Cyber Security
Compliance to the new CSA 290.7 Standard

M. Daley, R. Doucet, M. Echlin, M. MacDonald, V. Mihaylov, J. Sijs, and D. Trask
Canadian Nuclear Laboratories, Chalk River, Ontario, Canada
(Matthew.Daley@cnl.ca)

Abstract

Since 2008, the Canadian Nuclear Safety Commission (CNSC), similar to regulators of other critical industries, has requested their licensees to implement cyber security programs and conduct self-assessments without the benefit of an industry specific cyber security standard that provides common metrics for coverage and effectiveness of their programs. However, for the nuclear industry, a new CSA standard 290.7 entitled "Cyber security for nuclear power plants and small reactor facilities" [1], released in December 2014, will have the CNSC looking to facility operators to be compliant to the new standard.

This paper will discuss initiatives at Canadian Nuclear Laboratories to develop of a suite of tools, techniques, and best practices that can be used by the regulator and industry for assessing compliance and effectiveness of cyber security technology and implementations.

1. Introduction

Nuclear operators and regulators are faced with the never ending challenge of navigating the overwhelming, ever increasing, and continuously evolving volume of information across many industrial sectors to develop and maintain the knowledge, understanding, and capabilities required to design and implement cyber security solutions that are effective, practical, maintainable, and compliant.

In recognition of the need for cyber security solutions, Canadian Nuclear Laboratories (CNL) has been doing research to understand the cyber security landscape, with the primary goal of identifying tools, techniques, and best practices that will assist both the regulator and nuclear operator in implementing industry compliant solutions. In particular, the 2014 release of the new CSA standard entitled "Cyber security for nuclear power plants and small reactor facilities" [1], compels the nuclear industry to action.

As with most standards, CSA 290.7 captures requirements without prescribing any particular solutions. The challenge for users of the standard and enforcers of the standard is to come to agreement on what compliance should look like, measuring effectiveness of various detection and protection technologies, and understanding what defence-in-depth strategies are suitable for supporting the availability and integrity of information. Indeed, the list is long for the number of areas that the standard addresses and extends from policy and planning, to risk and vulnerability management, to incident planning and preparedness to name a few.

CNL has extensive experience managing IT infrastructure as well as developing, deploying and maintaining distributed control systems used in safety applications. Both domains are vulnerable to cyber threats. As a prelude to the work described in this paper, CNL has conducted a broad review of over 50 standards, guidelines, and regulations from recognized institutions covering safety, cyber security, and industrial communication networks including wireless communications. In particular, an analysis was performed to determine the application of these standards to small reactor remote monitoring and control via satellite communication technologies. This work resulted in recommendations being made to the CNSC to support their efforts for developing a regulatory position for securing remote communications to a small remote reactor facility.

CNL is currently undertaking a multi-year research project that builds on the cyber security work previously done, in order to provide state-of-the-art, relevant and practical cyber resources for regulators and nuclear operators. These resources will significantly contribute to their cyber security knowledge base and capabilities and will be used to enhance the security posture of Canadian nuclear facilities and critical infrastructure. The focus of this research is to develop best practice guidance, tools, and methodologies that will be used for assessing network architectures and system components against the requirements of CSA 290.7 [1] while accounting for various levels of risk and vulnerability. This work will be informed by system architectures currently in use at CANDU plants in order to ensure that discoveries and recommendations are relevant to operators. For example, it is recognized that it may be impractical to modify qualified systems or replace legacy hardware such that optimal solutions to cyber threats may not be realistic to implement. CNL's research will take these constraints into consideration and seek to find best in class alternatives and compliant solutions as evidenced via testing.

Testing is conducted using a demonstration test facility that has been assembled to emulate defence-in-depth architectures and the deployment of candidate cyber security products. A subsequent iteration of the test facility will model network architectures employed at a plant, and provide a platform that supports data gathering for the purposes of evaluating the capability and effectiveness of cyber security products and tools and measuring compliance to the requirements in CSA 290.7.

