ISSN 0511-5728
The West Indian Journal of Engineering
Vol.44, No.1, July 2021, pp.4-10

Effectiveness of Paired Next Generation Firewalls in Securing Industrial Automation and Control Systems: A Case Study

Eddison Jaggernauth [a,Ψ]; and Sean Rocke [b]

Department of Electrical and Computer Engineering, The University of the West Indies, St. Augustine, Trinidad and Tobago, West Indies;

[a]Email: eddison.jaggernauth@icloud.com
[b] Email: sean.rocke@sta.uwi.edu

[Ψ] *Corresponding Author*

(Received 22 December 2020; Revised 26 March 2021; Accepted 10 May 2021)

Abstract: *Industrial automation and control systems (IACS) are oftentimes the backbone of businesses and critical infrastructure (CI) around the world. They underpin control of nuclear plants, refineries, manufacturing and distribution systems. Today, organisations are routinely targeted by cyber-attackers. Cyberattacks have been increasing in frequency and sophistication. This is especially true of those attacks directed against high-profile operations such as petrochemical refineries. Attackers invest considerable time and money to study a target and probe inherent weaknesses, which they eventually attempt, and succeed in some cases, to exploit. Historically, industrial networks were kept separate from corporate networks. However, significant efficiency gains and demands for digital interconnectivity have driven a convergence between operational technology (OT) and information technology (IT) systems. The business of cybersecurity has been evolving dramatically, posing significant challenges to management teams, across all industries and business domains. Countries within the Caribbean, such as Trinidad and Tobago (T&T), are by no means an exception given their dependence on the energy sector and supporting IACSs. This paper examines the effectiveness of next generation firewalls (NGFWs) in their defense of Process Control Networks (PCNs) against malware. It focuses on the case of a process plant complex in T&T.*

Keywords: *Industrial Automation and Control Systems (IACSs), Information Technology (IT), Operational Technology (OT), Next Generation Firewalls (NGFWs), Process Control Networks (PCNs)*

1. Introduction

The demand for information and communications technology (ICT) services is ever increasing as people and businesses desire to be more connected. This is evidenced by the emergence of the fifth generation (5G) networks and prospects of the Fourth Industrial Revolution (Industry 4.0). While Industry 4.0 has been of increased prominence in recent times, it is important to note that legacy Industrial Automation and Control Systems (IACSs) were engineered using cyber-technologies and tools from as early as the 1970s. The IACSs include: Distributed Control Systems (DCSs), Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) and Process Control Networks (PCNs). This is in part due to the recognised benefits that cyber-technologies could provide for operations and management of PCNs and SCADA systems.

While the Internet of Things (IoTs) and Industrial Internet of Things (IIoT) improve the efficiency of remote monitoring and control of Process Control Networks (PCNs) and corporate networks, these technologies introduce security risk. Amongst these is the inherent vulnerability to cyber-attacks (Piggin, 2018).

Oversight agencies have compiled regulations and security standards to secure critical infrastructure (CI).. US-CERT (2006), under the remit of the Department of Homeland Security (DHS), established a Control Systems Security Programme (CSSP) of the National Cyber Security Division (NCSD). Its mandate includes the identification, analysis and reduction of cyber-risks associated with control systems. Table 1 enumerates other noteworthy IACS standards.

This paper provides a high-level insight into a case study undertaken within the energy sector of Trinidad and Tobago (T&T). The research findings are based on a real PCN production system rather than simulation-based data. A succinct overview of Next Generation Firewalls (NGFWs) and their role in cybersecurity are also included. A mix of industry experience, referenced scholarly content, and consultation of peers and solution providers, have provided support information, for the case study.

Every attempt has been made to anonymise organisation and vendor-sensitive information accessed, as part of the research initiative. The main study objectives were to:

https://doi.org/10.47412/MARQ2173

Table 1. IACS Security Standards Based on Public Citations

Document (s)	Publisher
Good Practice Guide. Process Control and SCADA Security.	Centre for the Protection of National Infrastructure (CPNI).
Cyber Security Procurement Language for Control Systems.	Department of Homeland Security (DHS).
21 Steps to Improve Cyber Security of SCADA Networks.	U.S Department of Energy (DOE).
CIP-002-1-CIP-009-1.	North American Electric Reliability Corporation (NERC).
Guide to Industrial Control Systems (IACS) Security.	National Institute of Standards and Technology (NIST).
System Protection Profile – Industrial Control Systems.	National Institute of Standards and Technology (NIST).
ANSI/ISA-99/ ISA62433	The International Society of Automation (ISA).
Cyber Security for Critical Infrastructure Protection.	U.S Government Accountability Office (U.S GAO).

