Interested in learning more about security?

SANS Institute InfoSec Reading Room

Tactical Data Diodes in Industrial Automation and Control Systems

In recent years, there has been an increased interest in the use of Data Diodes (also known as unidirectional gateways) within Industrial Automation and Control System (IACS) networks. As a result, there has been a substantial amount of confusion around where and how best to use this effective barrier technology. Although not a direct replacement for Firewalls, Data Diodes are well suited for specific tasks within IACS networks such as data replication, system state monitoring, remote backup management and patch manage...

Tactical Data Diodes in Industrial Automation and Control Systems

GIAC (GICSP) Gold Certification

Author: Austin Scott, ascott@cimation.com

Advisor: Richard Carbone

Accepted: May 18, 2015

Abstract

In recent years, there has been an increased interest in the use of Data Diodes (also known as unidirectional gateways) within Industrial Automation and Control System (IACS) networks. As a result, there has been a substantial amount of confusion around where and how best to use this effective barrier technology. Although not a direct replacement for Firewalls, Data Diodes are well suited for specific tasks within IACS networks such as data replication, system state monitoring, remote backup management and patch management. This paper demystifies the use of Data Diodes within the IACS domain by detailing the process and challenges of building a simple Data Diode and applying it an IACS network.

1. Introduction

Communication technology facilitates the exchange of information between devices and networks. A common practice in network architecture is to add barriers between trusted networks and untrusted networks. IACS guidelines would recommend multiple barrier devices between a Power plant control network and untrusted networks like a corporate network or the Internet (NIST, 2011). Firewalls are an omnipresent barrier technology because of their versatility as they operate on software based rule sets (Forrest, 2012). Due to their software foundation, historically, Firewalls have been susceptible to vulnerabilities, misconfigurations and backdoors leaving networks potentially exposed to threats (Kamara, 2001). Data Diodes are a seldom-used barrier technology that are inherently immune to misconfiguration, backdoors and vulnerabilities due to their simplistic nature (Westmacott, 2003). Data Diodes strictly enforce a single rule:

- Data will travel in only one direction between networks.

In the About Data Diodes section, the paper will explore the concept of a Data Diode, their history, benefits, challenges and place in Critical Infrastructure. In the Data Diode Form Factors section, the paper will introduce the typical methods used to build Data Diodes. In the Implementing a Data Diode section, the paper will provide a systematic process for building a Data Diode from readily available parts for a few hundred dollars. Finally, the Data Diodes for Industrial Control section will demonstrate methods for using Data Diodes in control networks and detail some real world scenarios. This paper aims to demystify Data Diodes and highlight the challenges and advantages of this often-misunderstood security barrier technology. The content of this paper will primarily focus on the potential uses for Data Diodes within Industrial Automation and Control Systems (IACSs).

2. About Data Diodes

International standards from IEC, ISA and NIST recommend that Industrial Automation and. Just as fences and gates protect physical perimeters, digital barriers protect the perimeters of network segments. The most commonly used digital barrier technology is a Firewall, which uses a software-based rule set to allow or deny traffic to a network. The software-based ruleset in a Firewall is its greatest strength and weakness (Kamara, 2001). Data Diodes are a form of digital barrier technology that implements a single rule that only allows network traffic to move in one

ascott@cimation.com

direction. This rule is enforced within a Data Diode by physically disconnecting the transmit connection or the receive connection, making it impossible for data to flow over that path.

Sometimes known as a Unidirectional Network or Unidirectional Gateway, Data Diodes ensure the safety of sensitive information within a network. In this paper we refer to "Data Diodes", as this term is more often used to refer to the simple tactical (military) version that implements the "data flows in one direction" rule. Figure 1below illustrates the basic concept of a Data Diode.

The term Unidirectional Gateway is used to describe a more sophisticated device that typically has a computer on both its Low and High side. Creating a physical barrier that only allows data transfers in one direction (hence the "uni" in unidirectional) can enhance security in one of two possible ways:

- Only allowing incoming data

OR

- Only allowing outgoing data

ascott@cimation.com

Figure 1 - Base Concept of a Data Diode.

2.1.Firewalls and Data Diodes

Firewalls are the ubiquitous barrier technology for separating trust levels in a network and are capable of enforcing complex software rulesets. The follow diagram shows an Industrial network that has been segmented from an Enterprise network using Firewalls:

ascott@cimation.com

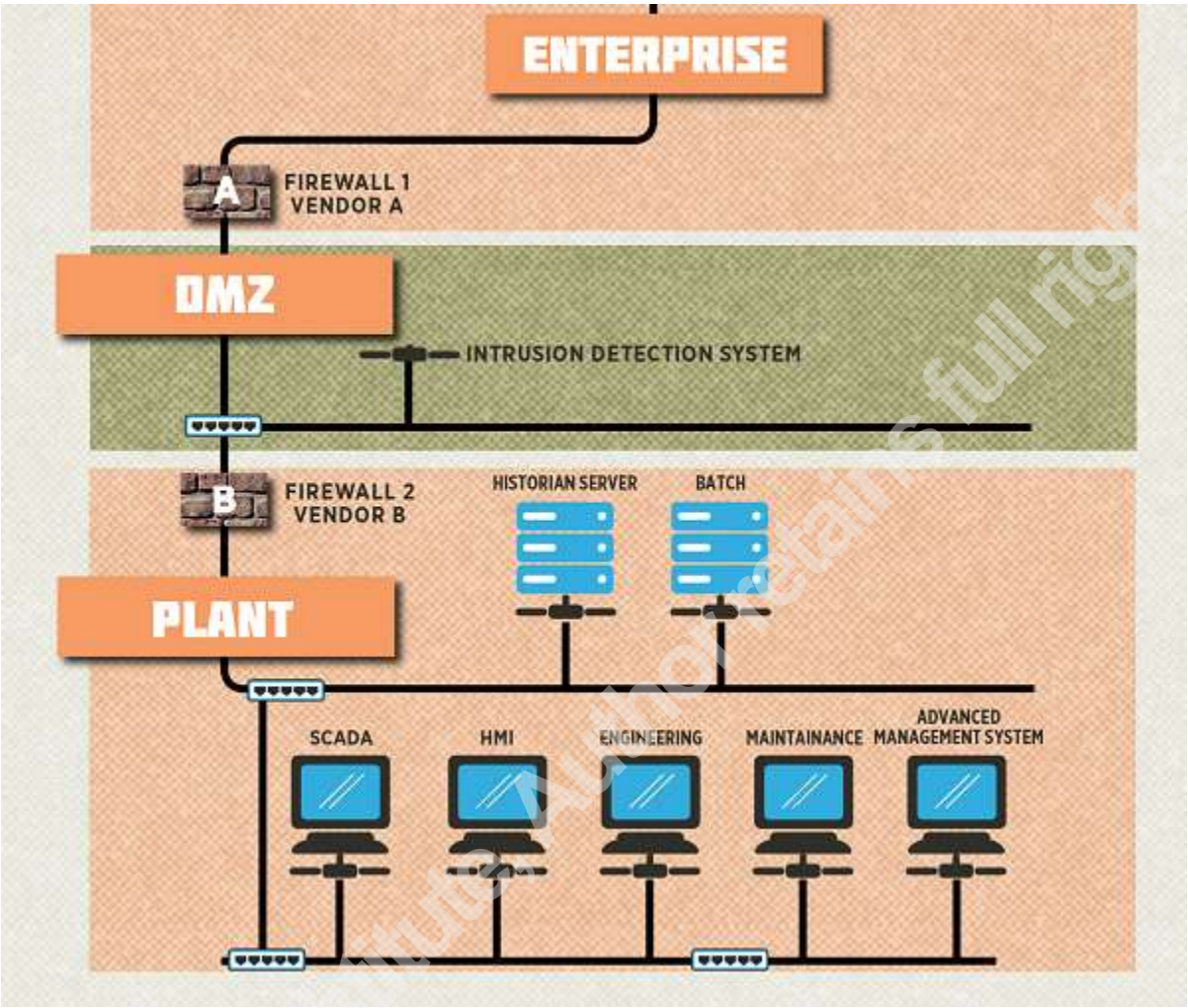

Figure 2 - Industrial Network Segmentation Using Firewalls.

