

Waterfall Security Solutions Ltd.



Applying NERC-CIP CAN-0024
Guidance for Data Diodes
To Unidirectional Security Gateways

Date: January, 2012

- Legal Notice & Disclaimer -

This document contains text, images and other information and/or materials which are proprietary to Waterfall Security Solutions Ltd., and constitute valuable intellectual property of Waterfall Security Solutions Ltd., protected by applicable patent, copyright and trade secret laws and by international treaty provisions. This document shall not be used in any manner that violates or misappropriates or could result in a violation or misappropriation of intellectual property rights of Waterfall Security Solutions Ltd., including, without limitation, copyrights, trademarks, trade secrets and/or patent rights. Under no circumstances shall any ownership rights in the content of this document be asserted nor Water Security Solutions Ltd.'s intellectual property rights be contested in any action or proceeding of whatever kind or nature, nor shall any action be taken that may prejudice, render generic, weaken or diminish the good will associated with Waterfall Security Solutions Ltd.'s intellectual property rights. Waterfall Security Solutions Ltd. reserves the right, without further notice, to pursue to the fullest extent permitted by law any and all criminal and civil remedies for the violations of its rights.

All information in this document is provided on an "AS IS" basis, and Waterfall Security Solutions Ltd. makes no warranties or representations and assumes no liability whatsoever as to the accuracy or completeness of the information presented in this document.

Any and all third party intangible and/or proprietary and/or intellectual property rights ("**Third Parties' Rights**"), mentioned herein, whether registered or not, including, without limitation, patents, trademarks, service marks, trade names, copyrights and computer applications, belong to their respective owners. Waterfall Security Solutions Ltd. disclaims any and all interest in all such Third Parties' Rights. It is forbidden to copy, modify, amend, delete, augment, publish, transmit, create derivative works of, create or sell products derived from, display or post, or in any other way exploit or use such Third Parties' Rights without the express authorization of their respective owners.

Except as specified herein, Waterfall Security Solutions Ltd. does not guarantee nor make any representations with regard to any and all third party tangible and/or intangible and/or proprietary and/or intellectual property ("**Third Party Property**") mentioned herein. Waterfall Security Solutions Ltd. does not endorse nor makes warranties as to the completeness, accuracy or reliability of such Third Party Property, and all such warranties are hereby expressly and strictly disclaimed.

- TABLE OF CONTENTS -

| | |
|---|-----------|
| EXECUTIVE SUMMARY | 3 |
| INTRODUCTION: CIP-002 AND ROUTABLE COMMUNICATIONS..... | 4 |
| DATA DIODES | 5 |
| SECURITY ADVANTAGES | 6 |
| WATERFALL SERVER REPLICATION | 7 |
| WATERFALL NON-ROUTABLE PROTOCOL | 9 |
| STAND-ALONE APPLIANCES..... | 9 |
| PAIRED UNIDIRECTIONAL SECURITY GATEWAYS..... | 10 |
| EMBEDDED NETWORK INTERFACE CARDS..... | 11 |
| CONCLUSIONS | 12 |

Executive Summary

Under the direction of the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC) is charged with enforcing reliability standards for the Bulk Electric System (BES) in North America. Reliability standards for the BES are created under NERC's supervision by an industry-driven process. Both physical security threats and cyber security threats are regarded as threats to the reliability of the BES, and as a result a set of Critical Infrastructure Protection (CIP) security standards have been adopted.

In December of 2011, NERC issued Compliance Application Notice (CAN) 0024 "CIP-002 R3 Routable Protocols and Data Diode Devices." The purpose of a CAN is to provide guidance to auditors who evaluate industry compliance with CIP reliability standards and who make findings that can lead to enforcement actions and monetary fines. CAN-0024 provides instruction for assessing whether the communication characteristics of data diode devices can be used to exclude cyber assets from consideration as Critical Cyber Assets (CCA) when a routable protocol is used when not at a control center.

"Data diodes" are hardware-enforced one-way or unidirectional communications. They permit data to flow from a protected network to an external network, but provide no physical data path for information, remote control attacks, or other cyber-attacks to flow back in to the protected network. Unidirectional hardware is used to provide strong security for connections through an Electronic Security Perimeter (ESP). Routable communications that cross an ESP are of concern under the NERC CIP standards because they can be a vector for attacking a control system.

