

1-1-2009

# Exploration Of A Method For Constructing An Industrial Ethernet With Ethernet Enabled Devices In An Industrial Environment Using A Cisco Adaptive Security Appliance

Uros Marjanovic

*Eastern Illinois University*

This research is a product of the graduate program in [Technology](#) at Eastern Illinois University. [Find out more](#) about the program.

---

## Recommended Citation

Marjanovic, Uros, "Exploration Of A Method For Constructing An Industrial Ethernet With Ethernet Enabled Devices In An Industrial Environment Using A Cisco Adaptive Security Appliance" (2009). *Masters Theses*. 700.  
<http://thekeep.eiu.edu/theses/700>

This Thesis is brought to you for free and open access by the Student Theses & Publications at The Keep. It has been accepted for inclusion in Masters Theses by an authorized administrator of The Keep. For more information, please contact [tabruns@eiu.edu](mailto:tabruns@eiu.edu).

### THESIS MAINTENANCE AND REPRODUCTION CERTIFICATE

TO: Graduate Degree Candidates (who have written formal theses)

SUBJECT: Permission to Reproduce Theses

The University Library is receiving a number of request from other institutions asking permission to reproduce dissertations for inclusion in their library holdings. Although no copyright laws are involved, we feel that professional courtesy demands that permission be obtained from the author before we allow these to be copied.

PLEASE SIGN ONE OF THE FOLLOWING STATEMENTS:

Booth Library of Eastern Illinois University has my permission to lend my thesis to a reputable college or university for the purpose of copying it for inclusion in that institution's library or research holdings.

  
\_\_\_\_\_

Author's Signature

5/4/09  
\_\_\_\_\_

Date

I respectfully request Booth Library of Eastern Illinois University **NOT** allow my thesis to be reproduced because:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_

Author's Signature

\_\_\_\_\_

Date

**This form must be submitted in duplicate.**

Exploration of a Method for Constructing an Industrial Ethernet with Ethernet Enabled

Devices in an Industrial Environment using a Cisco Adaptive Security Appliance

(TITLE)

BY

Uros Marjanovic

**THESIS**

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS  
FOR THE DEGREE OF

**Masters in Technology Degree**

IN THE GRADUATE SCHOOL, EASTERN ILLINOIS UNIVERSITY  
CHARLESTON, ILLINOIS

2009

YEAR

I HEREBY RECOMMEND THAT THIS THESIS BE ACCEPTED AS FULFILLING  
THIS PART OF THE GRADUATE DEGREE CITED ABOVE

*Samuel Guccione* 5/7/09

THESIS COMMITTEE CHAIR

DATE

*[Signature]* 5-7-09

DEPARTMENT/SCHOOL CHAIR  
OR CHAIR'S DESIGNEE

DATE

THESIS COMMITTEE MEMBER

DATE

*[Signature]* 5/07/09

THESIS COMMITTEE MEMBER

DATE

THESIS COMMITTEE MEMBER

DATE

*[Signature]* 5/07/09

THESIS COMMITTEE MEMBER

DATE

Exploration of a Method for Constructing an Industrial Ethernet with Ethernet Enabled  
Devices in an Industrial Environment using a Cisco Adaptive Security Appliance

by

Uros Marjanovic

A thesis submitted in partial fulfillment of a Masters in Technology Degree

School of Technology  
Eastern Illinois University  
Spring 2009

## Abstract

Industrial computing has been around for quite some time. It has just recently begun to show its true potential. Over recent years programmable logic controllers, or PLC, have become an integral part of an industrial operation; they have also become more and more powerful, faster and more accurate. One of the most current evolutions has been the integrated addition of Ethernet connectivity to these devices, previous to this a serial connection was used which is extremely slow and not always reliable. The addition of networking these devices has opened the door to many possibilities such as remote device control, increased data management, and real-time information.

Despite the amazing use of these devices, they need to be well protected, not just physically but on the hardware level as well. Anything that is connecting via Ethernet is not one hundred percent safe; there is always a chance that the device maybe hacked into from an unauthorized person. PLC's have been used to control multi-million dollar production lines that may consist of industrial level robots. If one of these devices were to become compromised, there can be huge consequences, such as loss of profits, as well as serious injury to human operators. One method of preventing this occurrence is by having the proper securities in place, this includes proper infrastructure of the network, as well as proper configuration of firewalls. This study will explore ways to achieve the proper security.

## Acknowledgements

I would like to take this opportunity to thank all those that have helped me in my endeavor to further experience and learn about myself here at Eastern Illinois University.

I would like to sincerely thank and express my deepest gratitude to my advisor Dr. Samuel Guccione, whom without I would not have even started the masters program here at Eastern Illinois University. You have always be there to continually encourage me to grow and learn more and more about the world and all it has to offer. Words cannot describe the amount of support, strength and devotion you have given me throughout the years. Your continual passion towards education, students and exploration will always be an inspiration to me.

I would also like to thank Dr. Peter Liu, my graduate coordinator, whom without I would not have able to join the masters program. I would like to thank him for help making sure I was on the right path.

Finally, but most importantly I would like to thank my family for there never ending love, support and encouragement. They have always supported me throughout my life and especially in my endeavor into graduate school and for that I am incredibly grateful.

Thank you!

## Table of Contents

|   |            |
|---|------------|
| <b>ABSTRACT</b> .....   | <b>II</b>  |
| <b>ACKNOWLEDGEMENTS</b> .....   | <b>III</b> |
| <b>TABLE OF CONTENTS</b> .....  | <b>IV</b>  |
| LIST OF TABLES .....  | 1          |
| LIST OF FIGURES .....   | 2          |
| <b>INTRODUCTION</b> .....   | <b>3</b>   |
| 1.1 STATEMENT OF PROBLEM .....  | 5          |
| 1.2 PURPOSE AND OBJECTIVES .....                                      | 6          |
| 1.3 DEFINITIONS OF TERMS .....  | 6          |
| 1.4 LIMITATIONS OF THE STUDY .....                                    | 8          |
| 1.5 DELIMITATIONS .....   | 8          |
| <b>REVIEW OF LITERATURE</b> .....                                     | <b>10</b>  |
| 2.1 PROGRAMMABLE LOGIC CONTROLLER .....                               | 11         |
| 2.2 ETHERNET/INDUSTRIAL PROTOCOL AND COMMON INDUSTRIAL PROTOCOL ..... | 12         |
| 2.3 NETWORKED AND NON-NETWORKED CONNECTIVITY FOR A PLC .....          | 15         |
| 2.4 NETWORK CONTROL SYSTEM (NCS) .....                                | 17         |
| 2.5 NETWORK SECURITY .....  | 18         |
| 2.6 TIERED ACCESS .....   | 19         |
| 2.7 ADAPTIVE SECURITY APPLIANCE .....                                 | 21         |
| 2.8 SERVER-CLIENT MODEL .....   | 22         |
| 2.9 SUMMARY .....   | 26         |
| <b>DESIGN METHODS</b> .....   | <b>27</b>  |
| 3.1 SUBNETS CONFIGURATION .....                                       | 29         |
| 3.2 SERVER ENVIRONMENT .....  | 30         |
| 3.3 CLIENT ENVIRONMENT .....  | 31         |
| 3.4 SOFTWARE STRUCTURE .....  | 32         |
| 3.5 ADAPTIVE SECURITY APPLIANCE COMMUNICATION .....                   | 32         |
| 3.6 MONITORING METHODS .....  | 33         |
| <b>IMPLEMENTATION</b> .....   | <b>35</b>  |
| 4.1 SERVER AND SUBNET ENVIRONMENT .....                               | 35         |
| 4.1.1 Autolab Subnet .....  | 35         |
| 4.1.2 Darkside Subnet .....   | 36         |
| 4.2 CLIENT ENVIRONMENT .....  | 38         |
| 4.3 ADAPTIVE SECURITY APPLIANCE COMMUNICATION .....                   | 41         |
| 4.4 MONITORING METHODS .....  | 46         |
| 4.4.1 Cisco ASA with Port Blocking Configuration .....                | 46         |
| 4.4.2 Cisco ASA VPN Configurations .....                              | 47         |
| 4.4.3 System Logging .....  | 48         |
| <b>ANALYSIS</b> .....   | <b>51</b>  |
| 5.1 NETWORK LAYOUT AND COMMUNICATION OVERVIEW .....                   | 51         |
| 5.2 ADVANTAGES OF THE INDUSTRIAL ETHERNET .....                       | 51         |
| 5.3 DISADVANTAGES OF THE INDUSTRIAL ETHERNET .....                    | 52         |
| 5.4 IMPLEMENTATION EXPERIENCE .....                                   | 53         |
| 5.4.1 PLC Communication .....   | 53         |
| 5.4.2 Simplicity and Location of the Network .....                    | 54         |
| 5.5 GENERAL PROCEDURE .....   | 55         |

**SUMMARY** ..... 56

**RECOMMENDATION FOR FUTURE WORK**..... 57

**REFERENCES:**..... 58

**APPENDIXES** ..... 61

*APPENDIX A* ..... 61

*APPENDIX B* ..... 63



## List of Tables

|           |                                    |    |
|-----------|------------------------------------|----|
| TABLE 4-1 | ACCESS LIST FOR PORT BLOCKING..... | 43 |
| TABLE 4-2 | VPN ACCESS LIST.....               | 44 |

## List of Figures

|   |    |
|---|----|
| FIGURE 2-1 SIGNAL INPUT INTO A PROGRAMMABLE LOGIC CONTROLLER.....                           | 12 |
| FIGURE 2-2 OSI MODEL FOR IDENTIFICATION OF CIP PROTOCOL.....                                | 14 |
| FIGURE 2-3 METHOD OF TRANSPORTING CIP PROTOCOL.....   | 15 |
| FIGURE 2-4 STATISTICS FOR PROTOCOL USAGE IN AN INDUSTRIAL ETHERNET.....                     | 18 |
| FIGURE 2-5 ARCHITECTURE OF AN INDUSTRIAL NETWORK.....                                       | 19 |
| FIGURE 2-6 SAMPLE NETWORK ARCHITECTURE OF AN INDUSTRIAL ETHERNET.....                       | 23 |
| FIGURE 2-7 OVERVIEW ON ARCHITECTURAL COMPONENTS.....  | 25 |
| FIGURE 3-1 LAYOUT FOR THE INDUSTRIAL ETHERNET.....  | 28 |
| FIGURE 3-2 HOW THE NAT SERVER HANDLES REQUESTS.....   | 29 |
| FIGURE 4-1 DHCP INFORMATION OF THE AUTOLAB SUBNET.....                                      | 36 |
| FIGURE 4-2 DHCP/BOOTP INFORMATION FOR THE DARKSIDE SUBNET.....                              | 37 |
| FIGURE 4-3 CONFIGURATION OF THE ETHERNET/IP DRIVER IN RSLINX.....                           | 38 |
| FIGURE 4-4 RSLINX DISCOVERING A PLC ON THE REMOTE DARKSIDE SUBNET.....                      | 39 |
| FIGURE 4-5 RSLOGIX IDENTIFYING WHICH PLC IT WILL BE COMMUNICATING WITH.....                 | 40 |
| FIGURE 4-6 LADDER DIAGRAM OF A PLC ON THE DARKSIDE SUBNET DISPLAYED FROM THE AUTOLAB SUBNET | 41 |
| FIGURE 4-7 VPN ACCESS TO THE DARKSIDE SUBNET.....   | 45 |
| FIGURE 4-8 NMAP SCAN OF THE CISCO ASA.....  | 48 |
| FIGURE 4-9 PART OF A SYSTEM LOG ON THE CISCO ADAPTIVE SECURITY APPLIANCE.....               | 49 |

## Chapter 1

### Introduction

Ever since the start of the industrial revolution, companies have been looking for ways to automate and control machines. At first, all machines had to be controlled and monitored by humans. Since the creation of computers that is no longer the case. Machines need to be constantly monitored, controlled and maintained; this is a perfect job for a computer, or even a microcontroller. These microcontrollers can be found in all sorts of industrial and production type environments. Production lines can consist of anything from a small automated machine that packages a product to a giant robotic arm used to weld car bodies together. These production lines have to have some sort of industrial computer to control them and tell them what to do and how to do it. These industrial computers or microcontrollers are called Programmable Logic Controllers, or PLC's. A PLC is a device that has a series of inputs and outputs. It is programmed through a computer language known as ladder logic. It works, basically this way: if a certain event or "input" is triggered, it then triggers some sort of logic that eventually causes an "output" to be triggered.

PLC's also are used to monitor current values on the production line, these values can include anything from temperature of motors, how many parts have been created and even how efficiently the line is running. This information has to be transmitted back to a control room. In the past, the only method of transmitting information to and from these PLC's has been through a serial connection. However, there are problems with serial a connection. First, it involves a one to one connection with the host to the machine. This means someone has to run to the machine, plug in a wire and plug the other end to the computer or laptop in order to upload a new program. Also, serial is extremely slow.

Ethernet technology allows transmission at over 100 times the speed of serial.

Ethernet has revolutionized the way information is transported. Ethernet can be adapted to an industrial setting and replace serial communications. For example PLC's can be networked and connected via Ethernet. Through the use of Ethernet, the creation of a fully functioning, high speed network can be created. This network can connect to multiple computers and PLC's, and it can all be done remotely.

Ethernet connections use electronic switches which take one connection and split that connection into multiple connections. It is now possible to remotely monitor, control, and upload new files to the PLC. Also, where a serial connection was a one-to-one connection with a computer, with Ethernet one can now transmit multiple programs to multiple PLC's quickly.

Although PLC's are simple computers, and they don't come with the protection that normal desktop computers come with, they need to be protected. An industrial Ethernet can be used, to help control, monitor and maintain PLC's in a safe and secure fashion. Once these types of networks are created and operational, the speed, accuracy and efficiency of production will increase.

Even though Ethernet offers many possibilities, there are several issues of concern. How will the network be protected? How will the network be laid out and constructed?

The first step in answering these questions is to determine how to protect the network. A device called a firewall will be needed to control the flow of information. A firewall is nothing more than a very powerful content filter for networks. A firewall can allow or restrict certain users and network traffic. If configured correctly it should be able to allow only information that is needed and block any sort of vulnerabilities or hacker attacks.

The layout of the network will need to be designed and constructed. To create a small home network is relatively easy, but once a network is expanded to a large scale basis, it becomes extremely complex. Large networks, such as an Industrial Ethernet require various types of hardware such as, switches, routers, servers, and even redundancy protection incase a piece of hardware fails.

Finally, a method of monitoring is needed as part of the protection of the network. There are various powerful software tools that can do constant scans of given ports or given networks. If these scans pick up the smallest error on the network they can be programmed to immediately alert administrators to correct the problem. Also, these scans can be used to correlate data, so as to collect data together to determine if there are security vulnerabilities on the network.

