systems that require merging physical components and computational components (National Science Foundation).

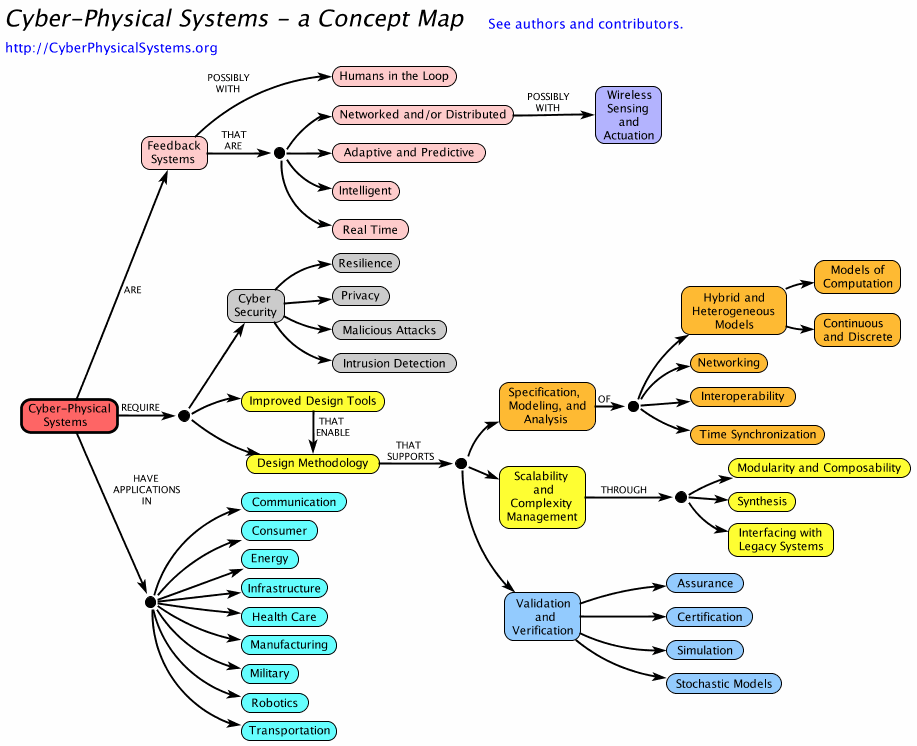


Figure 1 - A tree explaining cyber-physical systems (Cyber Physical Systems)

Cyber-physical systems can be explained using a well-designed flowchart, (see Figure 1 above). These systems usually have distributed using wireless technology. They must be able to change due to certain conditions and even expected changes to come in how the processes execute. CPS can learn from its environment, changing its behaviors. All of these can be done while it is executing commands in real-time to meet the required time restraints. (Cyber Physical Systems)

## How Do Cyber Physical Systems Work?

Cyber physical systems require strong cyber security. They have to be able to have strong privacy to protect the user’s information. They should be able to prevent malicious attacks such as viruses, Trojan horses, and denial of service attacks. Open networks are much easier to attack because there are more exposed vulnerabilities. Sometimes the CPS will still get attacked even if it is on a closed network though. No matter what, the cyber physical system should be able to handle something as mall as the wrong inputs or even something as big as a subsystem failing. (Cyber Physical Systems)

The cyber physical systems also need better tools that allow for the best design of the system. The design of the system needs to allow for the system getting more complex, while still allowing it to scale up in size. It also should be able to be verified and validated to the user’s specifications and best practices of the time. By keeping all these requirements in mind, the cyber physical system’s product owner can specify how they want their CPS to be modeled. The product owner can analyze their CPS and other CPS to determine the optimal product. (Cyber Physical Systems)

## How Are Cyber Physical Systems Used?

Cyber physical systems can be used in many different fields. Examples of each are listed below.

|  |  |
| --- | --- |
| Consumer | Examples of a consumer using CPS would be video systems, interactive games, and audio systems. |
| Health Care | In the health care field, technology provides important information to health care workers, such as the heart rate of a patient. The CPS can be used to help the flow of medical visits and assist in patient safely by integrating all the information into one location. |
| Energy | Smart buildings are become more popular from their use of CPS. CPS allows smart buildings to control and monitor functions such as lights and air conditioning from a control system. |
| Military | There is a large part of all military systems that are cyber physical systems to aid in the exchanging of information. |
| Transportation | Systems used for automotives, railroads, planes, traffic control, and even elevators and escalators are depended upon cyber physical systems. |
| Infrastructure | Infrastructure for society, such as power, roads, and water, can be maintained using cyber physical systems. These examples include monitoring of water safety, helping in disaster recovery, and working on the water distribution in the city. |
| Communication | Wireless communication is an example of a communication system that uses CPS. |
| Manufacturing | Computer-controlled systems and machinery used in production uses cyber physical systems. |
| Robotics | A couple of areas that CPS assists in the robotics field would be artificial intelligence and robotic motion control. |

Table 1 - Applications and examples of cyber physical systems (Cyber Physical Systems)

## Cyber Physical Systems and the Internet of Things

Cyber physical systems are also known as the Internet of Things (NIST).

# Purpose

The purpose of this report is to examine the various issues that affect security of cyber physical systems.

# Scope

This report will discuss the various security issues and vulnerabilities that occur within cyber physical systems, and give examples of potential solutions to these issues.

