ON THE CHALLENGES OF ACHIEVING IEC 62443 SECURITY REQUIREMENTS IN TIME SENSITIVE INDUSTRIAL NETWORKS

Co-authored by

Student: Davison Zvabva

Primary advisor: Pavol Zavarsky

Secondary advisor: Sergey Butakov

Project report

Submitted to the Faculty of Graduate Studies,
Concordia University of Edmonton

In Partial Fulfillment of the
Requirements for the Final
Research Project for the Degree

MASTER OF INFORMATION SYSTEMS SECURITY MANAGEMENT

Concordia University of Edmonton

FACULTY OF GRADUATE STUDIES

Edmonton, Alberta

April 2018

On the Challenges of Achieving IEC 62443 Security Requirements in Time Sensitive Industrial Networks

Davison Zvabva, Pavol Zavarsky, Sergey Butakov
Concordia University of Edmonton
Edmonton, Alberta, Canada.
dzvabva@csa.concordia.ab.ca, {pavol.zavarsky, sergey.butakov}@concordia.ab.ca

***Abstract*—The IEC 62443 security standards introduce the concepts of zones, conduits, and security levels as a way of segmenting and isolating sub-systems of an industrial control network. Network segmentation physically/logically partition the control network into separate communication zones to restrict unnecessary flow of traffic between zones of different trust level. Firewalls with deep packet inspection capabilities for filtering industrial control protocols are indispensable elements in implementing important security principles, standards, and best practices of IEC 62443. While partitioning of the industrial control network and placement of multiple firewalls at various locations provides defense-in-depth against cyber-attacks, it is important to consider the impact of these firewalls on nodes distributing time critical communications. This paper attempts to (i) study network performance impact introduced by the implementation of multiple firewalls in Modbus TCP/IP industrial control networks following IEC 62443 security standards and (ii) evaluate if time constraint requirements for communications are achievable. The results reveal that the latency and jitters introduced by multilayered firewalls makes it challenging to achieve real-time communications in some industrial applications when strict IEC 62443 security standards are followed.**

Keywords—network segmentation, industrial firewall, deep packet inspection, security zone, security level, latency, jitter

I. INTRODUCTION

Industrial Automation and Control Systems (IACS) collectively describe automated systems that control industrial production covering a broad spectrum of computers, control devices and network architectures [1]. Power generation, transportation and water distribution are some of the examples that reflects the critical importance of these networks. IACS have significant and unique cyber security requirements when compared to corporate IT environments where the priority is on safeguarding confidentiality, integrity and availability of systems and data. In IACS availability of the system and data integrity are the ultimate priority to safeguard both human life and plant safety [2].

The Design Basis Threat [3] assumes adversaries have various possible modes of attacking an industrial infrastructure from multiple entry points, hence the traditional flat IACS network provides limited security as the defense solution at the perimeter only succeed in defending against external attacks yet anyone with access to the IACS environment can access it entirely [4]. Network segmentation is recommended as an effective defensive countermeasure to mitigate risks and ensure safe and reliable IACS operations [5].

Network segmentation also known as network compartmentalisation is a defense-in-depth approach to security that partition the network into separate segments with communications between systems and devices in different segments controlled by multiple firewalls at various locations [6]. The rationale for network segmentation in industrial networks is to protect network resources by limiting unnecessary flow of traffic between zones which in turn provide significant security benefits: (i) containment of cyber incidents between segments, (ii) limiting network access for successful attackers, (ii) limiting the adversary's lateral movement and ability to pivot and access sensitive portions of the network, and (iv) increasing system reliability and robustness [7].

While network segmentation as required by IEC 62443 standards is an important defense mechanism in the protection of IACS environments, it is equally important to carefully evaluate the introduction of firewalls [8]. The industrial firewalls protecting each zone boundary must have deep inspection capabilities to differentiate between well-formed packets and malicious payload and allow only specific commands through the control network [9], [10], [11], [12]. Deep packet inspection increases message processing which may lead to additional transmission latency, jitters and packet loss, in some domains with fast dynamics this may be unacceptable. The IEC 62443 standards fall short in providing clear guidance on how network segmentation using deep inspection filtering devices can be achieved in time sensitive industrial networks without impacting communications.