This whitepaper introduces CIP-002, routable protocols that are used in "routable communications," and unidirectional communication concepts, and then applies the guidance in the CAN-0024 to three types of commonly-deployed hardware architectures for unidirectional communications. We conclude that Waterfall's Unidirectional Security Gateways, which do not use routable communications, can be used to exclude Cyber Assets from consideration as Critical Cyber Assets (CCA) in accordance with CAN-0024.

Introduction: CIP-002 and Routable Communications

The heart of the CIP standard consists of eight sections numbered 002-009. The CIP-002 standard defines the terms Critical Assets (CAs) and Critical Cyber Assets (CCAs):

- Critical Assets are physical assets essential to the reliability of the BES, and
- Critical Cyber Assets are computer and networking "cyber" assets essential to the correct operation of Critical Assets, provided the cyber assets meet certain criteria.

The Critical Cyber Asset designation arises when a cyber asset that is essential to the operation of a Critical Asset meets at least one of the following criteria:

- R3.1.** *The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,*
- R3.2.** *The Cyber Asset uses a routable protocol within a control center; or,*
- R3.3.** *The Cyber Asset is dial-up accessible.*

In short, the standard provides a methodology for designating cyber assets as CCAs in at least one of three high risk scenarios: (i) they are dial-up accessible, (ii) they use routable communications within a grid Control Center, or (iii) they use routable communications which pass through an Electronic Security Perimeter (ESP). NERC's CAN-0024 guidance and this whitepaper both focus on the use of data diodes as applied to the third case.

To round out our definitions, NERC defines an "Electronic Security Perimeter" as:

The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.

In effect, the ESP is a line drawn on a network diagram which is used in the process of classifying cyber assets, Access Points and other elements of the network.

The meaning of "control center" under CIP-002 R3.2 is generally regarded as a control system that controls or dispatches either two or more power plant sites or two or more transmission substations.¹ In practice, power plant control systems rarely control generating units at more than one site, and thus it is rare for a power plant control system to qualify as a control center for purposes of CIP-002 R3.2.

With these definitions established, we next consider the question of communications that use a routable protocol. Routable protocols use addresses and require those addresses to have at least two parts: a "network" address and a "device" address. Routable protocols allow devices to communicate between two different networks by forwarding packets between the two networks. Non-routable protocols only use a "device" address, and do not allow messages to be sent from one network to another, thus allowing communications to take place only on a single network.

¹ The term "control Center" under CIP-002 R3.2 is generally assigned the definition of "control center" that is published in NERC's 2010 "Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets."

At the network layer (layer 3 in the OSI model), the routable protocol in widespread use in North America is the Internet Protocol (IP). ISDN, X.25 and other layer 3 routable protocols are used in Europe and in other parts of the world, but these protocols are used only rarely within NERC's jurisdiction in North America. The function or purpose of Internet Protocol is to move datagrams through an interconnected set of networks. This is done by passing the datagrams from one internet module to another until the destination is reached. The internet modules reside in hosts and gateways in the internet system. The datagrams are routed from one internet module to another through individual networks based on the interpretation of an internet address. Significantly, Waterfall's Unidirectional Security Gateways do not have an assigned internet address, do not contain an internet module, do not transmit an internet address in the datagram header, and cannot be used to move datagrams directly from one internet module to another through an interconnected set of networks.

Note that the Internet Protocol is considered a routable protocol even when the only use of the protocol is within a local area network, and even when the only network addresses used are addresses reserved for LAN communications by the IP standard. It is the Internet Protocol itself which is considered routable, because the protocol defines network address fields in every message.

With these definitions established, the discussion below introduces unidirectional communications hardware in greater detail, and evaluates different hardware and software architectures in the context of the CAN-0024 guidance document.

Data Diodes

A "data diode" is communications hardware which permits information to flow in only one direction. The concept is straightforward, but the technologies behind truly unidirectional communications are generally more complex than laymen expect. For example, one could argue that an RS-232 cable with the Transmit and ground lines intact, but with the Receive line severed could serve as a primitive diode. A security expert might disagree, since a determined adversary might still force some information to be transmitted from the receiver to the sender through secondary lines such as Carrier Detect and Data Terminal Ready. Good "data diodes" have been examined by security experts and have been certified to contain no overt data channels which permit communications from the receiver back to the transmitter, and contain no covert channels either.