# General Discussion

In this section, we will answer the following questions:

1. What are the security objectives of cyber physical systems?
2. What are the challenges of securing cyber physical systems?
3. What are some of the vulnerabilities of cyber physical systems?
4. What solutions, if any, are available to secure cyber physical systems?

## Cyber Security and Cyber Physical Systems

The security of cyber physical systems is a major concern. As seen in Figure 1 (above), cyber security is a requirement of cyber physical systems. Table 2 lists the areas fall under the umbrella of cyber security in our cyber physical system flow chart, and gives an explanation of how they relate to cyber physical systems.

|  |  |
| --- | --- |
| Area | Description |
| Resilience | The ability of a system to continue operating satisfactorily when stressed by unexpected inputs, subsystem failures, or environmental conditions or inputs that are outside the specified operating range. |
| Privacy | The problem of protecting information about people from unauthorized access by other people or machines. |
| Malicious Attacks | Some particular risks for cyber physical systems include the following: back doors, denial of service attacks, Trojan horses, and viruses |
| Intrusion Detection | Both cyber and physical intrusions need to be considered. Two technologies can contribute to this: embedded vision and timing models. |

Table 2 – Cyber security areas in cyber physical systems (Cyber Physical Systems)

## Security Objectives of Cyber Physical Systems

Before discussing the security concerns of cyber physical systems, we must first establish the security objectives that must be accomplished by these systems. Table 2 (below) enumerates the four main security objectives of cyber physical systems. Each of these objectives can relate back to the items covered by the cyber security section of Figure 1 and Table 2.

|  |  |
| --- | --- |
| Objective | Description |
| Confidentiality | To prevent an adversary from interfering with the state of the physical system by eavesdropping on the communication channels. |
| Integrity | To achieve physical goals by preventing, detecting, or blocking deception attacks on the information sent and received by the system. |
| Availability | To always provide service by preventing computing, controls, communication corruptions due to hardware failures, system upgrades, power outages, or denial-of-service attacks. |
| Authenticity | To realize authentication in all the related processes such as sensing, communications, and actuations. |

Table 3 – Security objectives of cyber physical systems (Wang, Ye and Xu)

## Challenges and Vulnerabilities of Cyber Physical Systems

There are several different challenges appear in cyber physical systems. Some of these challenges stem from the fact that “they involve not only the communication and computation layers, but also the control layer and the physical system itself” (Kim and Kumar).

Many challenges that appear with cyber physical systems come from researchers who wish to expand the use of the systems. Kim and Kumar give the following challenges that researchers must find solutions for in order for cyber physical systems to advance and become more secure (Kim and Kumar):

* Fundamental theoretical frameworks need to be developed
* Complexity and productivity issues that arise in the design and development of these systems need to be addressed
* Software platforms with well-defined and appropriate levels of abstractions and architecture need to be developed
* Control methodologies need to be extended to broader contexts

Many of these challenges lead to vulnerabilities in various aspects of cyber physical systems.

The following issues specific to cyber physical systems cause additional vulnerabilities (Kim and Kumar):

* Controllers are computers prone to bugs and attacks
* Communication networks are open and can be large scale
* Increase in use of commodity solutions make them susceptible to the flaws of the components
* Control protocols are more open and accessible
* New functionality offered by these systems open new vulnerabilities.

These are just a few of the many challenges and vulnerabilities that researchers and professionals must overcome in order for cyber physical systems to improve and reach their full potential.

## Solutions for Cyber Physical Systems

The first step to solving the vulnerability problems with cyber physical systems is to be aware that they exist. It is crucial to perform regular vulnerability assessments and analyze the results to see where problem areas lie and securing those vulnerabilities.

Unfortunately, since cyber physical systems are a relatively new field, there has not been as much advancement in security for these systems as for other fields. This means that there aren’t many solutions out there that are suited to the needs of cyber physical systems. Many of the solutions that currently exist are either inapplicable, not viable, insufficiently scalable, incompatible, or unable to address the complexity of these systems (Mo, Kim and Brancik).

# Conclusion

(Shannon’s part of conclusion)

As cyber physical systems become more and more prevalent, the need for securing these systems will increase. Currently, the scale and complexity of these systems make it hard to ensure that these systems are fully secure.

# Bibliography

Baheti, Radhakisan and Helen Gill. "Cyber-Physical Systems." IEEE Control System Society. 13 April 2016 <http://www.ieeecss.org/sites/ieeecss.org/files/documents/IoCT-Part3-02CyberphysicalSystems.pdf>.

Cyber Physical Systems. 2012. 12 4 2016 <http://cyberphysicalsystems.org>.

Kim, Kyoung-Dae and P. R. Kumar. "Cyber-Physical Systems: A Perspective at the Centennial." Proceedings of the IEEE. 2012. 1287-1308.

Mo, Yilin, et al. "Cyber-Physical Security of Smart Grid Infrastructure." Proceedings of the IEEE. 2012. 195-209.

National Science Foundation. Cyber-Physical Systems (CPS). 13 April 2016 <https://www.nsf.gov/funding/pgm\_summ.jsp?pims\_id=503286>.

NIST. 8 July 2015. 13 April 2016 <http://www.nist.gov/itl/ssd/cyber-physical-systems.cfm>.

Wang, Eric Ke, et al. "Security Issues and Challenges for Cyber Physical System." 2010 IEEE/ACM International Conference on Green Computing and Communications & 2010 IEEE/ACM International Conference on Cyber, Physical, and Social Computing. IEEE Computer Society, 2010.