Article

Exponential Backoff and its Security Implications for Safety-Critical OT Protocols over TCP/IP Networks

Matthew Boeding , Paul Scalise , Michael Hempel * , Hamid Sharif , Juan Lopez Jr.

Posted Date: 28 April 2025

doi: 10.20944/preprints202504.2196.v1

Keywords: Operational Technology; Modbus TCP; DNP3; Industrial Protocols; Communication Security; OT Protocols; Mitigation Strategies

Article

Exponential Backoff and its Security Implications for Safety-Critical OT Protocols over TCP/IP Networks

Matthew Boeding [1], Paul Scalise [1], Michael Hempel [1,*], Hamid Sharif [1] and Juan Lopez Jr. [2]

1 Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, Lincoln, NE 68588, USA; mboeding@huskers.unl.edu (M.B.); pscalise@huskers.unl.edu (P.S.); hsharif@unl.edu (H.S.)
2 Oak Ridge National Laboratory, Oak Ridge, TN 37831, USA; lopezj@ornl.gov
* Correspondence: mhempel@unl.edu

Abstract: The convergence of Operational Technology (OT) and Information Technology (IT) networks has become increasingly prevalent with the growth of Industrial Internet of Things (IIoT) applications. This shift, while enabling enhanced automation, remote monitoring, and data sharing, also introduces new challenges related to communication latency and cybersecurity. Oftentimes, legacy OT protocols were adapted to the TCP/IP stack without an extensive review of the ramifications to their robustness, performance, or safety objectives. To further accommodate the IT/OT convergence, protocol gateways were introduced to facilitate the migration from serial protocols to TCP/IP protocol stacks within modern IT/OT infrastructure. However, they often introduce additional vulnerabilities by exposing traditionally isolated protocols to external threats. This study investigates the security and reliability implications of migrating serial protocols to TCP/IP stacks and the impact of protocol gateways, utilizing two widely used OT protocols: Modbus TCP and DNP3. Our protocol analysis finds a significant safety-critical vulnerability resulting from this migration, and our subsequent tests clearly demonstrate its presence and impact. A multi-tiered testbed, consisting of both physical and emulated components, is used to evaluate protocol performance and the effects of device-specific implementation flaws. Through this analysis of specifications and behaviors during communication interruptions, we identify critical differences in fault handling and the impact on time-sensitive data delivery. The findings highlight how reliance on lower-level IT protocols can undermine OT system resilience, and they inform the development of mitigation strategies to enhance the robustness of industrial communication networks.

Keywords: operational technology; Modbus TCP; DNP3; industrial protocols; communication security; OT protocols; mitigation strategies

1. Introduction

OT devices and thus communication protocols are widely being adopted into networked applications [1]. This is being expanded with the increasing adoption of Industrial IoT (IIoT) Networks, driven by the demand for greater automation, data sharing, and remote monitoring [2]. These networks may also rely on time-sensitive applications that may impact the safety of workers, for example, to shut down a production line when an incident is detected, or to protect energy grid systems in the event of a fault. Previously, delivery of communication over serial networks had limited distances to travel and set maximum delays for communication. As a result, these protocols were ideally suited for safety-critical applications. However, the translation to TCP/IP-based networked communication to better integrate and coexist with existing IT protocols has introduced additional latency and cybersecurity concerns for these communication networks.

In many cases, a complete retrofit of existing OT device deployments is not feasible due to the cost, complexity, and potential disruptions associated with upgrading legacy equipment. As a result, there is a growing reliance on solutions that bridge the gap between older OT systems and modern IT networks. Protocol gateways, which act as translators between different communication protocols, have become a common solution in these scenarios. These gateways facilitate the integration of OT systems that use legacy communication protocols, such as Modbus/RTU [3], with more modern network infrastructures using more sophisticated OT protocols, such as DNP3[4], by mapping protocol values through shared memory within the gateway device. However, while these gateways offer flexibility and interoperability, they also introduce new vulnerabilities into OT networks by making communication more accessible to external threats.

The security and timely communication of OT systems are critical, as vulnerabilities in communication protocols can have far-reaching consequences on both operational uptime and worker safety. OT protocols are often designed with limited security features and are sometimes not updated to address modern cybersecurity threats. This lack of robust security mechanisms leaves OT systems exposed to potential attacks, such as man-in-the-middle attacks, denial-of-service attacks, and unauthorized access. These vulnerabilities are often mitigated through a defense-in-depth strategy, which involves multiple layers of protection, including network segmentation, firewalls, and intrusion detection systems. However, these measures may not always prevent all vulnerabilities, especially those inherent in a device's protocol implementation [5].

The need to monitor and control OT systems across vast geographic areas has further complicated this issue. An example is the utilization of renewable energy resources and decentralized power grids, which requires the deployment of monitoring devices and sensors interconnected over a large geographical footprint. Remote monitoring, often achieved via wireless networks [6,7], is becoming essential for maintaining operational efficiency and system resilience. However, this shift introduces new challenges, particularly when communication failures occur between devices located at remote sites. These failures can lead to significant disruptions in system performance, delayed responses to critical events, and increased downtime.

In our previous works, we implemented both physical and emulated testbeds to evaluate the performance of specific OT protocols and their on-device implementations [8]. These studies revealed significant variability in the performance of the same protocol across different devices, highlighting the potential for device-specific implementation flaws to cause system-wide failures. In some cases, mismanagement of key protocol functions, such as flag handling or message synchronization, led to complete communication breakdowns.

Given the importance of reliable communication in OT systems, addressing the vulnerabilities introduced by integrating legacy protocols with modern IT systems is critical to improve the resilience and security of OT networks. Our ongoing efforts are centered around a systematic review of existing OT protocol specifications and the identification of potential vulnerabilities and safety concerns. As documented in our prior work, we've established the capabilities to then conduct extensive evaluations of any identified vulnerabilities – through simulation, emulation, and real-world testbeds. The current paper focuses on and contrasts the specifications of Modbus TCP and DNP3 – two widely used OT protocols that are often deployed in industrial environments – and highlights the potential impacts of these specifications' reliance on TCP/IP as the underlying protocol stack architecture, specifically when it comes to fault handling. We explore the challenges posed when these protocols experience communication interruptions through device errors or malicious content and explore how different protocol specifications can undermine the reliability of OT systems.