Modern next generation Firewalls can analyze data at all layers of the ISO model in order to adapt to the changing threat landscape. Firewalls need to be maintained by skilled resources who understand the complex ruleset language used to allow or deny packets between networks. There is a common misconception that Firewalls are impenetrable. An improperly configured Firewall can allow undesired traffic (or in some cases all traffic) into a network. Even with the most powerful Firewalls, complex rule sets will introduce delays (latency) in network traffic. For most Information Technology (IT) networks, a little latency will not affect network applications. However, IACS networks such as SCADA and DCS systems are sensitive to latency as they typically are considered “Real-Time”. IACS networks expect to be able to complete an operating cycle (Scan) within a predefined time window (Deterministic). Firewalls are capable of routing all types of network traffic and are compatible with most Industrial Automation and Control

ascott@cimation.com

System (IACS) protocols. Modern Firewalls vary in functionality; the following table details a few Strengths and Weaknesses of a typical Firewall:

Table 1 – Firewall Strengths and Weaknesses.

Firewall Strengths	Firewall Weaknesses
Configurable / Adaptable	Requires highly skill resource
Commonly used and well understood	Historically can be bypassed or flooded
Powerful ruleset language	Introduces network latency (relatively slower data transfers)
Capable of routing all types of network traffic in two directions.	Most attacks are designed with two-way traffic in mind.
Very inexpensive (thousands of dollars - $1,000+), low Capital cost (CAP-EX)	Long-term Operating cost (OP-EX) to maintaining and auditing Firewall rules and firmware over time.
It is relatively easy to find skilled resources who can work on Firewalls.	Very accessible to hackers to develop exploits.
Also is capable of routing network traffic.	Traffic through a Firewall can be routed to computers within a trusted network.

Firewalls are a well-understood and popular barrier technology and a safe bet for use in networks of all types. The use of Data Diodes poses some significant technical challenges and in many cases, the cons far outweigh the pros. For instance, the vast majority of modern communication protocols require two-way communications in order to function. Even most UDP-based protocols require two-way communication in order to operate. Bidirectional communication has numerous benefits including integrity, diagnostic reporting, flow control just to name a few. However, once configured correctly with software that is capable of taking advantage of unidirectional network traffic, Data Diodes provide a low latency, unbreakable network rule. A Data Diode can be an effective defense against data exfiltration (a military term for the covert retrieval of sensitive data) which many Advanced Persistent Threats (APTs) like Energetic Bear, Havex, Flame and the Night Dragon attacks are designed for. There are a few tactical uses for Data Diodes within process control networks that will be explored later.

ascott@cimation.com

The capabilities of modern Data Diodes can vastly vary; the following table lists a few strengths and weaknesses of a traditional Data Diode:

Table 2 – Data Diode Strengths and Weaknesses.

Data Diode Strengths	Data Diode Weaknesses
One-way traffic using a physical disconnect	Traditionally only capable of a single rule.
Secure, most attacks rely on two-way traffic; "Security through obscurity."	Unable to route the majority of network traffic. Breaks most protocols.
No reported cases of Data Diodes being bypassed or exploited to enable two-way traffic.	Not commonly used or well understood
Does not introduce latency (very fast data transfers)	No way of knowing if a packet is received
Lower long-term operating cost (OP-EX) cost as there are no rules to maintain. Although there will be software updates to be installed. Often these devices need to be maintained by the vendors.	Industrial grade Unidirectional Gateways are very expensive (hundreds of thousands of dollars $100,000+), high capital cost (CAP-EX). Not financially viable except for the most critical processes. (Ginter, 2012)
Difficult for hackers to get a hold of an Industrial Grade Unidirectional Gateway, which makes it very challenging to develop exploits. "Security through obscurity."	Requires specialized knowledge and skills to install. In most cases, only the Unidirectional Gateway vendors have the internal skills to configure and maintain their products that add to the expense of the device.
Traffic through the fiber optic channel of most vendor Unidirectional Gateways is a non-routable proprietary protocol that does not implement the TCP/IP stack.	Traffic through most vendor Unidirectional Gateways can only go to a single destination.
The Unidirectional Software layer cannot be configured to allow two-way traffic due the physical disconnection of the RX or TX line.	Most commercial Unidirectional Gateways rely upon Linux servers to support their software layer, which is a potential network vulnerability if the Linux kernels are not kept up to date.

ascott@cimation.com

2.2. Modern Data Diode Landscape

Data Didoes are an extremely simple concept and are believed to have been used by government organizations since the early 80s. In the past few years, we have seen an increased interest in Data Diodes within the general process control domain. Traditionally, we have seen widespread use of Data Diodes in only the most critical applications such as nuclear, military and highly classified network segmentation. Today there are a number of Data Diode vendors globally. In reading the marketing materials put out by the Data Diode vendors one will see they are sprinkled with military terms like “tactical deployment” and “warfighter operations” which is a clear indication of the audience they are targeting. Most Data Diodes on the market today have an impressive array of top level security certificates from countries around the world. The U.S. National Institute of Standards and Technology (NIST) provides a specific security control, SP 800-53 AC-4(7) (NIST, 2013), that describes hardware-enforced one-way information flow control as a threat mitigation method.

2.3. Data Diode Modes of Operation

By physically disconnecting either the transmit (TX) or the receive (RX) Ethernet connections, Data Diodes are capable of two basic modes of operation:

- Receive-only
- Transmit-only

In the following sections, we will explore these two modes of operation from the perspective of the Industrial Automation and Control System (IACS) using a very simple example. Our model separates a corporate network and an IACS network using a Data Diode. However, in practice one is more likely to use a Data Diode to separate a smaller, highly sensitive part of a network.

2.4. Receive-Only – High-Confidentiality Configuration

The following diagram illustrates a Data Diode that is providing a receive-only barrier in the industrial control system (High trust level side) from the corporate network (Low trust level side):

ascott@cimation.com

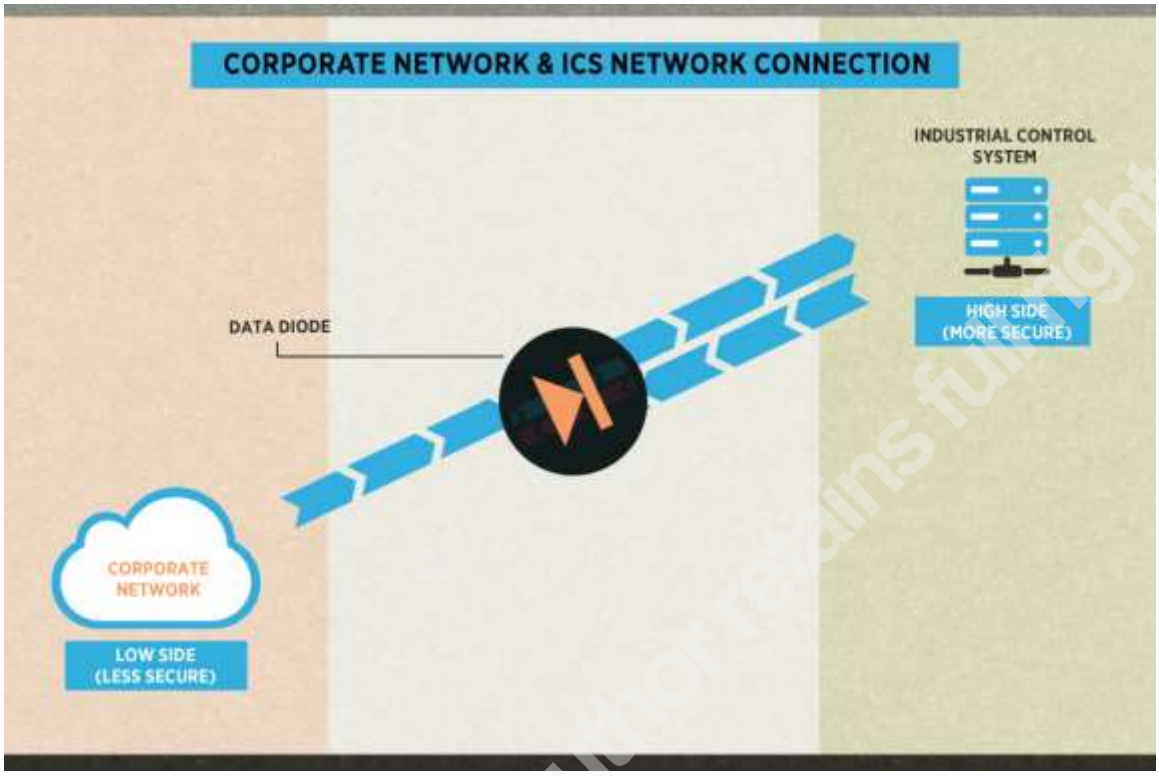

Figure 3 – Receive-Only Data Diode Configuration.