For the regulator, not only is it difficult to keep up with the latest in cyber threats and defences but they are faced with the challenges of sifting through and assessing large volumes of written material from each facility describing their security case. A goal of the research is to identify assessment capabilities and measurement criteria that can be adjusted to accommodate different levels of risk or vulnerability. As such, CNL's research efforts aim to take a systematic approach to developing assessment criteria for each of the CSA 290.7 requirements that takes into account, for example, layers of physical security, the presence of highly trained personnel, legacy systems, etc. As well, opportunities for automation will be investigated in order to provide real-time auditing and situational awareness of the plant's overall cyber security posture and status.

Although it is recognized that cyber security solutions and practices are already being successfully employed at our nuclear facilities, this research will endeavor to identify and share best practices, provide evidence based testing and assessments and where appropriate, identify new technology and designs that could more effectively respond to emerging threats. The following illustrate some of the

areas where researchers will be looking to industry to capture current technology and practices as a basis for conducting evaluations in order to identify already compliant practices and technologies as well as potential gaps and opportunities for improvement. The results will contribute to the requirements for the test facility and the preparation of a resource guide for complying to CSA 290.7:

1. What tools or processes are used to inspect/identify all active ports or nodes on a system? How would one know that all devices and connections have been identified?

2. What tools or processes are used to manage passwords, encryption keys, software versions and configurations at each device? How would one know that unauthorized changes have not been made in the field?

3. What testing is done or evidence provided to ensure that networks are properly decoupled?

4. What exercises have been done to test the cyber emergency response team, operators, managers, or staff? What are the criteria for measuring the effectiveness of an incident response and evaluating the coordination between supporting departments including physical security, personnel security, information protection, corrective action, supply chain, operations and maintenance, etc?

5. What testing is being done or evidence provided to ensure that any and all wireless devices or access points are known and secured? Are wireless scans being conducted, if so where and how often?

6. What processes or tools are employed to verify that firewalls and detection/prevention systems are configured properly and have not been modified? What best practices are being employed to configure the systems and are these the most effective? How often are these systems updated and verified?

The remainder of this paper is organized as follows. Section 2 describes the methodology of a technology survey undertaken by CNL in order to identify potential products that can be used to aid a system in becoming compliant to CSA 290.7, to aid nuclear operators in demonstrating compliance to CSA 290.7, and to aid the regulator in evaluating compliance to CSA 290.7. Section 3 describes CNL's Cyber Secure Industrial Remote Monitoring and Control Demonstration System. Conclusions and future work are presented in Section 4. Finally the references used by this paper are presented in Section 5.

2. Technology Survey

The technology survey is a systematic analysis of the latest products and technologies associated with protecting enterprise and control system networks from current and future cyber threats. The survey is conducted with consideration of the unique requirements and system architectures at nuclear plants and with the objective of identifying those products and technologies that show promise in supporting the achievement or evaluation of cyber security compliance.

Assessing products is a multi-step process. Firstly, the candidate product is categorized into one or more product type categories (i.e., access and identity management, boundary protection devices, detection devices, network and network-related devices, and security management). Secondly, the candidate is assessed against recognized security standards. The assessment leverages previously existing standards with a focus on FIPS-140 and the Common Criteria, since these standards have wide industry and government acceptance. It should be noted that claimed adherence to a standard such as FIPS-140 or Common Criteria is not a guarantee of suitability for use in a CSA 290.7 system as a product may have usage limitations, maintenance restrictions, or other attributes that would preclude its use in a plant environment. Finally, research is done to determine if there are any known exploits against the product by checking publically available databases that track this information.

The results of the market analysis is a matrix documenting features, limitations, vulnerabilities, assurance level, and associated costs. Ultimately, after gaining experience with various products, understanding their strengths and weaknesses and in what application or configuration they are best suited; recommendations will be made on how a particular tool or type of tool can be used to support compliance to 290.7, or the evaluation of compliance to 290.7.

In order to capture the breadth of information that this research will explore, the following sections describe the product types under investigation.

2.1 Product Type

As previously indicated, a product types can be one of access and identity management, boundary protection devices, detection devices, network and network-related devices, and security management.

2.1.1 Access and Identity Management

Access and identity management tools give the right individuals access to the right resources at the right times for the right reasons. They are broadly classified as access and identity managers and biometric systems and devices.