Specifically, in this study, we identify specific stages within the Modbus TCP and DNP3 specifications that outline separate behavior for re-establishing communication, identify specific issues for time-sensitive data, and implement a multi-tiered OT testbed to demonstrate the implications of these behaviors in a realistic industrial setting. Using this testbed, we then assess the effectiveness of different mitigation strategies that address these issues. We document a specific safety concern we identified and validated within Modbus TCP that applies to virtually all Modbus TCP devices, as it is an integral behavior of the protocol stack itself. The results provide critical insights into how reliance on lower-level IT protocols may lead to unintended consequences for OT protocol use cases – with potentially far-reaching implications for their use.

2. Related Works

The security of OT protocols has been extensively studied through various methods such as formal verification, simulation, and physical testbeds [9,10]. As OT equipment in the field becomes increasingly interconnected with accessible IT data networks, it presents greater opportunities for improved maintenance, safety, and operability. However, these advancements also introduce new security and safety risks, as connected devices can potentially become entry points for malicious actors into a previously well-isolated OT system. The growing integration of OT systems with IT networks expands the attack surface and raises significant challenges in securing these systems.

A comprehensive review by the authors in [11] examines attacks on DNP3 and other OT protocols over the past 15 years, shedding light on various vulnerabilities that attackers have exploited. Their review includes attacks targeting OT IP filtering systems and emphasizes the need for defense-in-depth strategies, protocol hardening, encryption, and anomaly detection mechanisms to prevent such attacks. In a more specific case, [12] proposes an Artificial Neural Network (ANN) to detect reconnaissance attacks on the DNP3 protocol. While the approach shows promise, the authors note limitations, particularly the model's inability to generalize, resulting from the limited size and diversity of the training and test datasets. This issue is common in OT security research, where available datasets are often insufficient to model the full range of attack scenarios.

In [13], the authors take a different approach, by training a deep neural network to serve as an Intrusion Detection System (IDS) specifically for detecting attacks against DNP3. Their system demonstrated an impressive 99% accuracy in identifying attacks, showcasing the potential of machine learning to enhance OT security. However, this study also highlights the challenges of maintaining high detection accuracy across various attack vectors and real-world conditions. Building on this work, Dangwal et al. [14] compared the efficacy of various intrusion detection models, including decision trees, deep neural networks, and transformer neural networks. Their results, based on seven testbed packet traces, showed that transformer neural networks achieved the highest accuracy, with a detection rate of 99.56%. This further underscores the potential for deep learning models to improve the robustness of OT security systems.

The integration of serial OT protocols with modern communication networks, such as the internet, is another critical area of concern. These communication interfaces provide greater connectivity but also introduce new risks related to interoperability and security. The work in [15] presents an interworking model between Modbus and IoT devices, validated in a scenario involving solar energy equipment. This research highlights the complexities of integrating legacy OT protocols with emerging technologies, where maintaining both security and seamless functionality is often a delicate balance. Similarly, in [16], the authors assess the performance of Modbus and DNP3 protocols through both simulation and testbed environments. Their findings indicate that wireless technologies like WiFi, while widely used, are not suitable for meeting the strict latency and security requirements of OT systems. The results suggest that OT systems may require more specialized communication protocols or hybrid solutions to ensure both performance and security.

In [17], a security enhancement for the Modbus/TCP protocol is proposed through the use of Chaskey-12 Message Authentication Codes (MACs), as defined in IEC 29192-6. This cryptographic technique provides an additional layer of security by ensuring the integrity and authenticity of Modbus messages, helping to prevent unauthorized access or manipulation of data during communication.

Another important consideration in OT security is the scalability of communication networks, particularly in large-scale deployments. In [18], the authors demonstrate that, due to the sequential polling method of the Modbus protocol, reliable communication becomes infeasible in environments with higher Bit Error Rates (BER), where re-transmissions are required, even before reaching the maximum number of servers supported by the protocol. This highlights the challenges faced in

doi:10.20944/preprints202504.2196.v1

large-scale OT systems, where communication reliability and scalability are crucial for maintaining system performance and security.

This scalability issue is further addressed in [19], where the authors design and configure a hardware-in-the-loop testbed based on the 2000-bus Texas synthetic grid. This testbed is monitored by DNP3 using real-world equipment, providing valuable insights into the challenges of scaling OT communication protocols while ensuring both operational efficiency and security.

Similarly, [20] explores how the larger packet frame of DNP3 can reduce computational and transmission times, particularly in large-scale Distributed Energy Resource (DER) networks. Through network emulation with an OPAL-RT simulator, the study demonstrates that DNP3's design is well-suited to support high-volume data exchanges in large-scale OT systems, providing both operational efficiency and improved performance in communication-heavy environments.

The contribution of our work presented in this paper is the exploration of underlying assumptions when delivering application data over IT protocols, that is, the timely and reliable delivery of data. We show that the resilience of communication utilizing these protocols may be different based on the outlined behavior of each device within the protocol. Specifically, we focus on the impacts of the single-ended method of communication outlined in Modbus and how that affects reliability. We collect extensive results on a multi-tiered testbed to show the implications of communication issues within safety-critical applications.

3. Methodology

In our previous work [21], we outlined the critical states for the Modbus protocol, and the implications to the protocol's operation from the lack of defined timeout requirements for any communication errors. With that, however, we must also consider these issues for the underlying layers of TCP/IP that transport our Modbus data. For this method, we carefully reviewed the specifications and investigated the implementation guides for both Modbus TCP and DNP3, and found differing rules for connection loss and connection re-establishment between the two protocols, which would lead to differing performance with communication outages and time-sensitive data.

3.1. Identification of Possible Communication Failures

The implementation guide for Modbus TCP closely aligns with the traditional operating conditions of Modbus over serial communication media [22], in particular RS-232 and RS-485. In these conditions, the client is always the only device initiating a connection to the server. We found from our review of the protocol specification that this operating principle was similarly applied to Modbus TCP, in which clients are still the only devices allowed to make TCP connections. Thus, if a device crashes or has a communication failure, it is the responsibility of the client to reestablish its TCP communication, even if the server is able to detect that communication failure and may even have pending data. In the case of a single device disconnecting, we refer to this as a single-ended communication failure. The procedures for handling these scenarios are largely dependent on the underlying transport technology – in this case, TCP/IP. These failures are subsequently remedied by the client re-initiating a handshake. However, failure to respond expands the retry time based on TCP's exponential backoff. We contrast this to DNP3's implementation guide [4], which allows for connection establishment by both Master and Outstation. In DNP3's implementation, there are also rules that connections can be established as soon as data is available. Overall, we found from our review that Modbus TCP's protocol specification is in large parts driven by its serial communication roots, whereas DNP3 more aptly considers its TCP/IP-based operating environment.