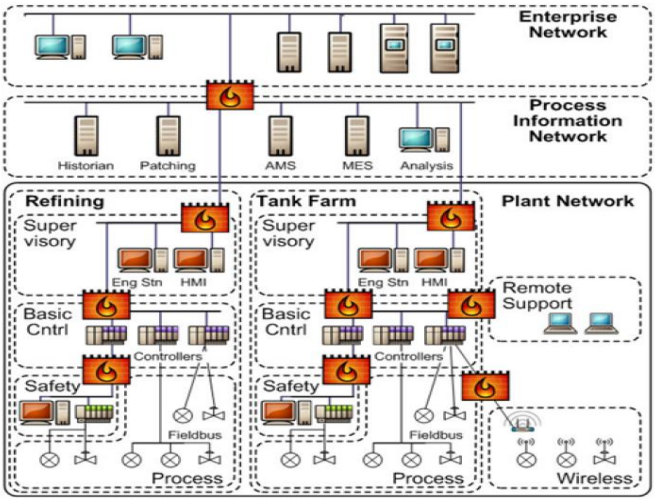

Fig. 1. An example of IACS segmentation using firewalls [6]

This paper presents an experimental evaluation of network packet latency, jitters and packet loss caused by the introduction of open source Linux firewalls in Modbus TCP/IP industrial networks following IEC 62443 security standards. In [8], [13] an open source Linux based firewall using iptables u32 match for deep packet inspection of IACS protocols is presented to show how organisations can leverage on the open source firewall solution to protect their networks. This study instead, takes into account the timing requirements in some IACS environments and seeks to evaluate latency, jitters and packet loss introduced when the open source firewall is implemented at multiple locations to protect segments of a partitioned industrial control network. The results of the evaluation will enable IACS operators to carefully consider the placement of security solutions in fast dynamic environments when implementing cybersecurity protections in accordance with best practices prescribed by prevailing standards and guidelines such as IEC 62443.

The remaining sections of this paper are organised as follows: Section II provides an overview of the related works. Section III presents the methodology, experimental setup and the tools used for the evaluation in our approach while Section IV reports on the various measurements and tests performed. Our findings are also discussed in this section. Finally, Section V presents the conclusion and future work.

II. Related Work

Part A provides a review of network segmentation in IACS, part B reviews industrial firewalls for IACS and part C presents a review of performance issues associated with firewall implementation on the network.

A. Network Segmentation for IACS Security

The Purdue Model for Control Hierarchy (PMCH) forms the baseline for IACS reference architecture [14]. The PMCH widely segments devices and equipment into hierarchical functions and it identifies five zones and six levels of operations as shown in Fig. 2. Best practices for the implementation of segmentation in IACS environments such as the IEC 62443 [6] and the Defensive Computer Security Architecture [9] are based on the baseline provided in the Purdue model. The high level segmented industrial network in Fig. 1 can be evaluated to see how it maps to the PMCH depicted in Fig. 2. The plant network maps to the cell/area zone of the PMCH whereas the supervisory zone (hosting the HMI and engineering workstations) and basic control zone (hosting controllers) maps to the Level 2: Area Supervisory Control and Level 1: Basic Control zones of the PMCH. The same mapping also exists for the process and safety zones respectively. However, in Fig.1 some zones of the partitioned network are separated by boundary firewalls.

Firewalls are indispensable elements in achieving network segmentation in industrial automation and control networks [9]. The firewalls enforce segmentation by monitoring and controlling communications at zone boundaries. This multiple layer protection strategy of having redundant security mechanisms overlap each other provides defense-in-depth and minimises the impact of failure of one mechanisms. If comprehensively implemented, defense-in-depth ensures the capability to detect, prevent, respond to, mitigate, and recover from any possible unauthorized acts within an industrial network [3].

Fig. 2. Purdue Model for Control Hierarchy [14]

The defense-in-depth approaches recommended for securing IACS are however not only associated with management complexity, but also possible packet delays, jitters and packet loss which may be an issue for time sensitive industrial applications. Unlike in traditional IT networks, in some IACS data transfer must be in real time, hence performance metrics such as minimal latency and timing jitter are critical for the requirements to be met [30]. IEEE standards for use of time sensitive networking in industrial networks [31] require bounded low latency and low jitter to ensure real time data transfer between communicating industrial devices and applications. In a segmented industrial automation and control network, communications for devices in different zones may pass through multiple firewalls located at different zone boundaries leading to increased latency, jitter, packet loss and failure to meet the expected time requirements.

B. Industrial Firewalls for IACS

Firewalls for industrial automation and control system protection known as industrial firewalls come from various vendors and have deep inspection capability to filter data commands at the application layer [10]. An example of an industrial firewall solution for Modbus TCP/IP protocol is presented in [11]. The solution consists of three components: the physical security appliance that is placed at network segment boundaries; the loadable security modules that provides predefined firewall rules through software plugins and the configuration management platform that enables configuration of the appliance. The firewall can be configured to allow limited read only commands from trusted devices in different network segments and block any unauthorised messages that change settings and integrity of data or programs.

A network filtering approach to timely detect and mitigate attacks targeting SCADA environments based on the concept of critical state where an attacker has to modify the state of an industrial system from secure to critical in order to damage is

presented in [15]. The critical state model predicts whether the system is leading to a critical state by tracking changes of critical state distance and providing an early warning. However, anomaly-based firewalls may lead to false negatives and false positives a situation that is unacceptable in some time sensitive IACS environments.

Hachana et al. [16] examined the limitations of security solutions borrowed from IT environment in mitigating attacks in industrial control networks through simulations of Modbus TCP/IP fuzzing, flooding and operational oriented attacks in an environment protected by an SiN40 industrial firewall. It is reported that the industrial firewall is not able to stop operational oriented attacks that are specific to industrial process networks. It is proposed that an Organization Based Access Control (ORBAC) model providing flexible and dynamic contextual security rules fitting the requirements of the complex SCADA security needs be implemented in a firewall. The proposed model requires buffering several sessions of communications a situation that may result in network latency issues.

Nivethan and Papa in [8], [13] experimentally evaluated the use of open source firewalls for dynamic inspection of DNP3 and Modbus TCP/IP message payloads using iptables firewall's advanced u32 match feature that goes beyond the normal header filtering on TCP/IP packets. It is demonstrated that iptables u32 feature could be extended in open source Linux firewall to provide deep packet inspection filtering for IACS protocols. For example, in [13] firewall rules for deep inspection of most common Modbus TCP/IP attacks were configured and successfully tested to validate if they could stop the malicious traffic reaching the slave nodes. Our study leverages on the open source firewall proposed in [13] and seeks to evaluate whether the solution can achieve timing requirements for communications when implemented in a multilayered approach to enforce zone boundary protection.

C. Industrial Firewall Performance Issues in IACS

In IACS, the underlying TCP/IP network is an important communication link for the various sub-systems. Any network delays or failure as a result of implementation of security measures will impact the performance of the entire IACS network [32]. A cybersecurity testbest designed by NIST to measure the performance impact of introducing security protections in networked control systems [17], provides fifteeen quantitative dynamic metrics for measuring network performance in IACS environments. Our study focuses on three of these critical performance measures namely packet path delays (latency), packet delay jitter and packet loss.

The deployment of dedicated firewalls in industrial control networks should be carefully considered as firewalls introduce additional delay in transmission (latency) and reduce network throughput [8], [12]. It is further noted that regardless of the performance of a firewall, a targeted denial of service attack may overload the firewall and affect the timely delivery of messages between nodes in different network segments, a situation that may impact reliability of the IACS system. The RFC 3511 [18] by the Internet Engineering Task Force (IETF) provides some important methodologies to benchmark the performance of firewalls. Four testing areas for firewall performance namely latency, forwarding, connection, and filtering are discussed. The IETF RFC 3511 document reflects the state of the knowledge almost fifteen years ago and is based on one size fits all environments.

The work in [19], [20], [21] reflects some of the several studies in existence on firewall performance analysis. The studies provide values for latency, jitters, packet loss and throughput obtained for standard protocols including TCP/IP, FTP, HTTP among others commonly found in the traditional IT environments and do not reflect those from specific firewall solutions adopted in industrial control networks. K. Salah et al. [19] evaluated the performance of a network firewall based on delays and throughput when a denial of service (DoS) attack is directed at filtering rules placed at the bottom of a complex and larger rule base. Similarly, Hayajneh et al. [20] evaluated the firewall performance and resiliency under various security attacks. They also show that regardless of firewalls' performance, DoS attacks result in communication delays.

Latency introduced in IACS networks by the Tofino industrial firewall with deep packet filtering of Modbus TCP/IP traffic is assessed in [17]. When the firewall's deep packet inspection features are enabled, latency is impacted by jitters with communication delay becoming unpredictable. It is noted that there is a direct relationship between the number of Modbus firewall rules enabled and latency and considerations for protection using deep inspection is recommended in those segments where communications are not time sensitive.

The work in [23] evaluated the impact and behavior of commercial firewalls in networked control systems and determining acceptable safe operating margins of delays that could be tolerated in IACS networks due to the presence of an industrial firewall with deep packet inspection of the Modbus TCP/IP industrial protocol. Using various performance stress conditions with tighter timeouts, an acceptable and safe operating margin for latency when an industrial firewall is introduced to protect critical infrastructure is determined.

The performance of three different commercial off the shelf industrial firewalls provided by Fortinet, Belden-Hirschmann and Moxa is examined in [24]. Latency and Modbus/TCP performance measurements are tested based on both general purpose and industry-oriented performance indexes. The results of the experiment demonstrate that the firewall from Fortinet whilst it provides the performance regarding latency, it however lacks deep packet inspection capabilities for the Modbus protocol. On the other hand, whereas the Belden firewall complies with the Modbus protocol specification, it exhibits the longest delays. According to the authors in [24], the latency testing results show that industrial firewalls from Moxa and Belden introduce twice the latency compared to the firewall from Fortinet.

Overall, none of the above studies on firewall performance in IACS comprehensively considered the impact on network performance brought by the implementation of firewalls in a typical industrial network following a defense-in-depth approach to security as recommended best practice standards and guidelines. Our approach to network performance evaluation in IACS networks is different from the work of

previous studies. Firstly, our evaluation is based on IACS networks following IEC 62443 security standards [6], our network is segmented into separate zones [25] and protected by multilayered firewalls with deep inspection filtering capability. Secondly, other than latency evaluation, we also seek to study variations in latency (jitter), packet loss and evaluate if time constraints for communications are still achievable when messages between devices in different zones of the network pass through multiple filtering devices.

III. Experimental Setup

The experimental testbed in Fig. 3 below consisting of two security levels each with two zones separated by boundary firewalls is implemented to analyse and evaluate latency, jitter and packet loss introduced to communications when multiple firewalls at different locations enforce network segmentation in IACS. The testbed reflects recommended defense-in-depth network security strategy in IACS following the IEC 62443 security standards. The experimental evaluations for latency, jitter and packet loss is based on Modbus TCP/IP communications between supervisory control devices in Security Level 2 (SL2) and basic control devices in SL1 of the Purdue Model for Control Hierarchy [14]. The Modbus TCP master is connected to firewall FW1's port X dedicated to Zone 2A network, whereas the Modbus TCP slave is in SL1, Zone 1A network segment connected to firewall FW3 port Y.

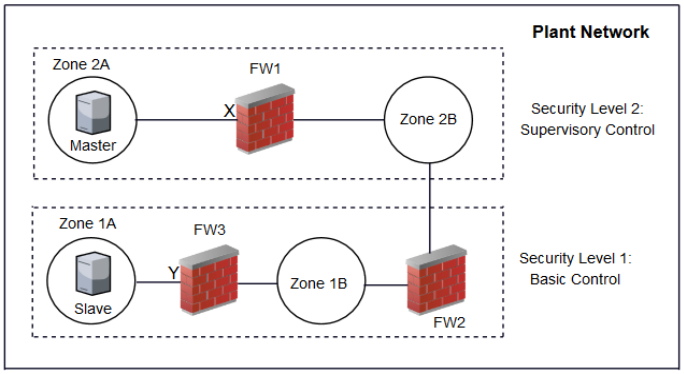

Fig. 3. Architecture of experimental setup

A. Modbus TCP Master and Slave

The Modbus TCP master in our setup is built on a Windows computer with a Modbus Poll [26] application for the Modbus protocol stack communication. The application is configured to initiate and send TCP requests every 100µs to the slave node and the request messages contain Modbus read/write holding registers function code 23 (0x17). This function code executes a single Modbus transaction that combines one read operation and one write operation with the write operation executed before the read. The request and response messages associated with function code 23 are always of the same size, hence this enables us to evaluate latency, jitters, and packet loss under same message conditions in our testbed. The Modbus TCP slave is built on a Windows computer running a simple and open source Java ModbusPal application [27]. The Modbus TCP slave node receives requests from the Modbus TCP master and responds with the appropriate Modbus TCP reply. The response message contains the data from the group of registers that were read.

B. Industrial Firewall

The open source Linux firewall in our testbed implements deep packet inspection of Modbus messages, and is based on the firewall solution proposed in [8]. The firewall extends a dynamic inspection feature of iptables called u32 match to perform the deep inspection of the Modbus message payloads. The u32 match directs the extraction of 32 bits from the message at any specified location and performs a comparison with the given value.

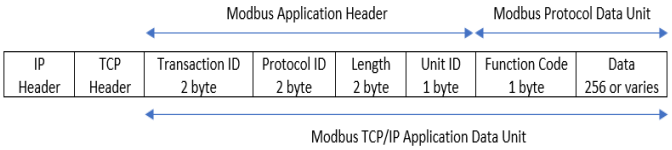

Fig. 4. Modbus TCP/IP message structure

The function code field of the Modbus TCP/IP Application data unit [28] located at byte 7 is one of the most critical field to inspect using deep packet inspection filters in a Modbus message as it contains the actual data commands from the master node to the slave node. Based on the Modbus message structure shown in Fig. 4 above, a simple firewall rule for allowing Modbus messages for Read/Write Holding Registers from host 192.168.2.2 can be configured as follows:

iptables -A INPUT -s 192.168.2.2 -p tcp --dport 502 \! -f -m u32 "0>>22&0x3C @12>>26&0x3C @7>>24&0x0f=0x17" -j ACCEPT

The above rule can be explained in conjunction with Fig. 4 as follows:

1) 0>>22&0x3C@ which directs the skipping of IP headers and 12>>26&0x3c@ to also skip the TCP headers. Once the IP and TCP headers are skipped, checking can now start on any specified location of the Modbus message against a given value.

2) 7>>24&0x0f=0x17 which skip the Modbus application protocol header and move to location at byte 7 containing the data commands and verify if the function code is set to 0x17 (Read/Write Holding Registers). If the field value does not match the required one, the packet is dropped by the firewall.

C. Network Performance Measurement

The network performance evaluation of multilayered firewalls to achieve segmentation in our experimental setup is based on latency, jitter and packet loss rate. Latency evaluation is based on registering timestamps on each of the Modbus TCP/IP packet between firewall FW1 port X and firewall FW3 port Y using dumpcap packet capture software, the firewall clocks are synchronised. Modbus master request timestamp is first captured at FW1 port X and also when it exits FW3 port Y whereas the slave reply timestamp is captured first at FW3 port Y and when it exits FW1 port X (refer to Fig. 3). After successful capture, the files are uploaded on a separate Splunk indexing server [29] for post processing and analysis. Latency introduced by the zone boundary firewalls as packets traverse

between the master and slave nodes is calculated as follows (*see Table I*):

- Master Request Latency = T2 – T1
- Slave Response Latency = T4 – T3

Jitter and packet loss rate are evaluated based on the changes in the number and complexity of Modbus TCP/IP deep inspection filter rules configured. We compute the jitter for two consecutive packets between the master and the slave using timestamps as shown in Table I as follows:

- Master to Slave Jitter = (T6-T2) – (T5-T1)
- Slave to Master Jitter = (T8-T4) – (T7-T3)

TABLE I. PACKET TIMESTAMPS BETWEEN FW1 AND FW3 (SEE FIG. 3)

Timestamp	Modbus Master	Modbus Slave
T1 (port X)	send packet 1	
T2 (port Y)		receive packet 1
T3 (port Y)		send reply packet 1
T4 (port X)	receive reply packet 1	
T5 (port X)	send packet 2	
T6 (port Y)		receive packet 2
T7 (port Y)		send reply packet 2
T8 (port X)	receive reply packet 2	

IV. FINDINGS AND DISCUSSSIONS

In this section results from the measurement of latency, jitter and packet loss introduced to communications by multiple deep packet inspection firewalls at different zone boundaries are presented. The experimental tests have been repeated several times and are based on a set of identical 1,000 Modbus TCP/IP messages for the read/write holding registers function performed under the following:

1) *Firewalls with basic filter rules*. In this mode, we only analyse TCP/IP headers and we seek to evaluate latency, jitter, and packet loss when the number of basic filter rules on each of the three firewalls is increased.
2) *Firewalls with deep packet inspection of the Modbus protocol*. In this mode, (see Section II B) in addition to the basic firewall rules above, we configure Modbus specific rules to examine the message payload (data commands).

A. Latency Evaluation

The results from our testing of latency introduced by the multilayered firewalls with basic filter rules is summarised in Table II. The tests have been repeatedly done on the same Modbus messages (function code 23) with varying number of basic filtering rules configured that is 1, 9 and 18 respectively for ten times. The goal is to understand how latency is affected by the increasing number of rules on each of the three firewalls in our setup (see Fig. 3). For both the Modbus master request messages and slave response messages, the maximum latency increases proportionally to the number of filtering rules configured. Whilst there are no filter rules configured for response messages coming from the slave node, the responses are also affected by latency. Experiments for latency introduced by configuring additional rules for Modbus TCP/IP filtering is summarised in Table III. Latency values have been collected under varying number of rules. It can be seen that the maximum latency for master request messages reach 4799.5µs when one Modbus firewall rule is configured on each of the three firewalls, this is approximately 3 times higher when compared to same number of rules under basic filtering in Table II where latency is 367.7µs. Modbus deep inspection greatly affects latency.

Whereas experimental evaluations of latency in [24] show that commercial industrial firewalls for Modbus introduce twice the request latency when compared to firewalls with basic filtering capabilities, the results from our tests show an even higher value of latency (3.5 times more) introduced. Firstly, unlike in [24] where latency evaluations are based on a single firewall, our testbed on the other hand comprises of 3 firewalls protecting different zone boundaries and each firewall introducing additional delays to messages through deep packet inspection. Secondly while our maximum number of rules are lower than those in [24], it is possible that complexity of the iptables firewall rules configured in our testbed also plays a part in the resulting higher values for master request latency obtained. Similarly, Modbus slave response messages are also greatly affected by latency. For example, when 18 basic rules are configured the maximum latency is 4141.9µs whereas with the same number of rules for Modbus rules, the maximum latency is 14192.5µs. In both directions of the Modbus TCP/IP communication, when additional deep inspection filter rules are configured on three firewalls and testing executed for 9, 18 and 27 rules, the delays introduced by the firewalls become increasingly high for both the master requests and slave responses.

TABLE II. LATENCY INTRODUCED WHEN BASIC FIREWALL RULES ARE CONFIGURED

	rules	Avg(µs)	Std(µs)	Min(µs)	Max(µs)
Master Request	1	397.4	424.2	112.1	1367.7
	9	542.1	651.3	108.7	5991.4
	18	3320.9	1859.3	129.9	7177.8
Slave Response	1	384.4	406.3	386.9	2047.3
	9	500.4	396.6	174.2	2937.8
	18	2769.5	1126.1	213.9	4141.9

TABLE III. LATENCY INTRODUCED WHEN MODBUS TCP\IP DEEP INSPECTION FIREWALL RULES ARE CONFIGURED

	rules	Avg(µs)	Std(µs)	Min(µs)	Max(µs)
Master Request	1	566.6	532.8	104.2	4799.5
	9	658.1	657.5	127.5	4695.9
	18	1718.5	1265.5	209.4	19170.3
Slave Response	1	559.1	1022.6	592.9	2778.6
	9	908.9	978.4	170.2	7733.9
	18	970.1	1067.9	449.3	14192.5

B. *Jitter Evaluation*

The evaluations of jitter were carried out by sending Modbus packets with function code 0x17 continuously from the master to the slave with 100µs interval. A positive value for jitter reflects that packets are received with more than 100µs interval while negative jitter means packets are arriving in less than 100µs intervals. Positive jitter is an indicator that delay is increasing and less favorable for the underlying application. In time-sensitive industrial applications, jitter should be as low as possible.

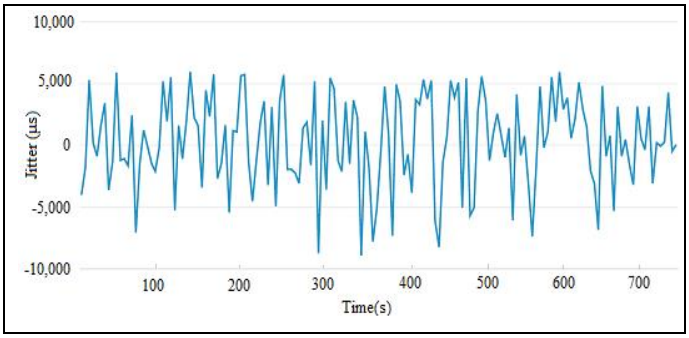

Fig. 5. Master to slave jitter when basic rules are configured.

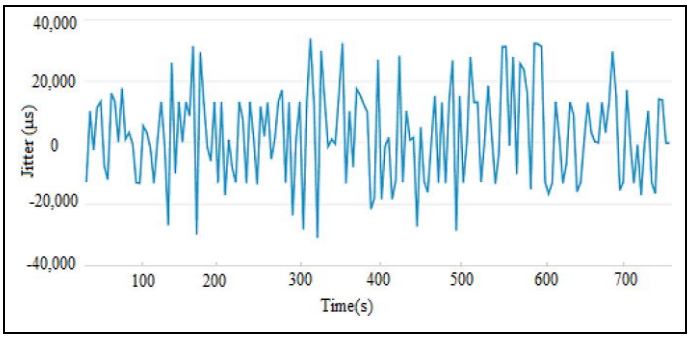

Fig. 6. Master to slave jitter when basic and Modbus rules are configured.

The first set of measurements for jitter was aimed at evaluating how basic filter rules configured on firewall FW1, FW2 and FW3 were able to affect variations in latency for Modbus messages between the master and slave nodes. The results for jitter from variations for Modbus request messages from the master to slave are shown in Fig. 5. It is clear from the results that the presence of more than one firewall regardless of the filtering enabled, the consecutive packets are affected by jitter. The communication delay variations are predictable in a pattern with a maximum jitter value of 5,000µs.

In the second set of measurements, we evaluate jitter when the firewalls have Modbus filter rules configured to analyse in detail the message payload. Again, our jitter evaluation is for Modbus request messages from the master to slave.Variations to latency introduced when deep packet inspection rules for Modbus are enabled is plotted in Fig. 6. When the rules are configured on each of the three firewalls, latency is affected by jitters with communication delays between consecutive packets becoming unpredictable and maximum jitter reaching 30,000µs. In comparison with the jitter results when basic filtering is enabled (refer to Fig. 5), when deep packet inspection for Modbus is configured on all firewalls jitter increase by six times. It is evident that the additional increase in latency variations is likely caused by the interference of the deep inspection filtering rules.

Overall, in both communication directions, latency is greatly affected by jitters when Modbus deep inspection filter rules are configured. The summary values for positive jitter is presented in Table IV. The results show that in either of the filtering modes, the firewalls introduce high positive jitters to packets. This situation may not be a problem as long as the positive jitter introduced per packet is still low. The average jitter per packet with basic rules is lower at 3,053µs when compared to the one when Modbus rules are configured on the firewalls which is 4.5 times higher at 13,667µs.

TABLE IV. MASTER TO SLAVE POSITIVE JITTER VALUES

	Basic rules	**Modbus rules**
Percentage of packets with positive jitter	50.9 %	57.83 %
Average jitter per packet with positive jitter	3,053µs	13,667µs

C. *Packet Loss Evaluation*

Packet loss rate evaluation for Modbus messages was carried by analysing the percentage of packets failing to reach the slave or master respectively. The results from our evaluation show that communications are received in either direction without any packet loss. However, as the number of firewall rules configured on each of the firewall increases in either of the two filtering modes, the average TCP Fast Retransmissions increase. The increase is more significant when Modbus filtering is configured. It is likely that the request messages are arriving late to the slave due to firewall increased deep inspection processing, triggering retransmissions. The results of the percentage of TCP Fast Retransmissions triggered per 1,000 Modbus TCP/IP messages (function code 23) under varying number of firewall rules in each of the two filtering modes is depicted in Fig. 7 below.

Similar experimental simulations using the same number of Modbus request messages for a different function code (15 - write multiple coils) repeated for several times confirm that the more number of deep inspection rules configured, the more TCP fast retransmissions introduced to communications.

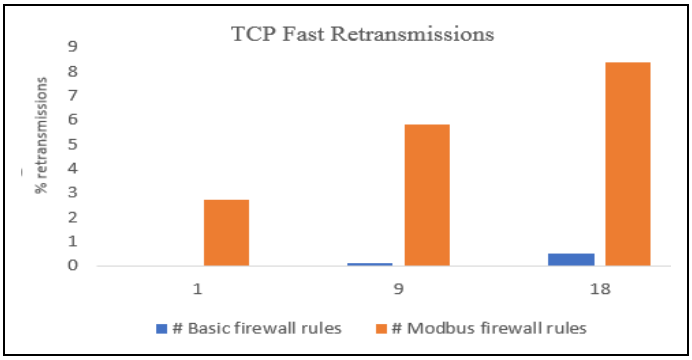

Fig. 7. Average TCP Fast Retransmissions in different filtering modes

V. Conclusion

In this paper, results of the evaluation of latency, jitter and packet loss introduced to communications by industrial firewalls at different locations when the industrial network is segmented via security levels, zones and conduits following the IEC 62443 security standards are reported. Measurements have been collected when the industrial firewalls are configured with basic filtering rules and Modbus TCP/IP protocol filtering rules. The results show that when Modbus TCP/IP firewall filtering rules are configured, latency and jitter is greatly affected. The latency becomes unpredictable and very high whereas the average jitter for packets with positive jitter significantly increase. While no packet loss is noted in our results, when Modbus filtering rules configured increase, TCP Fast Retransmissions increases significantly due to message processing delays by the firewalls. The research results demonstrate that achieving low latency and low jitter as required in some time-sensitive IACS is not possible when strict IEC 62443 security standards are applied. Therefore, it is recommended that inline placement of multilayered deep inspection firewalls to enforce zone boundary security should be considered between those zones where messages are not time-critical. Instead compensatory controls including intrusion detection and prevention systems could be considered in time-sensitive zones as they have less impact on performance compared to industrial firewalls. As future work, we plan to introduce commercial industrial firewalls in our testbed and evaluate delays, jitter and packet loss in similar firewall operating conditions.

References

[1] NIST Special Publication 800-82 Revision 2, Guide to Industrial Control Systems (ICS) Security, 2015.

[2] P.Huitsing, R.Chandia, M.Papa and S.Shenoi, “Attack taxonomies for the Modbus protocol”, in International Journal on Critical Infrastructure Protection, pp 37-44, 2008

[3] P.Zavarsky, “Computer Security at Nuclear Facilities”, Nagaoka University of Technology, Japan, 2017.

[4] J. Pollet, "Innovative defense strategies for securing SCADA and control systems", Technical Papers of ISA, vol. 459, pp.115-128, 2005.

[5] ANSI/ISA 62443-3-3: 2013 Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security Levels.

[6] Tofino Security (2014), “Using ISA/IEC 62443 Standards to Improve Control System Security” [Online]. Available at: https://info.belden.com/hubfs/resources/knowledge/white-papers/using-isa-iec-62443-to-imp rove-control-system-security.pdf

[7] M.Hassan and H.Mouftah, "Latency-Aware Segmentation and Trust Stystem Placement in Smart Grid SCADA Networks”, in IEEE Computer Aided Modelling and Design of Communication Links and Networks, Toronto, 2016.

[8] J.Nivethan and M.Papa, "On the use of open-source firewalls in IACS/SCADA systems", in Information Security Journal: A Global Perspective, 2016.

[9] Computer Security Techniques for Nuclear Facilities, Draft Technical Guidance, 2017.

[10] "How to choose the right industrial firewall: the top seven considerations", [Online]. Available at: http://www.ee.co.za/article/ choose-right-industrial-firewall-top-seven-considerations.html

[11] “Honeywell selects Tofino Modbus Read-only Firewall to Secure Critical Safety Systems”, [Online]. Available at: https://www.tofinosecurity.com/article/honeywell-selects-tofino%E2% 84%A2 -modbus-read-only-firewall-secure-critical-safety-systems

[12] Belden Security, "Understanding Firewall Technology for Industrial Cybersecurity", [Online]. Available at: http://info.belden.com/iit/ understanding_firewall_technology_industrial_cyberse curity-bc-lp.

[13] J.Nivethan and M.Papa, "A Linux-based firewall for the DNP3 protocol", in IEEE Technologies for Homeland Security, Waltham, 2016

[14] L.Obregon, "Secure Architecture for Industrial Control Systems", SANS Institute, 2015. Available on: https://www.sans.org/reading-room/white papers/IACS/secure-architecture-industrial-control-systems-36327

[15] I.Fovino, A.Coletta, A.Carcano and M.Masera, "Critical State-Based Filtering System for Securing SCADA Network Protocols", in IEEE Transactions on Industrial ElectronIACS, vol 59, pp. 3943 - 3950, 2012

[16] S.Hachana, F.Cuppens, and N.Boulahia, “Towards a new generation of industrial firewalls: Operational process aware filtering,” in 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, 2016.

[17] R.Candel, D.Anand and K.Stouffer, " A Cyber Security Testbed for Industrial Control Systems", in Process Control and Safety Symposium, Texas, 2014.

[18] B.Hickman, D.Newman, S.Tadjudin and T. Martin, "Benchmarking Methodology for Firewall Performance", April 2003. Available at: https://tools.ietf.org/html/rfc351

[19] K.Salah, K.Elbadawi and R.Boutaba,"Performance Modeling and Analysis of Network Firewalls”, in IEEE Transactions on Network Service Management, vol 9, no 1, pp 12-21, 2012

[20] T.Hayajneh, B.Mohd, A.Itradat and A.Quttoum, "Performance and Information Security Evaluation with Firewalls", in International Journal of Security and Its Applications, vol.7, no 6, pp.355-372, 2013

[21] M.Aziz, "Performance Analysis of Application Layer Firewall", in IEEE Symposium on Wireless Technology and Applications, Bandung, 2012

[22] M.Cereia, I.Berolotti, L.Durante and A.Valenzano, "Firewall Latency Evaluation of IACS Networks Based on Tofino Firewall" in IEE Emerging Technology and Factory Automation Conference, Barcelona, 2014.

[23] M.Cheminod, L.Durante and A.Valenzano and C.Zunino, "Performance Impact of Commercial Firewalls on Networked Control Systems", in Emerging Technology and Factory Automation, Berlin, German, 2016.

[24] M.Cheminod et al, "Performance of Firewalls for Industrial Applications", in 4th International Symposium for IACS and SCADA Cyber Security Research 2016, Belfast, 2016

[25] "Segregate Networks and Functions", Information Assurance Directorate, 2016

[26] Modbus Poll tool. Available: http://www.modbustools.com/modbus_ poll.html

[27] ModbusPal slave simulator tool. Available at: https://sourceforge.net/ projects/modbuspal/files/modbuspal/RC%20version%201.6b/

[28] Modbus Application Protocol Specification V1.1b3, [Online]. Available: http://www.modbus.org/specs.php

[29] Managing Indexers and Clusters of Indexers, [Online]. Available at: https://docs.splunk.com/Documentation/Splunk/7.0.1/Indexer/Aboutinde xesandindexers, 2018.

[30] NIST IT Security for Industrial Control Systems: Requirements Specification and Performance Testing, 2004.

[31] IEEE Standards for Time Sensitive Networking for use in Industrial AutomationNetworks, 2017 Available: http://standards.ieee.org/ downloads/TSN_for_Industrial_Networks.pdf

[32] NISTIR 8188 Key Performance Indicators for Process Control System Cybersecurity Performance Analysis, 2017.