Source: Adapted from Sommestad et al. (2010)

1) Monitor a production PCN and an interconnected corporate LAN, for a one (1) month period, to capture statistics relating to the number of failed and successful penetrations of the PCN.
2) Test the hypothesis that having paired NGFWs minimise the risk of PCN threat penetration, from connected networks, by at least 50 %, and
3) Perform a cybersecurity audit and present recommendations for improvement, consistent with NIST SP 800-82 and ISA62443 standards.

The succeeding sections include an overview of cybercrime. This is followed by a summary of PCNs - their architecture, and some documented attacks against them. Highlights of Commercial Off The Shelf (COTS) products which support IACS cybersecurity is next. This is followed by an introduction to NGFWs. The paper then describes the research framework and presents the high-level results obtained. The paper ends with prospective steps.

2. Cybercrime on the Rise

A joint study between Accenture and Ponemon Institute suggested that out of approximately 1,000 cyberattacks, malware was the most prevalentoverall and, in many countries, the most expensive to resolve (Accenture, 2019). People-based attacks demonstrated some of the largest increases over that year. Ransomware attacks increased by 15 percent over one year and had more than tripled in frequency over two years. Phishing and social engineering attacks were experienced by 85 percent of organisations - an increase of 16 percent over one year. Those were disconcerting as people continued to be a weak link in cybersecurity defense. Figure 1 provides a comparison of average annual cost of cybercrime based on the study.

ICS-CERT (2016) conducted assessments in 12 of the 16 CI sectors in 2016. Those included the Chemical (7 assessments), Commercial Facilities (4), Communications (5), Critical Manufacturing (5), Dams (2), Emergency Services (3), Energy (22), Food and Agriculture (3), Government Facilities (10), Information Technology (3), Transportation Systems (10), and Water and Wastewater Systems (56).

The Water and Wastewater Systems and Energy Sectors, represented 60 percent of the overage assessments. Those industries were both heavily dependent on IACS to manage operational processes. Table 2 highlights the most prevalent weaknesses.

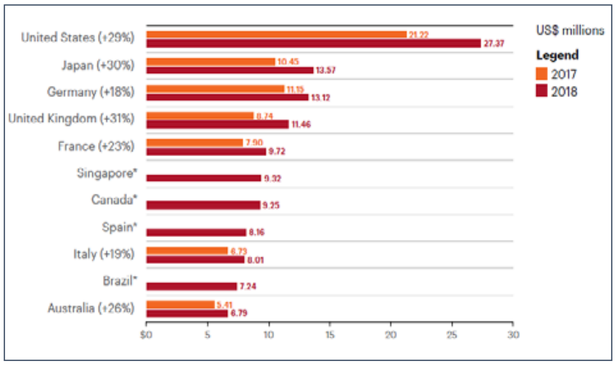

Figure 1. Average Annual Cost of Cybercrime by Country
Source: Abstracted from Accenture and Ponemon (2019)

3. PCN Architectures

A plant network may be considered as having four (4) layers or levels. Honeywell (2016) based on its Purdue model defines these levels as per Table 3 and Figure 2. ISA 62443 and NIST SP 800-82 also define similar levels.

Level 1 nodes are the heart of the control system. This network segment contains controllers, connections for servers and operator stations, supervisory control, connection to Level 1 and protection for Level 1, with access lists.

Level 2 nodes are the primary server, view and advanced control nodes for the process control system. Examples of Level 2 nodes include servers, stations, Advanced Control Environment (ACE) nodes, and Process History Database (PHD) collector nodes. These nodes are essential for operation of the process, but not as critical to control as the Level 1 nodes.

Level 3 nodes provide connections for Historians and Advanced Control. It also provides routing and access list controls.

Level 3.5 typical nodes are: Windows Server Update Services (WSUS), Anti-Virus Server, and Terminal Server. This level provides connectivity for devices to be accessed from the Corporate LAN and PCN. It forms a security zone between the PCN and outside networks.