Access and identity managers are used to control cyber assets within a company's internal network. Services provided by access and identity managers may include directory services, access control, password managers, single sign-on, and security tokens.

Biometric systems and devices are used to authenticate individual using unique biometric properties of the individual such as eyes, fingers, or voice print. Biometric devices can accurately authenticate employees for physical access through doorways, entrances to restricted areas, and act as username and password credentials on workstations.

2.1.2 Boundary Protection Devices

Boundary protection involves the monitoring and control of information on an internal network to keep cyber assets protected from both cyber security risks originating in the outside world as well as

possible internal risks. Boundary protection devices are categorized as intrusion prevention systems (IPS), host intrusion prevention systems (HIPS), endpoint all-in-one security solutions, wireless intrusion prevention systems (WIPS), and unified threat management (UTM) systems.

An IPS detects, prevents, and logs intrusions using a set of policies and rules. For example, denying connections from a range of IP addresses known to host malware or limiting the range of ports that allow incoming connections are rules that can be configured in an IPS to mitigate potential incoming sources of cyber attack. An IPS will typically be used as the entry point for defence from the internet to the internal corporate LAN. To provide high availability, a failover unit can be placed after the first unit to provide redundant protection should the first unit fail to operate properly.

A HIPS is similar to an IPS except that the HIPS prevents threats at the host level and are thus usually seen on workstations and servers on the corporate LAN.

Endpoint all-in-one security solutions are software that run on a host workstation or server that implements a combination of security solutions such as anti-virus, anti-malware, firewall, data loss protection (DLP), file and removable media protection, application control, device control, and cold boot attack protection. Such integrated solutions must be designed to use minimal computer resources in order to ensure that computer performance is maintained in order to avoid adversely affecting employee productivity.

A WIPS is an IPS that protects against wireless intrusion threat vectors by continuously scanning all wireless bands capable of connecting to Wi-Fi endpoints. Proper implementation of a WIPS significantly reduces the risk inherent to wireless technologies by controlling access so that only approved devices are allowed on the network, and otherwise isolating or completely denying access to non-approved devices.

UTM devices are all-in-one threat management systems that combine the functionality of an IPS device with anti-virus, anti-malware, anti-spam, web filtering, state-inspection firewall and IPSec VPN. As such, UTM devices are typically used to prevent threats from the Internet from making their way onto the corporate LAN. As with IPS devices, UTM devices are often partnered with redundant devices in order to minimize downtime in the event of a failure with the primary device.

2.1.3 Detection Devices

Detection devices detect cyber intrusions at the host and network level and are typically classified as file activity monitors, intrusion detection systems (IDS), or multi-engine anti-virus solutions.

File activity monitoring is used on a host workstation to detect designated unauthorized file and folder changes such as permission changes, moves, copies, and deletions.

IDSs are similar to the previously discussed IPS systems, except that an IDS is only able to detect threats while an IPS is able to both detect and attempt to clean or fix the threat. Because of limited functionality compared to IPS systems, IDS systems are slowly being phased out in favour of IPS systems.

Multi-engine anti-virus solutions aim to increase the virus detection rate through diversity – running multiple anti-virus scanners from multiple vendors simultaneously.

2.1.4 Network and Network-Related Devices

Network and network-related devices are the devices that connect disparate devices into one integrated network, and range in complexity from a simple switch connecting multiple end-user devices to a virtual private network (VPN) connecting external users to the internal corporate network via virtual "tunnels".

Firewalls are devices with a set of rules that are used to control connections in and out of a network. A firewall can consist of a hardware-only device or a software firewall needing to run on a server. Since the Internet is a high-risk entry point into a corporate network, firewalls are typically used to control incoming and outgoing connections as needed.

Routers are used to route and restrict traffic between different networks.

Switches route traffic between devices on the same network. There are two types of switches: unmanaged and managed. An unmanaged switch simply routes traffic as requested whereas a managed switch provides the ability to configure, manage, and monitor network traffic.

Virtual private networks (VPN) allow for the corporate network to be securely extended across the Internet, allowing employees to connect to the corporate network via a secure encrypted line through the internet.