Research is needed to determine the proper construction of Industrial Ethernets and determine they work as designed. Once constructed correctly, Industrial Ethernets will be able to change the way a company operates and help control the way information travels, from the PLC, to the end user that is checking the status of an order online. This form of connection is part of supply chain management.

### *1.1 Statement of Problem*

Creating a full functioning operational computer network has never been an easy task; there are always many variables to take into consideration. This especially holds true for Industrial Ethernets, where additional devices are placed on the network. Some of the problems that may arise include:

1. Properly creating and securely hardening an Industrial Ethernet Network to protect and control Programmable Logic Controllers and other important production machines in an Industrial Environment
2. Securing the network while allowing for full connectivity to other users on the network
3. Actually monitoring and controlling the network once it has been created and configured

### *1.2 Purpose and Objectives*

The purpose of this research is to study and evaluate possible solutions to the three problems identified above. The objective will be to explore the types of network configurations that would support a fully operational Industrial Ethernet. Once an Industrial Ethernet has been constructed it will be evaluated to see how viable of a solution it would be.

### *1.3 Definitions of Terms*

This research includes a large amount of terminology. These terms relate to both the technical aspect of the subject as well as terms relative to the research process itself:

Adaptive Security Appliance (ASA) – A product produced by Cisco that is used to protect networks. This product contains multiple features such as a firewall, routing protocol, VPN, access control, DNS, DHCP, and NAT.

Bootstrap Protocol (BOOTP) – Protocol used to automatically allow devices to acquire an IP address when powered on.

Common Industrial Protocol (CIP) – An application layer protocol that encapsulates instructions within other protocols such as TCP/IP and CAN, and is used to control remote industrial devices. CAN is a method of transportation between microcontrollers that allows communication between devices without a host computer.

Demilitarized Zone (DMZ) – An area of a network that is used for public access, while the rest of the internal network is protected from outside sources.

Dynamic Host Configuration Protocol (DHCP) – A protocol that allows the distribution of IPs to hosts on a network.

Domain Name System (DNS) – A protocol that translates domain names to IP addresses and vice versa.

Ethernet/IP Protocol– The CIP protocol when used over Ethernet.

Firewall – A type of setup that monitors and controls information that is passing through the network via ports and packet information.

Industrial Ethernet (IE) - A network that connects servers, hosts, and Industrial Devices to an Ethernet Network.

Network Address Translation (NAT) – A network protocol that is often used to mask a private network behind a single public IP address. NAT is commonly used with IP masquerading.

Penetration Testing - The act of purposefully attacking a network to test to security vulnerabilities.

Programmable Logic Controller (PLC) – An industrial computer that controls digital and analog input and outputs, can be connected and controlled via serial or Ethernet.

Router – A device that forwards IP address to other networks. Routers are used to connect two or more networks over a distance.

Server – A computer that controls different aspects and protocols of network. There are usually multiple servers that run various protocols in a network.

Switch – A device that allows multiple Ethernet connections on a network and it used for connectivity of multiple devices.

Transmission Control Protocol/Internet Protocol (TCP/IP) – A two part Internet Protocol suite that is used to connect to devices. The IP is an identifier each computer, or host receives to uniquely identify themselves on a network, this allows communication of hosts on a network. The TCP is used for higher level communication between programs

User Datagram Protocol (UDP) – A stateless protocol that is faster and more efficient then TCP/IP but is used for smaller messages.

Virtual Private Network (VPN) – A type of connection that allows a remote computer to be placed on another network through the Internet, usually a large distance away.

#### *1.4 Limitations of the Study*

Limitations of this study will be:

1. All operations will be done in a closed and controlled network setting

#### *1.5 Delimitations*

Delimitations of this study will be:

1. The server will be running Windows 2003 server edition



2. Network security implementation using Cisco Adaptive Security Appliance
3. Programming needed for running the PLC controller will be written using Rockwell RSLogix 500 Software
4. Program needed for communication with PLC will be Rockwell RSLinx Software
5. Running capabilities of the Micrologix 1100 Programmable Logic Controller

## Chapter 2

### Review of Literature

What is an Industrial Ethernet network? What makes it different than a standard Ethernet network? To answer these questions requires, knowing the basics of a network, how it works and what parts are required for correct operation.

A very simple network can consist of a couple of computers connected together via Ethernet cables. These computers can be set up so that they can share information locally. The next step can consist of introducing a server into the network. A server is basically a computer that controls how other computers, called hosts, run and operate. Hosts usually don't store very much information, it is passed on to the server and then the server distributes the information further. When servers and hosts are connected together, it is called a server-client network. This type of network is very popular and extremely useful method for computer networking

In order to distribute information globally the need to start to connect networks together. This can be done by using switches and routers. Switches as previously stated above are used to distribute one connection and make more connections or paths. Routers are primarily used to connect multiple LANs together. Routers are an extremely intelligent piece of equipment, they know where certain destinations, or networks are located. When one computer wants to connect to another computer, the routers job is to make that connection happen. The way it does that is by redirecting information towards its proper destination.

One question to consider is what happens if a non-standard computing device is connected to the network? What if the traditional network is not in an office building but in a warehouse filled with production line machinery? What if this networks main task is not for

browsing the Internet for research or other information but rather used to monitor and control machines? What if this networks main goal is to transmit production line information to a control room that monitors each and ever machine in the building? These are examples of why an Industrial Ethernet network is different then standard Ethernet.

### *2.1 Programmable Logic Controller*

One essential part of an Industrial Ethernet is the actual production machine that is doing some sort of process. Like most machines and processes, this machine needs some set of directions. A programmable logic controller, or PLC, is a computer-like device that contains inputs and outputs. These inputs and outputs can be connected to the machine as well as other external devices and then can control the machine, as well as gather data.

“Information is power. The ability to gather time-critical data, digest it, and react upon it is the only way manufacturing companies have to stay in touch with customers’ needs and demands” (Marchant, 2007). The PLC has the ability to make decisions based on that data that is coming in. It can do this based on the help from external devices such as sensors. For example, if a PLC gets a signal that there is a problem with the quality of the product that is being made, it can then transmit an alarm to the control room and make operators aware there is a problem. It needs to do this in near real-time, in mere milliseconds, almost instant because the data that is being transmitted is time sensitive. Ethernet can potentially cause delays because it is a stateless transfer of information, but there are built-in features in the Ethernet protocol to make sure that that data integrity stays intact through the transfer.

Ethernet is a very powerful and flexible protocol for transferring information, “For example, TCP, IP, UDP, SNMP, Modbus/TCP, HTML, SMTP, and OPC can all operate in parallel” (Marchant, 2007). Before Ethernet, there were slower means of communication,

including token ring and serial. These types of connections were slow, typically require a one to one connection, and only allow one direction of communication at a time while Ethernet can be full-duplex. One of the reasons that these connections were slower was because they were half-duplex, which means that the device could either send or receive data at one time. Full-duplex means that the devices can send and receive data at the same time.

Ethernet also allows remote connectivity from the control room. If a programming change needed to be made from the control room, it can be done through the Ethernet.

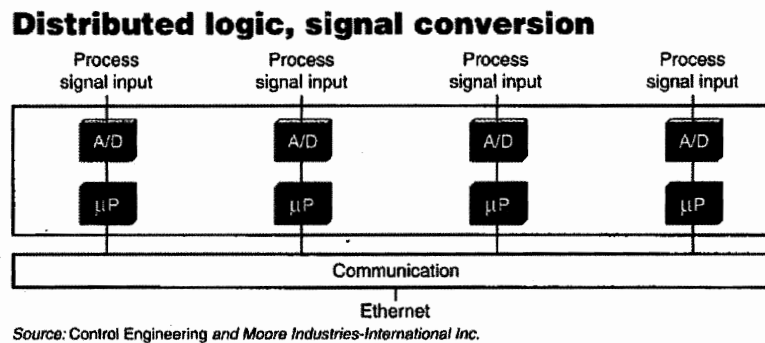


Figure 2-1 (Marchant, 2007)

### Signal input into a Programmable Logic Controller

As shown in Figure 1, a PLC can take multiple signal processes from various internal and external devices, such as sensors, process the signal, and then relay that further through the Ethernet connection. Figure 1 shows that each signal is independent from one another allowing increase speed for time-critical data, and deters single-point of failure (Marchant, 2007).

### 2. 2 Ethernet/Industrial Protocol and Common Industrial Protocol

When PLCs were first developed they used a standard serial connection for device communication. As technological advancements were made, PLCs used Ethernet as a standard communication using the TCP/IP protocols. In order for the proper device

communication to take place, the TCP/IP protocol must be slightly modified to make room for device identification and directions. This protocol is known as Common Industrial Protocol (CIP). CIP is an extended TCP/IP packet that is encapsulated inside the standard TCP/IP packet; see appendix A for more information on TCP/IP. This form of encapsulation is known as Ethernet/IP.

“Ethernet/IP is an application layer protocol that is transferred inside a TCP/IP Packet. That means that Ethernet/IP is simply the way data is organized in a TCP or UDP packet” (Rinaldi, 2007) Ethernet/IP also has specific data values in which it carries. EIP holds information in what is known as attribute form, where similar attributes are grouped together and transmitted, which is called an object. These objects carry values, which then can get feed into a database and information can be recorded. Ethernet/IP is very similar to the standard TCP/IP protocol in the sense that both types of packets can be routed through the network; they can be traced and manipulated.

Common Industrial Protocol, CIP, is also extremely common in an Industrial Ethernet setting. CIP is a protocol that “defines two methods to exchange data over a network- explicit messaging and implicit messaging” (Ixxat Inc, 2008). Explicit messaging uses a point-to-point communication to exchange data, implicit messaging relays real-time I/O data between one producing endpoint to one or multiple other endpoints. The transport layer for explicit messaging is used through TCP/IP, while the transport for implicit messaging is used through UDP/IP” (Ixxat Inc, 2008).

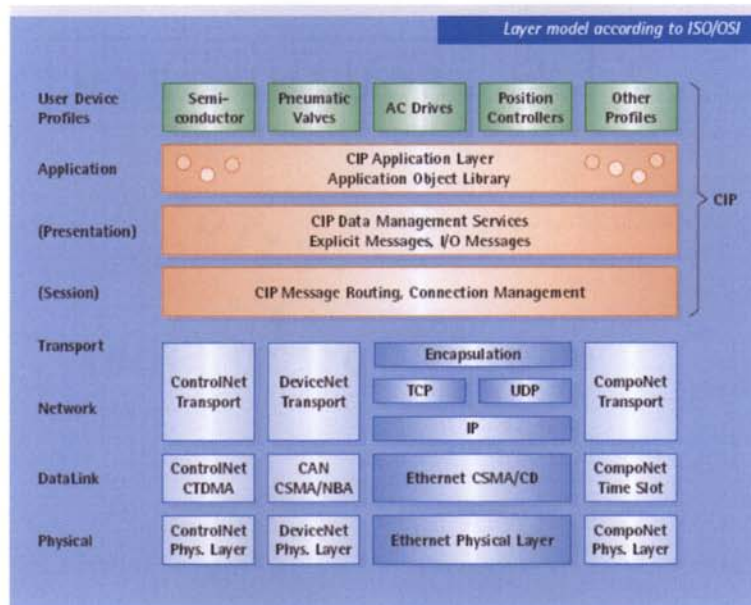


Figure 2-2 (Ixxat Inc, 2008)

### OSI model for identification of CIP protocol

Figure 2 shows how the CIP protocol is “encapsulated”, which means it encapsulates itself and then uses the TCP/IP protocol for distribution. As Figure 2 shows, the CIP information is in the top layers of the Open Systems Interconnection Basic Reference Model (OSI model). The OSI model shows how information is transmitted between computers and networks. For transportation, all of the layers above the transport layer need to be encapsulated; there is a special place transport layer for the encapsulated data. Once the transport packet is formed, it is then sent to the destination address, and the data is then extracted and the directions are processed.

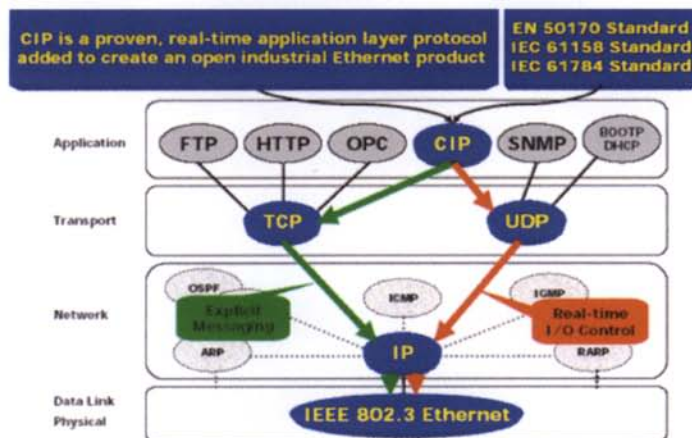


Figure 2-3 (HMS Industrial Networks, 2008)

### Method of transporting CIP protocol

Figure 3 shows how the CIP protocol interfaces and connects through the Ethernet. If an explicit message, such as PLC instructions, is being sent from a host computer to a PLC, the communications program uses the TCP protocol. If there is a real-time monitoring program viewing the PLC, that data is being transmitted via the UDP protocol.

### *2.3 Networked and Non-Networked Connectivity for a PLC*

PLCs accept data using the same I/O instruction whether it is Ethernet or serial communication. Therefore, the information that is being transport has not been changed, merely the method at which it is delivered.

Using an Industrial Ethernet provides an advantage of not only seeing and communicating with a remote PLC, but also viewing all of the other PLCs and/or other devices that are on the network. The continuous improvements of Ethernet, directly affect Industrial Ethernet. For example, a big concern in any network is the collision of data packets, or collision of pieces of data that are being transmitted. These collisions usually end up in the destruction of the pieces of information that were transmitted. Despite the fact that

collisions usually end up with destruction of packets and information, there are built-in recovery systems where the request for that packet gets resent, this ensures that that information gets delivered intact.

Before the mid 1990, Ethernet ran on what is known as a half-duplex network, meaning as one machine is transmitting, the other machine is receiving. If for some reason or another, both machines start transmitting at the same time information will be lost. Also, in the mid 1990's, the development of the communication process called full duplex was complete. Full duplex allows both the sending and receiving of data and information at the same time. "With the advent of full duplex switched Ethernet in the mid 1990's, backbone collisions were virtually eliminated and performance improved" (Ronche, 2008). With the creation of full duplex, a good majority of data was no longer being lost or destroyed, instead if one side of the network did not acknowledge that it received the proper information it contacts the other side and requests that the specific information be sent again.