Table 2. Risk Associated with FY 2016 Most Prevalent Weaknesses

Weakness Area (by Rank)	**Risk**
Boundary Protection	Undetected unauthorised activity in critical systems and weaker boundaries between IACS and enterprise networks.
Least Functionality	Increased vectors for malicious party access to critical systems and Rogue internal access established.
Identification and Authentication	Lack of accountability and traceability for compromised account and increased difficulty in securing accounts as personnel leave the organisation.
Physical Access Control	Unauthorised physical access to field equipment and locations provides increased opportunity to: Maliciously modify, delete, or copy device programmes and firmware, access the IACS network, steal or vandalise cyber assets and add rogue devices to capture and retransmit network traffic.
Audit Review, Analysis and Reporting	Without formalised review and validation of logs, unauthorised users, applications, or other unauthorised events may operate in the ICS network undetected detection.
Authenticator Management	Compromised unsecured password communications and password compromise could allow trusted unauthorised access to systems.

Source: Adapted from ICS-Cert (2016)

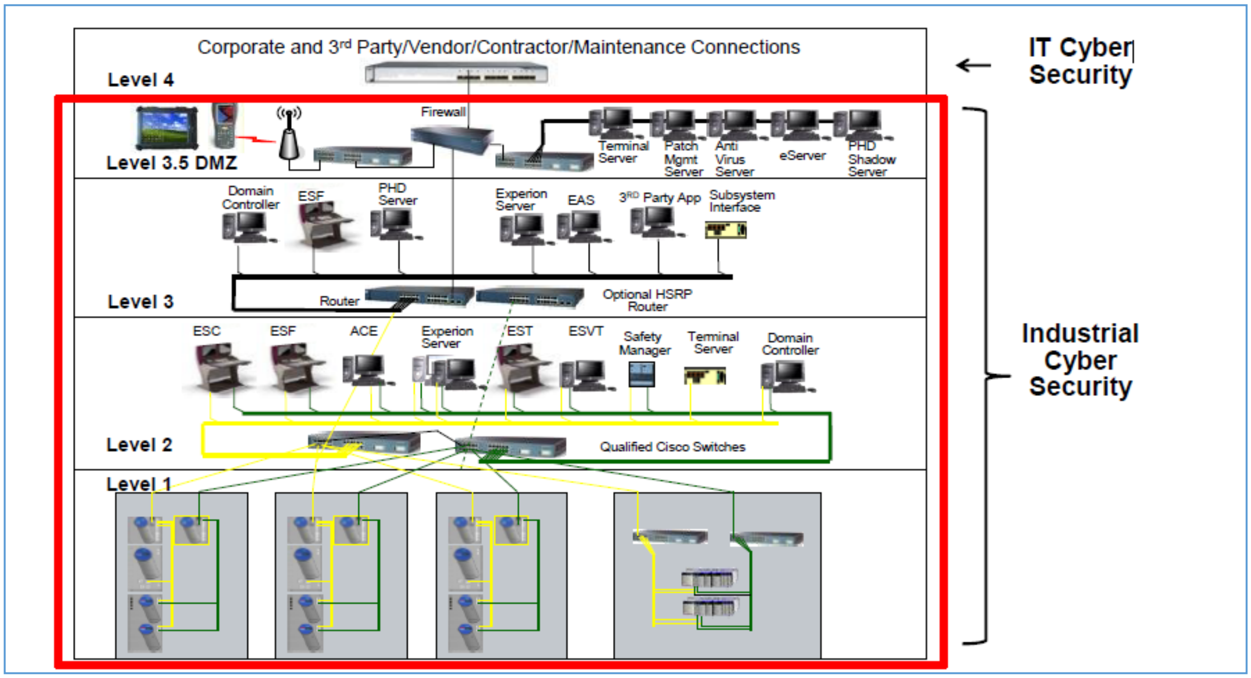

Figure 2. Depiction of Typical PCN 4 Level Architecture
Source: Based on Honeywell (2016)

Table 3. Plant Network Levels

Level	**Node Descriptions**
4	Plant Level Applications; clients for Historians and Advanced Control Applications.
3	Alarm servers and Advanced Applications (Non-Critical Control Applications).
3.5	Demilitarised Zones (DMZ) accessed from the Business LAN and the PCN.
2	DCS Stations, Supervisory Control, Operator Human Machine Interface (HMI) and Supervisory Controllers.
1	Real Time Control (controllers and Input - Output (IO)).