2.1.5 Security Management

Security management is the identification of an organization's cyber assets, followed by the development, documentation, and implementation of policies and procedures for protecting those cyber assets [2].

Incident response is the ability for a corporation to detect, respond and recover from a cyber attack. Various tools are available for detecting and logging intrusions and performing forensics in order to identify the source of the intrusion and whether data was compromised. Incident response as a service is also available, which is a subscription-type service with 24/7 support via Internet and telephone support.

Finally, system information and event management (SIEM) gives the ability to gather logs from each cyber asset and analyze them in a way that provides feedback to determine if a cyber attack is underway or has already happened. SIEM can be provided as software, appliances, or via a subscription service, although the latter may not be a viable option for organizations that do not want to share information with a service provider over a public network. SIEM tools are also used to log security data and generate reports for compliance auditing purposes.

2.2 Common Criteria and FIPS-140 Methods

Common Criteria provides and assurance level as to how well a product complies with cyber security standards. Specifically, a Common Criteria evaluation involves testing a product at an independent and certified testing facility and then evaluating and accrediting the product for conformance to the Common Criteria for IT Security Evaluation (ISO Standard 15408). Products are granted a certificate with an Evaluation Assurance Level (EAL) [3] which quantifies the product's adherence to Security Assurance Requirements (SAR) on a scale of 1 (low) to 7 (high). A SAR describes the procedures taken during development and evaluation of the product to assure compliance with the claimed security functionality [4].

FIPS-140-1 and 140-2 are a set of security requirements for cryptographic modules. There is a Cryptographic and Security Testing (CST) laboratory that performs conformance testing of cryptographic modules to ensure compliance to the requirements set forth in the National Voluntary Laboratory Accreditation Program (NVLAP) [5]. Modules validated as conforming to FIPS 140-1 and FIPS 140-2 are accepted by the Federal Agencies of both the United States and Canada for the protection of sensitive information. It should be noted that unvalidated cryptography is viewed by NIST as providing no protection to the information or data. The Canadian Government provides a listing of approved cryptographic algorithms via Communications Security Establishment Canada. For the purposes of the technology survey, the outcomes for products that have been assessed under Common Criteria or FIPS-140-1 and 140-2 are captured in the product evaluation matrix.

2.3 Vulnerability Assessment

The final part of a product evaluation is a vulnerability assessment. Vulnerabilities were identified by searching for exploits that have been identified in the real world. Sources of vulnerability include the National Vulnerability Database (NVD) maintained by the National Institute of Standards and Technology (NIST) which is sponsored by the U. S. Department of Homeland Security (DHS), as well as the Canadian Cyber Incident Response Centre which circulates security bulletins that communicate information about security updates to software that were found to be vulnerable to specific flaws in software design, use or implementation.

3. Cyber Secure Industrial Remote Monitoring and Control Demonstration System

The Cyber Secure Industrial Remote Monitoring and Control Demonstration System is a prototype cyber security demonstration system at CNL. It is designed to give CNL an initial testing capability for evaluating cyber tool functions and features and how they might be used to support CSA 290.7 compliance. The demonstration system has been designed around a reference architecture that uses a defence-in-depth strategy as required by CSA 290.7, allowing for different cyber security products (intrusion detection systems, firewalls, web filters, Virtual Private Networks (VPN), etc.) to be tested against postulated threat vectors. Lessons learned and experience gained through the design and operation of the demonstration system will be used in the implementation of the full-scale cyber secure test bed.

The strength of the demonstration system is that it not only allows for simulation of a traditional industrial control system (ICS) in which the ICS is in a segmented zone within the corporate network, but that it also allows for simulation of the remote monitoring and operation of the control system. This builds on previous work done by CNL on Cyber Security for Remote Monitoring and Control of Small Reactors [6] which assessed the possibility of using satellite communications for the remote monitoring of small unmanned reactors in remote locations such as remote northern communities or mining camps.