PLC's work on the same principles as host computer work on a standard network, In order to be seen and acknowledged by the network the PLC needs a unique address, or designation, called an IP address. An IP address is assigned by a server computer, which is running a DHCP service. In order to be considered "on a network" a computer or device must have a valid IP of that network. Typically IPs are distributed using a service called Dynamic Host Configuration Policy (Pcmag.com, 2008), but for a device such as a PLC where it is not as sophisticated as a desktop computer, it uses a service called BOOTP instead of DHCP. When a PLC is plugged in to the network, it immediately asks and acquires an IP address through the BOOTP service (Pcmag.com, 2008). The difference in services makes



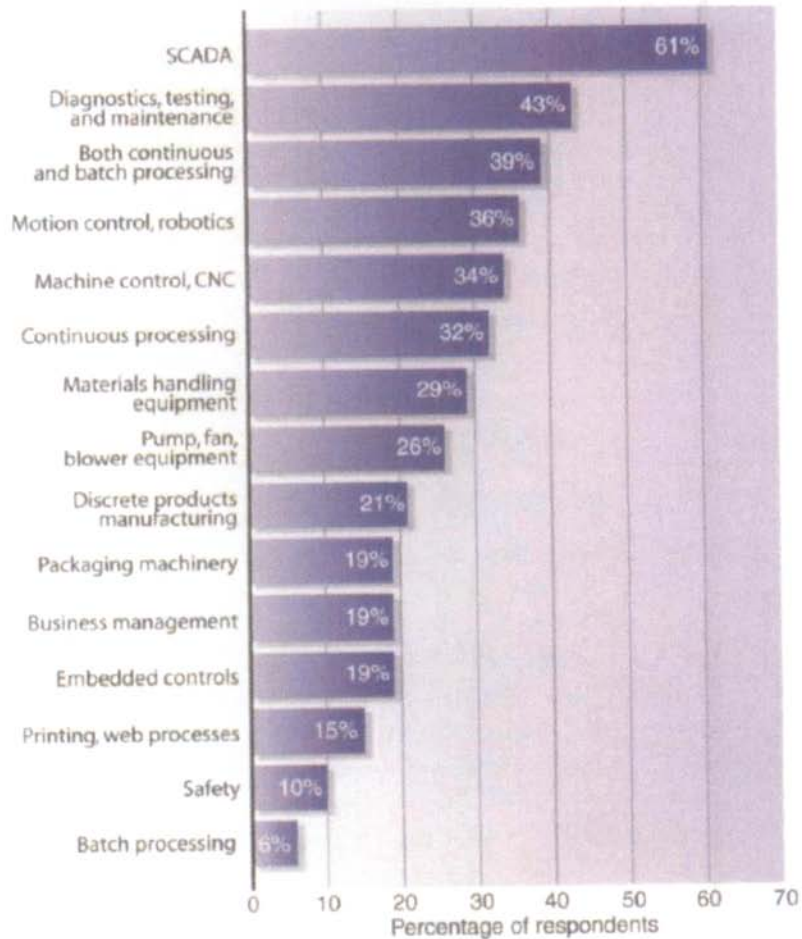
little to no difference for the PLC that is on the network. Now that the PLC is on the network, it can see other devices and computers that are on the network as well.

Being able to connect to a PLC from anywhere using an Ethernet network has caused a demand in cross communication with legacy systems. Using Ethernet and TCP/IP, the data stored in PLC's as well as in other network devices can be made available to others and in real-time.

#### *2.4 Network Control System (NCS)*

A NCS provides a way for an administrator to view, change and operate different aspects of the Industrial network. This type of control system is usually in a centralized location where all aspects and information of the plant comes in. An example of such a NCS is what is referred to as a SCADA network. SCADA, or Supervisory Control and Data Acquisition refers to a system that “collects data from various sensors at a factory, plant or in other remote locations and then sends this data to a central computer which then manages and controls the data” (Tech-FAQ.com, 2008). The use of SCADA is just one of the many applications that are used in plant operations using Industrial Ethernet. Below is a statistical chart of other such applications used in an Industrial Ethernet. As shown, SCADA is the most important applications used (Johnson, May 2008).

### Primary plant-floor applications— industrial Ethernet protocols \*



\* Percentages total more than 100% due to multiple responses  
Source: Control Engineering and Reed Corporate Research

Figure 2-4 (Johnson, May 2008)

#### Statistics for Protocol usage in an Industrial Ethernet

##### 2.5 Network Security

Securing an Industrial Network is a very important process. Depending on the configuration of the network and plant operations, if one Ethernet device gets compromised it could severely affect the rest of the production line. For example, one robot could be sorting parts for an assembly line process, if the PLC controller for that robot were to be either shutoff or have the code change; it would disrupt the entire assembly line. Having layers for

security for Ethernet devices is necessary. The steps to secure an industrial process are: add tiered access and range checking, network recovery if compromises do happen, and adding firewalls and Internet Security devices to prohibit network traffic that is not directly related to the industrial process (Industrial Ethernet Security Issues, October 2008)

Some of the most common network control system vulnerabilities are, inadequate policies, insufficient defense, remote access without proper access control, non-dedicated communication channel for control of the devices, and adequate monitoring of the network (Welander, April 2007). It is important when developing and creating a network, especially for Ethernet devices, that these points are thoroughly investigated and configured properly.

### 2.6 Tiered access

Configuring a network in layers, or tiers is a very simple but an effective preventative measure for Ethernet security.



Figure 2-5 (Wilcox, 2008)

Architecture of an Industrial Network

As Figure 5 shows, the framework starts at the top with enterprise zone network. This level is considered to be the standard computer network with normal internet traffic, such as day-to-day business. The next zone is a Demilitarized zone or DMZ. This zone is a barrier which protects the internal network, Level 3 and below, from the external zone, Level 4 and 5. This DMZ may contain such security devices as an Adaptive Security Appliance, which require authentication if one wants to access the internal network from the external network. This internal network is broken up into more layers. The top layer is the operation and control network. Which is the monitoring of what each industrial device or process is doing. This layer involves devices such as Human Machine Interfaces (HMI) that are linked to the PLC's, which are deeper in the network. The next layer is the work cell area, where the PLC's are connected to the production machines. Between the control layer and the work cell layer, other security devices can be added to further enhance the security of the PLC and the production machines. The work cell area is the most important layer in regards to network connectivity, management and security. According to Rockwell and Cisco (Wilcox, 2008), this security model is called defense in depth and it has very strong advantages, including protecting the interior, guarding the endpoints and even physical security of the devices (Wilcox, 2008).

It is obvious that personal security of employees should be the highest concern for companies. Personal security means that the protection and wellbeing of employees is being preserved so that no injuries occur while in the workplace. This layer requires the most protection from becoming compromised. If a hacker or intruder accesses the work cell area, through the network, and breaks in to the network devices such as a PLC, they could

ultimately reprogram a production machine to physically hurt a human or cause severe damage to the machine, production line, or even the building (Wilcox, 2008).

### *2.7 Adaptive Security Appliance*

Today's constant threats of virus and intruder attacks force network administrators to be constantly look to protecting their network. There are many ways to protect a network; but one of the best ways is to create a firewall or add a security appliance. Specifically the Cisco ASA is one of the newest security appliances currently on the market. The Cisco ASA has many roles that help protect the network. One of its many roles is in the monitoring and control of services and traffic. The Cisco ASA monitors traffic that is passing through and if it is unauthorized, it will block that traffic. One example of this is peer-to-peer file sharing (Cisco Solutions, 2008). The Cisco ASA can even block traffic on the port level, so any traffic passing through a certain port is blocked, such as web traffic on port 80.

Another capability of the Cisco ASA is its "threat-protected" virtual private network (VPN) accessibility. A VPN is a tool that allows "secure site-to-site" and remoter-user access" to other outside networks (Cisco Solutions, 2008). This is an extremely useful tool for network administrators and programmers that need access to a work network while they are away from their office.

Despite the extreme versatility of a Cisco ASA and other security appliances, they are not a cure-all for network protection. They need to be properly configured as well and the proper location in the network. If there were only one security appliance on a network and it failed, the entire network would be open to attack; this is called single point of failure. For this reason, multiple security devices are placed on the network to help alleviate the workload. According to Gold, "vendors can show you marvelous numbers for their firewall

performances, but turning on [intrusion-prevention systems] and other functions can cripple the device, and it won't be able to keep up with enterprise requirements" (Robb, May 2007). It is advised to separate the devices for each function to "meet the security requirements" (Robb, May 2007).

### *2.8 Server-Client Model*

The server-client model is an architectural model of structuring servers and hosts in a network. This model can be further expanded to include such devices as PLCs, HMIs, and any other Ethernet-based device. In a large manufacturing process, the number of devices can become large which could overpower the network. A solution to this is the creation of subnets, i.e. breaking down the network into smaller, more manageable networks. This is a very common practice in all forms of computer networking.

One concern in an industrial setting is that the various numbers of controllers will all report directly to one master control room and potentially overpower the control room, causing delays, latencies and crashes. "Due to the complexity of such industrial systems, a conventional automation system can only undertake simple tasks and is not capable of providing information management and high-level intelligent approaches, as achieving these functionalities requires the support of comprehensive data management and co-ordination between system devices" (Wu, Buse, Sun, & Fitch, 2003).

To remedy this problem it is important to create groups for subsystems and then have those subsystems report to the main control room. This can be done by designing, creating and implementing network architecture. An aspect to consider in this architecture is traffic flow and direction, required bandwidth to maintain real-time data transfer, and remote agents as well as various security aspects. An example of network architecture is shown in Figure 6.



This network architecture shows a general overview and lay out of how a network could be created. It also lists security techniques to help protect the network as much as possible. Various security devices are identified in this diagram to show that different layers of security involved. As shown in the figure, the diagram starts from the outside Internet and goes to the lowest level, the basic control machines, such as PLC's and HMI's.

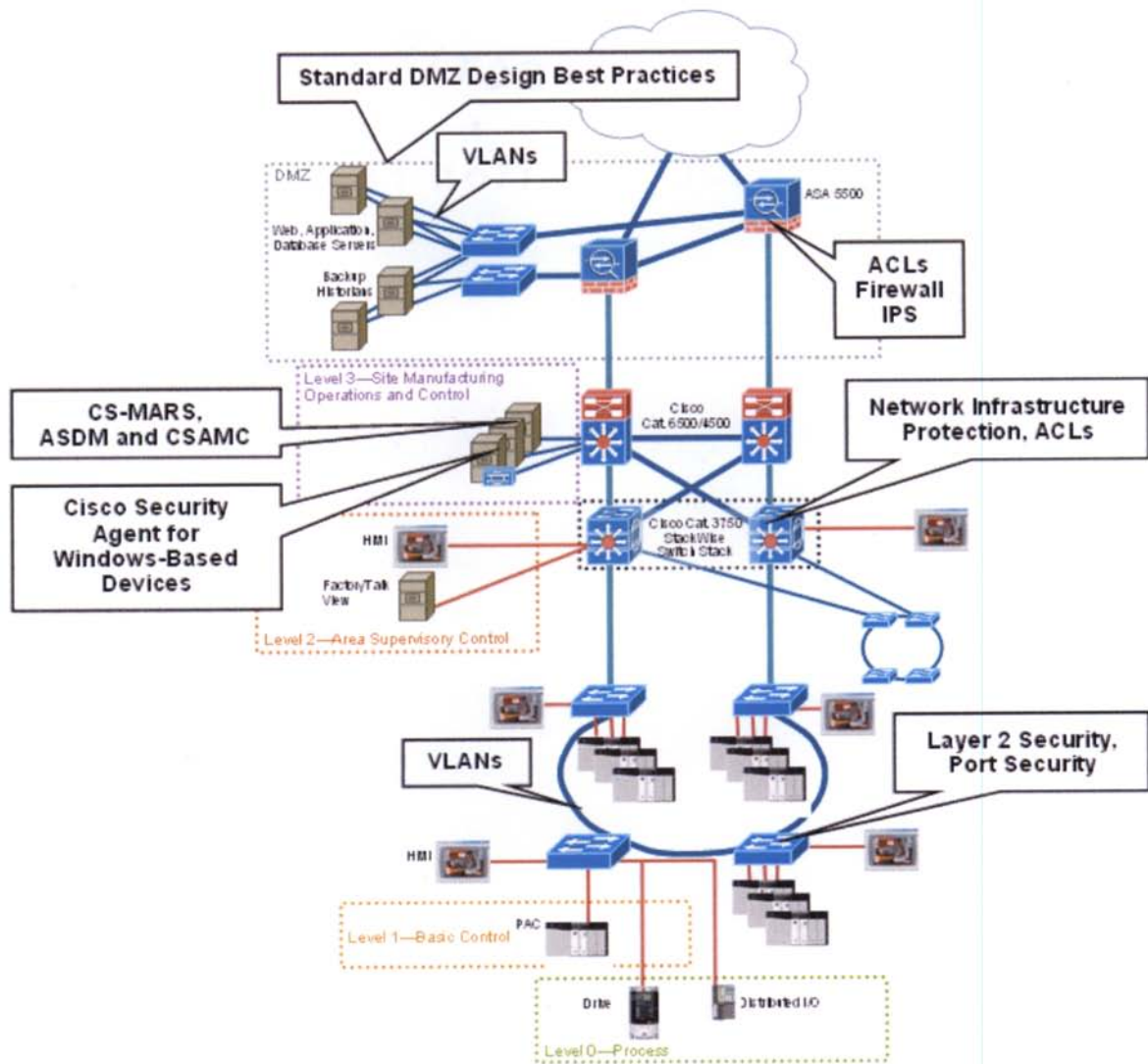


Figure 2-6 (Wilcox, 2008)

Sample Network Architecture of an Industrial Ethernet

The first part of designing a network is to list all of the required technologies, devices and protocols that will be on the network. “Within the Internet protocol suite, there are two alternative transport protocols: the User Datagram Protocol (UDP), and the transmission control protocol (TCP), both of which make use of the Internet Protocol” (Wu, Buse, Sun, & Fitch). These are the same protocols used by PLC’s and other Ethernet enabled industrial devices. In addition, a list of required software is needed. For example, RSView and RSLogix are two software’s required for the control and monitoring of PLC’s. Other proprietary programs maybe needed for additional devices. Once the devices and software’s are identified, the next step is to identify where to place them in the architecture.

The first architecture design step that is required is to determine the topology of the network; creating a good network topology allows for easier placement of hardware. Topologies can have various different configurations and each one can be unique depending on the needs of the network. Once a topology is created, the hardware must be located in the network. The important point to remember about hardware is that it needs to cater to high-speed data transfer. This includes the addition of 10/100MB switches or faster as well as the UDP/TCP/IP protocols to “achieve higher bandwidths and to reduce delay due to collision detections mechanism being used in classic Ethernet” (Wu, Buse, Sun, & Fitch). Other hardware implementations include the addition of HMI, and Industrial Transactional Managers.

The next architecture structure step is the software architecture, which is split into two parts, the LAN and the WAN. The LAN involves the internal network with the PLC and the industrial control as well as the databases and any other computers involved in the



industrial process. The WAN involves the connection to the outside internet as well as the user and host computers. Figure 7 shows the LAN and WAN integrated architectures.