When the IACS network is protected by a barrier countermeasure that enforces transmit-only, attacks and exploits can be sent from the corporate network. However, no reconnaissance information can be transmitted back through the network. Furthermore, the attacker will have no way of knowing if their attack was completed successfully. The receive-only barrier would protect the confidentiality of the IACS and prevent sensitive information (proprietary formulas or processes) from being exfiltrated from the network. The focus of the receive-only Data Diode configuration is on Confidentiality, as confidential data cannot be leaked from the High side (secure) to the Low side (less secure).

2.5. Transmit-Only – High-Availability Configuration

The following diagram illustrates a Data Diode that enforces a transmit-only barrier from the IACS (High trust level side) to the corporate network (Low trust level side):

ascott@cimation.com

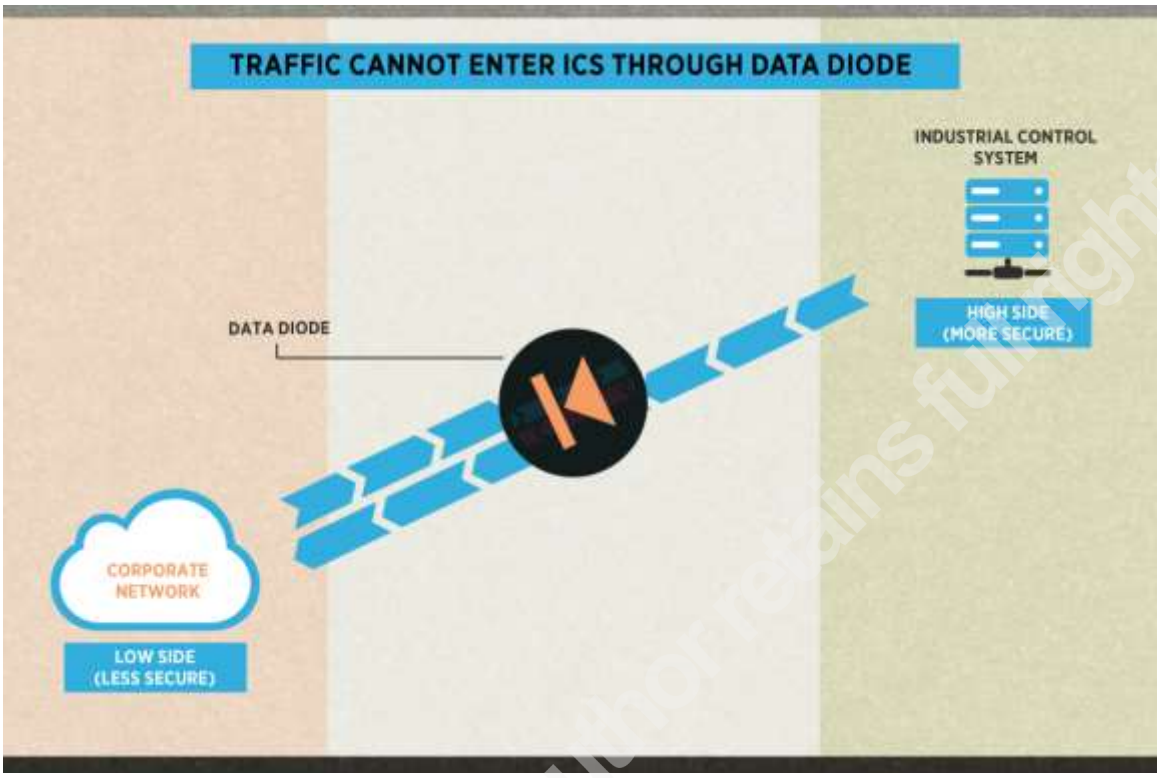

Figure 4 - Transit Only Data Diode.

When the corporate network is unable to send data to the IACS network, it cannot be remotely scanned, attacked or controlled. Enforcing transmit-only is a countermeasure that protects both the availability and the integrity of the IACS network in this example. In transmit-only mode, a denial of service attack is impossible through the Data Diode. The focus of the Transmit-only Data Diode configuration is on Availability, as the Low side (less secure) cannot send data that might interfere with the High side (more secure) side of the network. This configuration is more conducive to the Industrial Network environment as real-time networks are particularly sensitive to outside traffic. The following diagram shows the CIA priorities of an IT network compared to an IACS network:

ascott@cimation.com

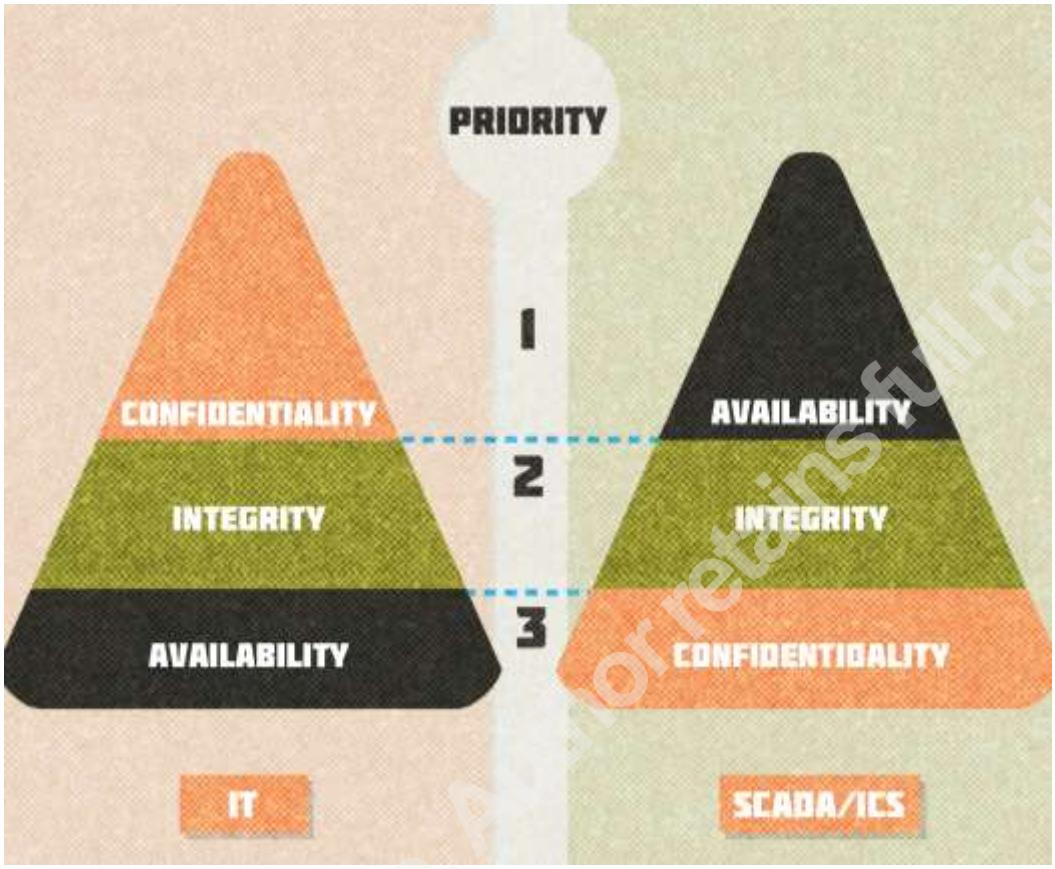

Figure 5 - CIA Triad Priorities in IT versus IACS.