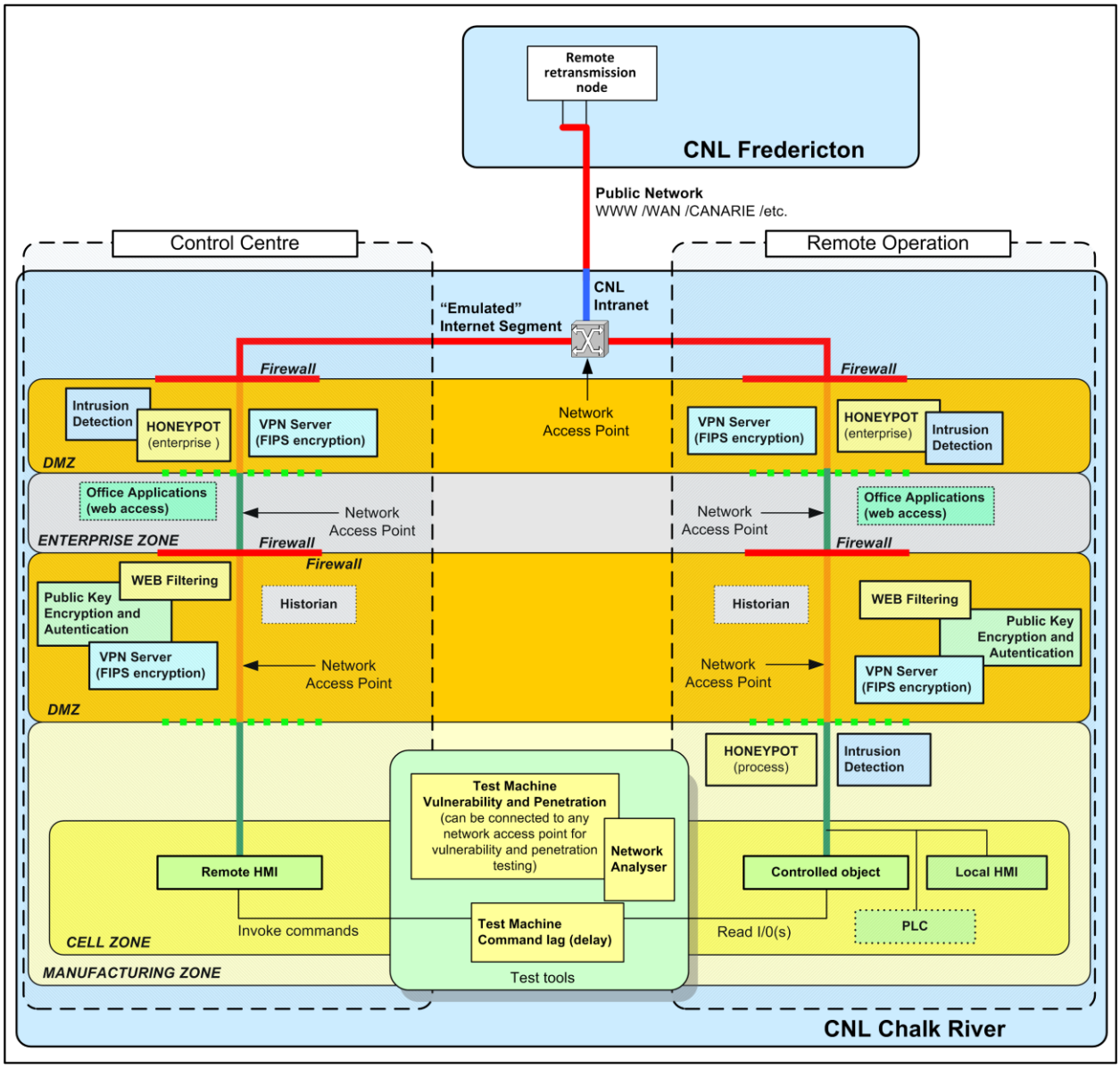

Figure 1 Demonstration System Architecture

As shown in Figure 1, the demonstration system is logically divided into “Control Centre” and “Remote Operation” partitions. The “Control Centre” partition simulates the location where the system operators are physically located, while the “Remote Operation” partition simulates the system under control. For realistic simulation of remote operations, communications can be routed between CNL’s Deep River, Ontario location and CNL’s Fredericton, New Brunswick location. To simulate longer delays, such as would occur over satellite communication links, test tools can be used to interject command lags.