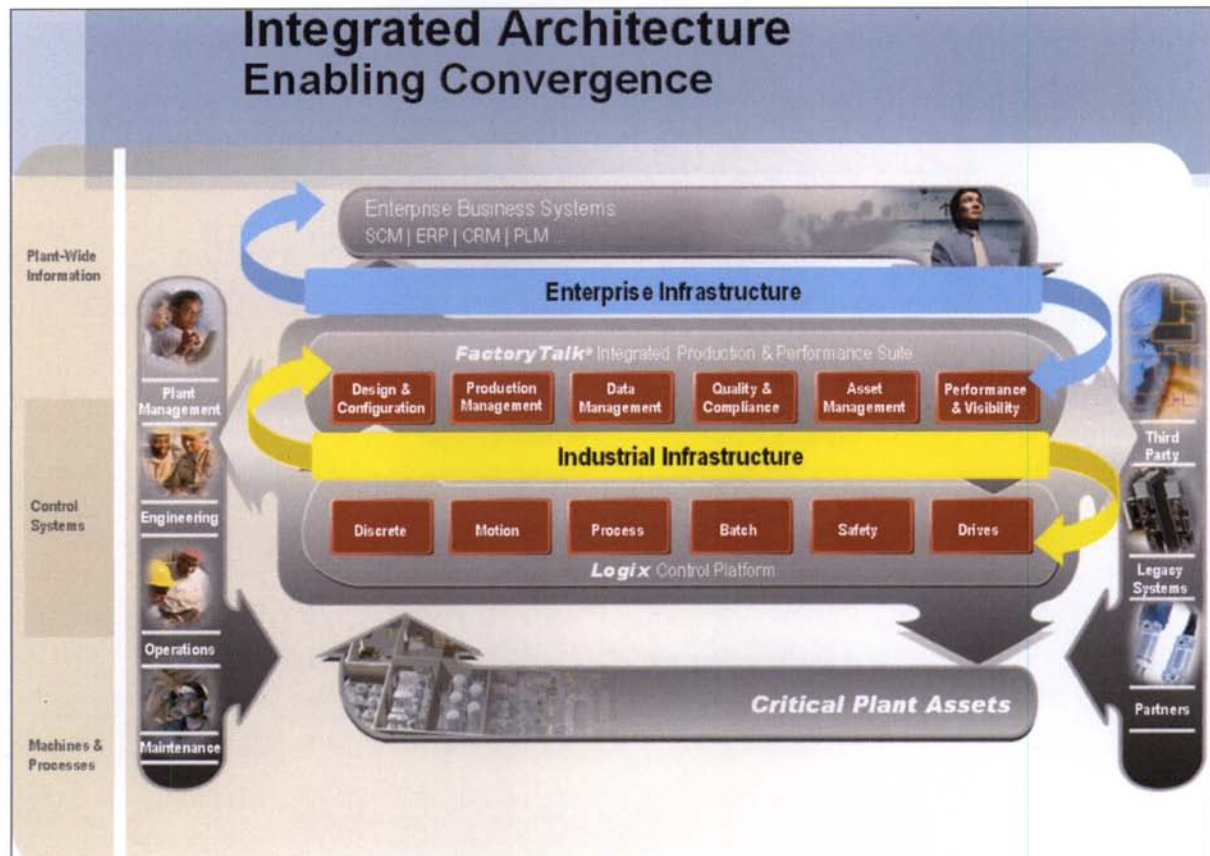


Figure 2-7 (Wilcox, 2008)

#### Overview on Architectural components

The connection between the Enterprise and Industrial infrastructures should be minimal if any at all. The top priority of the Industrial infrastructure is to be as protected as possible; this may include not having any network connectivity between the WAN and the LAN networks.

Finally, everything needs to be connected to one another. The various services and agents need to be identified. These agents include monitoring equipment, such as SCADA hardware, database agents for data logging and transactions to the user level of who will be doing specific tasks on the network.

As long as all the devices that will be placed on the network and the traffic flow on the network are reasonable, a fully operational Industrial Ethernet network would exist. As previously mentioned it is important to make various amounts of subgroups or subnets so that the amount of traffic becomes manageable for the control room.

### *2.9 Summary*

PLCs play a very important role in industry and production. They are an extremely versatile and powerful machine to use. PLCs have the capability to carry large amounts of various processes simultaneously at the same time, report back critical data to an operator or control room. It is even possible to place a PLC on an Ethernet network so that multiple devices can be used in parallel. Networking these devices and other Ethernet-based devices is very powerful for a company because it could potential increase the efficiency of a process line. Placing these devices on a network can cause potential hazards for the safety of the device and the work place. Ethernet is always vulnerable to attack from inside and outside users, it is important to protect all Ethernet based devices including host computers. Using devices such as Cisco's Adaptive Security Appliance is just one method of protecting the network from intruders. Other methods include creating a well organized and proper architecture for the network, such as tiered access. This study will research the integrity of various types of network designs as well as security configurations.

## Chapter 3

### Design Methods

The goal of this study was to explore how a well protected Industrial Network could be constructed, while still maintaining connectivity and full operation. It is well known that no computer network can be one hundred percent secure from outside attack or even vulnerability. The goal here was to explore how to create and secure a network to prevent attack or vulnerabilities.

Once a network has been implemented, it is important to test such a network to make sure connectivity exists. Once the network is operational, it is important to maintain it and keep it protected. The best way to do this is by interrogating the network. Methods of interrogation include running network port and IP scans, and monitoring traffic flow through the network. If an assault on the network is a success and vulnerabilities are revealed, they can be corrected. An Industrial Ethernet was constructed and configured to explore methods to see where security holes or vulnerabilities were located and how they could be corrected. The following hardware was used to construct such a network in the School of Technology Automation Laboratory.

The Industrial Ethernet consisted of the parts listed below connected as shown in Figure 8.

1. Computers configured to be hosts
2. Computer with windows 2003 server software for the AutoLab subnet Industrial Ethernet
3. Computer with windows 2003 server software for the Darkside subnet Industrial Ethernet

4. Cisco Adaptive Security Appliance
5. Two Ethernet ready 10/100 switches
6. Ethernet ready Programmable Logic Controllers

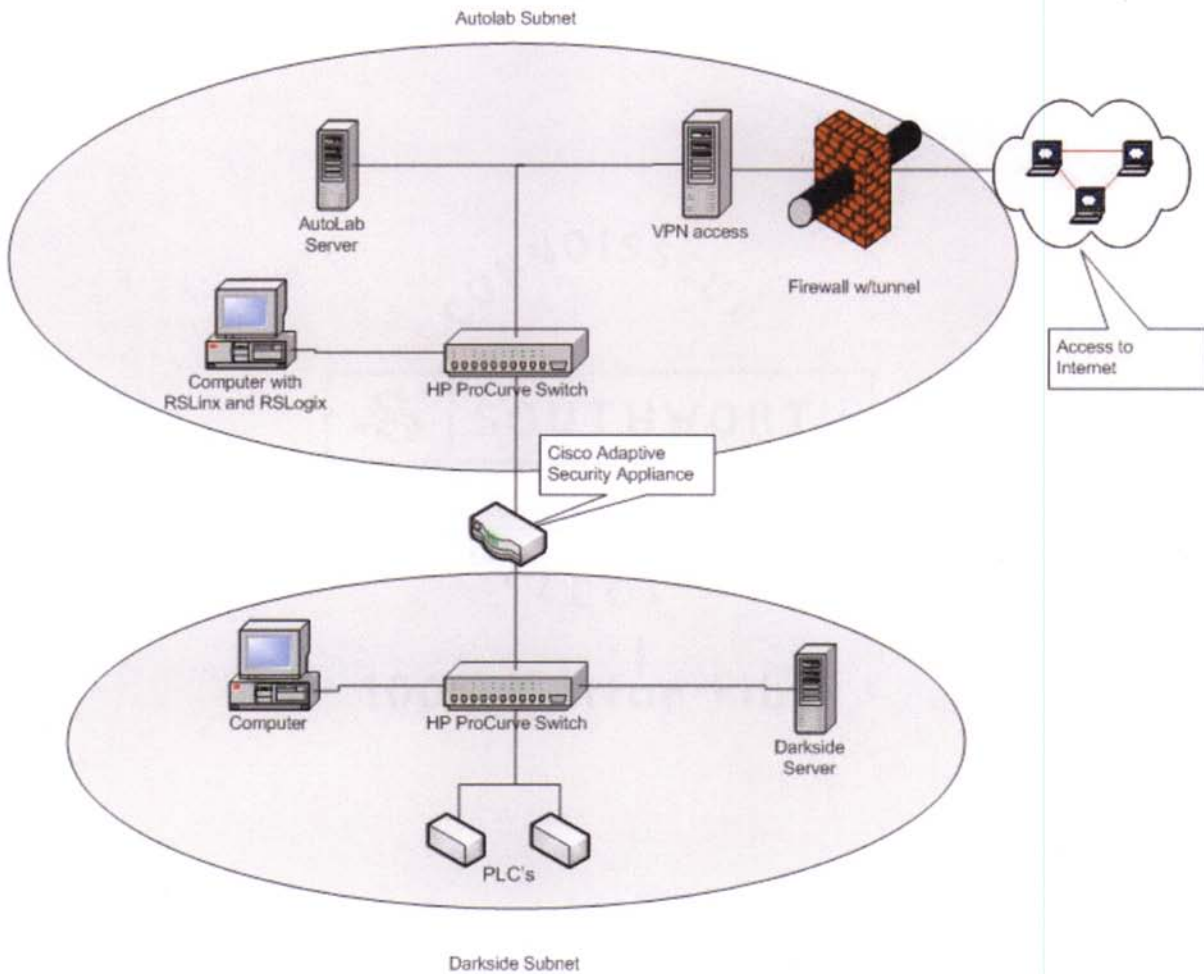


Figure 3-1

### Layout for the Industrial Ethernet

The following industrial software was used to program, control and monitor the PLC's in the internal network.

1. RSLinx Classic Communication software
2. RSLogix 500 Programming and Monitoring software

### 3.1 Subnets Configuration

Using the hardware and software, the Industrial Ethernet was organized into two subnets, Autolab, and Darkside. Autolab was created to be able to serve host computers that would have access to Rockwell software and also the Internet. The Autolab subnet is where the operators of the PLC's are. Since this network would only allow certain people to be on it, i.e. operators, a private non-routable IP was distributed, 10.253.138.xxx. The Autolab network was protected from the outside Internet by having a NAT/Firewall in place that used IP masquerading to forward requests. The only possible way for information to enter the Autolab network was if a request was initiated from within the Autolab subnet or if a user connected to the VPN that was configured on the NAT server, see figure 9.

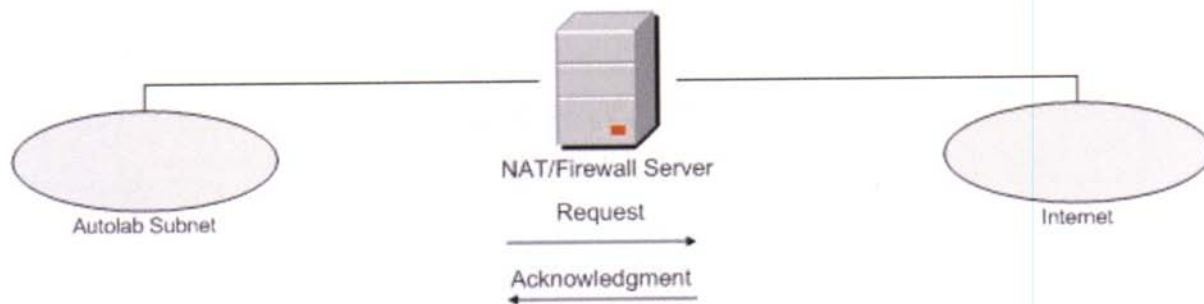


Figure 3-2

How the NAT server handles requests

The Darkside network was created to host the PLCs and any other Industrial Ethernet devices. This network was completely off limits to any user unless they were an operator. To protect this network various different types of protection was used to limit access, some forms included VPN, and port blocking. Darkside was also identified as a private network

and so private non-routable IP were distributed, 10.253.14.xxx. Also, most Industrial devices that are Ethernet ready require that the BOOTP protocol be used in order for the device to obtain an IP from the DHCP server, so this configuration was added only on the Darkside network. Since Darkside needs to be as protected as possible, there were no routes configured to allow Darkside to have access to the Internet, only to the Autolab subnet.

Each subnet had a server which governed that subnet. The main purpose of these servers was to give out IP's, and route distributions to the devices and hosts that were connected to the network.

The two networks were connected together via the Cisco ASA, which had one connection from each network. The Cisco ASA was programmed to allow appropriate traffic between the two networks. If for some reason the traffic had not been approved by the CISCO ASA, it was discarded. If the traffic was passed, it then went to the target destination. The traffic that was allowed between the two networks was user controlled and configured to allow and block traffic according to the users needs.

The type of network routing between the two subnets was configured using static routes instead of using a network address translation (NAT). One of the reasons for this is that NAT uses many-to-one mapping for its protocol, where static uses one-to-one mapping. Using a static route allows information that travels, to be more closely monitored. Since the inner Darkside network is smaller and a more controlled network, it was easier to set up, monitor and maintain the static routes to it.

### *3.2 Server Environment*

The main focus on the server environment was to have some sort of control over the hosts, as one would in an actual production setting. The servers provide dynamic IP



addresses for all the devices that are connecting to the subnet, including PLC's. Using the server, static IP's can be assigned to individual PLC if so needed. This would be done using the reservation feature in DHCP. The server also provided hosts and PLC's with gateway and routing information so they know how to get to other devices via the TCP/IP protocol. Each subnet had a dedicated server which was connected to a switch so that communication existed with the hosts.

### *3.3 Client Environment*

Each host on either subnet had full access to its respected server as well as other hosts on their respected subnet. Each host was connected to their own dedicated switch or switches on their subnet.

Hosts on the Autolab subnet had restricted access to getting on the Darkside network. Only certain authorized users were able to talk to the PLCs on the Darkside subnet. Accessing the Darkside network was only for changing or editing configurations on devices such as PLCs or any other Ethernet enabled device. To gain access to the Darkside network information needed to travel through the Cisco ASA. Various types of configurations of the Cisco ASA were used for gaining access to the Darkside subnet. Host machines on the Autolab subnet contained RSLogix 500 that allowed for communication between the host on the Autolab subnet and PLCs that were located on the Darkside subnet. Upon proper authentication with the ASA, a host on Autolab with RSLogix 500 would access the PLC that was on the Darkside subnet and edit the PLCs configuration file.

Only certain authorized users had access to the configuration of the Cisco ASA. This authorization was only for administrators that were knowledgeable and trained on how to configure a Cisco ASA, properly.

Hosts on the Darkside subnet had access to Autolab network but did not have access to outside Internet sources. PLC's connected to the Darkside network would have full connectivity with other hosts on their respected subnet. The Darkside subnet needed to be as protected as possible because of the importance of the equipment on that subnet.