Industrial Networks have traditionally been engineered specifically for high-speed (real-time) data collection and monitoring.

2.6. Data Diode Challenges in ICS

The largest challenge when using a Data Diode is that there are no modern communication protocols that can pass through it. The so-called "three-way" handshake build into TCP/IP will prevent any TCP/IP-based protocol from passing through a Data Diode. UDP based protocols do not have a built in connection check, but even so, most UDP protocols require two-way communication. As we will learn in the Proxy Gateway form factor section, most modern Data Diode vendors have an added software layer at each end of the Data Diode to overcome these challenges. However, most Data Diode products on the market today have not been validated and approved for use by SCADA and DCS vendors that limit their application in the process control domain.

ascott@cimation.com

Another challenge when implementing Data Diodes is error control. It is impossible to know if a packet made it to its intended destination and, therefore, there is no way of resending the data if required.

3. Data Diode Form Factors

Before creating our own simple Data Diode, let take a quick survey of the types of commercially available products on the market today. There are many Data Diode solutions on the market today, each with their own feature set. Data Diode products are hardware based (physical disconnection of a transmit or receive link) or software based (using a software rule set, which will not be touched on in this paper). Hardware based Data Diodes are either Ethernet-based or Fiber Optic based. Furthermore, most hardware Data Diodes on the market today also include a software Proxy Gateway layer that is where the real functionality occurs. These intelligent Data Diodes are more commonly known as Unidirectional Gateways.

3.1. Hardware Based Data Diodes

Two cables are used to create a network connection, one for the transmit signal (TX) and one for the receive signal (RX). The disconnection of one of the transmit/receive pairs leaves the computers with a single connection on which one computer may only transmit, and the other may only receive. The following diagram is an example of a hardware-based Data Diode Network connection:

ascott@cimation.com

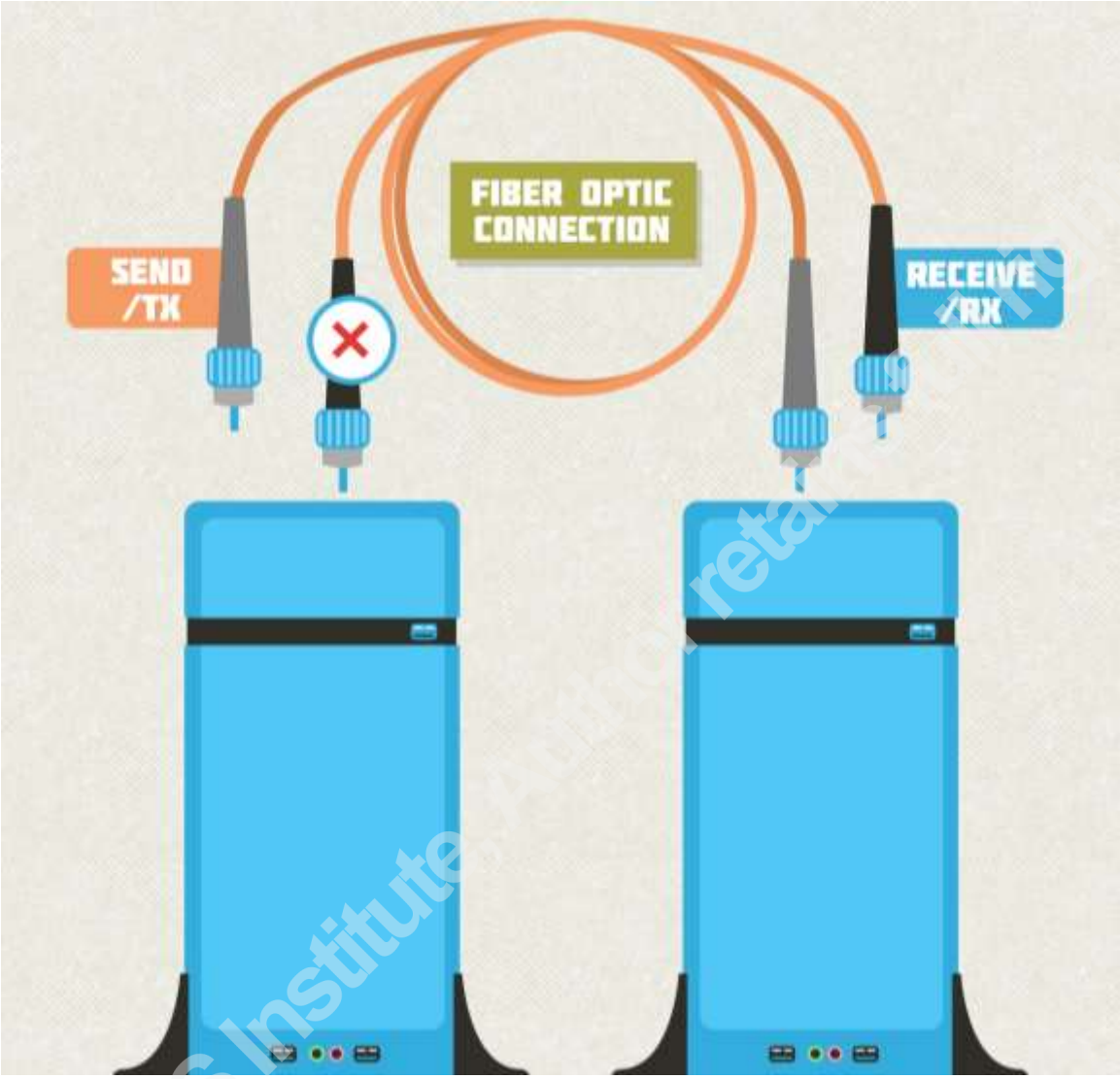

Figure 6 Military style simple Data Diode.

3.2. Unidirectional Gateways

Modern Data Diodes usually include a software layer that helps normal network traffic (both TCP and UDP) to pass through it in one direction. In order to establish a normal TCP connection between two devices, each device must send a SYN and receive an ACK. The TCP connection check is better known as "the three-way handshake" and is required before any TCP communication can take place. Naturally, this is impossible over a traditional Data Diode because two-way communication is not allowed. In order to overcome this issue, modern Data Diode vendors have created a software proxy gateway at both ends of the Data Diode which will

ascott@cimation.com

automatically respond to the SYN requests with ACK and allow the TCP communications to pass the SYN ACK test.