Both the simulated control centre and the remote system under control are segmented into zones. Adjacent zones are separated by Demilitarized Zones (DMZ). The boundaries of each zone are protected by paired firewalls. Paired firewalls prevent direct communication between the zones. The effectiveness of this solution is illustrated in Figure 2 which is a reference architecture that originates from the NIST guideline [7].

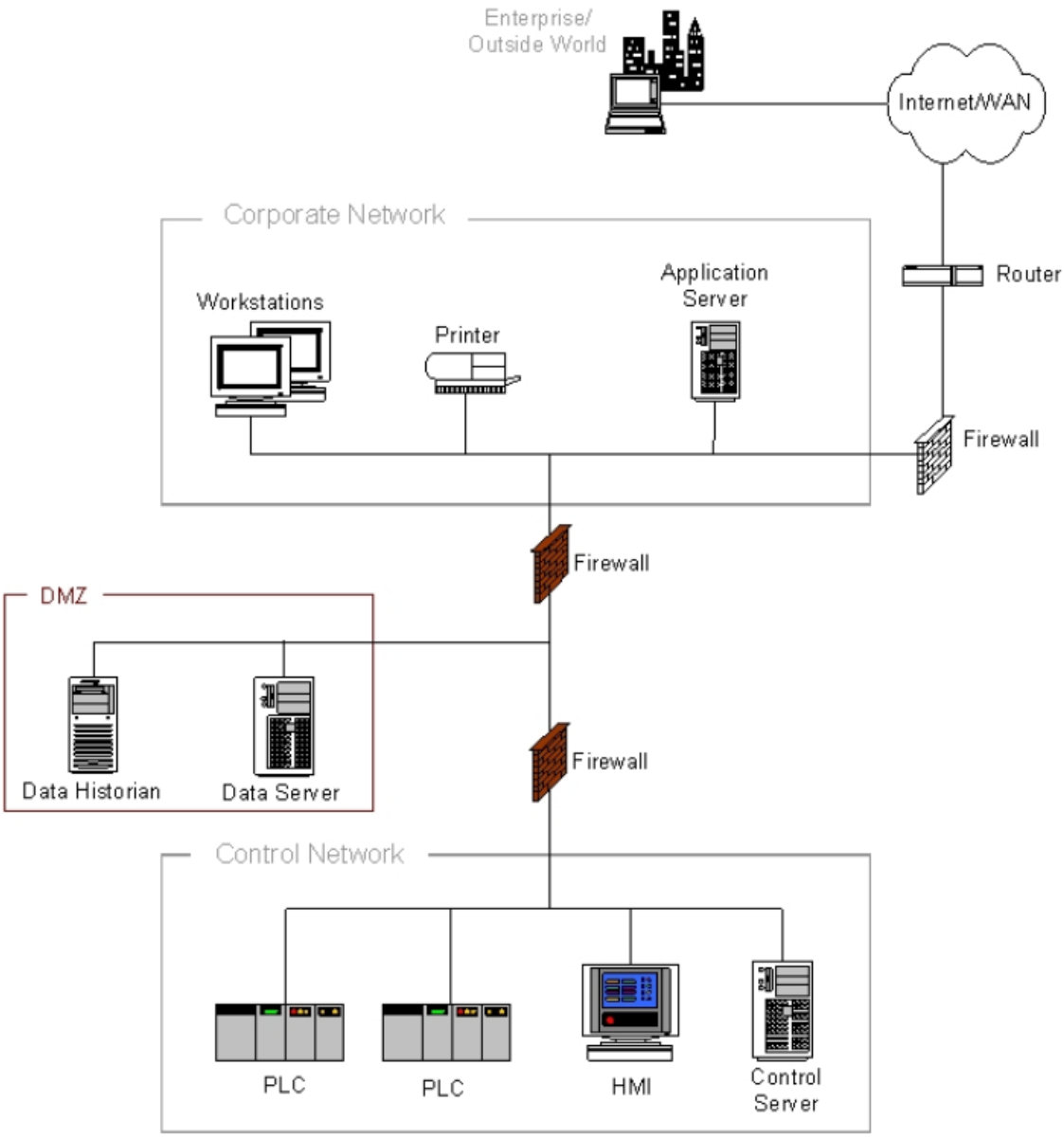

Figure 2 Paired Firewalls between Corporate Network and Control Network

Zones are an effective way to group assets according to their security importance and allows for the applications of security measures by zone as opposed to being applied uniquely to each separate equipment item. This requires that cyber assets be inventoried to ensure that no equipment is overlooked that, while benign in of itself, may in fact be a conduit to more sensitive information or safety-important cyber assets and thus require security at the same level of the cyber asset to which it is connected. The inventory includes identifying the importance of each asset, personnel who interface with each asset, current safe-guarding practices, etc., so that a complete profile of the state of each asset can be determined and used to drive the development of a security strategy [6].

The reference architecture shown in Figure 2 demonstrates the scenario in which analysts working on the main corporate network require process values from the control network. Rather than access the control network directly, the analyst accesses a data historian in the DMZ and the data historian is able to receive values pushed up from the control network while the paired firewalls prevent the corporate and control networks from directly communicating with each other.

Using the zone-based security approach, lower-level security zones are prevented from communicating to higher level zones. In the demonstration system, both the simulated control centre and the simulated system under control are at the same zone, but because they are physically separated, any communication between the control centre and the system under control must pass through zones with a lower level of security.

This apparent conundrum is resolved using virtual point-to-point (P2P) tunnelling protocols and VPN communications. The P2P connection combined with traffic encryption make it possible to virtually extend private networks over shared communications; VPN servers hosted in different zones allow for establishing virtual P2P connections between the zones.

4. Conclusions and Future Work