The main focus on both the subnets is to be as separated and protected as possible but allowing enough connectivity for the industrial processes to not be hindered or halted.

### *3.4 Software Structure*

To establish a connection between a host and the PLC, the user would use a program called RSLinx to create a connection. This program scanned the target subnet, i.e. Darkside, for any type of registered PLC. Once a PLC was found and verified, the user was then able to connect to it. RSLinx would display all available PLC's on the subnet so multiple connections could occur.

Once a connection was established, software called RSLogix 500 was used to extract the configuration file from the PLC to the host. PLC's use a language called ladder diagrams for their instruction set. Once a user is done configuring a PLC's the ladder code is transmitted back on the PLC. Ladder code on the PLC is persistent so even if loss of power occurs, the code is still safe.

### *3.5 Adaptive Security Appliance Communication*

The Cisco ASA will be communicating through both subnets using standard CAT 5 Ethernet cables. One Ethernet port of the Cisco ASA was connected to the Autolab subnet, while another Ethernet port of the Cisco ASA was connected to the Darkside subnet. This allowed the Cisco ASA to filter traffic that was going through it, and thus protecting the Darkside subnet, which contained the PLC's and other Ethernet enabled devices. The filters,



also known as Access Control Lists, or ACLs, were completely customizable so that only certain traffic is allowed. ACLs were added to incoming traffic and outgoing traffic. For this study this ability was used extensively, because of the ability to filter out any content that is not directly related to the communication of the PLC's, but allowing authorized traffic to pass right through.

There are multiple other abilities that the Cisco ASA used. One of which was the built-in Virtual Private Network, VPN. A VPN was set up so that any host computer on the Autolab network could authenticate and login to the Darkside network. Doing so allows the host computer to act as if it were physically connected to the Darkside network, allowing users to access any Ethernet enabled device. VPN provides a very safe connection between host and a private network, if configured properly, it can support up to 256-bit encryption.

There are numerous ways to configure the Cisco ASA. One way is to connect to the Cisco ASA using the Cisco Adaptive Security Device Manager, ASDM software. The ASDM software provides a detailed graphical interface for editing and changing the configuration of the Cisco ASA. The second way is to connect to the ASA through a Secure Shell connection, or SSH. SSH provides a text based interface to login and edit the configuration for the ASA. Using these methods of connecting to the ASA, authorized users could go in and make the appropriate changes to the Cisco ASA.

### *3.6 Monitoring Methods*

Network monitoring is a vast and complicated area in the computer technology field. The basics of monitoring network traffic for this specific example were summed into three categories. Does the host exist with a valid IP, what ports are open on the host, and how accessible is the host?

A powerful tool called Network Mapper, or NMAP, is a free download that can interrogate almost any aspect of a network. NMAP allows the user to change almost any characteristic of the source IP packet to try and confuse or fool the destination host.

Another power monitoring tool was built-in to the Cisco ASA, system logging, or syslog. System logging is nothing more than storing information about any connection or scans attempted on the Cisco ASA. Whether or not a connection was valid, or denied the Cisco ASA would keep track of absolutely everything. All information would be time stamped so that administrators would know when a problem occurred.

## Chapter 4

### Implementation

This chapter describes the process used to create, configure and scan an Industrial Ethernet for vulnerabilities. The Industrial Ethernet consists of four vulnerable parts: a) server and subnet environment, b) client environment and software structure, c) Cisco ASA configuration d) monitoring tools.

#### *4.1 Server and Subnet Environment*

The server is the first part of an Industrial Ethernet. The server computer used Microsoft Windows Server 2003 edition. Both networks had a dedicated server on there respected subnet. A full class 'A' network address was allocated for the network design but only two subnets were used, one for each network. Details on both server configurations are as follows:

##### *4.1.1 Autolab Subnet*

The domain name for the Autolab subnet was named Autolab.EIU. Once installation was complete, the DHCP server was activated for distribution of IP addresses. The Autolab subnet used a network address of 10.253.138.xxx with subnet mask of 255.255.255.0, see figure 10.

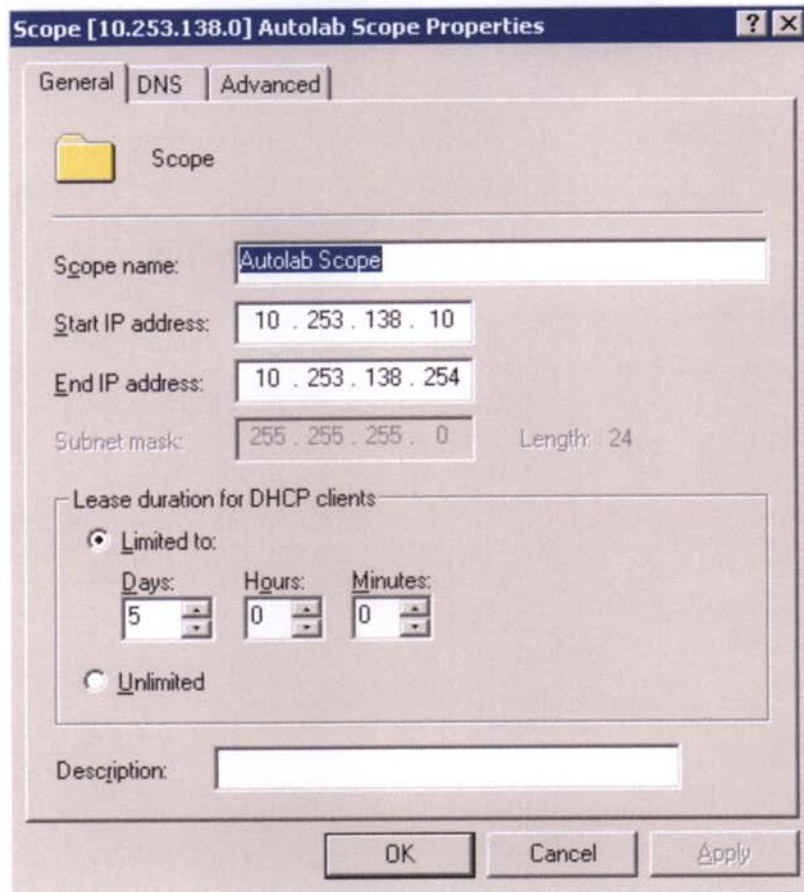


Figure 4-1

#### DHCP information of the Autolab Subnet

The DNS server was configured to use Eastern Illinois University DNS name servers for Internet access. The route for accessing outside the subnet was through the VPN/Firewall that was protecting the Autolab subnet from the outside Internet. This VPN/Firewall was a requirement to protect our lab and Eastern network from any unsolicited network traffic. This VPN/Firewall ran openvpn and had a very specific access list for entry.

#### *4.1.2 Darkside Subnet*

The domain name for the Darkside subnet was Darkside.EIU. The Darkside subnet used a network address of 10.253.14.xxx with subnet mask of 255.255.255.0. Since, this

subnet will be used with Industrial devices, BOOTP was enabled to provide them with IPs, see figure 11.

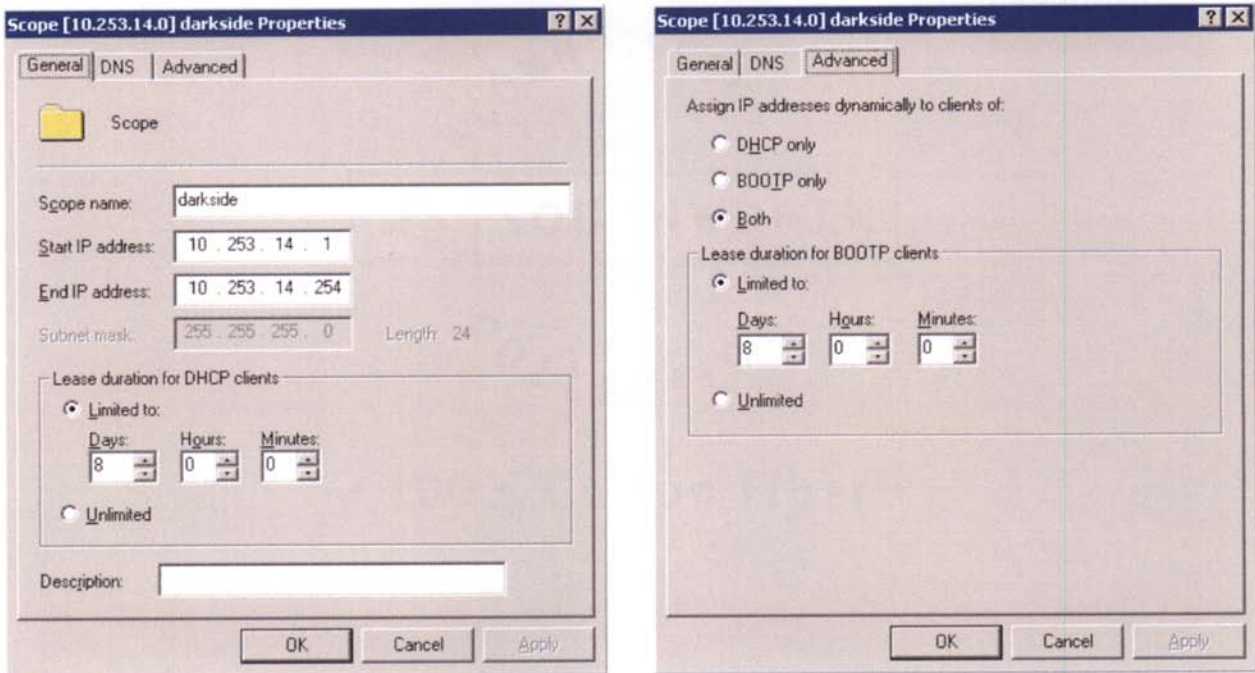


Figure 4-2

#### DHCP/BOOTP information for the Darkside Subnet

The DNS server and routing information was not configured for Internet access. It was better that the Darkside subnet be only accessible from within the Autolab subnet. This in turn allowed another layer of security to be placed on the Darkside network. The route for accessing outside the subnet, to the Autolab network, was to the Cisco ASA that was protecting the Darkside subnet from the Autolab subnet. If a host wanted to get to outside the Cisco ASA a request had to be submitted. Once the request passed specific ACLs on the Cisco ASA, the network traffic would be passed through.

## 4.2 Client Environment

Clients on their respected subnets were joined as members of their respective domain. Each client used fully patched and updated Windows XP. Each client was connected to a Hewlett-Packard Procurve switch that allowed them access to communication to other devices such as the server. One computer from each subnet had a version of RSLogix 500 installed local so that they could communicate with the PLCs.

To create a connection to a PLC, RSLinx needs to browse the subnet and discover available PLCs. In RSLinx a driver must be configure to tell it what type of protocol the PLC is using for its communication, in this case it is Ethernet/IP. As shown in figure 12, configuration of RSLinx required specifying the Darkside subnet.

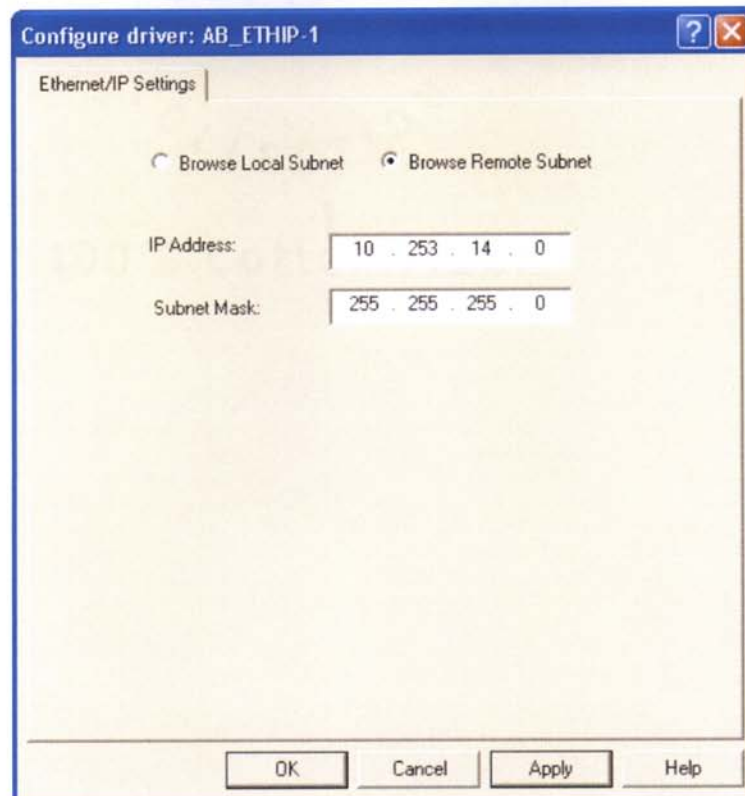


Figure 4-3

Configuration of the Ethernet/IP driver in RSLinx



Once the driver is created, RSLinx goes to look for available PLCs to connect to; figure 13 shows that there is an available PLC with IP of 10.253.14.3.

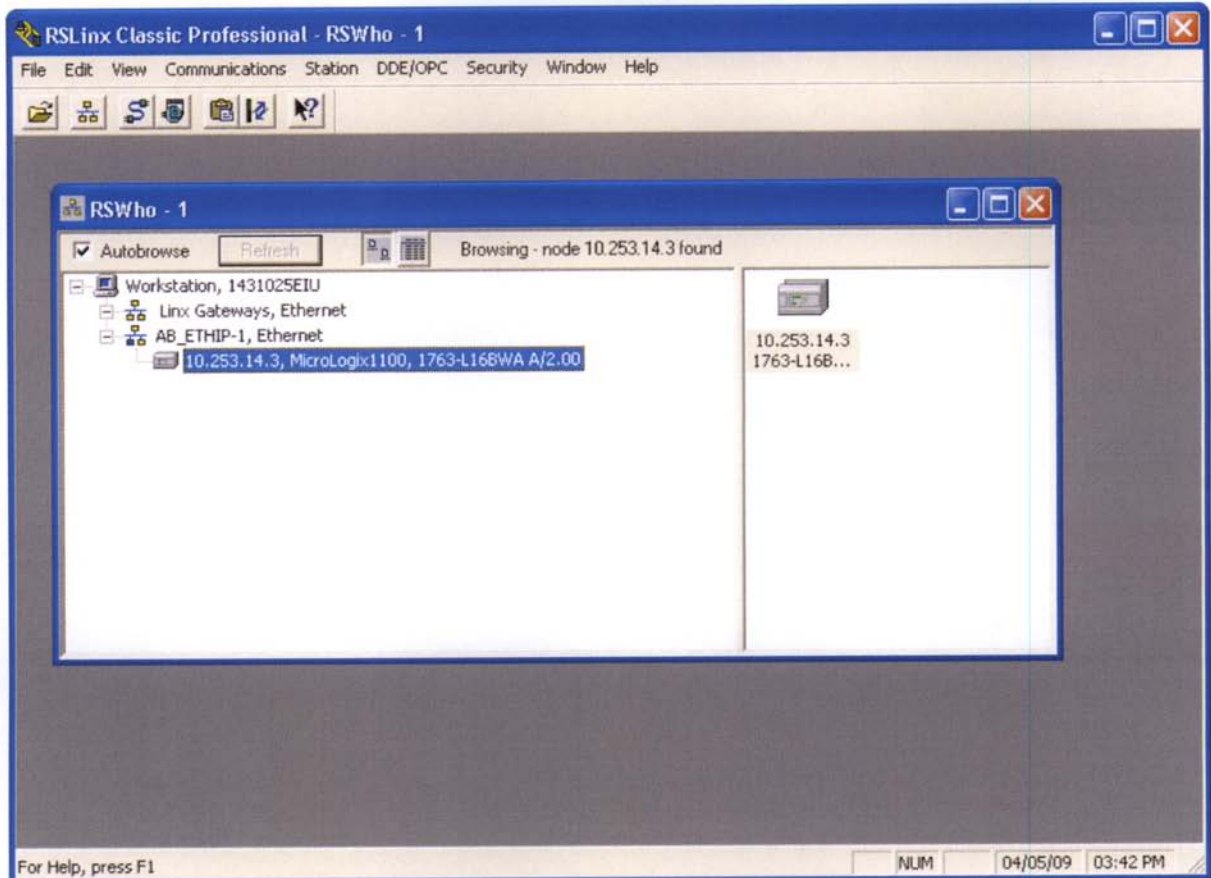


Figure 4-4

RSLinx discovering a PLC on the remote Darkside Subnet

Now that a connection exists and RSLinx is aware of it, RSLogix can be opened and used to access the ladder diagram of the PLC. To do this, RSLogix was opened and the PLC was selected from the communications menu, see figure 14.