The following diagram illustrates a typical Unidirectional Gateway device configuration:

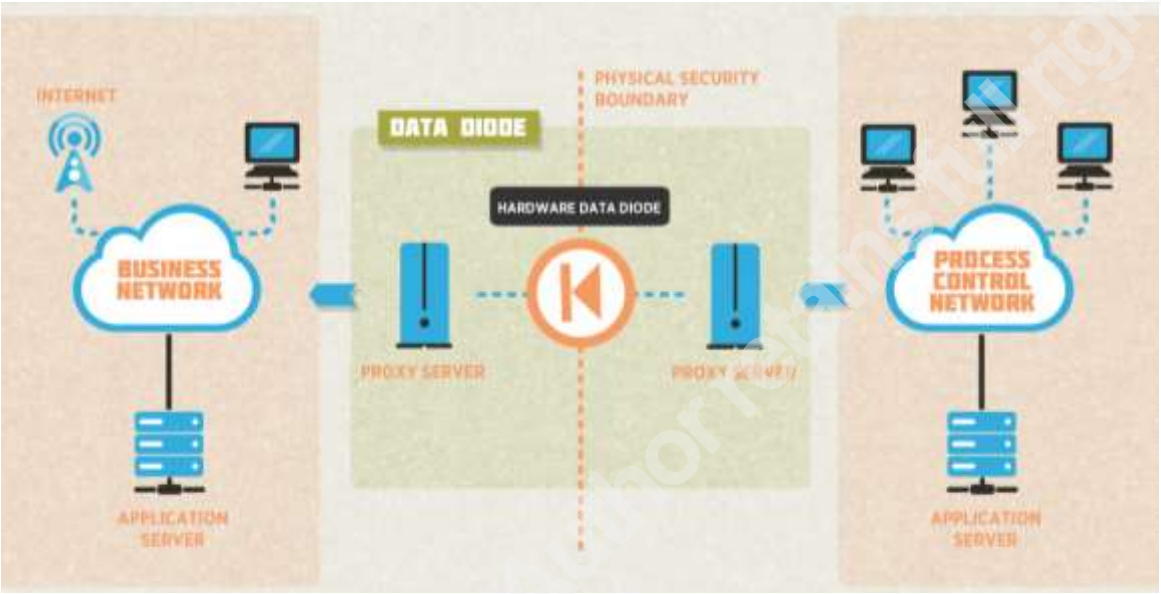

Figure 7 Unidirectional Gateway Network.

Most modern protocols will require additional intelligence from the Proxy Gateway in order to emulate a two-way connection. The biggest challenge in the ICS space is the lack of DCS and SCADA vendor approval of Data Diodes. That said, we are starting to see a handful of vendors approving the use of Data Diodes with their products. Most IACS operators would not risk the high cost of a modern Data Diode without first knowing that their DCS or SCADA platform can operate reliably over it. After all, in an Industrial Network availability takes precedence over confidentiality and integrity.

4. Building a Functional Data Diode

In order to fully understand the challenges of using a Data Diode in an IACS environment, we will build a functional Data Diode using off the shelf components. In this paper we will build a historically military type, Confidentiality focused (unidirectional transfer from Low side/ less secure to the High side / more secure) Data Diode. The direction is easily reversed to an Availability focused Data Diode (unidirectional transfer from High side to Low side) by

following the same process. The following section will detail the challenges one would encounter and the solutions one could use to implement a Data Diode.

4.1.Safety Warning – Loss of Control / Loss of View

The designer of any control scheme must consider the potential failure modes of control paths and, for certain critical control functions, provide a means to achieve a safe state during and after a path failure. Examples of critical control functions are emergency stop and over-travel stop that may include the following capabilities:

- Separate or redundant control paths must be provided for critical control functions.
- System control paths may include communication links. Consideration must be given to the implications of unanticipated transmission delays or failures of the link.
- Each implementation of a control system must be individually and thoroughly tested for proper operation before being placed into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

This white paper is not comprehensive for any systems using the given architecture and does not absolve users of their duty to uphold the safety requirements for the equipment used in their systems or compliance with both national or international safety laws and regulations.

4.2.Building a Functional Data Diode Step 1 - Create a Two-Way Network

The first step in creating a Data Diode or unidirectional network connection is to create a working bi-directional network connection. Once we ensure that all the network equipment works in both directions, it will be easier to troubleshoot issues we encounter once we switch to a single direction. A Fiber Optic based Data Diode is used because the receive (RX) and transmit (TX) connections are already physically separated from two fiber connections. So in theory if one can simply disconnect the RX or TX connector they will have a Data Diode. Two StarTech ST Fiber Optic Media Converters and one Multimode Duplex ST/ST Patch Cable will need to be purchased:

ascott@cimation.com

Table 3 – Data Diode Parts and Prices.

Item	Cost
StarTech.com 10/100 Fiber to Ethernet Media Converter Multi Mode ST 2 km (MCM110ST2)	$45
StarTech.com 10/100 Fiber to Ethernet Media Converter Multi Mode ST 2 km (MCM110ST2)	$45
StarTech.com Multimode 62.5/125 Duplex Fiber Patch Cable ST - ST - 1m (FIBSTST1)	$20
TOTAL COST	**$110.00**

Figure 8 – StarTech Fiber Media Converter.

ascott@cimation.com

Figure 9 - ST Fiber Optic Patch Cable.

There are a number of different form factors available in the world of Fiber Optic networking that goes beyond the scope of this white paper. The Fiber Optic ST form factor was selected for its wide availability and ease of use. Two laptop computers will represent the network; one will act as the secure side (High side) and the other insecure site (Low side). First, the computers are normally connected using the Fiber Optic Media Convertors in order to ensure everything is working correctly. As there are no switches or routers in the setup, the assignment of static IP addresses to each computer is required.

ascott@cimation.com

Table 4 –Static IP Addresses

End Point	IP Address
High – Secure	192.168.1.103
Low – Insecure	192.168.1.102

In order to test the connection between these two machines, the windows Ping utility in the command line can be used. First, the Firewall must be temporarily disabled on both the High and Low computer in order to send a Ping between the machines over the Fiber Optic link and confirm the connection.

Once the Fiber Optic connection has been verified with Ping, a protocol must be selected to transfer data across our Data Diode. A UDP-based protocol will be easiest to implement over the unidirectional connection. The Trivial File Transfer Protocol (TFTP) is a very simple UDP-based protocol that is capable of sending ASCII and Binary files across a network (without authentication). TFTP is rarely used within modern computer networks and but is still frequently seen loading firmware on hardware appliances. The TFTP protocol is simple enough to be easily manipulated and diagnosed over our Data Diode. Microsoft still provides a Windows TFTP client that we can install on the Low side, and there is an open source solution called Open TFTP Server that can be installed on the High side.

Figure 10 - Fiber Optic Link Setup Using Media Convertors.

ascott@cimation.com

4.3. Building a Functional Data Diode Step 2 – Disconnecting the RX

In theory, all we need to do is disconnect one of the Fiber Optic patch cables in order to create our Data Diode. Upon disconnecting the RX connection between the two Fiber Optic converters, the Link light went dark. In addition, in Windows the Fiber Optic connection media was listed as disconnected. After disconnecting the RX connection, our Windows pings are no longer being sent or received.

4.4. Building a Functional Data Diode Step 3 – Physical Layer Issues

Our first challenge with creating the Data Diode occurs on Layer 1 (Physical Connection) of the ISO 7 Layer mode. Specifically, Fiber Optic technology uses an Optical Carrier (OC) signal to ensure an end-to-end connection is present. Once we disconnected the RX connection, the Carrier signal was lost, and the Ethernet connection was considered disconnected. In the next section, we detail the steps required to overcome this issue using a third Fiber Optic Media Converter. In order for an Ethernet link to be considered connected, a Carrier signal must be present on the Receive (RX) connection of both ends of the link. When we disconnected the RX of one of our links, we broke the Carrier signal, and the link is now seen as disconnected. In order to overcome this issue, we will add a third media converter that will transmit a carrier signal into the RX of our disconnected fiber and provide a valid carrier signal.

ascott@cimation.com

Figure 11 – RX / TX Connection Carrier Signal From A Third Media Convertor.

We will need to purchase another media converter and add it to our total Data Diode cost:

Table 5 – Updated Data Diode Parts and Prices.

Item	Cost
StarTech.com 10/100 Fiber to Ethernet Media Converter Multi Mode ST 2 km (MCM110ST2)	$45
StarTech.com 10/100 Fiber to Ethernet Media Converter Multi Mode ST 2 km (MCM110ST2)	$45
StarTech.com 10/100 Fiber to Ethernet Media Converter Multi Mode ST 2 km (MCM110ST2)	$45
StarTech.com Multimode 62.5/125 Duplex Fiber Patch Cable ST - ST - 1m (FIBSTST1)	$20
TOTAL COST	**$155.00**

Now that we have our carrier signal for our RX connection, the Fiber Optic media converters believe the connection has been established and in Windows, we can see that the media is connected at both end-points. However, when we try to establish a TFTP connection we

ascott@cimation.com

can see that the packets are being sent out from the Low side but are not being received on the High side. In the next section, we will explore the solution for our packet transmission issue.