CNL is leveraging previous research and experience in cyber security by embarking on a multi-year research effort into cyber security for nuclear power plants and small reactor facilities. The ultimate goal of this research is to identify the tools, techniques, and best practices that can be used to assist facility operators in implementing cyber security solutions that are effective and practical and that can be used by the regulator to assess implementation plans.

In the past fiscal year, CNL's cyber security research program has begun to identify potential products that can be used for access and identity management, boundary protection, cyber intrusion detection, network protection and management, and security management. As well a Cyber Secure Industrial Remote Monitoring and Control Demonstration system was constructed as a first iteration at assembling a test bed in order to support testing of cyber secure architectures and products under various risk conditions.

The next phase of research will build on these results. Firstly, knowledge obtained during the construction of the demonstration system will be used to design a full-scale cyber secure test bed. To the largest extent possible, this will be done with actual plant network designs in mind to ensure that results obtained are relevant to nuclear operators. Using the test bed, promising cyber security products and tools identified through the technology survey will be systematically exercised and evaluated. The research will yield practical solutions that take into account the unique strengths and constraints of the nuclear industry.

5. References

[1] "Cyber security for nuclear power plants and small reactor facilities", CSA Standard N290.7-14, 2014.

[2] "SAINT - NERC compliance", SAINT Corporation. [Online]. Available: https://www.saintcorporation.com/solutions/NERC.html. [Accessed 13 April 2015].

[3] "Product compliant list", National Information Assurance Partnership Evaluation & Validation Scheme. [Online]. Available: https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm. [Accessed 13 April 2015].

[4] "Common criteria scheme", Communications Security Establishment, 7 April 2015. [Online]. Available: https://www.cse-cst.gc.ca/en/canadian-common-criteria-scheme/main. [Accessed 13 April 2015].

[5] "Security requirements for cryptographic modules", Federal Information Processing Standards Publication FIPS PUB 140-2, 2001 [Online]. Available: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. [Accessed 13 April 2015]

[6] D. Trask, C. Jung, and M. MacDonald, "Cyber security for remote monitoring and control of small reactors", The 19th Pacific Basin Nuclear Conference (PBNC 2014), Vancouver, British Columbia, Canada 2014 August 24-28

[7] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ICS) security", National Institute of Standards and Technology (NIST) Special Publication 800-82, 2011 June.