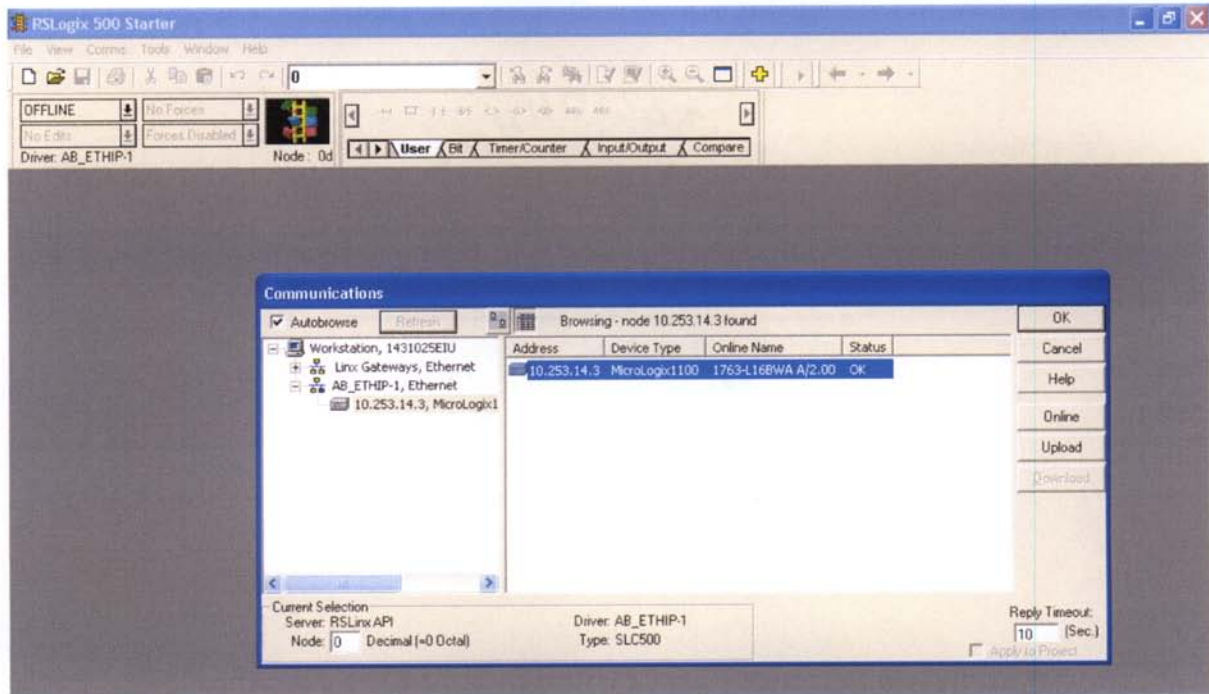


Figure 4-5

RSLogix identifying which PLC it will be communicating with

Once RSLogix knew which PLC it would connect, to and once the connection became active, or “online”, it automatically created a file on the local host that would contain the current system configuration and ladder diagram of the PLC. As shown in figure 14, the host absorbs all system information of the PLC and displays it. A fully operational remote connection exists between the host on the Autolab subnet and a PLC on the Darkside subnet.



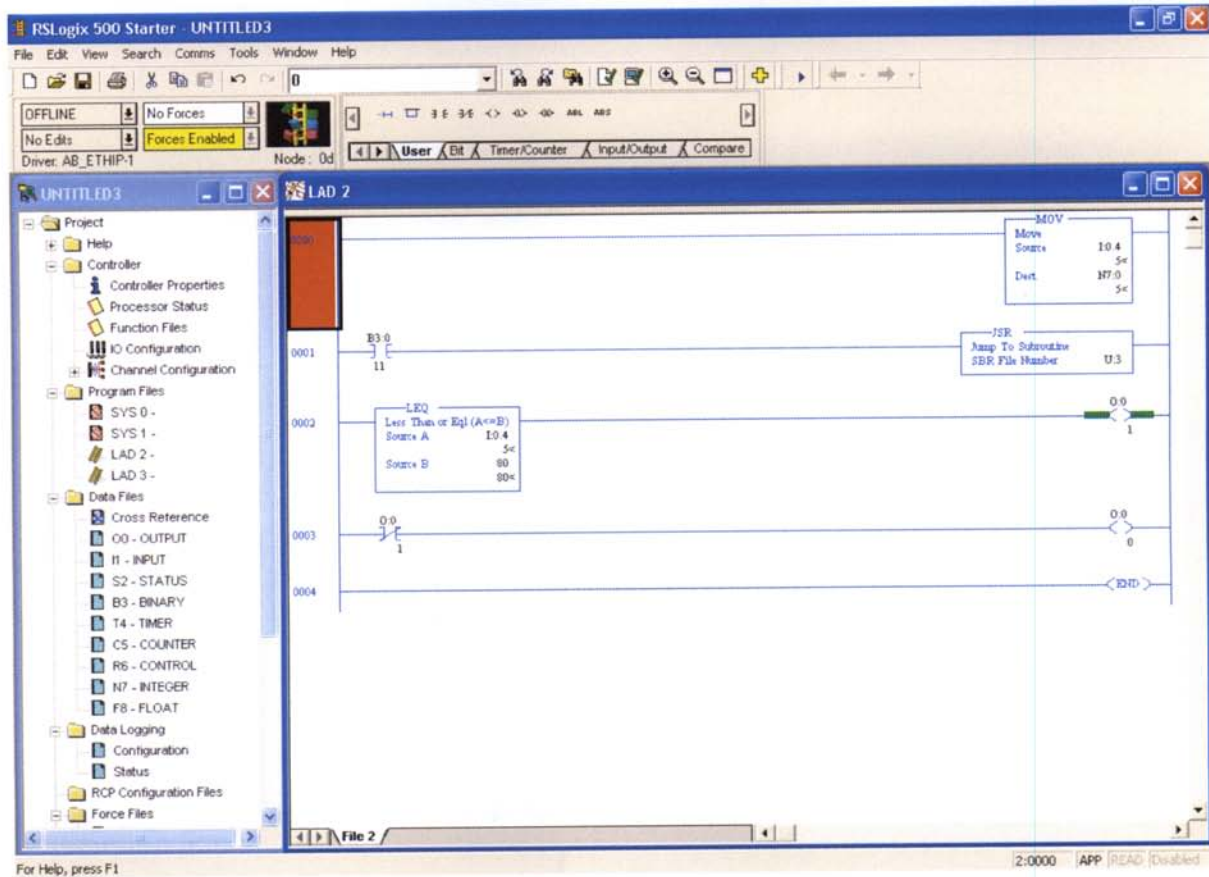


Figure 4-6

Ladder Diagram of a PLC on the Darkside subnet displayed from the Autolab subnet

### 4.3 Adaptive Security Appliance Communication

Is it important to have full connectivity from one subnet to the other, but it is also important to know how the connection was being created; The Cisco ASA is the middle man in all this and with it controls whether a connection is allowed or not.

The Cisco ASA for this study used version 7.2(4) image from Cisco. A few configurations were explored on with the Cisco ASA and the overall security of the network. Different configurations had their own strengths and weaknesses. The goal of using the Cisco ASA is to link both subnets together in the most secure possible way.

The first configuration of the ASA involved blocking all incoming traffic that was not specific to the PLC. PLCs communicate on port 44818 using the TCP protocol. By creating an access list in the ASA, it allows all traffic on port 44818 to pass through. One problem that occurred was that even though the PLC sends data through that port using the TCP protocol, it also requires the IP protocol. In order for full connectivity between RSLinx and the PLC, another access list was needed to allow the IP protocol to pass through. Unfortunately, this protocol is very broad and allows more than just PLC traffic through. To remedy this problem additional access lists were created to block all non-essentials services or protocols. An example of this would be ICMP (ping) requests for echo and echo reply. Table 1 shows a sample access list that was used for this experiment. A more detailed configuration of the ASA could be found in Appendix B.

As shown in table 1, the first access list rule allows all TCP-UDP traffic to pass through on port 44818. The following rule blocks ping request that are made through the ASA. Blocking the ping command is a very well used access control list rule, if somehow the subnet would become compromised it would be very difficult to know where critical systems are with out being able to ping them.

Table 4-1  
Access list for Port Blocking

| #                               | Enabled | Source | Destination | Service             | Action | Logging | Description   |
|---------------------------------|---------|--------|-------------|---------------------|--------|---------|---------------|
| dmz (1 implicit incoming rules) |         |        |             |                     |        |         |               |
| 1                               |         | any    | any         | ip                  | Deny   | Default | Implicit rule |
| inside (4 incoming rules)       |         |        |             |                     |        |         |               |
| 1                               | TRUE    | any    | any         | tcp-<br>udp/44818   | Permit | Default |               |
| 2                               | TRUE    | any    | any         | icmp/echo           | Deny   | Default |               |
|                                 |         |        |             | icmp/echo-<br>reply |        |         |               |
| 3                               | TRUE    | any    | any         | ip                  | Permit | Default |               |
| 4                               |         | any    | any         | ip                  | Deny   | Default | Implicit rule |
| outside (4 incoming rules)      |         |        |             |                     |        |         |               |
| 1                               | TRUE    | any    | any         | tcp-<br>udp/44818   | Permit | Default |               |
| 2                               | TRUE    | any    | any         | icmp/echo           | Deny   | Default |               |
|                                 |         |        |             | icmp/echo-<br>reply |        |         |               |
| 3                               | TRUE    | any    | any         | ip                  | Permit | Default |               |
| 4                               |         | any    | any         | ip                  | Deny   | Default | Implicit rule |

Additional rules can be placed here as desired. The final rule allows IP requests so that connectivity can be made with the PLC via RSLinx. PLC communication requires both TCP and IP protocols for full connectivity.

The second configuration for the Cisco ASA involved blocking all incoming communication from the Autolab subnet to the ASA, while allowing outgoing communication from the Darkside subnet to exist. In order to have connectivity to the PLC's for monitoring and connectivity a virtual private network was used for access control. As

shown below in Table 2 the Cisco ASA was blocking anything from entering the Darkside subnet.

Table 4-2  
VPN Access list

| #                                   | Enabled | Source | Destination                    | Service           | Action | Logging | Description   |
|-------------------------------------|---------|--------|--------------------------------|-------------------|--------|---------|---|
| dmz (1 implicit incoming rules)     |         |        |                                |                   |        |         |   |
| 1                                   |         | any    | any                            | ip                | Deny   | Default | Implicit rule   |
| inside (7 incoming rules)           |         |        |                                |                   |        |         |   |
| 1                                   | TRUE    | any    | any                            | tcp-<br>udp/44818 | Permit | Default |   |
| 2                                   | TRUE    | any    | any                            | ip                | Permit | Default |   |
| 3                                   | TRUE    | any    | any                            | icmp6             | Permit | Default |   |
| 4                                   | TRUE    | any    | any                            | icmp              | Permit | Default |   |
| 5                                   | TRUE    | any    | any                            | tcp               | Permit | Default |   |
| 6                                   | TRUE    | any    | any                            | udp               | Permit | Default |   |
| 7                                   |         | any    | any                            | ip                | Deny   | Default | Implicit rule   |
| outside (2 implicit incoming rules) |         |        |                                |                   |        |         |   |
| 1                                   |         | any    | Any less<br>secure<br>networks | ip                | Permit | Default | Implicit rule:<br>Permit all<br>traffic to less<br>secure<br>networks |
| 2                                   |         | any    | any                            | ip                | Deny   | Default | Implicit rule   |

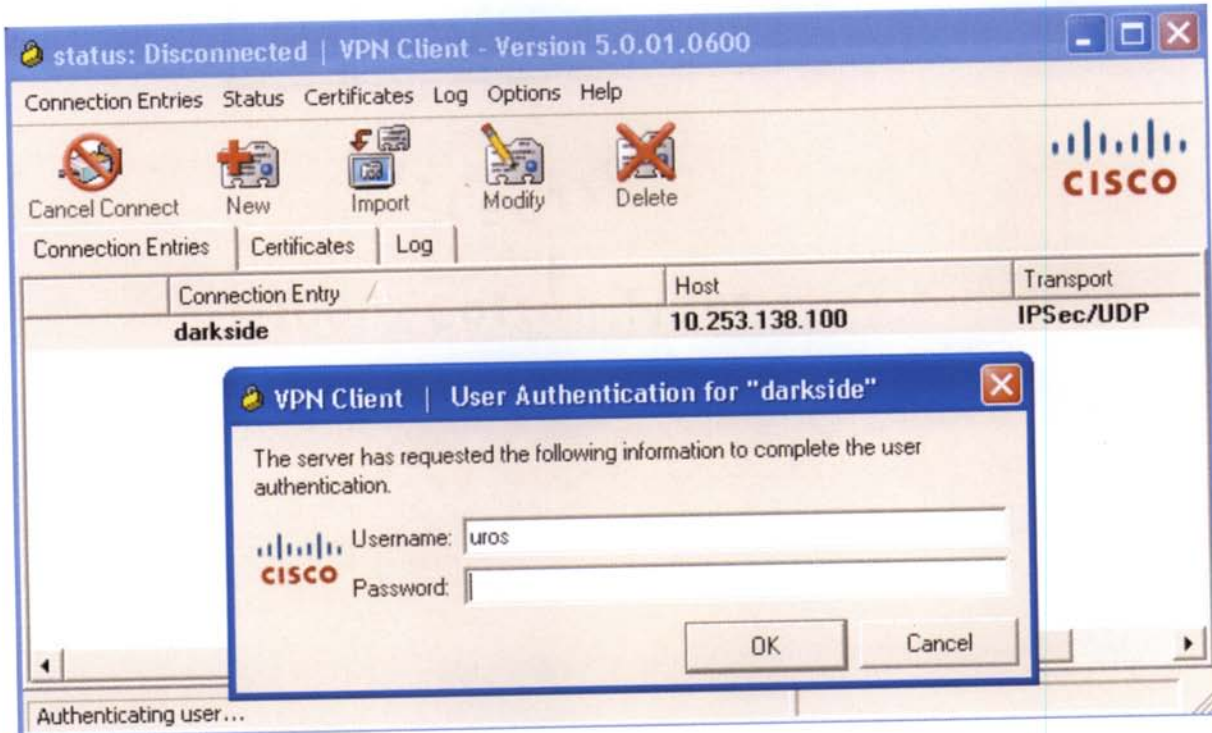


Figure 4-7

## VPN access to the Darkside Subnet

The full configuration of the Cisco ASA for the use of a VPN can be found in Appendix B. With the creation of the VPN, the use of split tunneling was not used. Split tunneling allows a connection to the network currently used as well as a bridge to the network connecting to the VPN client, see figure 16 on how the VPN looks and operates. When connecting to the Darkside subnet using the VPN all network connections to the Autolab network were cut. The host was virtually on the Darkside subnet while physically being on the Autolab network.