Source: Based on Honeywell (2016)

Level 4 is not part of the control network. It is usually managed by the Business IT department, separated by firewall and utilises open system LAN technology.

4. PCN Threats

Researchers continue to propose security enhancements for IACSs. However, there is scope for new research and subsequent solutions for securing control systems. These typically have their own specificity, when compared with securing traditional ICT networks (Cárdenas et al., 2011).

Credible threats that have penetrated PCNs include the Stuxnet worm. This is a malware which has the ability to reprogramme process plant controllers. Stuxnet can have malicious consequences, and it is inherently very difficult to detect by ICT defense systems. It exploits zero-day vulnerabilities, and as such, anti-virus software is not sufficient to preempt an attack (FortiGuard Centre 2016).

Cárdenas et al. (2011) suggested that the Stuxnet worm was one of the first cyber-attack against a SCADA system. The worm is extremely complex in design and targets specific IACS vulnerabilities. It was discovered as a programme, which spies on and reprogrammes IACSs; this is consistent with the work personified by FortiGuard Centre (2016).

Table 4. IACS Cybersecurity Incidents are Escalating

Year	Event	Year	Event
2000	A former employee of Hunter Watertech, the automation supplier to Maroochy Shire, took control of the wastewater management system, and released approximately 80,000 liters of sewage into local parks, rivers and the grounds hotel.	2013	Drug traffickers caught hacking into Antwerp container management system to locate containers with hidden drugs. The attack commenced with malicious software being emailed to staff, allowing remote access.
2003	The Davis-Besse nuclear power plant in Ohio, US, was infected with the Microsoft SQL "Slammer" worm, which resulted in a five-hour loss of safety monitoring.	2013	Alleged Iranian proxy hacktivist group attacked the Haifa Camel Tunnels - the largest tunnels in Israel - resulting in multiple closures over several days.
2005	Several rounds of Internet Worm infections disabled 13 of Daimler Chrystler's US automotive manufacturing plants offline for almost an hour. The Worm mainly affected Microsoft Windows 2000 systems, and (earlier versions) of Microsoft Windows XP.	2014	The Energetic Bear group, thought to be responsible for a reconnaissance malware designed to "discover" SCADA systems, that was detected on 2014 July 01; it targeted energy facilities located mainly in Europe and North America.
2010	Stuxnet worm discovered as the first IACS worm used to attack the Iranian nuclear programme and other targets.	2015	A Ukraine power company suffered from a power outage that impacted large regional area, the attack was carried out by hackers using Black Energy malware. The bug was planted into company's network using spam emails.
2011	Hack attacks on water utilities in the US widely reported, such as the Houston waste water intrusion by the hacker known as 'pr0f'.	2016	Thousands of computers in Saudi Arabia's civil aviation agency and other Gulf State organisations wiped in a second Shamoon malware attack.
2011	Duqu reconnaissance malware discovered and software components linked to Stuxnet. Duqu was a Trojan target at IACS vendors in Europe in order to gather data and cryptographic keys to authenticate software, for use in future attacks.	2016	Cyber-attackers tripped breakers, in 30 substations, turning off electricity to 225,000 customers in a second attack.
2013	Telvent attacked, allegedly by a highly active Chinese group. Attackers installed malicious software and stole SCADA project files.	2017	APT33: An alleged Iran-linked cyber-espionage group commenced attacks on the aviation and energy sectors.

Source: Adapted from Piggin (2014), and Hemsley and Ronald (2018)

In 2012, malware was discovered at a power plant when an employee was experiencing issues with a Universal Serial Bus (USB) drive in the United States. The USB drive was routinely used for backing up control systems configurations within the control system environment. The employee asked an IT person to check the USB drive. The IT staff inserted the drive into a computer with up-to-date anti-virus software.

The software identified three (3) malware hits. Two (2) were common malware and one was a sophisticated malware. Two engineering workstations were infected with the advanced malware (RISI, 2018).

According to Cardenas et al. (2011), there was a Siberian Pipeline Explosion, in 1982, whereby a Trojan penetrated a SCADA system software, which subsequently led to an explosion. In 2000, hackers seized control of a Russian natural gas pipeline. In that same year, in Maroorch Shire, an ex-employee gained unauthorised access into the SCADA system, of a sewage treatment plant using a wireless Internet device, and triggered some "accidents".