"Data diode" technologies can be more complex than first appearances suggest for a second reason: compatibility. If you replace bidirectional communications hardware with unidirectional hardware, then as a rule any existing applications using the affected communications channel malfunction. The vast majority of communicating applications assume bidirectionality. As a result, a majority of "data diode" implementations include some software support as well as hardware components. The most common software supports:

- A primitive file transfer mechanism,
- A UDP/IP stack which works even in the absence of the usual ARP and other bidirectional support protocols, or
- A primitive TCP/IP proxy.

As a rule this primitive software is not sufficient to seamlessly replace existing bidirectional communications channels in industrial settings. Deploying unidirectional communications equipment with only primitive software support generally results significant infrastructure changes,

customization, and costly, custom software development in order to integrate the unidirectional communications channel into existing power grid control system applications.

To address the need for seamless integration into existing infrastructures, Waterfall Security Solutions provides Unidirectional Security Gateways, a combined hardware and software solution. The hardware portion of the Waterfall solution is comparable to data diodes, though the Waterfall solution includes a variety of data integrity and security measures not found in simple diodes. The software portion of the Waterfall solution replicates a wide variety of industrial servers through the unidirectional hardware, rather than expose primitive unidirectional communications to high-level applications. Details of how the Waterfall solution communicates in order to replicate industrial servers are provided in the section “Waterfall Server Replication” below.

Security Advantages

The reason NERC entities adopt Unidirectional Security Gateways, rather than conventional bidirectional network connections or firewalls, is security. True unidirectional communications hardware permits useful information to flow out of a protected network, without putting assets inside that network at risk. In conventional bidirectional communications, any communication out of a protected enclave introduces a risk that messages returning on the bidirectional communications channel might be constructed or corrupted in such a way as to exploit security vulnerabilities in the sender or in intervening communications components such as firewalls. A Unidirectional Gateway is a hardware-enforced one-way information flow, and so does not put the safety, integrity or availability of the sending network at risk in any way.

One might look at the above argument and conclude that CIP-002 should have been written to include unidirectional communications as a criterion to exclude cyber assets from being considered high-risk CCAs. Unfortunately, when the CIP standards were written, unidirectional communications were not used as widely as they are today, and so no such provision was included in the standard. At present, many sites have deployed Waterfall Unidirectional Security Gateways and these sites might think to argue to NERC auditors that unidirectional hardware protections of cyber assets constitutes strong security and so should exempt those assets from consideration as CCAs. No such argument sways the auditors, though. The language of the standard is clear - only the presence of dial-up communications or routable communications determine whether cyber assets essential to the BES should be classified as Critical Cyber Assets – hence the discussion in CAN-0024 about the applicability of the term “routable” to unidirectional communications.

A majority of the discussion in this whitepaper is focused on routable communications because the topic of our discussion is CAN-0024, and routable communications is the focus of the CAN. It is, however, important to remember that hardware-enforced unidirectional communications is fundamentally more secure than any type of bi-directional communication. Generators and other entities which are able to deploy unidirectional communications technologies exclusively in the defense of their network perimeters find that the technology protects their control networks absolutely from all attacks originating on external networks. This includes viruses, worms, denial-of-service attacks and targeted remote-control attacks.

While the discussion below focuses on how to manage unidirectional communications within the CIP standards, in a sense the most significant message in CAN-0024 is not the guidance regarding protocols, but is implicit in the existence of the CAN itself. NERC does not issue guidance for

technologies or situations which NERC auditors encounter only rarely. That the CAN was published suggests that, unlike when the CIP standards were created, today NERC auditors encounter unidirectional communication technologies on a regular basis. This is arguably the most significant development in the security posture of the BES since the introduction of the CIP standards. The increasing deployment of unidirectional communications technology measurably improves the security of the Bulk Electric System.

With this background, the next two sections return to the question of communications protocols, routable and otherwise. The discussion explores in some detail how components in Waterfall Unidirectional Gateway server replication solutions communicate, which parts of those communication are routable, which are not routable, and why. Following that, the next three sections consider three cases of unidirectional hardware architectures and evaluate each case for the presence of routable communications as directed by the guidance in CAN-0024.