#### *4.4 Monitoring Methods*

Network Mapper or NMAP is a free distribution that was downloaded and installed on any host machine. From the Autolab subnet scans were taken with the various Cisco ASA configurations to see how effective they were.

##### *4.4.1 Cisco ASA with Port Blocking Configuration*

With this port blocking configuration, all IP requests were permitted, TCP was permitted but only on port 44818, and all ICMP requests are denied. The first observation was that RSLinx acquires a link with the PLC on the Darkside subnet. This connection allows full functionality with the PLC from the Autolab subnet. This connection shows that ports are open for passing through, but would they be visible on a scan?

Performing a NMAP scan with host discovery of the Darkside subnet yielded some very interesting results. NMAP thought that it was able to see the entire subnet but after a lengthy scan it started returning errors saying that all ports were filtered and no hosts were available. This error would have been caused by the blocking of the ICMP request ACL in the configuration file. It also has to do with the order of the ACL's in the Cisco ASA.

Host discovery on NMAP means that NMAP first verifies that the target host is alive, or active, once NMAP has confirmed that the host is alive, it then checks for open ports. Running a port scan with host discovery disabled allowed NMAP to forcefully scan each host whether it was active or not.

. Upon further investigation of NMAP, altering certain parameters of how NMAP scans hosts and ports, i.e. disabling host discovery, the entire subnet was revealed and open ports were discovered. This was a major security vulnerability that discovered. Just because a

host is not responsive to a standard ping or scan does not mean that it is not alive. Adding more specific ACLs would need to be required to properly fix this vulnerability.

A consideration for the creating of ACL would be to place them in the correct order. An example would be if the ICMP protocol as a whole was allowed first but the following line was disabling only ICMP ping requests. When a packet enters the Cisco ASA, the Cisco ASA runs through the ACL's in order to check if the packet is allowed to pass or not. If a ping request would be sent to through the ASA, its first rule would be that ICMP is allowed, the ping request would then get forwarded through the ASA without even knowing that the next ACL would be blocking it. Therefore, it is common practice to first add denial rule and then add exemptions.

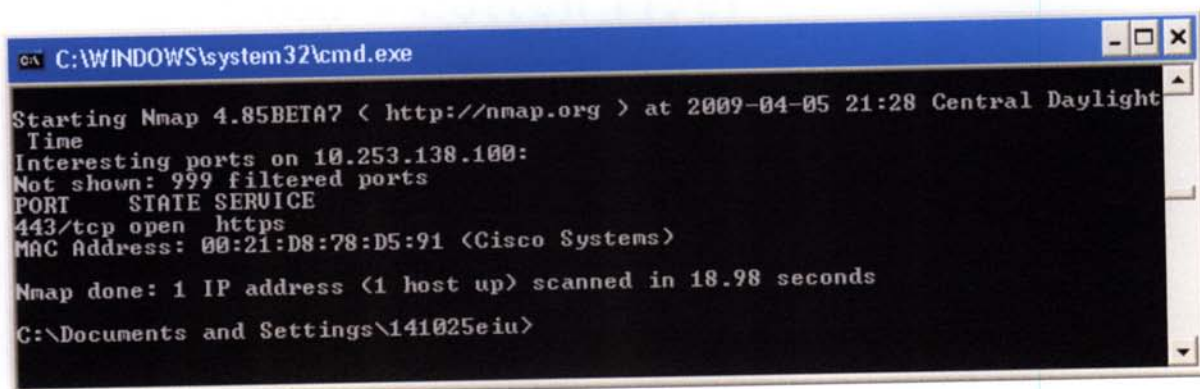
A scan of the Autolab interface also yielded the same results. All ports were considered filtered except for 443, which is a secure port for the web interface. This port allowed access to the ASA configuration via a web GUI. This open port was a vulnerability because it allows a user to access the ASA configuration through the web GUI; this was a major security vulnerability. To fix this vulnerability, disabling the web GUI from any host from the Autolab subnet was performed in the system configurations.

#### *4.4.2 Cisco ASA VPN Configurations*

With this configuration, all incoming requests were automatically declined. The only way to access the Darkside subnet was to have a VPN connection enabled. With this configuration the first thing that was noticed that was there was no possible way to access the PLC on the Darkside network, ping fails and so did a request from RSLinx. It appeared that Darkside was completely locked down. With the VPN connection disabled, a NMAP scan



was performed on the Autolab interface of the Cisco ASA. As shown in figure 17 the only open port of the Cisco ASA is 443, which is a secure port for the web interface.



```

C:\WINDOWS\system32\cmd.exe
Starting Nmap 4.85BETA7 < http://nmap.org > at 2009-04-05 21:28 Central Daylight
Time
Interesting ports on 10.253.138.100:
Not shown: 999 filtered ports
PORT      STATE SERVICE
443/tcp   open  https
MAC Address: 00:21:D8:78:D5:91 <Cisco Systems>

Nmap done: 1 IP address (1 host up) scanned in 18.98 seconds
C:\Documents and Settings\141025eiu>

```

Figure 4-8

#### NMAP scan of the Cisco ASA

This open port was a vulnerability because it allows a user to access the Cisco ASA configuration through the web GUI; this was a major security vulnerability. To fix this vulnerability, disabling the web GUI from any host from the Autolab subnet was performed in the system configurations. With this vulnerability fixed the Cisco ASA doesn't not even register with an NMAP scan with any ports open, only that the IP is in use

Once the VPN connection is established by authenticating the user, the host on the Autolab subnet was now a part of the Darkside subnet, giving access to everything there. One advantage of using this type of connection is that the host machine is completely cut off from communicating with the Autolab subnet. This method continues to protect the Darkside subnet from being exposed to any network other than its own.

#### 4.4.3 System Logging

System Logging is a very basic and easy to use technique to monitor any type of network device. In most cases system logging is a built in function of the device; in the case



of the Cisco ASA it is simply a matter of enabling it. System logging records any type of information that is happening to the device, such as authorizing access to a web interface or allowing certain requests to pass through.

As shown in figure 18, system logging can be very detailed for the Cisco ASA. When monitoring and protecting a subnet, such as Darkside, the more detailed the better to determine where vulnerability is or has already occurred. As figure 18 shows, there is a date and timestamp, as well a source and destination IP followed by what event was taking place.

The screenshot displays the 'Log Buffer' window of a Cisco ASA. The window title is 'Log Buffer' and it contains a menu bar with options like Refresh, Copy, Save, Clear, Color Settings, Create Rule, Show Rule, Show Details, and Help. Below the menu is a 'Filter By:' section with a 'Filter' button and a 'Find:' search box. The main area is a table with columns: Severity, Date, Time, Syslog ID, Source IP, Destination IP, and Description. The table contains multiple log entries, each starting with a severity icon (yellow triangle with an exclamation mark) and a date of 'Apr 05 2009'. The descriptions include various system events such as 'Login permitted from 10.253.138.25 to outside:10.253.138.100/https for user "uros"', 'User authentication succeeded: Uname: uros', 'AAA transaction status ACCEPT : user = uros', 'Device completed SSL handshake with client outside:10.253.138.25/2059', and 'Built inbound TCP connection 428 for outside:10.253.138.25/2059 (10.253.138.25/2059) to NP Identity Ifc:10.253.138.100/443 duration 0:00:00'. At the bottom of the window, there is a section for '%PIX|ASA-6-605005. Login permitted from source-address/source-port to interface/destination/service for user "username"' and a 'Recommended Action' section with a 'Details' button. A legend at the bottom shows severity levels: Emergencies, Alerts, Critical, Errors, Warnings, Notifications, Informational, and Debugging.

| Severity | Date        | Time     | Syslog ID | Source IP     | Destination IP | Description   |
|----------|-------------|----------|-----------|---------------|----------------|---|
| 6        | Apr 05 2009 | 19:29:39 | 605005    | 10.253.138.25 | 10.253.138.100 | Login permitted from 10.253.138.25/2059 to outside:10.253.138.100/https for user "uros"   |
| 6        | Apr 05 2009 | 19:29:39 | 611101    |               |                | User authentication succeeded: Uname: uros  |
| 6        | Apr 05 2009 | 19:29:39 | 113008    |               |                | AAA transaction status ACCEPT : user = uros   |
| 6        | Apr 05 2009 | 19:29:39 | 113012    |               |                | AAA user authentication Successful : local database : user = uros   |
| 6        | Apr 05 2009 | 19:29:39 | 725002    | 10.253.138.25 |                | Device completed SSL handshake with client outside:10.253.138.25/2059   |
| 6        | Apr 05 2009 | 19:29:39 | 725003    | 10.253.138.25 |                | SSL client outside:10.253.138.25/2059 request to resume previous session.   |
| 6        | Apr 05 2009 | 19:29:39 | 725001    | 10.253.138.25 |                | Starting SSL handshake with client outside:10.253.138.25/2059 for TLSv1 session.  |
| 6        | Apr 05 2009 | 19:29:39 | 302013    | 10.253.138.25 | 10.253.138.100 | Built inbound TCP connection 427 for outside:10.253.138.25/2059 (10.253.138.25/2059) to NP Identity Ifc:10.253.138.100/443 duration 0:00:00 |
| 6        | Apr 05 2009 | 19:29:30 | 302014    | 10.253.138.25 | 10.253.138.100 | Tear down TCP connection 427 for outside:10.253.138.25/2058 to NP Identity Ifc:10.253.138.100/443 duration 0:00:00                          |
| 6        | Apr 05 2009 | 19:29:30 | 725007    | 10.253.138.25 |                | SSL session with client outside:10.253.138.25/2058 terminated.  |
| 6        | Apr 05 2009 | 19:29:30 | 605005    | 10.253.138.25 | 10.253.138.100 | Login permitted from 10.253.138.25/2058 to outside:10.253.138.100/https for user "uros"   |
| 6        | Apr 05 2009 | 19:29:30 | 611101    |               |                | User authentication succeeded: Uname: uros  |
| 6        | Apr 05 2009 | 19:29:30 | 113008    |               |                | AAA transaction status ACCEPT : user = uros   |
| 6        | Apr 05 2009 | 19:29:30 | 113012    |               |                | AAA user authentication Successful : local database : user = uros   |
| 6        | Apr 05 2009 | 19:29:30 | 725002    | 10.253.138.25 |                | Device completed SSL handshake with client outside:10.253.138.25/2058   |
| 6        | Apr 05 2009 | 19:29:30 | 725003    | 10.253.138.25 |                | SSL client outside:10.253.138.25/2058 request to resume previous session.   |
| 6        | Apr 05 2009 | 19:29:30 | 725001    | 10.253.138.25 |                | Starting SSL handshake with client outside:10.253.138.25/2058 for TLSv1 session.  |
| 6        | Apr 05 2009 | 19:29:30 | 302013    | 10.253.138.25 | 10.253.138.100 | Built inbound TCP connection 427 for outside:10.253.138.25/2058 (10.253.138.25/2058) to NP Identity Ifc:10.253.138.100/443 duration 0:00:00 |
| 6        | Apr 05 2009 | 19:29:23 | 302014    | 10.253.138.25 | 10.253.138.100 | Tear down TCP connection 426 for outside:10.253.138.25/2057 to NP Identity Ifc:10.253.138.100/443 duration 0:00:00                          |
| 6        | Apr 05 2009 | 19:29:23 | 725007    | 10.253.138.25 |                | SSL session with client outside:10.253.138.25/2057 terminated.  |
| 6        | Apr 05 2009 | 19:29:23 | 725007    | 10.253.138.25 |                | SSL session with client outside:10.253.138.25/2057 terminated.  |
| 6        | Apr 05 2009 | 19:29:23 | 605005    | 10.253.138.25 | 10.253.138.100 | Login permitted from 10.253.138.25/2057 to outside:10.253.138.100/https for user "uros"   |
| 6        | Apr 05 2009 | 19:29:23 | 611101    |               |                | User authentication succeeded: Uname: uros  |
| 6        | Apr 05 2009 | 19:29:23 | 113008    |               |                | AAA transaction status ACCEPT : user = uros   |
| 6        | Apr 05 2009 | 19:29:23 | 113012    |               |                | AAA user authentication Successful : local database : user = uros   |
| 6        | Apr 05 2009 | 19:29:23 | 725002    | 10.253.138.25 |                | Device completed SSL handshake with client outside:10.253.138.25/2057   |
| 6        | Apr 05 2009 | 19:29:23 | 725003    | 10.253.138.25 |                | SSL client outside:10.253.138.25/2057 request to resume previous session.   |
| 6        | Apr 05 2009 | 19:29:23 | 725001    | 10.253.138.25 |                | Starting SSL handshake with client outside:10.253.138.25/2057 for TLSv1 session.  |

Figure 4-9

Part of a system log on the Cisco Adaptive Security Appliance

System logging is a very strong monitoring tool because of its detail, but a weak prevention tool. System logging could be combined with off loading system logs to remote servers so that in case the network device becomes compromised, part of the system log remains intact.

## Chapter 5

### Analysis

This study explored the structure and creation of an Industrial Ethernet using Ethernet enabled devices. Advantages and disadvantages discovered during the design and implementation process are summarized below with an overview.