In 2014, the Energetic Bear group was thought to be the mastermind behind a SCADA reconnaissance malware that targeted energy facilities in North America and Europe (Piggin, 2014). New IACSs-attacking malware, exhibits strains of rootkit engineered for control systems.

This software is oftentimes verified and electronically signed by trusted certificate authorities. As a result, it is very difficult to prevent and detect these attacks based solely on ICT information (Cardenas et al., 2011; FortGuard Centre, 2016; Hentea, 2008). Table 4 provides an overview of several documented IACS breaches across the globe.

5. Commercial Off The Shelf (COTS) IACS Solutions

There are several Commercial Off the Shelf (COTS) IACS solutions on the market. The Cyber Exposure Company provides visibility, security and control across operational technology (OT) environments. Tenable is a vulnerability management platform which helps organisations understand and reduce cybersecurity risks (CEA, 2020). Darktrace offers Darktrace Enterprise, an Artificial Intelligence (AI) cyber-defense solution that uses AI and Machine Learning (ML) to protect networks; and Darktrace Industrial, a specially designed tool used to identify threats and vulnerabilities in SCADA systems and IT networks.

The company also has Darktrace Cloud - Darktrace Software as a Solution (SaaS) product. It has adapted innovative mathematical models to IACS data for machines, networks, and users within environments, which spots previously unidentified anomalies in real-time (Darktrace, 2020).

In 2019, Honeywell launched a new industrial IoT analytics platform called Honeywell Forge which collects operational data, analyses that data and provides suggestions for infrastructure optimisation.

Honeywell Forge Cybersecurity Platform is a unified platform that enables consolidated, secure remote access to industrial plants and sites; scalable platform enabling asset discovery, inventory, monitoring, risk monitoring, secure file transfer with threat detection, automated updates (patches and virus signatures), and comprehensive activity logging. Cybersecurity as a service is one of the offerings of Honeywell Forge (Honeywell, 2020; CEA, 2020).

6. Next Generation Firewalls - What are They?

Traditional firewalls alone are not sufficient to protect the enterprise from dangers of the Internet. Next Generation Firewalls (NGFWs) equipped with advanced packet inspection functionality, and advanced reporting features can improve security around the access gateways (Skybakmoen, 2018).

NGFWs have added new features to better enforce policy (application and user) control or detect new threats. These include: additional Intrusion Prevention System (IPS) functionality, sandboxing and threat intelligence (Young and Pescatore, 2010). NGFWs provide more granular control within the firewall rules. They have the ability to allow or block content based on user access credentials or group membership, such as allowing only the Process Engineering team to use YouTube, for work purposes (Thomason, 2012).

Gartner (2020) defines NGFWs as deep-packet inspection firewalls that move beyond port/protocol inspection and blocking. They add application-level inspection, intrusion prevention, and bring intelligence from outside the firewall.

According to Thomason (2012), a minimum of five (5) basic requirements are essential to be classified as a NGFW.

1) It must have deep packet inspection ability and must be able to scan all files for threats, including encrypted files.
2) It must provide application intelligence with the ability to know what applications are traversing on http and https ports, and what each application is doing.
3) As NGFWs perform deeper analysis of packets, performance can become an issue. The system is still expected to perform all its functions at ‘wire’ speed.
4) A NGFW needs to have good reporting abilities which are easy to understand. It should provide much more than just the source and destination IP addresses and ports.
5) It needs to be manageable: Most system failures are due to human errors and misconfiguration. NGFWs will have sound interfaces which allow them to be managed centrally via a console.

7. Research Framework

The research endeavor reviewed existing literature and was supported by interviews with experts in the application space. The approach was to use real traffic, to monitor the IACS environment and the associated risks. An attempt was made to use that data, to identify markers that provide early indication of malicious behavior or behaviors that *run afoul of the organisation's policies*.

Event logging was enabled from the NGFW appliances to send their logs to a Syslog server. This previously existed on the Corporate LAN and was used for collecting logs from other existing Corporate LAN systems and applications. A new instance of Splunk was created on the Corporate LAN to read data from the Syslog Server, specific to the exercise (see Figure 3).

Rules were created on the PCN NGFW (NGFW_P) to allow its data to be incorporated into Splunk (analytics tool). NGFW_E represents the Corporate LAN perimeter defense appliance set. Initially, consideration for enabling a Mirrored Port on the main PCN switch was considered. The objective was to have a parallel set of PCN traffic copied to a laptop for analysis. However, the PCN solution provider advised against using that method, given the inherent risks.

8. Results and Analysis

The standard NGFW reporting tools were very useful in providing a summary of prospective threats, categorised as low, medium and high risks based on the devices’

Table 5. Firewall Considerations for PCNs

Recommendations	
The base rule set should be Deny All, Permit None. All permit rules should be both IP address and TCP/UDP port specific, if appropriate.	All rules shall restrict traffic to specific IP address or range of addresses.
All traffic on the PCN is typically based on routable IP protocols, either TCP/IP or UDP/IP. Any non-IP protocol should be dropped.	Prevent traffic from transiting directly from the PCN network to enterprise network. All traffic should terminate in the DMZ.
Any protocol allowed between PCN and Demilitarised (DMZ) is explicitly NOT allowed between DMZ and enterprise networks (and *vice versa*).	All outbound traffic from the PCN to the enterprise to be restricted by service and source and destination ports, using static firewall rules.
Allow outbound packets from the PCN or DMZ only if those packets have a correct source IP address assigned to the PCN/ DMZ devices.	All management traffic should be routed either via a secured (separate) management network or over an encrypted network with two-factor authentication. Traffic should also be restricted by IP address to specific management stations.
PCNs shall not be directly connected to the Internet, even if protected via a firewall. Consider deploying a DMZ with Control Zones to reduce the attack surface and increase the layers of PCN protection against attacks, emanating from the Internet.	Ports and services between PCN and an external network should be disabled. Access only granted based on specific business justification.

Source: Adapted from NISCC (2005) and Byres (2018)

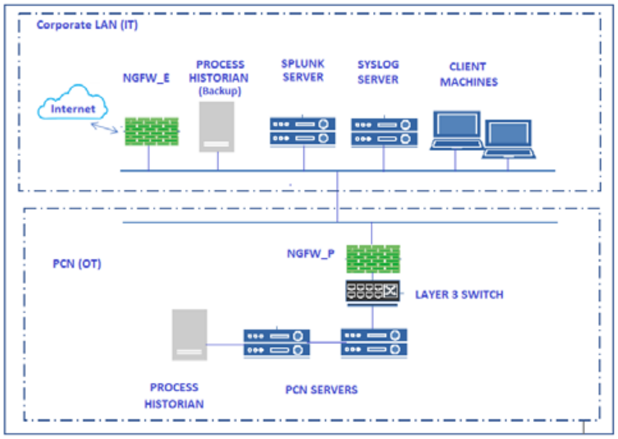

Figure 3. Depiction of Data Collection Architecture

preset criteria. Those datasets were further analysed using Splunk reports and Matlab.

Figure 4 provides a summary of the threats which emanated from the Internet. With the exception of the Bandwidth Consuming Application, the threats were mitigated by the NGFW_E, based on the configuration to restrict traffic based on specific parameters. Bandwidth Consuming Applications were initially considered as low risks based on the attendant rules defined within the (edge) NGFWs. Hence, this category was reviewed periodically and corrective action taken where necessary.

Reports from the NGFW_P, confirmed that no matching log data was available relating to Threat Detection and Data Exfiltration from the Corporate LAN. Therefore, from Top-Down perspective, it can be inferred that no observable malicious traffic needed to be filtered by NGFW_P. It was apparent, however, that the NGFW_P blocked events from within the PCN attempting to access the Internet, to upgrade their system software.

Subsequently, it was recommended that each of those blocked conversations be reviewed to identify the best means of disabling them rather than having the NGFW restrict them. That meant removing or disabling unnecessary services or closing the respective ports. Moreover, with the aid of Wireshark protocol analyser, it was determined that Modbus TCP, Network Time Protocol (NTP) and ARP messages were found to be allowed via the NGFW_P.

Engagement of the PCN vendor confirmed that NTP was allowed for time synchronisation, Modbus TCP traffic as was allowed for inter-device communications. A limited amount of ARP traffic was also allowed for network establishment.

Traffic and protocols which should have been allowed, consistent with the PCN, vendor's procedures and guide were assessed and corroborated against the recommendations in Table 5. Peers within the energy sector were also consulted to discern what levels of security they had to support their IACSs. It was apparent that most had a similar PCN architecture, designed by the same solution provider. However, various Security Information and Event Management (SIEM) tools were in use across the industry.

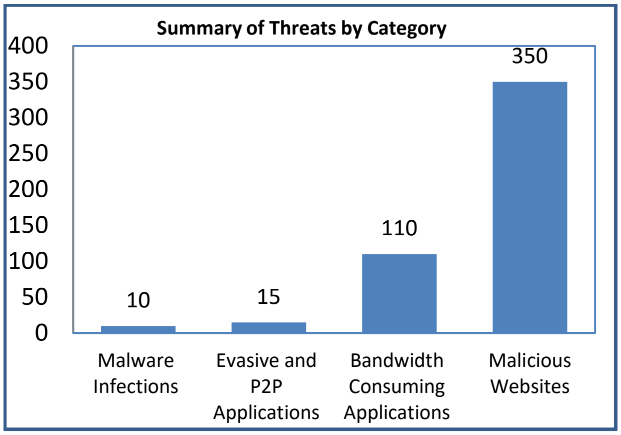

Figure 4. Summary of Threats Emanating at the Edge of the Corporate LAN

9. Conclusion and Future Work

The review of literature, expert feedback and data from a real PCN system corroborated each other. The interconnectivity of corporate networks with PCNs brings potential security threats. Nationally, companies have taken tangible steps to secure their CIs with access controls. The importance of protecting PCNs cannot be overstated, given the potential impact of a malicious attack. Consider the costs highlighted in Figure 1, and the threats mentioned within Section 4. Organisations must conduct the necessary risk assessments and endeavor to use contemporary tools as best as practicable. Naturally, an overarching security framework that assesses and treats with People, Process and Technology must be adopted. Inherent therein will be a critical role for NGFWs, considering the top (boundary protection) risks based on ICT-CERT (2016) study.

NGFW is an essential appliance in the defense against current and future cyber-threats in business networks and PCNs. For firewall considerations for PCN (see Table 5), the tool is not infallible and where possible, it should be used within a tiered architecture to have multiple layers of defense. NGFWs used within PCNs should be industry-grade with fault tolerance and online health monitoring functionality.

It was evident that the tiered NGFWs worked in complementary fashion. They allowed only trusted communication protocols and traffic to communicate across the two interconnected networks. The standard NGFW reports provided invaluable information regarding prospective threats. This was in keeping with the characteristics of NGFW highlighted by Thomason (2012). However, the entire architecture inclusive of the corporate network must continually be assessed. It cannot be overstated that a cybersecurity campaign requires the integration of People, Process and Technology. It is not a one-off process.

Based on the findings, it can be concluded that NGFWs do play an invaluable role in PCN cybersecurity. The hypothesis proved to be true that paired NGFWs do restrict malware by at least 50%. It is noteworthy that the associated literature to date, appears to be predominantly simulation – based data rather than data from production systems. Contrastingly, this research utilised actual data from a PCN in operation. A prospective next step is to engage in an in-depth assessment for a period of at least six (6) months. Additionally, using AI to support cybersecurity – end-user behaviour analytics across PCNs is currently being considered.

References:

Accenture (2019), *The Cost of Cybercrime Study 2017*, Accenture and Ponemon Institute, Accessed March 26, 2019. https://www.accenture.com/bg-en/insights/security/cost-cybercrime-study.

Byres, E. (2018), Interviewed with the Chief Technology Officer, Tofino ISA Committee Member/Consultant, December 12, 2018 (by author, via online).

Cárdenas, A.A., Amin, S., Lin, Z-S. Huang, Y-L., Huang, C-Y., and Sastry, S. (2011), "Attacks against process control systems: risk assessment, detection, and response", *Proceedings of the 6th ACM Symposium on Information, Computer and Communication Security (ASIACCS 2011)*, Hong Kong, China, March 22-24, pp. 355-366.

CEA (2020), "Cybersecurity Excellence Awards", https://cybersecurity-excellence-awards.com/

Darktrace (2020), "World leaders in Autonomous Cyber AI", Accessed December 01, 2020, https://www.darktrace.com/en/

FortiGuard Centre (2016), "Threat Research and Response", Accessed April 09, 2017. http://www.fortiguard.com/antivirus/.

Gartner (2020), *Gartner IT Glossary 2020*, https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

Hemsley, K.E. and Ronald, E.F. (2018), "History of Industrial Control System Cyber Incidents", Accessed November 13, 2020. https://www.osti.gov/servlets/purl/1505628/

Hentea, M. (2008), "Improving security for SCADA control systems", *Interdisciplinary Journal of Information, Knowledge, and Management*, Vol.3, No.1, pp.73-86.

Honeywell (2015), "Continuous Industrial Cyber Risk Mitigation with Managed Services Monitoring and Alerting". https://cupdf.com/document/continuous-industrial-cyber-risk-mitigation-with-managed-services-monitoring-58b8f83d936f4.html

Honeywell (2016), *Industrial Communication Protocols White Paper*, Honeywell, Sensing and Productivity Solutions, Accessed May 21, 2018. https://sensing.honeywell.com/honeywell-white-paper-communication-protocol-002415-1-en2.pdf

Honeywell (2020), "Honeywell Forge Cybersecurity Suite" https://www.honeywellprocess.com/EN-US/EXPLORE/PRODUCTS/FORGE-CYBERSECURITY/pages/default.aspx. Accessed December 01, 2020.

ICS-CERT (2016) *Annual Assessment Report Industrial Control Systems Cyber Emergency Response Team FY 2016*, ICS-CERT / National Cybersecurity and Communications Integration Center (NCCIC), Accessed December 01, 2020. https://uscert.cisa.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508c.pdf.

ISA (2016), *Standards for Industrial Automation and Control Systems*, Industrial Automation and Control, 62443.

NISCC (2005), *Good Practice Guide, On Firewall Deployment for SCADA and Process Control Networks*, National Infrastructure Security Co-ordination Centre / British Columbia Institute of Technology

NIST (2018), *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Accessed 29 March, 2019.

Piggin, R. (2014), "Industrial systems: Cyber-security's new battlefront", *Engineering and Technology*, Vol.9, No.8, pp.70-74.

Piggin, R. (2018), "Securing critical services: The Network and Information Systems (NIS) Directive", *ITNOW*, Vol.60, No.2, pp.58-61 DOI: 10.1093/itnow/bwy057

RISI (2018), *Online Incident Database 2018*, Accessed March 29, 2019. http://www.risidata.com/Database/event_date/desc

Skybakmoen, T. (2018), *NSS Labs - Next Generation Firewall Comparative Report: Security*, Fortinet (NASDAQ: FTNT), Accessed July 17, 2018.https://www.fortinet.com/resources-content/fortinet/assets/analyst-reports/file/nss-labs-2018-ngfw-comparative-report-security.

Sommestad, T., Ericsson, G.N., and Nordlander, J. (2010), "SCADA system cyber security: A comparison of standards", *Proceedings of the 2010 IEEE Power and Energy Society General Meeting*, July 25-29, Minneapolis, Minnesota, USA, pp. 1-8.

Thomason, S. (2012), "Improving network security: Next generation firewalls and advanced packet inspection devices", *Global Journal of Computer Science and Technology*, Vol.12, No.13, pp.47-50

US-CERT (2006), *Control System Documents*, United States Computer Emergency Readiness Team, Accessed April 09, 2017. http://www.us cert.gov/controlsystems/csdocuments.html.

Young, G., and Pescatore, J. (2010), "Magic Quadrant for Enterprise Network Firewalls", *Gartner RAS Core Research Note G00174908*, March; https://www.neteye-blog.com/wp-content/uploads/2010/03/gartnermq2010.pdf

Authors' Biographical Notes:

Eddison Jaggernauth *received his BSc (Hons) in Computing and Information Systems from The University of London, MBA from Heriot-Watt University, and MASc degree in Electrical and Computer Engineering, with a major in Communication Systems, from The University of the West Indies (UWI), St. Augustine. He is currently a PhD Candidate in Electrical and Computer Engineering at The UWI. He is also a Chartered IT Professional certified by the British Computer Society and a Project Management Institute certified Project Management Professional. His interest includes: IACS Cybersecurity, Deep Learning and Management Information Systems (MISs).*

Sean Rocke *received his BSc in Electrical and Computer Engineering from The University of the West Indies in 2002, his Masters in Communications Management and Operational Communications from Coventry University in 2004, and his PhD in Electrical and Computer Engineering from Worcester Polytechnic Institute in 2013. His areas of interest include signal processing and optimisation techniques relating to wireless communications management application and biosensor development and biological data mining, as well as and emergency communication systems.* ■