Waterfall Server Replication

This section explores two examples of server replication and the following section details communications mechanisms used in both replication solutions. The two solutions are historian server replication and OPC server replication. In these examples, each solution replicates a particular server from a protected control system network to an external business network. In each case, the Waterfall software is designed to make the replica as true to the original server as is practical. In replacing firewalls with unidirectional server replication solutions, it is common to find that end users and application software on the business network are not aware that they are accessing a replica. The replica is so faithful a copy of the protected server that no end user procedures or application integration configurations were changed in the deployment of the replica.

In the historian replication example, this faithful replication comes about as a result of the TX agent software and RX agent software illustrated in Figure (1).

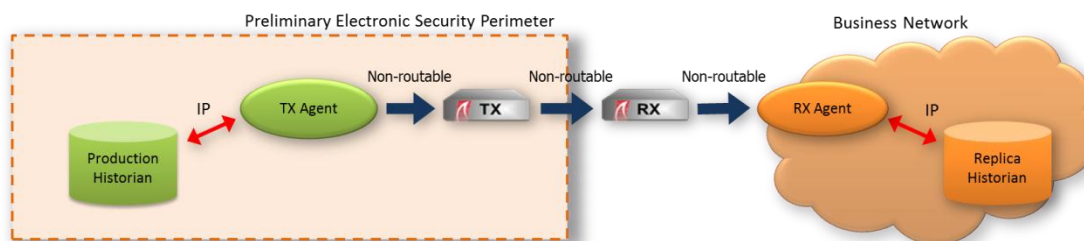


Figure (1) Waterfall Historian Replication

The TX agent software is manually configured to register with a specific production historian server at a specific IP address. The TX agent registers as a conventional historian client, and uses the historian vendor’s Application Programming Interface (API) libraries to request a copy of all new data arriving in the historian. The libraries use the historian’s proprietary, IP-based, client access protocol to make the request, and to receive the data from the historian. The agent then extracts historical data and meta-data from the data structures returned by the historian API. The agent sorts that data by data types, packages it in type-specific, labeled data structures, and sends the historical data through the unidirectional subsystem to the Waterfall RX agent.

The RX agent is manually configured to register with a specific replica historian at a specific IP address as a “data collector.” Different historian vendors call these components by different names, but most historian vendors have the concept of an application which collects data from devices, stores the data temporarily if necessary, and then deposits the data into the historian database. The RX agent receives the data from the TX agent, and extracts the data from the type-specific data structures. The agent may store the data for a period of time, for example if the replica historian is not ready to receive the data. Ultimately, the RX agent passes the data to the replica historian API libraries for delivery to the replica historian, using whatever, typically IP-based, proprietary protocols the API libraries use to communicate with their historian.

At no time did the Waterfall solution attempt to emulate or proxy a proprietary, IP-based historian access protocol. The agents use vendor-supplied libraries, which in turn use the vendor protocols. The agents extract the values returned by the vendor APIs and then pass only the extracted data through the Unidirectional Gateways, not the vendor protocol messages.

The OPC-DA server replication scenario is similar, and is illustrated in Figure (2).

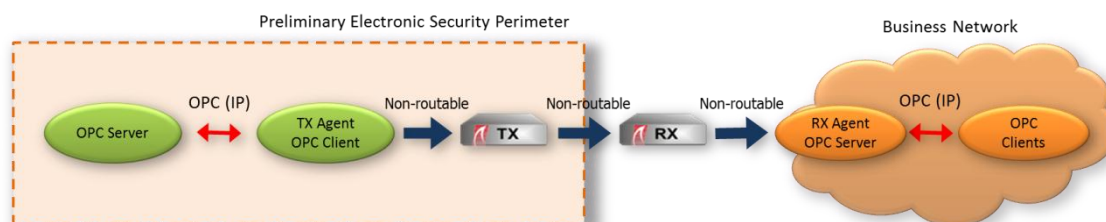


Figure (2) Waterfall OPC-DA Server Replication

The OPC-DA protocol is a complex, intensely bi-directional protocol encapsulated within DCOM, which is encapsulated within IP. Waterfall is often asked “how can you possibly emulate OPC through a unidirectional medium?” The answer is that the Waterfall OPC server replication solution makes no attempt to emulate the OPC protocol, or to transmit any part of the protocol through the Unidirectional Gateways. In the OPC-DA replication scenario, the TX agent is a true OPC client, and is configured to gather device data from OPC servers on the control network using the true, bidirectional, routable, OPC-DA protocol. The agent then extracts OPC data and meta-data from the OPC communications. The agent sorts that data by data types, packages it in type-specific, labeled data structures, and sends only the device data through the unidirectional subsystem to the Waterfall RX agent.