4.5. Building a Functional Data Diode Step 4 – Network Layer Issues

Our next challenge with building our Data Diode occurs at Layer 3 (Network Layer) of the OSI model, specifically with the network routing that maps IP Addresses to MAC Addresses. A MAC address is the unique identifier provided to a Network Interface Card (NIC), and is used by OSI Layer 2 (Datalink Layer) to uniquely identify each network endpoint (similar to a house number). In order for packets to be sent between disparate networks, network endpoints are assigned IP addresses that designate the location of the end-point (similar to a Zip code). In a normal network, Switches would send out an Address Resolution Protocol (ARP) Network broadcast in order to determine the mapping of IP Addresses to MAC addresses. A network that uses a Data Diode cannot rely upon ARP to provide the required mapping of IP to MAC addresses. The devices on the other side of the Data Diode cannot reply to the ARP broadcasts in order to provide their MAC to IP mapping because of the unidirectional network connection. In order to overcome this issue, static ARP entries must be created on Switches and end-points.

The method for adding a static ARP entry varies depending on the version of Windows / Linux / UNIX being used, so it is not detailed in this white paper. Once the static ARP entry has been added to our ARP Table, we will start to see our packets being received on the High side of our network. However, when we initiate a Windows TFTP Client transfer we receive a timeout error. In WireShark, we can see packets being received from the Low side of the network to the High side of the network, and the High side attempting to send some packets back. In the next section, we will work to overcome the Application layer issues introduced by a Data Diode.

4.6. Building a Functional Data Diode Step 5 – Application Layer Issues

The final challenge when creating a Data Diode occurs on the Application Layer (Layer 7) of our network. The UDP based TFTP protocol requires two-way communication in order to acknowledge that a packet was received. In order to initial a file transfer, the Microsoft Windows TFTP client will send a Request to Write (WRQ) packet on port number 69.

ascott@cimation.com

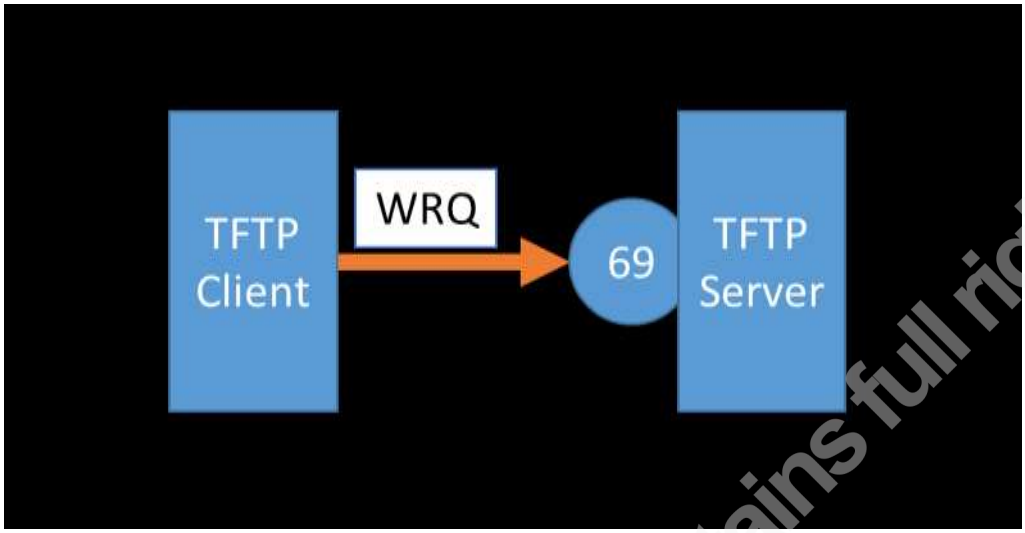

Figure 12 - TFTP Request To Write Packet.

The Microsoft Windows TFTP client will not transfer the next packet until it receives the acknowledgment (ACK) that the previous packet is transferred successfully. The acknowledgment allows the Microsoft Windows TFTP client to resend a packet in the event of packet loss (RFC,1981). The TFTP client will wait for a predetermined amount of time for the ACK before sending the same packet again.

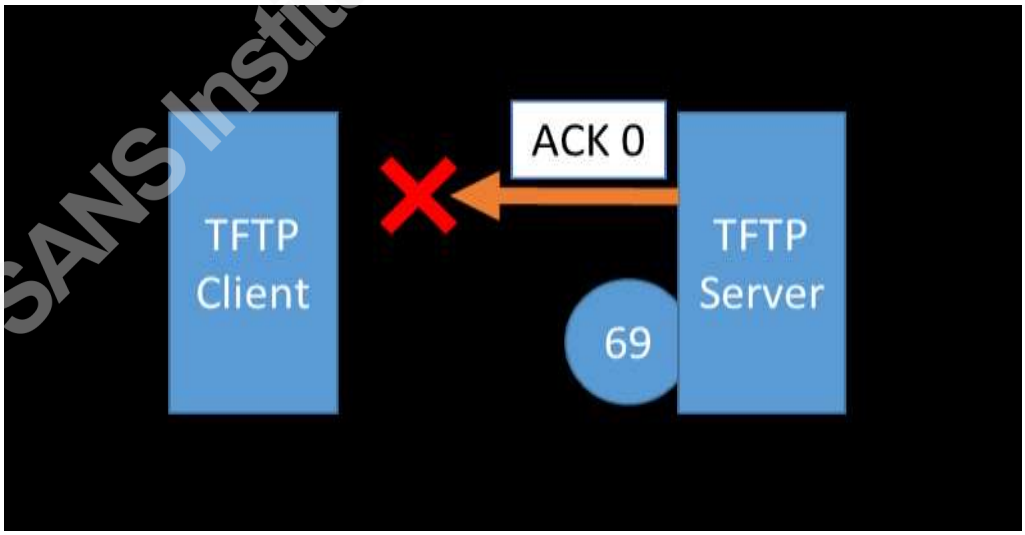

Figure 13 - TFTP Acknowledge Packet Timeout.

The Microsoft Windows TFTP client will try this a few times before producing a timeout error code and disconnecting.

ascott@cimation.com

In order to overcome this challenge, we will need to replace the Microsoft Windows TFTP client with our version that does not require the Acknowledge packet to be sent back to it.

We will write a customized version of the TFTP Client using PowerShell, as it is readily available on all Windows-based computers. The PowerShell script will start a file transfer with a TFTP server and wait for ten milliseconds between sending each packet rather than waiting for the server Acknowledgment. The PowerShell script can be easily copied and pasted into Windows PowerShell ISE and run from any Windows machine making it essentially Agentless (no installation, no registry changes, no hard disk changes, no long term impact to the system).

```
# Written by Austin Scott (ascott@cimation.com)
# Created January 2, 2015
# Requires Windows PowerShell 3.0+
# Declare Configuration Values
[String] $localFile  = "Test.zip" # Default file name
[int] $opCode     = 2     # Tftp Opcodes: 1=Read,2=Write,3=Data,4=Ack,5=Error
[String] $modeType  = "octet"  # TFTP Modes: octet, netascii, mail
[int] $transferPort  = 30000
[int] $waitAfterPacketMS = 10
$ipAddress = [system.net.IPAddress]::Parse("192.168.1.103")

# Init Variables
[int] $packetNum = 1
$Enc = [System.Text.Encoding]::ASCII

# Create TFTP Write File Request Frame
$sndBuffer = @()
$sndBuffer.Clear()
[byte[]] $sndBuffer += @([byte] 0x00)
$sndBuffer += @([byte] $opCode )
$sndBuffer += $Enc.GetBytes($localFile)
$sndBuffer += @([byte] 0x00)
$sndBuffer += $Enc.GetBytes($modeType)
$sndBuffer += @([byte] 0x00)

# Create Endpoints
$requestEnd = New-Object System.Net.IPEndPoint $ipAddress, 69

# Create Socket
```