#### *5.1 Network Layout and Communication Overview*

An Ethernet network was designed and created in this study to simulate a potential Industrial Ethernet. Its functions include:

1. One class B, non-routable address was used for the entire network, which was divided into two subnets. One subnet used for operators and hosts, and one subnet was used for the Ethernet enabled devices.
2. Subnets were connected via a Cisco Adaptive Security Appliance
3. Network connectivity available on demand.
4. Autolab subnet, used by operators, was connected to the Internet, while the Darkside subnet, used by Ethernet devices, was isolated from the Internet.
5. Subnets that could be used for future expansion. Each independent of the other which allows for versatility. Additional subnets were available to be created and connected to the network.

#### *5.2 Advantages of the Industrial Ethernet*

Based on the prototype network constructed above, major advantages of the network included increased layers of protection, size of the network, and flexibility of security configurations.

1. The topology of the prototype network was constructed in a linear bus formation. Linear network topology means that the subnets are chained together, with one leading to the next, i.e. daisy chain. With this setup the Darkside subnet was at the end of the chain, while the Autolab subnet was in the middle and connected to the Internet. Between each subnet was a form of firewall or layer of security. To access the Autolab network, authentication was required for the VPN. Also, access to Darkside from Autolab required a form of authentication. This topology seems to be a good choice for a small network. Adding an extra layer of security between the Autolab and Darkside subnet allowed for greater protection.
2. The size of the network was small and allowed for simple changes and editing of various configurations. A smaller network allows for quicker changes to occur, and allows the effects of such changes to occur faster. Having a larger network with more complex services could cause changes to not occur until the next day.
3. The ability to make massive or minor changes to the Cisco ASA was valuable. It was easy to make changes to the ASA, such as adding additional rules. Once a change was made and saved, that change was applied immediately. This allows for faster fine tuning of the network to see exactly how various configurations would behave.

### *5.3 Disadvantages of the Industrial Ethernet*

Based on the prototype network constructed, major disadvantages included single point of failure, flaws in various security configurations and physical location.

1. Constructing this network in a linear formation could potentially cause problems. The linear formation, although fairly secure would allow for a single point of failure to occur. Failure of the Autolab VPN would take out Internet and connectivity to the

entire network, both the Autolab and the Darkside subnets. Failure between the Autolab and Darkside subnets would only take out the Darkside subnet.

2. With the port blocking configuration of the Cisco ASA, a few problems arose. One problem was that the ports would constantly be left open. This could pose a security problem, if a hacker would discover those open ports. It would give a hacker ample time and access to use those ports to exploit the network.
3. With the VPN configuration of the Cisco ASA, any authorized user could access the network from anywhere. Establishing a VPN connection creates a direct tunnel between the host and the subnet the VPN is connecting to. This tunnel is very open and usually unprotected. If the host would be infected with a virus it could be transmitted to the secure subnet with very little difficulty.

#### *5.4 Implementation Experience*

During the construction of this network, multiple areas of networking and industrial information came together and were united. Some of the major knowledge gained during the design and implementation is summarized below:

##### *5.4.1 PLC Communication*

1. The Programmable Logic Controllers, PLC, are the core of controlling a production environment, with out having some form of communication with them very little can be done. This form of communication link between the host and the device can be on-demand or always connected. This was one of the first and major experiences of this study. A persistent link between an operator station and the PLC was not a necessary requirement. Once the PLC has its instructions the link could be broken without failures.

2. PLC's are very powerful devices, but are not very intelligent at discovering network routes and settings on their own. In order for a PLC to be aware of its surroundings and other subnets, several possible scenarios can occur. One is that a host simply takes control of it and the PLC does not know the difference. The PLC would get all the information it needs from the host. The other way of informing the PLC of its surroundings is through the DHCP/BOOTP service. Using this service, proper gateways or routes can be configured to guide the PLC to go where it needs to go. These routes or gateways can be changed for the entire network or for specific subnets

#### *5.4.2 Simplicity and Location of the Network*

1. This prototype network was not installed in an actual industrial environment. It needs to be installed in an actual industrial environment because only so much could be simulated accurately in a lab environment. The full functionality and issues that may arise in a prototype environment cannot be guaranteed in an actual production environment. One example of this would be the amount of network traffic and load. Instead of having one server and one PLC on the subnet it would be possible to have multiple servers and PLC's on the network all transmitting very important information. This would demonstrate how the network behaves under load and what changes are required for efficiency.
2. The creation of the prototype Industrial Ethernet was very basic and simple. This was primarily because the focus was on proper connectivity and various configurations. Having a more complicated network design would greatly increase the accuracy of simulating such an Industrial Ethernet.

### *5.5 General Procedure*

In general, a proper Industrial Ethernet design proceeds through the following phases:

a) layout b) design, c) implementation, d) security and e) monitoring. It is usually recommended to go through the phases constantly to continually improve the network. A general procedure used for an Industrial Ethernet is described below:

1. A systems layout must be constructed before any type of equipment is to be connected. Once a general idea of how certain machines will operate and be configured, equipment may be brought in. When reevaluating the layout of the network it is important to consider how effective it is and if it is hindering any future expansions.
2. Designing the Industrial Ethernet involves connecting all the pieces together and making sure all the proper configurations are in place. When reevaluating the design, it is important to note if changing the physical location of certain devices would help efficiency. Also, if any type of fine tuning of configurations would be required as well.
3. Implementing an Industrial Ethernet means that all the proper devices have proper communication with the hosts and vice versa.
4. Once an Industrial Ethernet has been designed and implemented security and monitoring should be on the network at all times to make sure that no compromises have occurred.

All tests and procedures should continually be used as methods of improving and fine tuning this design to make it more efficient and effective.

## Chapter 6

### Summary

This study provides detailed information on creating and exploring various aspects of Industrial Ethernet networks for Ethernet enabled devices. One aspect that this study presents is that there are multiple methods of constructing an Industrial Ethernet network. It would be hard to state that there is one specific method of constructing a network. Each type of industrial network has its own purpose and specific requirements that require a great deal of customizing.

This prototype network simulates the main core parts of what a possible production type industrial network. Major functions and issues included:

1. Establishing and creating a preliminary layout of how the network would operate and be physically connected.
2. Network connectivity must be maintained at all times to simulate a production type industrial network, specifically within subnets. Servers must be able to communicate with their respected hosts.
3. Clients must be properly configured with appropriate security measures in place if connecting to a restricted system, such as a Programmable Logic Controller.
4. Proper configuration must be in place for the Adaptive Security Appliance (ASA) for it to be effective in protecting certain networks. Without a properly configured Cisco ASA, the entire network could be placed in jeopardy.
5. Monitoring tools should be used to help watch and protect the entire network from any form of attacks.



## Chapter 7

### Recommendation for Future Work

The study of Industrial Ethernet Networks is a new and emerging area, more research is recommended to further enhance this field of study. Some potential topics include:

1. Creating and using different network topologies for an Industrial Network.
2. Applying various and more detailed access control lists on the Cisco ASA and using high security methods.
3. Using other types of security equipment other than the Cisco ASA.
4. Using addition network tools for monitoring network security.
5. Implementing more real-time monitoring tools to help monitor and protect the network
6. Implementing the network in a real Industrial Setting

## References:

- Cisco Solutions (2008), Cisco ASA 5000 Series Firewall Edition for the Enterprise Solution Overview, Retrieved on November 15, 2008 from:  
[http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod\\_brchure0900aecd8048dba8.html](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_brchure0900aecd8048dba8.html)
- Cisco Systems (2008), Understanding TCP/IP, Retrieved on March 28, 2009 from:  
<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ap1.htm#xtocid10>
- HMS Industrial Networks (2008), Industrial Ethernet Protocol, Retrieved on November 6, 2008, from: <http://www.anybus.com/technologies/ethernetip.shtml>
- Industrial Ethernet security issues. (2008, October). *Control Engineering*, Retrieved November 14, 2008, from Academic Search Premier database.
- Ixxat Inc., Ethernet/IP (2nd ed.) [Brochure]. Bedford, NH, Retrieved on November 6, 2008 from: [http://www.ixxat.com/download/flyer\\_ethernet\\_ip\\_e.pdf](http://www.ixxat.com/download/flyer_ethernet_ip_e.pdf)
- Johnson, D. (2008, May). Protocols for Industrial Ethernet. *Control Engineering*, 55(5), 64. Retrieved November 15, 2008, from Applied Science & Technology Abstracts database.
- Marchant, V. (2007, April). Make the right decisions on Ethernet I/O systems. *Control Engineering*, 54(4), 20-21. Retrieved November 6, 2008, from Academic Search Premier database.
- PCMag.com (2008), Definition of: DHCP, Retrieved on November 12, 2008, from:  
[http://www.pcmag.com/encyclopedia\\_term/0,2542,t%3DDHCP&i%3D41220,00.asp](http://www.pcmag.com/encyclopedia_term/0,2542,t%3DDHCP&i%3D41220,00.asp)

PCMag.com (2008), Definition of: BOOTP, Retrieved on November 12, 2008, from:

[http://www.pcmag.com/encyclopedia\\_term/0%2C2542%2Ct%3DBOOTP&i%3D38854%2C00.asp](http://www.pcmag.com/encyclopedia_term/0%2C2542%2Ct%3DBOOTP&i%3D38854%2C00.asp)

Rinaldi, John (2007), EtherNet/IP Overview: An Application Layer Protocol for Industrial Automation. Retrieved on November 6, 2008, from:

<http://www.rtaautomation.com/ethernetip/>

Robb, D. (2007, May 7). Security Appliances: Are They Good Enough?. *Computerworld*, 41(19), 30-32. Retrieved November 15, 2008, from Academic Search Premier database.

Roche, M. (2008, August). Ethernet communication tips. *Control Engineering*, 55(8), 40-42. Retrieved November 6, 2008, from Academic Search Premier database.

Tech-FAQ (2008), What is SCADA? Retrieved November 12, 2008, from: <http://www.tech-faq.com/scada.shtml>

Welander, P. (2007, April). 10 Control System Security Threats. (Cover story). *Control Engineering*, 54(4), 38-44. Retrieved November 15, 2008, from Academic Search Premier database.

Wilcox, Gregory (April, 2008). Rockwell Automation and Cisco Best Practices for Manufacturing Networking. Retrieved November 6, 2008 and presented online at: <https://www.software.rockwell.com/userexperience/logon/index.cfm?site=Extranet&Bookmark=http://www.software.rockwell.com/extranet/KnowledgeNetwork/index.cfm&CFID=112559&CFTOKEN=15646908>

Wu, Q., Buse, D., Sun, P., & Fitch, J. (2003, April). AN ARCHITECTURE FOR E-AUTOMATION. *Computing & Control Engineering*, 14(2), 38. Retrieved November 15, 2008, from Academic Search Premier database.

## Appendixes

### *Appendix A*

#### Introduction to Basic TCP/IP

Transmission Control Protocol (TCP) / Internet Protocol (IP) are two of many protocols used for daily communications. TCP/IP is most commonly used in computer networks such as Ethernet networks or token ring networks. In order for one host to talk to another host it needs to store that information somewhere along the lines of the communication. To do this, the Network Access Layer was developed and created. This access layer's main purpose is to connect two hosts together, whether they are computer, routers or other devices.

The Network Access Layer uses what are known as frames to transmit information across the physical network. Within a frame is a lot of information, frames contain information such as where the source host is and what address it has, it also contains information on the destination and what address it has. These source and destination addresses are IP addresses, which are unique identifying numbers that each host is assigned. No two hosts on a network can have the IP address. So with the use of frames, hosts can communicate and are very smart in terms of getting from where they are to where they need to be.

One of the advantages of these frames is that they can be encapsulated, which means data can be appended on to a standard frame to provide more information. This is how Ethernet/IP works; it is nothing more than appending extra, machine specific data, which gets transported through the network just like any other frame. Once the frame reaches its

destination, the host will know that a certain part of the frame needs to go to a specific part of the host while the rest is handled normally.

*Appendix B*

## Running Configuration of Cisco ASA

```
: Saved
:
ASA Version 7.2(4)
!
hostname ciscoasa
domain-name darkside.eiu
enable password nbPv.bHpxjhdLUBi encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 10.253.14.1 255.255.255.0
 ospf cost 10
!
interface Vlan2
 nameif outside
 security-level 90
 ip address 10.253.138.100 255.255.255.0
 ospf cost 10
!
interface Vlan3
 no forward interface Vlan2
 nameif dmz
 security-level 50
 no ip address
 ospf cost 10
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
no ftp mode passive
clock timezone CST -6
clock summer-time CDT recurring
dns domain-lookup inside
dns domain-lookup outside
```

```
dns server-group DefaultDNS
  name-server 10.253.138.254
  name-server 10.138.14.254
  domain-name darkside.eiu
object-group service PLC tcp-udp
  port-object eq 44818
object-group protocol TCPUDP
  protocol-object udp
  protocol-object tcp
access-list inside extended permit object-group TCPUDP any any eq 44818
access-list inside extended permit ip any any
access-list inside extended permit icmp6 any any
access-list inside extended permit icmp any any
access-list inside extended permit tcp any any
access-list inside extended permit udp any any
access-list 100 extended permit udp any any
access-list inside_nat0_outbound extended permit ip any 10.253.14.128
255.255.255.192
pager lines 24
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
ip local pool vpnpool 10.253.14.150-10.253.14.160 mask 255.255.255.0
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-524.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
access-group inside in interface inside
route outside 0.0.0.0 0.0.0.0 10.253.138.100 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
aaa authentication ssh console LOCAL
aaa authentication http console LOCAL
http server enable
http 10.253.138.21 255.255.255.255 outside
http 10.253.138.0 255.255.255.0 outside
http 10.253.14.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto dynamic-map outside_dyn_map 20 set pfs
crypto dynamic-map outside_dyn_map 20 set transform-set ESP-3DES-MD5
crypto dynamic-map outside_dyn_map 40 set pfs group1
crypto dynamic-map outside_dyn_map 40 set transform-set ESP-3DES-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
crypto ca trustpoint asatrust
```



```
enrollment terminal
serial-number
ip-address 10.253.138.21
password *
crl configure
crypto isakmp enable outside
crypto isakmp policy 10
  authentication pre-share
  encryption 3des
  hash sha
  group 2
  lifetime 86400
client-update enable
telnet timeout 1
ssh 10.253.138.21 255.255.255.255 outside
ssh timeout 60
console timeout 0
dhcpd auto_config outside
!
dhcpd address 10.253.14.2-10.253.14.33 inside
!

webvpn
username uros password xenof81fe.Fa9yEU encrypted privilege 15
tunnel-group darkside type ipsec-ra
tunnel-group darkside general-attributes
  address-pool vpnpool
tunnel-group darkside ipsec-attributes
  pre-shared-key *
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect esmtp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect sip
    inspect netbios
    inspect tftp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:009163e7c06c29fe7748901b2466e9c9
```

```
: end  
asdm image disk0:/asdm-524.bin  
no asdm history enable
```