For the one-sided communication crashes in Modbus TCP, we can examine them as client-based, shown in Figure 1 and server-based, shown in Figure 2. The client crashing or losing communication in some form performs similarly to standard TCP connection establishment, as the client will send a SYN packet to the server to establish a new link. This can, however, cause issues for time-sensitive communications, as the server may not accept the client's request if ports are reused until the Keep-Alive timeout occurs or the client's new synchronization packet prompts the server to reset the connection.

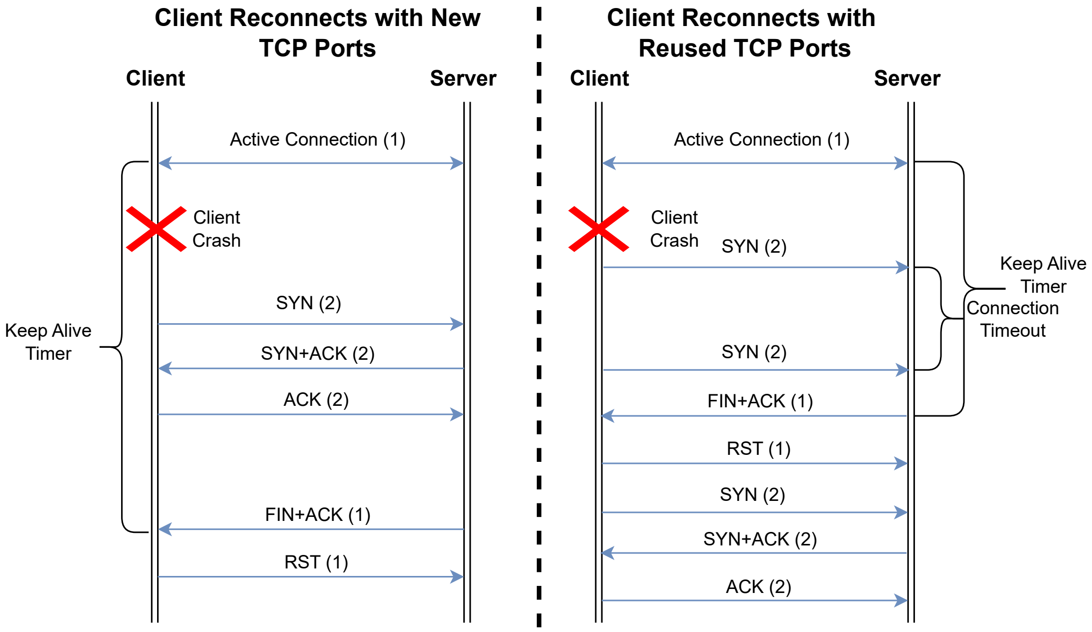


Figure 1. Client Crash Connection Establishment

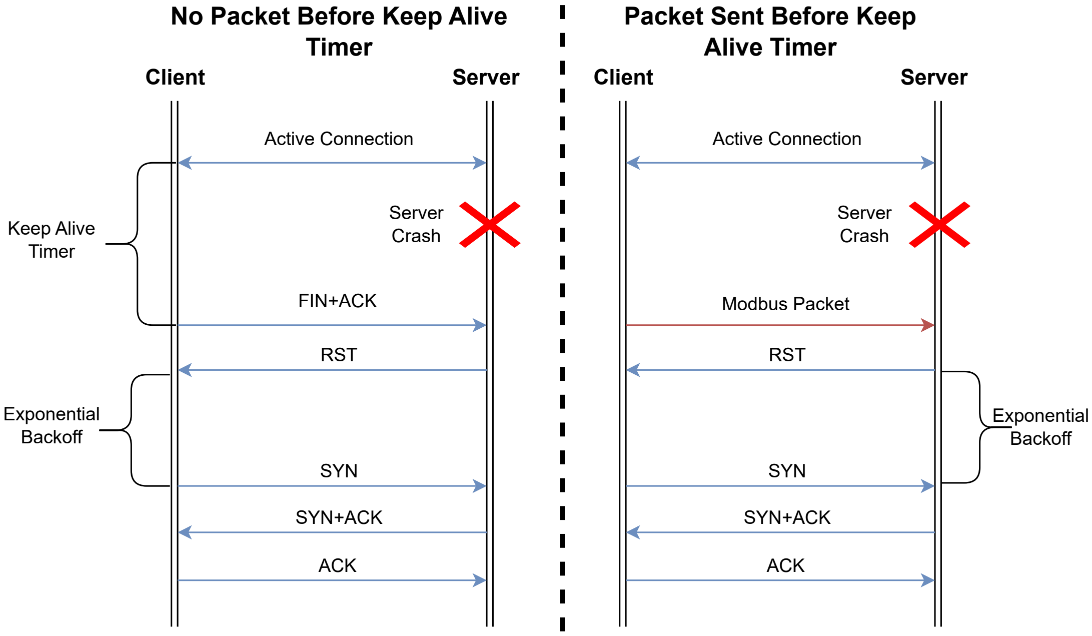


Figure 2. Server Crash Connection Establishment

Furthermore, our review found that server crashes are more severe in their potential ramifications on OT operations, because they may, in effect, cause more time delays in re-establishment due to the exponential backoff implemented by Modbus TCP clients. In this case, a client that is unable to connect on its first attempt will increase the time between attempts until the maximum is reached, typically 64 seconds. This can become increasingly important, as this can easily be exploited by a malicious actor sending malicious packets that interrupt communication and thereby force the exponential backoff to approach its upper limit. As a result, the connection will remain interrupted for extended periods of time, with significant repercussions for safety-critical applications, as shown in more detail below.

3.2. Active Network Implications

To identify and evaluate the implications of these findings on an active network, we introduce the testbed depicted in Figure 3. This testbed employs a process-level network utilizing serial Modbus communication for a pump, linear actuator, and temperature sensor. These devices are connected to a Programmable Logic Controller (PLC), which converts Modbus TCP communications into Modbus RTU messages to control the physical processes.