ascott@cimation.com

```
$Saddrf  = [System.Net.Sockets.AddressFamily]::InterNetwork
$Stype  = [System.Net.Sockets.SocketType]::Dgram
$Ptype  = [System.Net.Sockets.ProtocolType]::UDP
$Sock   = New-Object System.Net.Sockets.Socket $saddrf, $stype, $ptype
$Sock.TTL = 26

# Send TFTP Write File Request Frame
$Sock.Connect($requestEnd)
$len = $Sock.Send($sndBuffer)
Start-Sleep -m $waitAfterPacketMS
# Create Binary Reader
$binaryReader = New-Object System.IO.BinaryReader([System.IO.File]::Open($localFile,
[System.IO.FileMode]::Open, [System.IO.FileAccess]::Read,
[System.IO.FileShare]::ReadWrite))
$transferEnd = New-Object System.Net.IPEndPoint $ipAddress, $transferPort
$Sock.Connect($transferEnd)

do
{
  $sndBuffer = @()
  $sndBuffer.Clear()
  $sndBuffer += @([byte] 0x00)
  $sndBuffer += @([byte] 0x03)
  $sndBuffer += @([byte] (($packetNum -shr 8) -bAnd 0xff))
  $sndBuffer += @([byte] ($packetNum -bAnd 0xff))
  $sndBuffer += @($binaryReader.ReadBytes(512))
  $len = $Sock.Send($sndBuffer)
  $packetNum++
  Start-Sleep -m $waitAfterPacketMS
}
until ($sndBuffer.Length -lt 516)

$Sock.Close()
$binaryReader.Close()
```

When executed, the PowerShell TFTP client successfully overcomes the Timeout issue when transferring data to a TFTP server. However, there is still a secondary issue with TFTP. The default port number for TFTP is known to be 69, and this port is used to initiate a TFTP connection. However, on initialization of a file transfer, the TFTP protocol negotiates a second

port (usually in the 30000 range) on which the actual data transfer occurs. Without a two-way connection, the PowerShell TFTP client has no way of knowing the incoming data transfer port number for the TFTP Server. We must limit the port number used on both the PowerShell TFTP client and Open TFTP server to a single value so that the port number negotiation step is not required. The PowerShell TFTP Client script above always uses port number 30000 to transfer data. We must also configure the Open TFTP Server only to accept connections on this port. The Open TFTP Server has a configuration file we can edit to accomplish this, called:

```
OpenTFTPServerMT.cfg
```

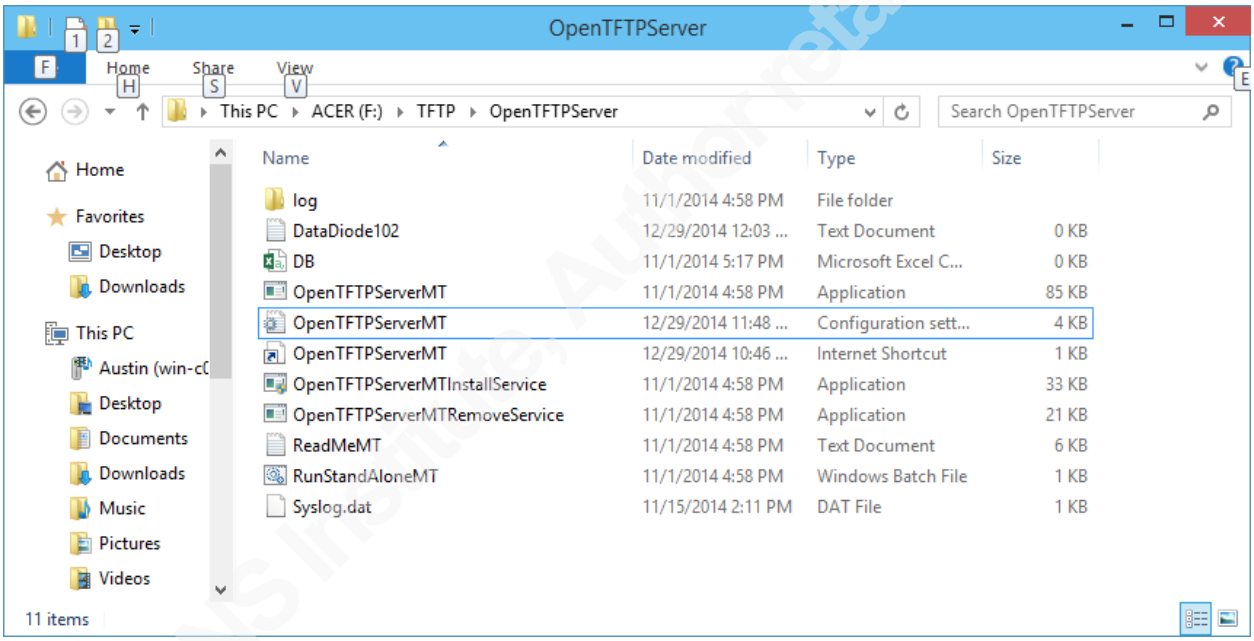

Figure 14 – OpenTFTP Server Configuration File.

By adding an entry into our Open TFTP Server configuration:

```
port-range=30000-30000
```

Also, we needed to enable file writing from clients with the configuration setting:

```
write=Y
```

The TFTP Server is now limited to the port number 30000 for file transfers. As a side effect, our ability to transfer files is limited to one at a time. The single simultaneous file transfer limit

ascott@cimation.com

would create a problem for us in an operating environment, but for the purposes of our simple example will work fine.

4.7. The Functional Data Diode – Binary File Transfer

Now that the Data Diode challenges have been overcome, and an application for transferring files has been configured to work over a unidirectional network connection, a file can be transferred across our network. Using the TFTP client PowerShell script and the properly configured Open TFTP Server we can copy binary and ASCII files over our Data Diode connection.

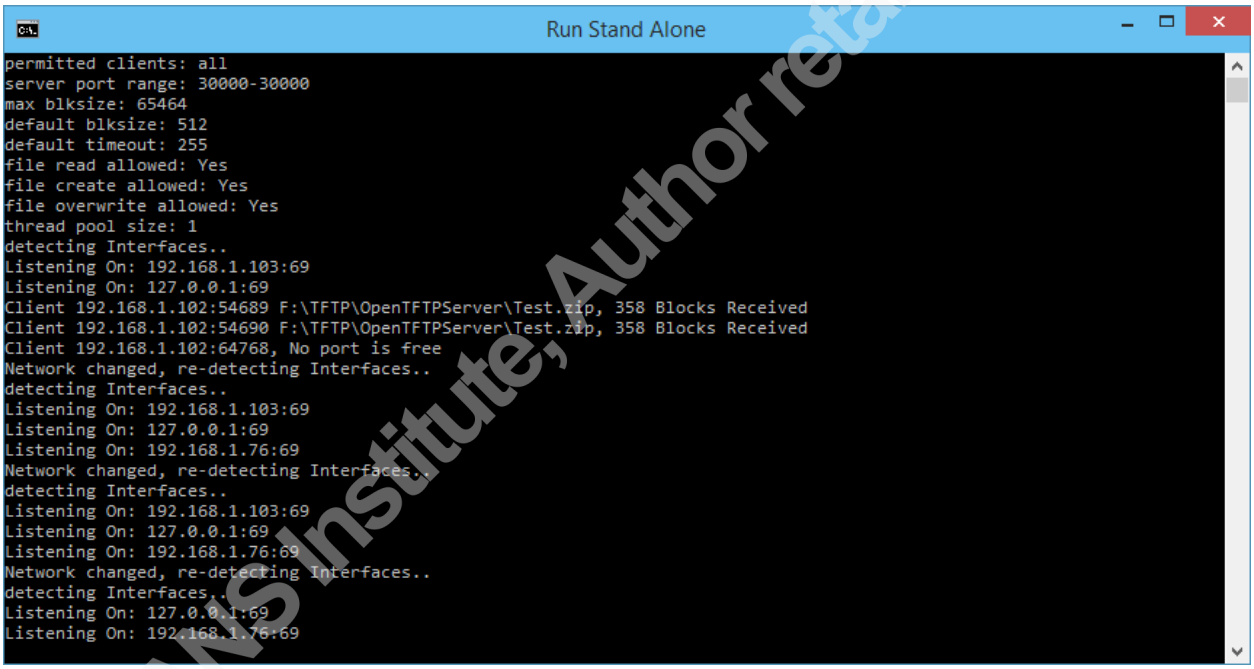

Figure 15 – A Successful Data Diode Binary File Transfer.