The RX agent is a true, standard OPC-DA server. The RX agent / OPC server receives data from the TX agent / OPC client via the Unidirectional Gateways, and extracts the data from the type-specific data structures. The RX agent then generally stores the data for a period of time, until a user or client asks for the data. When the RX agent receives an OPC-DA request for data from a user or application, the agent responds to that request using the stored data.

At no time did the Waterfall solution attempt to emulate or proxy the very complex, intensely bidirectional, OPC-DA protocol over unidirectional media. Both agents use the true, bidirectional, OPC-DA protocol to communicate with OPC components on their respective networks. The TX agent

transmits only data and metadata in proprietary type-specific data structures through the Unidirectional Gateways.

Waterfall Non-Routable Protocol

In all replication scenarios, the TX agent host is connected to the TX gateway with a conventional network interface card and a conventional, copper, twisted-pair Ethernet cable. This agent host network interface has no IP address assigned, and has the IP drivers disabled. The TX agent puts type-specific data structures directly into the payload of OSI layer 2 Ethernet frames. This payload contains no IP header information and no IP addresses. The same is true on the receiving side of the solution, with the connection between the RX Gateway and the RX agent host. Similarly, there are no IP addresses assigned to the fiber optic interfaces on the Unidirectional Gateways, no IP software drivers enabled for those network interfaces, and no IP header information or IP network addresses in communications between the gateways.

Each type-specific data structure is labeled with a channel ID. The channel ID identifies the data type and the format of data in the data structure, as well as which application on the RX agent host is to process the data. For example, a TX agent host and an RX agent host could each be host to both an OPC-DA replication agent, and a historian replication agent. In a typical configuration, the OPC data structures would be assigned 6-10 channel IDs, one for each type of data, and the historian data structures would be assigned another 6-10 channel IDs. The channel ID assignment is done manually through configuration screens on each agent host, and channel IDs for each application and each type of data must match exactly in order for the RX agents to correctly decode data received from the RX gateway.

Thus, while the channel ID fields do identify data types associated with replication applications, they are not layer 3 network addresses. A layer 3 address uniquely identifies a host in a potentially large network. In the Waterfall architecture, replicated data is always sent from the TX agent host to the RX agent host. Channel IDs have no meaning outside of this pair of hosts. Channel IDs identify types of data flows, rather than network host addresses.

In summary then, the RX and TX agents each use routable protocols to interact with equipment on their respective networks. However, all communications between the agents via the gateways take the form of OSI layer 7 application data, in labelled, type-specific data structures, which are embedded in the payload of OSI layer 2 Ethernet frames and OSI layer 2 optical communications frames.

With this background on how Waterfall Server Replication communications occur, the sections below review the guidance in CAN-0024, and apply that guidance to Waterfall Unidirectional Gateway solutions.

Stand-Alone Appliances

The first architecture addressed in CAN-0024 is the "stand-alone" appliance illustrated in Figure (3). The solution consists of a network appliance, externally exposing at least two conventional network connections. Unidirectional communications may occur on either of the external interfaces, or may occur inside the appliance somehow.

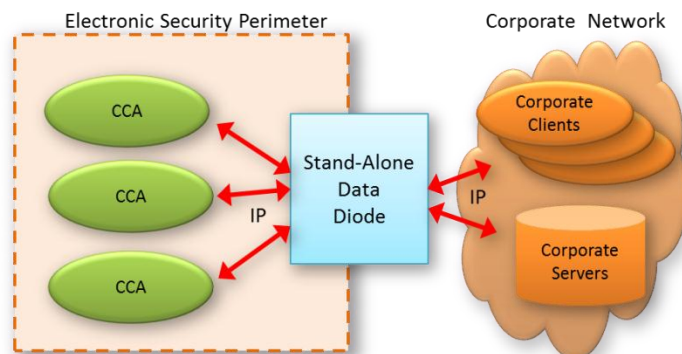


Figure (3): Stand-alone appliance using Routable Communications

Regarding such devices, CAN-0024 states:

An easy way to assess the connectivity is to determine if the network interfaces on the stand-alone data diode device are configured with IP addresses. If the stand-alone data diode device has one or more IP addresses, it is “using” a routable protocol for communication.

Thus, the stand-alone device is judged to use a routable protocol if one or more of its external interfaces have an IP address.

Conclusion: Stand-alone equipment with IP addresses on one or more external network interfaces is specifically identified in CAN-0024 as using a routable protocol. Cyber assets communicating through an ESP via stand-alone unidirectional equipment with IP addresses are using routable communications and cannot be excluded as CCAs.

Paired Unidirectional Security Gateways

The most widely-deployed unidirectional communications solution, both for protecting industrial networks generally and for protecting Bulk Electric System sites specifically, is the paired Waterfall Security Solutions Unidirectional Security Gateway solution. A general server replication solution is illustrated in Figure (4).

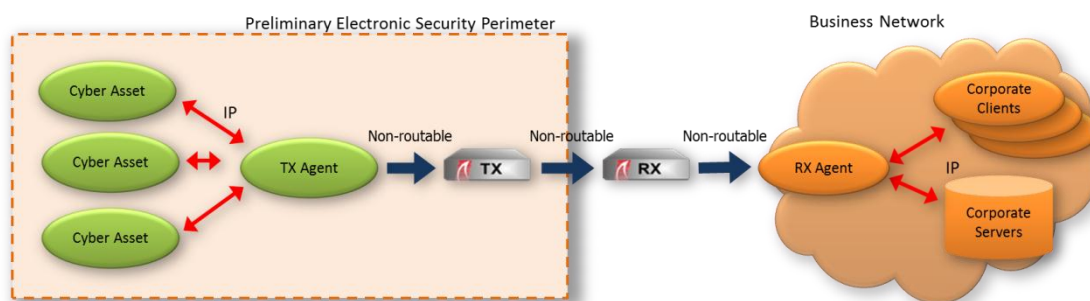


Figure (4): Paired Unidirectional Security Gateway Appliances

The solution consists of a pair of Unidirectional Gateway network appliances, one which can transmit, but not receive, and one which can receive, but not transmit. Access to each appliance is controlled by a conventional agent host computer, running the TX and RX replication agents. The software agents replicate industrial servers from inside the ESP to outside the ESP. The most common deployment in NERC-CIP applications has the preliminary ESP drawn through the single fiber optic cable connecting the TX appliance to the RX appliance.

Details of the Waterfall architecture were described in earlier sections and are summarized here. The Waterfall architecture utilizes a pair of TX and RX appliances for unidirectional communication without use of a routable protocol. None of the network interfaces on the TX and RX appliances has an IP address. The network cable connecting each appliance to its respective agent host computer is a conventional Ethernet twisted-pair cable running a proprietary Waterfall protocol – not IP. The protocol embeds layer 7 application data into the payload of non-routable layer 2 frames. The Waterfall layer 7 data structures contains channel IDs, which identify types of data flows, but channel IDs are not routable network host addresses. Similarly, the fiber-optic cable running between the Waterfall appliances is also running a proprietary, layer 2 protocol without IP or other routable WAN addresses. And finally, the network interfaces which connect the agent host computers to the Waterfall Gateways have no IP addresses either. In fact, those host network interfaces are configured to disable the Internet Protocol communications module entirely.

Since none of the network interfaces on either the TX or RX appliances have IP addresses, or indeed use IP or any other routable protocol, the communications in this scenario, in addition to providing strong security, qualify as cyber assets which do not use a routable protocol to communicate outside the Electronic Security Perimeter.

Conclusion: According to CAN-0024, Waterfall Unidirectional Gateways carrying out server replication over a non-IP, non-routable protocol, do not trigger the routable communications clause in CIP-002 R3.1 and therefore do not trigger the classification of cyber assets as CCAs.

Embedded Network Interface Cards

The other scenario CAN-0024 considers involves unidirectional Network Interface Cards (NICs) embedded in conventional computers, such as the example illustrated in Figure (5). In practice, the majority of such equipment is deployed with the ESP drawn across the cable connecting the TX NIC to the RX NIC as illustrated in the figure.

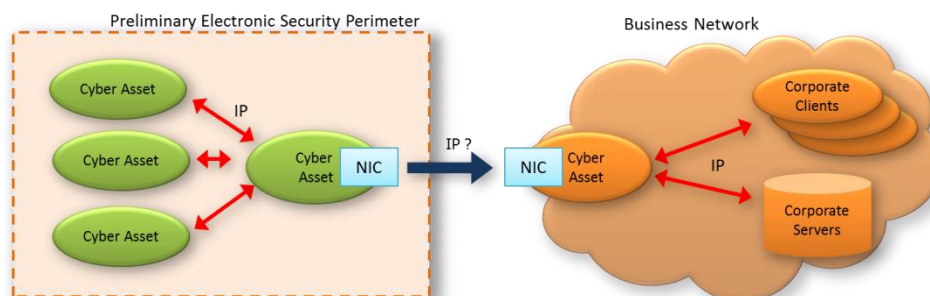


Figure (5): Embedded Network Interface Cards

The scenario in Figure (5) is described in CAN-0024 as follows:

Another type of data diode device consists of network interface cards that are installed into existing Cyber Assets, and which provide the same uni-directional communication as stand-alone data diode devices. For the purpose of this CAN, these will be referred to as “embedded data diode devices” to distinguish them from stand-alone data diode devices. In this case, the data does not use a routable connection to cross the ESP, and the Cyber Assets do not meet the connectivity requirement.

In this paragraph, CAN-0024 attempts to distinguish stand-alone data diode devices from embedded data diode devices. Concluding that all embedded data diodes do not use routable protocols is a surprising, overly broad statement. The focus of CIP-002 R3.1 is on whether a routable protocol is used for communication, not on hardware design. A common configuration of embedded data diode devices is to assign IP addresses to the unidirectional NICs and to pass messages using UDP or other routable transport layer protocols from the transmitting NIC to the receiving NIC. Since the CAN repeatedly asserts that the use of a routable protocol to communicate to cyber assets outside the ESP will subject cyber assets to the CIP standards as CCAs, the assertion that embedded data diode devices do not use a routable connection to cross the ESP must be read in the context of the entire discussion in CAN-0024.

Conclusion: Absent further clarification the discussion of embedded data diode devices in CAN-0024, expect unidirectional embedded network interface cards to be a source of confusion for auditors for the foreseeable future.

Conclusions

The NERC CIP approach to cyber security is to focus on critical BES assets and their essential cyber assets. The language of CIP-002 R3.1 recognizes that routable communications place cyber assets at greater risk than do other kinds of communications.

The CAN-0024 guidance makes it clear that data diode devices which do not use routable communications, such as the Waterfall Unidirectional Security Gateways, do not meet the test set forth in CIP-002 R3.1. When sites which are not control centers use Waterfall Unidirectional Gateways, the risk of cyber assault are significantly reduced and the use of the Unidirectional Gateways does not subject cyber assets to the NERC CIP standards. The compliance cost savings from such a reclassification can be significant, reflecting the substantially reduced risk to cyber assets protected by Unidirectional Security Gateways.

Protecting the Bulk Electric System from cyber assault is a worthy goal. When the only communications from a control network are via Waterfall’s Unidirectional Security Gateways that do not use a routable protocol, the cyber assets within the control network are protected absolutely from outside network attacks. The security of the BES would benefit measurably from increased use of Waterfall’s Unidirectional Gateway hardware.

About Waterfall Security Solutions

Waterfall Security Solutions Ltd. is the leading provider of Unidirectional Security Gateways™ and data diodes for Control networks, SCADA systems, Remote Monitoring and Segregated Networks. Waterfall's security solutions assist Utilities and Critical Infrastructures to easily and comfortably achieve compliance with NERC-CIP, NRC, NIST and other regulations as well as cyber-security best practices. Waterfall's products have been deployed in many utilities, critical national infrastructures, mission critical environments and homeland security agencies throughout North America, Europe and Israel. Waterfall's offerings include support for leading industrial applications, such as: OSIsoft PI™ Historian, GE Proficy™ iHistorian, the Siemens SIMATIC™ and the GE OSM™ remote monitoring platforms, and leading industrial protocols, such as: OPC, Modbus, DNP3 and ICCP. More information about Waterfall can be found in the company's website at: www.waterfall-security.com.