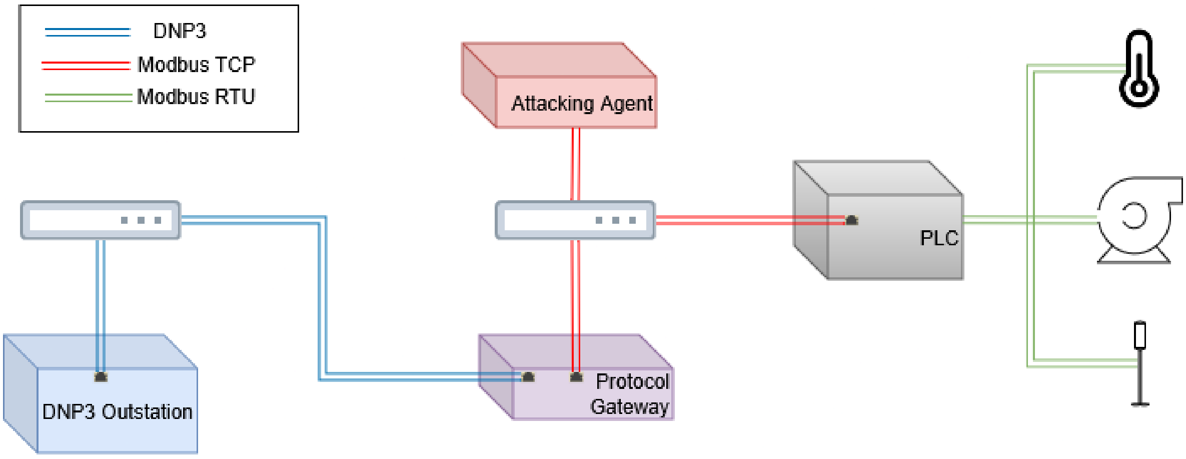


Figure 3. Physical Testbed Hierarchical Diagram

The PLC subsequently communicates with a protocol translation gateway between Modbus TCP and DNP3. This gateway facilitates bi-directional communication, allowing values from the DNP3 network to be mapped to the Modbus network. For this study, the Modbus network reads register values to determine the required position of the motor and linear actuator in the serial network. The gateway is the only Master device in the DNP3 network and uses only solicited data, polled at regular intervals.

3.3. Mitigation Strategies

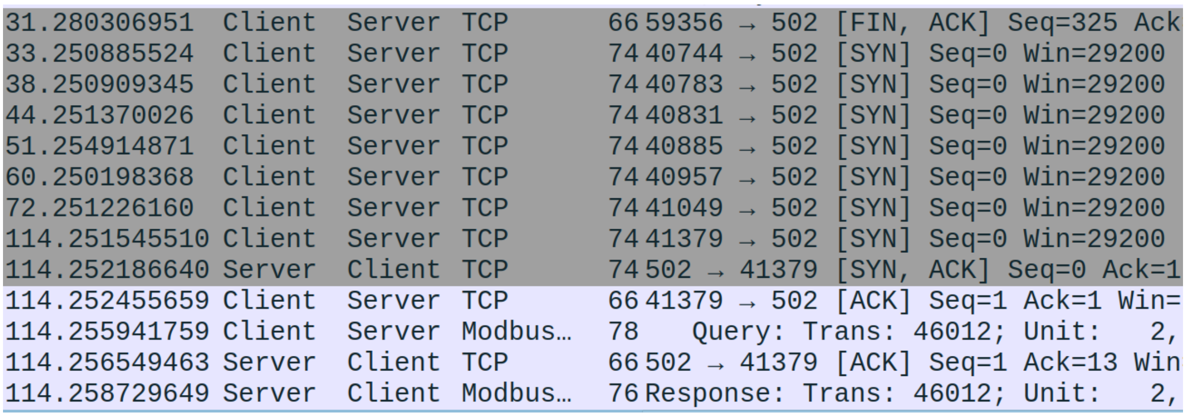
The configuration and commissioning of OT networks can incorporate a variety of security strategies to help mitigate failures in specific devices. In this study, we leveraged the built-in security features of the gateway device and introduced additional security components, such as a security gateway that acted as a firewall for both Modbus and DNP3 networks, as well as a software-defined switch to control the physical routing between devices. Each device was evaluated individually to assess its contributions to failure mitigation within the OT network.

For example, the communication gateway includes several security features aimed at mitigating failures. Specifically, we tested an IP whitelist, SYN scan protection, SYN-flood protection, and Denial-of-Service (DoS) prevention. The security gateway functions as a physical firewall between networks. Since both OT networks utilize TCP-based protocols, we implemented two separate firewall filters: one allowing all TCP traffic and another permitting traffic only within a specified port range for current TCP connections.

The final security appliance tested was a software-defined switch, which replaces a standard managed or unmanaged switch more commonly found in traditional OT networks. For this, we utilized an OpenFlow-configurable switch designed for OT network configurations, which is capable of enforcing physical routing restrictions. For testing, each switch was configured to allow communication exclusively between the Gateway and its respective OT devices on each bus, namely the DNP3 outstation and the PLC.

4. Results

For the initial testing of the Exponential Backoff behavior, the server was disconnected from the testbed. The backoff, as shown in Figure 4, increased until the server was reconnected, in this case, the last delay being 42 seconds. However, as we show further below, this could be compounded by malicious traffic that can prolong the re-connection phase.



```
31.280306951  Client  Server  TCP       66 59356 → 502 [FIN, ACK] Seq=325 Ack
33.250885524  Client  Server  TCP       74 40744 → 502 [SYN] Seq=0 Win=29200
38.250909345  Client  Server  TCP       74 40783 → 502 [SYN] Seq=0 Win=29200
44.251370026  Client  Server  TCP       74 40831 → 502 [SYN] Seq=0 Win=29200
51.254914871  Client  Server  TCP       74 40885 → 502 [SYN] Seq=0 Win=29200
60.250198368  Client  Server  TCP       74 40957 → 502 [SYN] Seq=0 Win=29200
72.251226160  Client  Server  TCP       74 41049 → 502 [SYN] Seq=0 Win=29200
114.251545510 Client  Server  TCP       74 41379 → 502 [SYN] Seq=0 Win=29200
114.252186640 Server  Client  TCP       74 502 → 41379 [SYN, ACK] Seq=0 Ack=1
114.252455659 Client  Server  TCP       66 41379 → 502 [ACK] Seq=1 Ack=1 Win=
114.255941759 Client  Server  Modbus…   78    Query: Trans: 46012; Unit:   2,
114.256549463 Server  Client  TCP       66 502 → 41379 [ACK] Seq=1 Ack=13 Win
114.258729649 Server  Client  Modbus…   76 Response: Trans: 46012; Unit:   2,
```

Figure 4. Increasing Impact of Exponential Backoff

4.1. *Testbed Effects of Malicious Traffic*

The focus of the testbed experiments was to validate our protocol review findings regarding the Modbus protocol's safety implications and also to illustrate the issues with connection re-establishment in Modbus TCP implementations. Towards that goal, we first conducted baseline performance measurements focusing on characterizing latency with and without security features, comparing the use of external security gateways and a software-defined switch. UDP broadcast packets were generated by the attacking agent, emulating additional background traffic from an active network. While each packet was routed to the interfaces of the OT devices, the packets had no data intended for the devices and were expected to be discarded during normal operation. The results, shown in Table 1, demonstrate minimal impact from the additional security features. This is likely due to the low link requirements of OT devices (operating at 100 Mbps) and the efficient processing capabilities of both the security gateway firewall and the software-defined switch.

Table 1. Latency Introduced by Security Gateway, Modbus TCP Traffic

Latency (ms)	**Background Traffic (Mbps)**										
	5	10	15	20	25	30	35	40	45	50	55
Gateway	2.898	3.123	2.880	2.896	2.835	2.924	2.865	2.931	2.886	3.107	3.117
Security Gateway	3.001	3.201	3.0331	3.277	3.210	3.070	3.093	3.900	3.086	3.002	3.192
Difference (ms)	0.103	0.078	0.153	0.381	0.374	0.146	0.227	0.968	0.199	-0.104	0.074

Since the TCP connection time was the focus of our tests, and the security appliances added limited latency to the communication, the attacking agent was subsequently utilized to imitate new connection requests using SYN messages to the server side, and Reset (RST) requests to the client, as shown in Figure 5.

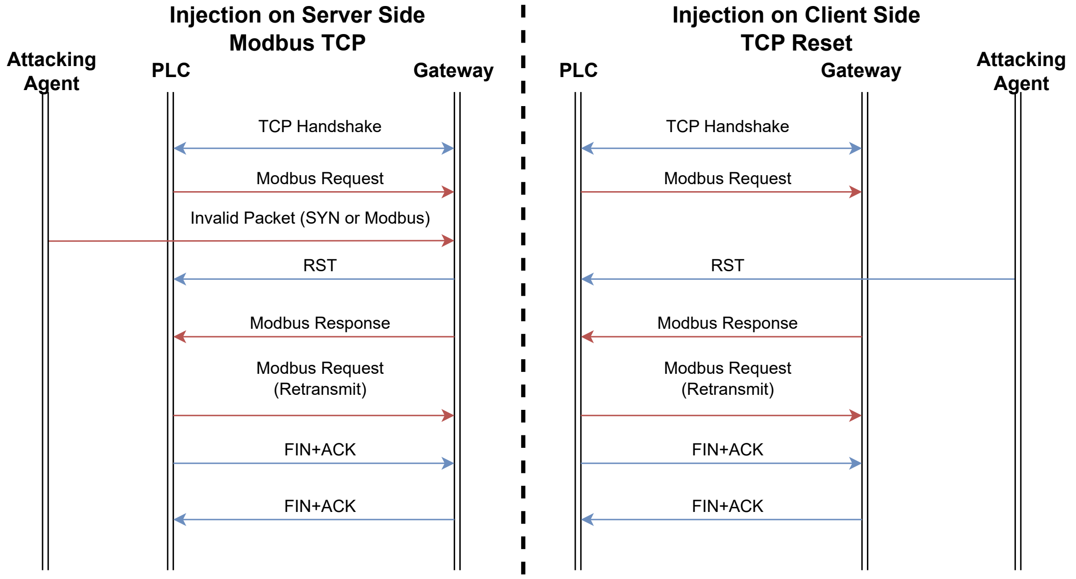


Figure 5. Generated Traffic for Single-Sided TCP Connection Closure

This attack mimics a SYN-Flood attack that might be carried out on other TCP connections. However, by changing the IP and MAC addresses listed within the packet, we can successfully trick the gateway into sending the reset packet to the PLC. This, in effect, tells the PLC (client) that the connection has been closed and a new one needs to be initiated. The effect of this can be seen in Figure 6. If these attacks are applied consistently over a long period of time, the communication can effectively be stopped between the two devices, requiring minimal effort by the attacker.

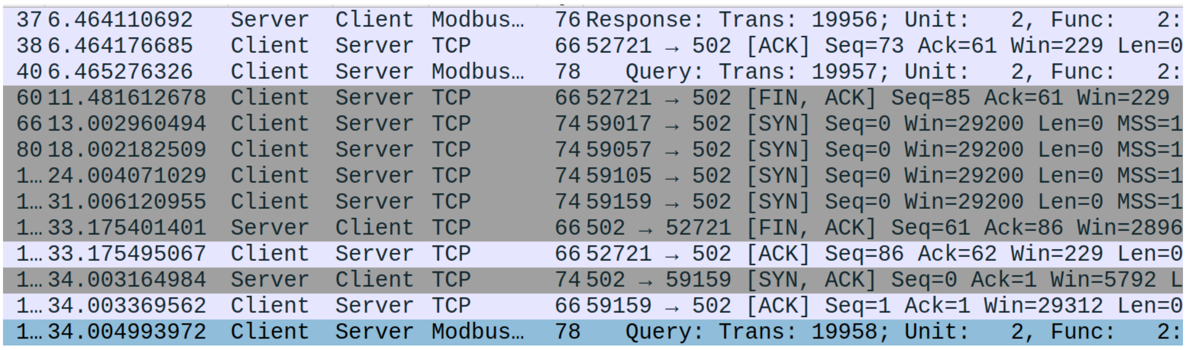

```
37 6.464110692   Server  Client  Modbus…   76 Response: Trans: 19956; Unit:   2, Func:   2:
38 6.464176685   Client  Server  TCP       66 52721 → 502 [ACK] Seq=73 Ack=61 Win=229 Len=0
40 6.465276326   Client  Server  Modbus…   78    Query: Trans: 19957; Unit:   2, Func:   2:
60 11.481612678  Client  Server  TCP       66 52721 → 502 [FIN, ACK] Seq=85 Ack=61 Win=229
66 13.002960494  Client  Server  TCP       74 59017 → 502 [SYN] Seq=0 Win=29200 Len=0 MSS=1
80 18.002182509  Client  Server  TCP       74 59057 → 502 [SYN] Seq=0 Win=29200 Len=0 MSS=1
1… 24.004071029  Client  Server  TCP       74 59105 → 502 [SYN] Seq=0 Win=29200 Len=0 MSS=1
1… 31.006120955  Client  Server  TCP       74 59159 → 502 [SYN] Seq=0 Win=29200 Len=0 MSS=1
1… 33.175401401  Server  Client  TCP       66 502 → 52721 [FIN, ACK] Seq=61 Ack=86 Win=2896
1… 33.175495067  Client  Server  TCP       66 52721 → 502 [ACK] Seq=86 Ack=62 Win=229 Len=0
1… 34.003164984  Server  Client  TCP       74 502 → 59159 [SYN, ACK] Seq=0 Ack=1 Win=5792 L
1… 34.003369562  Client  Server  TCP       66 59159 → 502 [ACK] Seq=1 Ack=1 Win=29312 Len=0
1… 34.004993972  Client  Server  Modbus…   78    Query: Trans: 19958; Unit:   2, Func:   2:
```

Figure 6. Increasing Impact of Exponential Backoff

However, there are built-in mitigation strategies within many devices for this case. An example is the SYN-Flood protection available within the Gateway's configuration. However, this protection seems to only come into effect after 50 or more packets are received per second, which we tested in increments of 5, as shown in Figure 7. This figure shows that even with SYN-flood mitigation attempts that act to prevent Denial of Service, access to the network makes communication disruption possible and trivial.

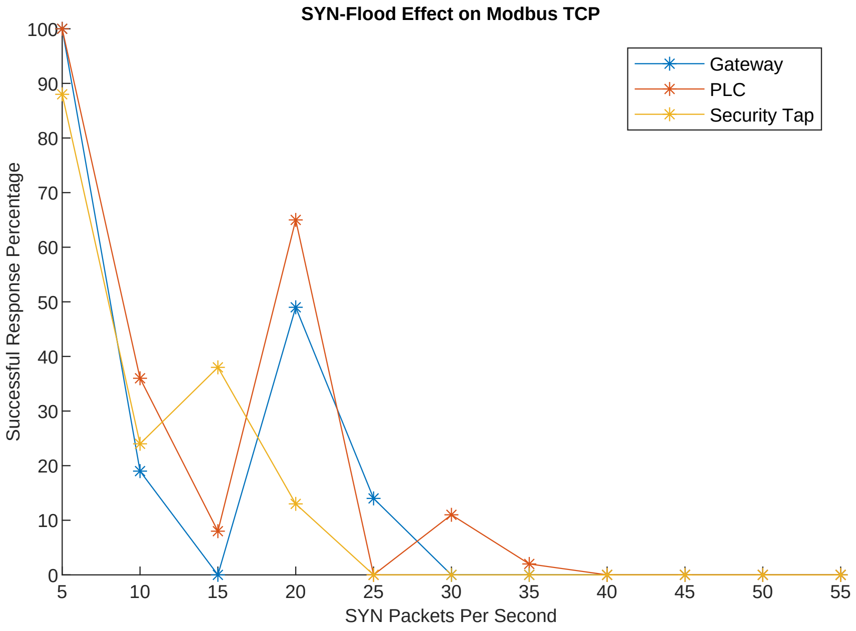


Figure 7. Modbus TCP Effective Transactions in Response to SYN-Flood Traffic

A further interesting observation from this behavior was that the PLC failed to correctly filter the packet for the correct port number. To have the intended effect, the attack packet needed to be timed to arrive while the PLC was awaiting a Modbus response. Any packets received outside of this window were handled correctly. Additional testing revealed that the PLC did not correctly filter these packets based on port numbers, sequences, or acknowledgment numbers. Thus, subsequent connection attempts could also be reset by the same reset packet. However, these packets required the sequence and acknowledgment numbers to increment to avoid being processed as retransmissions.

As previously mentioned, recovery from the SYN flood attack was significantly complicated by Modbus TCP's back-off mechanism. When the connection was abruptly terminated, the PLC would increase the time between reconnection attempts. As a result, prolonged attack traffic caused longer outages. During testing, the communication link took anywhere from 20 seconds to 5 minutes to re-establish, depending on the length of the SYN flood attack.

Furthermore, we observed adverse effects on the gateway's response time, even though the Modbus TCP communication link remained functional. As shown in Figure 8, PSH+ACK packets occasionally triggered large latency spikes of up to 100 ms. These spikes were unpredictable, which could lead to issues in systems requiring low latency. Interestingly, when these spikes were absent, the gateway responded consistently within 3 ms without having to retransmit packets during the study.

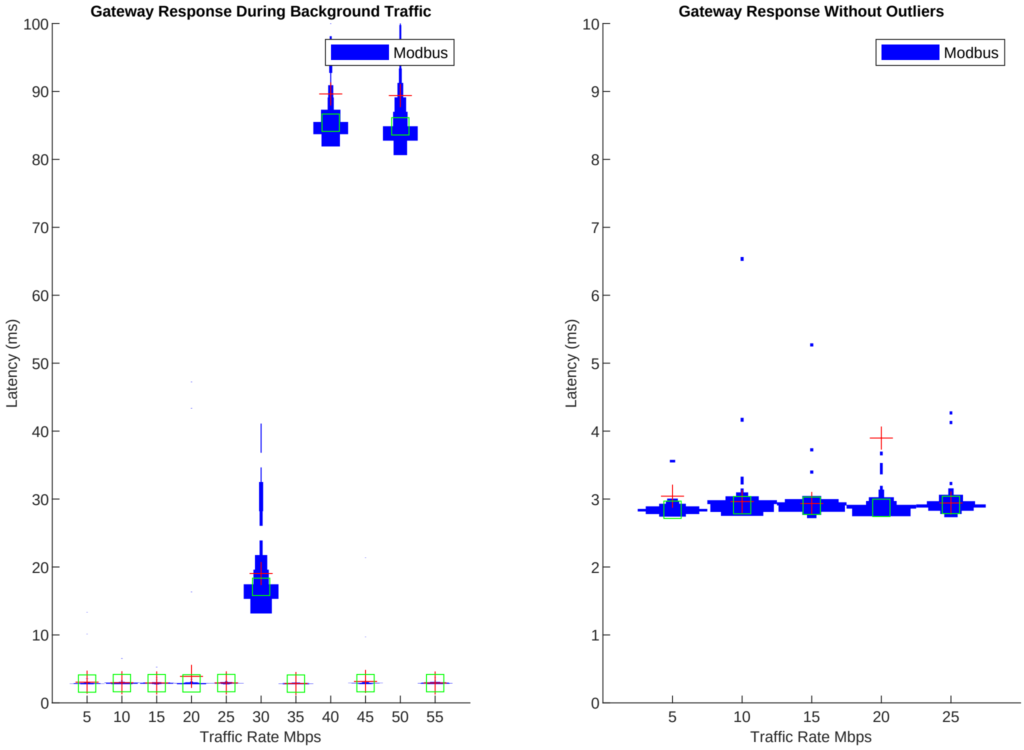


Figure 8. Response Time Deviation in Response to Additional PSH-ACK Packets

Several optional security features were enabled on both the protocol and security gateways to gauge their effectiveness in preventing the aforementioned attacks. These features included SYN-Flood protection, SYN-scan protection, and DoS protection on the protocol gateway. The security gateway acted as a physical firewall and was tested by limiting traffic to TCP and restricting specific port ranges. Finally, the software-defined switch was reintroduced with static route declarations to ensure that only the PLC and protocol gateway could communicate over Modbus TCP. A second switch was added to the DNP3 network to ensure that only the DNP3 outstation and protocol gateway could communicate with each other.

The results of these tests are summarized in Table 2. From these results, it is evident that the software-defined switch effectively mitigates external attacks, as any attacks would require physical alteration of a device or access to the switch configuration. However, several security features aimed at addressing the vulnerabilities identified in the tests failed to prevent communication loss. The protocol gateway's SYN-Flood protection, for instance, only triggered when the rate of SYN packets exceeded 50 packets per second. Therefore, attacks with fewer than 50 packets per second were capable of disrupting Modbus TCP communication without triggering the protection. Similarly, the DoS prevention mechanism encountered similar limitations, as the attack traffic did not meet the threshold required to activate packet blocking.

The security gateway had more success mitigating SYN-Flood and RST attacks by filtering traffic to specific ports. However, standard firewall features that restricted traffic to TCP alone failed to prevent SYN attacks, and port filtering only worked if the SYN flood did not duplicate the restricted ports.

Table 2. Effect of Security Features on Vulnerabilities

Protection Tested	Attacks			
	SYN-Flood	**RST Attack**	**External Connection**	**Background Traffic**
None	X	X	✓	✓
Gateway				
SYN-Flood Protection	X	X	✓	✓
DoS Prevention	X	X	✓	✓
Security Gateway				
All TCP Allowed	X	X	✓	✓
Port Specific Filtering	✓	✓	✓	✓
Software Defined Switch				
Static Route Configuration	✓	✓	✓	✓

*✓ - Attack Prevented X - No effect

5. Results Discussion

The results of our protocol review and subsequent testbed validation experiments highlight significant disparities in the resilience and responsiveness of Modbus TCP and DNP3 when subjected to communication failures. One of the primary issues identified was the impact of Modbus TCP's reliance on a single-ended communication model, which delegates all responsibility for connection re-establishment to the client. This architecture, inherited from Modbus' serial communication roots, lacks the robustness required for time-sensitive operations within modern OT environments, and was clearly illustrated by our experimental results. We also showed that the exponential backoff mechanism, while a standard feature of TCP/IP to prevent congestion, introduces unacceptable delays in scenarios where prompt data transmission is critical, such as when OT protocols are used in safety-critical environments or scenarios. Our tests revealed that connection recovery delays can approach or exceed 40 seconds, which could be catastrophic in industrial contexts requiring real-time actuation or monitoring.

In contrast, DNP3's more symmetrical approach to connection management, where both the Master and Outstation may initiate communication, provides enhanced resilience. The specification's support for re-connection upon data availability ensures quicker recovery from network disruptions, particularly in distributed or resource-constrained environments. These protocol-level behaviors underscore the importance of selecting communication standards based not just on compatibility or performance, but also on fault tolerance and the expected operational environment.

Our testbed simulations further reinforced these findings. The integration of Modbus TCP with DNP3 via a gateway offered a practical bridge between legacy and modern OT systems but also introduced new potential points of failure. In particular, gateway devices, if misconfigured or targeted by malicious traffic, may become bottlenecks or vulnerabilities in the network. However, our implementation of defense-in-depth mitigations, including a dedicated security gateway and software-defined switching, proved to be effective. Despite introducing minor additional latency (as shown in Table 1), these tools can significantly enhance the security posture of OT networks with negligible performance penalties.

Importantly, these mitigations help address a broader concern observed in related works: the lack of intrinsic security in many legacy OT protocols. Unlike newer industrial communication standards, both Modbus TCP and DNP3 were not originally designed with cybersecurity threats in mind. While DNP3 has evolved to include secure authentication, the default behavior of many deployed systems still reflects legacy assumptions. Therefore, supplementary protection mechanisms, such as whitelisting and SYN-flood prevention, remain essential components in securing these networks.

Our results also align with findings from previous literature. Similar to other studies that identified the performance degradation of Modbus in high-BER environments [18], our observations show that the protocol's resilience is further reduced under real-world failure conditions. Moreover, the minimal additional latency introduced by modern OT security appliances supports the position advocated by [17] that security enhancements can be applied without sacrificing system performance.

6. Conclusions

In this study, we examined the behavioral differences and vulnerabilities inherent in two widely used OT protocols, Modbus TCP and DNP3, within the context of communication failure scenarios and security threats. Driven by our protocol specification review, we identified reconnections as a critical consideration and differentiator between these two protocols, especially for safety-critical OT applications. Through a multi-tiered testbed, we then validated our finding that Modbus TCP's dependence on single-ended recovery mechanisms and TCP-level exponential backoff creates significant latency issues in time-sensitive applications. Conversely, DNP3's dual-role communication model provides more resilient recovery behavior in the face of disruptions.

The results emphasize the importance of protocol-aware design in OT system architectures, particularly when integrating legacy systems into modern networked infrastructures. Furthermore, we showed that defense-in-depth strategies, such as the deployment of security gateways and software-defined switches, can effectively mitigate common vulnerabilities without imposing considerable overhead.

As the convergence between IT and OT continues, and as Industrial IoT deployments grow in scale and complexity, future work should focus on developing adaptive protocol frameworks that combine the backward compatibility of legacy standards with the fault tolerance, scalability, and security required in today's industrial environments. Additionally, broader adoption of protocol-aware intrusion detection systems and protocol-hardening techniques will be essential in safeguarding critical infrastructure from evolving threats.

Author Contributions: Investigation, M.B., P.S., M.H., and H.S.; writing—original draft preparation, M.B., P.S., and M.H.; writing—review and editing, M.B., P.S., M.H., H.S., and J.L.; supervision, H.S. and M.H.; project administration, H.S., M.H.; funding acquisition, H.S. and M.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially funded by the University of Nebraska-Lincoln's Nebraska Center for Energy Sciences Research (NCESR) under Cycle 16 Grant# 20-706.

References

1. Boeding, M.; Boswell, K.; Hempel, M.; Sharif, H.; Lopez Jr, J.; Perumalla, K. Survey of cybersecurity governance, threats, and countermeasures for the power grid. *Energies* **2022**, *15*, 8692. https://doi.org/10.3390/en15228692.
2. Manias, D.M.; Saber, A.M.; Radaideh, M.I.; Gaber, A.T.; Maniatakos, M.; Zeineldin, H.; Svetinovic, D.; El-Saadany, E.F. Trends in Smart Grid Cyber-Physical Security: Components, Threats and Solutions. *IEEE Access* **2024**. https://doi.org/10.1109/ACCESS.2024.3477714.
3. Modbus Organization, I. MODBUS Application Protocol Specification v1.1b3. *Modicon Inc. Ind. Autom. Syst. Tech. Rep* **2012**.
4. Power, I.; Society, E. IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3). *IEEE Std 1815-2012 (Revis. IEEE Std 1815-2010)* **2012**, pp. 1–821. https://doi.org/10.1109/IEEESTD.2012.6327578.
5. Labs, V. OT-Icefall: The legacy of "insecure by design" and its implications for certifications and risk management, 2022.

6. Porcu, D.; Castro, S.; Otura, B.; Encinar, P.; Chochliouros, I.; Ciornei, I.; Hadjidemetriou, L.; Ellinas, G.; Santiago, R.; Grigoriou, E.; et al. Demonstration of 5G solutions for smart energy grids of the future: a perspective of the Smart5Grid project. *Energies* **2022**, *15*, 839. https://doi.org/10.3390/en15030839.
7. Jafary, P.; Supponen, A.; Repo, S. Network Architecture for IEC61850-90-5 Communication: Case Study of Evaluating R-GOOSE over 5G for Communication-Based Protection. *Energies* **2022**, *15*. https://doi.org/10.3390/en15113915.
8. Boeding, M.; Hempel, M.; Sharif, H. End-to-End Framework for Identifying Vulnerabilities of Operational Technology Protocols and Their Implementations in Industrial IoT. *Future Internet* **2025**, *17*, 34. https://doi.org/10.3390/fi17010034.
9. Banik, S.; Manicavasagam, R.; Banik, T.; Banik, S. Simulation and analysis of cyber-attack on modbus protocol for smart grids in virtual environment. In Proceedings of the Science and Information Conference. Springer, 2024, pp. 384–401. https://doi.org/10.1016/j.dcan.2022.09.013.
10. de Brito, I.B.; de Sousa Jr, R.T. Development of an open-source testbed based on the modbus protocol for cybersecurity analysis of nuclear power plants. *Applied Sciences* **2022**, *12*, 7942. https://doi.org/10.3390/app12157942.
11. Rodriguez, J.D.P.; Boakye-Boateng, K.; Kaur, R.; Zhou, A.; Lu, R.; Ghorbani, A.A. SoK: A Reality Check for DNP3 Attacks 15 Years Later. *Smart Cities* **2024**, *7*, 3983–4001. https://doi.org/10.3390/smartcities7060154.
12. Ozdogan, E. Structured Defense Model Against DNP3-Based Critical Infrastructure Attacks. *Arabian Journal for Science and Engineering* **2024**, pp. 1–19. https://doi.org/10.1007/s13369-024-09577-3.
13. Kelli, V.; Radoglou-Grammatikis, P.; Sesis, A.; Lagkas, T.; Fountoukidis, E.; Kafetzakis, E.; Giannoulakis, I.; Sarigiannidis, P. Attacking and defending DNP3 ICS/SCADA systems. In Proceedings of the 2022 18th International Conference on Distributed Computing in Sensor Systems (DCOSS). IEEE, 2022, pp. 183–190. https://doi.org/10.1016/j.compeleceng.2024.109828.
14. Dangwal, G.; Mittal, S.; Wazid, M.; Singh, J.; Das, A.K.; Giri, D.; Alenazi, M.J. An effective intrusion detection scheme for Distributed Network Protocol 3 (DNP3) applied in SCADA-enabled IoT applications. *Computers and Electrical Engineering* **2024**, *120*, 109828.
15. Elamanov, S.; Son, H.; Flynn, B.; Yoo, S.K.; Dilshad, N.; Song, J. Interworking between Modbus and internet of things platform for industrial services. *Digital Communications and Networks* **2024**, *10*, 461–471.
16. Bastidas, A.J.C.; Méndez, G.L.A.; Revelo-Fuelagán, J.; Candelo-Becerra, J.E. Performance evaluation of modbus and DNP3 protocols in the communication network of a university campus microgrid. *Results in Engineering* **2024**, *24*, 103656. https://doi.org/10.1016/j.rineng.2024.103656.
17. Katulić, F.; Sumina, D.; Groš, S.; Erceg, I. Protecting modbus/TCP-based industrial automation and control systems using message authentication codes. *IEEE access* **2023**, *11*, 47007–47023. https://doi.org/10.1109/ACCESS.2023.3275443.
18. Rodríguez-Pérez, N.; Domingo, J.M.; López, G.L.; Stojanovic, V. Scalability evaluation of a Modbus TCP control and monitoring system for Distributed Energy Resources. In Proceedings of the 2022 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). IEEE, 2022, pp. 1–6. https://doi.org/10.1109/ISGT-Europe54678.2022.9960319.
19. Huang, H.; Davis, C.M.; Davis, K.R. Real-time power system simulation with hardware devices through dnp3 in cyber-physical testbed. In Proceedings of the 2021 IEEE Texas Power and Energy Conference (TPEC). IEEE, 2021, pp. 1–6. https://doi.org/10.1109/TPEC51183.2021.9384947.
20. Moldovan, D.; Ayyanar, R. DNP3 Implementation in a High DER Penetration Distribution System. In Proceedings of the 2024 IEEE Kansas Power and Energy Conference (KPEC). IEEE, 2024, pp. 1–5. https://doi.org/10.1109/KPEC61529.2024.10676137.
21. Boeding, M.; Hempel, M.; Sharif, H. Vulnerability Identification of Operational Technology Protocol Specifications Through Formal Modeling. In Proceedings of the 2023 16th International Conference on Signal Processing and Communication System (ICSPCS), 2023, pp. 1–6. https://doi.org/10.1109/ICSPCS58109.2023.10261127.
22. Modbus Organization, I. MODBUS Messaging on TCP/IP Implementation Guide V1.0b . *Modicon Inc. Ind. Autom. Syst. Tech. Rep* **2012**.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.