5. Data Diodes for Industrial Control

The Data Diode created in the previous exercise, although functional, is far from an industrial strength solution. It could not be trusted to handle mission-critical applications in a high-availability industrial environment. The Data Diode we created from off the shelf parts is certainly not ruggedized enough to handle the extreme conditions of an offshore platform or factory floor. Most of the Industrial Unidirectional Gateways on the market today are aligned with NERC CIP regulation for protecting critical infrastructure and are approved to work with

some of the IACS vendor product lines. Our Data Diode did provide insights into the challenges and potential uses of a Data Diode solution. In the following section, we will explore some potential use case scenarios within an Industrial environment.

5.1. Using a Data Diode in Place of an Air Gap

One of the most common scenarios we see in Unidirectional Gateway white papers is the use of a Data Diode in place of an Air Gap. An Air Gap is simply a complete disconnect between two levels of trust on a network. A truly Air Gapped network is completely isolated from the outside world. There was a time in Industrial Networks where Air Gaps did, in fact, exist. Today the existence of Air Gaps in Industrial networks is widely considered a myth. The value to the business of the Data coming out of an Industrial Network is far too valuable to cut completely off. A high-availability Data Diode configuration is used in place of an Air Gap to provide data up to the corporate network and not allow data to enter the control network (High to Low). A high-availability Data Diode provides information about the process for the business and prevents malicious data from entering the corporate network. This configuration is often used in electrical utility companies and nuclear power generation.

5.2. Database Replication

Another frequently used high-availability reference design is database replication. Most Industrial Control networks will contain a Historian server that maintains historical information about the process being monitored. Historical data is critical to a business for performance, maintenance, regulatory and financial reporting. As Data Diodes can achieve much faster speeds than Firewalls for data transfers as they do not need to apply software rules to the data in flight. The high transfer rate capability of Data Diodes makes it the well suited for Database Replication across levels of trust on a network.

5.3. Two-way Protocol Emulation

Some Unidirectional Gateway manufactures provide two-way protocol emulation for a one-way connection of certain protocols. TCP protocols used for file transfers, windows updates, event log collection to be sent through a Unidirectional Gateway using conventional protocols. There is no need in these cases, to implement customized protocols like the TFTP one we created

ascott@cimation.com

for our Data Diode file transfer. Some vendors even have added support for simple real-time industrial protocols like Modbus. This two-way data emulation can be used in a high-confidentiality configuration (read only from the IACS perspective) for cyber risk controls such as antivirus updates, windows updates and software patches. Or in a high-availability configuration (write only from the IACS perspective) for cyber risk control such as event log collection, real-time control system monitoring from the corporate network, historian data collection, backup management, and video surveillance feeds.

5.4. Mitigating Cyber Risk of Exposed or Infected Systems

Today within the many operating assets there are mission critical processes running on obsolete and insecure operating systems. Managing the cyber risk of these systems is one of the biggest challenges within IACS industry. By implementing a high-availability configuration, (write only from the IACS perspective) these obsolete systems can be safely monitored and protected from network-based attacks.

Another challenge that is frequently faced by the industry is mission critical systems that have been infected. Either infected components cannot be taken offline, or they are in remote locations and cannot be remediated. In order to prevent the infection from spreading, a high-confidentially configuration (read only from the IACS perspective) could be implemented. Commands or updates could be sent to the component, but the infection would not be able to spread out into the network.

6. Conclusion

There are many factors to be considered when developing a secure network architecture.

- Cyber Risk Reduction
- Capital Cost
- Operating Cost
- Human Resource Cost
- Sustainability
- Reliability

ascott@cimation.com

Industrial Cyber Security is cyber risk management within an operating process. The goal of any organization that has implemented a cyber-security program that reduces the most risk for the resources consumed.

Data Diodes perfectly implement a single cyber risk control: unidirectional data flow. The simplistic implementation of a Data Diodes makes it highly reliable and repeatable. A basic Data Diode does not have a software ruleset to implement and allows the data to flow through without introducing latency. Also without a software ruleset to configure and maintain, Data Diodes are hard to implement incorrectly, rarely require changes and are relatively easy to audit. Without the flexibility afforded by a software ruleset, the applications of Unidirectional Network technology is limited. Moreover, when compared to other barrier technologies, the capital cost of a Data Diodes is at least one hundred times more expensive. Typically, this technology is being implemented only within critical infrastructures such as power grids and power generation. Many of the commercially available Unidirectional Gateways on the market today can emulate two-way traffic with a one-way connection for a few select protocols.

The IACS industry is starting to see more control system vendors approving the use of Data Diodes in preapproved reference architectures. Wider approval from control system vendors will be a critical step for the more general adoption of Data Didoes in IACS. As more vendor approved, reference architectures become available we will see more Unidirectional Gateways being implemented and their price point coming down. Once the price of a Unidirectional Gateways more closely aligns with the cost of other barrier technologies (like Firewalls), we will likely see more widespread adoption within other industrial verticals such as energy and manufacturing.

Today we are seeing the Unidirectional Gateway vendors evaluating the use of their technology as a direct replacement for other barriers technologies such as Firewalls and Whitelisting. The better evaluation to perform is how these technologies can be used together to reduce cyber risk to as low as reasonability possible. It is not a matter of which technology is better; it is a matter of which is better suited for the specific cyber risk reducing implementation. Unidirectional Gateway vendors should focus on producing vendor approved network architectures that maximize the effectiveness of their technology rather than highlighting the weakness of other barrier technologies.

ascott@cimation.com

7. References

Forrest, K. I. (2012, 02 1). *A History and Survey of Network Firewalls*. Retrieved from University of New Mexico: http://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf

Ginter, A. (2012). *UTC*. Retrieved from UTC.org: http://www.utc.org/sites/default/files/public/UTC_Public_files/Stronger%20than%20Firewalls%20and%20Cheaper%20Too.pdf

K. R. Sollins (1981) *THE TFTP PROTOCOL (REVISION 2)*. Retrieved from ietf.org: http://tools.ietf.org/html/rfc783

Kamara, S. (2001). *Analysis of Vulnerabilities in Internet Firewalls*. Retrieved from Purdue.edu: https://www.cs.purdue.edu/homes/fahmy/papers/firewall-analysis.pdf

NIST. (2011, 6). *NIST 800-82: Guide to Industrial Control System (ICS) Security*. Retrieved from NIST.Gov: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

NIST. (2013, 4). *Security and Privacy Controls for Federal Information Systems and Organizations*. Retrieved from NIST: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Westmacott, J. (2003). *SANS GIAC*. Retrieved from http://www.giac.org/paper/gsec/2848/unidirectional-networking/104817

ascott@cimation.com

Last Updated: July 27th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Oslo Autumn 2017	Oslo, NO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS DFIR Prague 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZUS	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS AUD507 (GSNA) @ Canberra 2017	Canberra, AU	Oct 09, 2017 - Oct 14, 2017	Live Event
Secure DevOps Summit & Training	Denver, COUS	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VAUS	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Berlin 2017	Berlin, DE	Oct 23, 2017 - Oct 28, 2017	Live Event
Security Awareness Summit & Training 2017	OnlineTNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced