Hindawi
Security and Communication Networks
Volume 2018, Article ID 3794603, 21 pages
https://doi.org/10.1155/2018/3794603

Research Article

Vulnerability Analysis of Network Scanning on SCADA Systems

Kyle Coffey, Richard Smith, Leandros Maglaras, and Helge Janicke

De Montfort University, Leicester, UK

Correspondence should be addressed to Leandros Maglaras; leandrosmag@gmail.com

Received 14 September 2017; Revised 5 December 2017; Accepted 5 February 2018; Published 13 March 2018

Academic Editor: Jianying Zhou

Supervisory Control and Data Acquisition (SCADA) systems and Industrial Control Systems (ICSs) have controlled the regulation and management of Critical National Infrastructure environments for decades. With the demand for remote facilities to be controlled and monitored, industries have continued to adopt Internet technology into their ICS and SCADA systems so that their enterprise can span across international borders in order to meet the demand of modern living. Although this is a necessity, it could prove to be potentially dangerous. The devices that make up ICS and SCADA systems have bespoke purposes and are often inherently vulnerable and difficult to merge with newer technologies. The focus of this article is to explore, test, and critically analyse the use of network scanning tools against bespoke SCADA equipment in order to identify the issues with conducting asset discovery or service detection on SCADA systems with the same tools used on conventional IP networks. The observations and results of the experiments conducted are helpful in evaluating their feasibility and whether they have a negative impact on how they operate. This in turn helps deduce whether network scanners open a new set of vulnerabilities unique to SCADA systems.

1. Introduction

ICS and SCADA systems are an integral aspect of the modern industrial environment and the Critical National Infrastructure (CNI). For many years, SCADA and ICS networks were a completely independent sector of any business or agency, where the field devices and industrial mechanisms which interacted with physical assets were separate from the corporate networks or intranet. However, as Internet technologies became ever more integrated into modern society, and as corporations began to grow exponentially around the globe, the demand for remote auditing and control of industrial systems increased. This resulted in the merging of Internet Protocol (IP) and SCADA/ICS technologies, which in turn exposed the older field devices to a new set of attack vectors, leading to unprecedented vulnerabilities when integrated with IP [1]. In an age where threats from the cyberdomain are ever evolving, the tools used to perform security audits and penetration tests against IP systems are subsequently being used on the older SCADA/ICS networks. These tools, without the correct configuration, could cause substantial damage to the SCADA devices connected to a business's infrastructure, rather than helping to protect and audit them [2].

SCADA and ICS technologies are prevalent not only within manufacturing industries, but also within the organisations responsible for the safety and wellbeing of citizens around the globe [3]. Water treatment facilities, electrical grids, and nuclear power stations all rely on a combination of SCADA and IP networks in order to control the distribution and regulation of the services they provide [4]. As these industries have become greater in both scale and complexity, the automation and upkeep of all the technology within these environments must be handled by machines and computers. Having the ability to remotely monitor and control large industrial sights allows companies and industries to expand their capabilities in order to provide more services to the general public, whilst at the same time making the data accessible to the staff responsible for operating and engineering the technologies in question. Half of significant security incidents that are occurring are due to a particular element, which has not been changed since the inception of information security management, which is people [5]. All the examples stated above contain resources which not only are essential to the operation of modern-day life but could potentially have devastating consequences if any of these systems were to malfunction. These systems threaten not only the lives of the people who use this technology but also the environments and the civilisations which surround these facilities [6].

Similar to when a cyberattack is launched against a company's database or web server, the exploitation or misuse of the devices found on a SCADA network can have negative effects on both the clientele and the corporation [7]. However, unlike the IP networks in abundance today, SCADA systems are threatened not only by hackers wishing to exploit vulnerabilities in software or firmware but also by the tools commonly associated with monitoring, auditing, and securing networks. Using tools which have not been configured to interact with the bespoke devices that reside on SCADA networks could cause the devices to become unresponsive [2] or alter the data being received by the device or being stored on the device [7]. In such an event, field devices including water pumps, electricity generators, or pneumatic instruments could either stop functioning or begin to behave erratically, causing damage to either the devices themselves, the products they interact with, or the customers who use their facilities. Whereas IP networks can cause significant damage to intellectual property and personal privacy, there is evidence that malfunctioning SCADA systems have caused physical damage [8], all of which could be an effect of using the wrong security tools on incompatible networks.

Although there has been recognition within the industry that the improper use of IP scanners has caused failures within an industrial control process, there has been a lack of resources directed at educating people on exactly why these IP scanners cause issues and whether there are any alternative methods which can facilitate a stable scan of a SCADA system. The existing literature highlights that IP scanners are being used to gain information about SCADA systems [9], the types of devices that are potentially vulnerable when scanned [10], and the consequences of performing scans on live systems [7].

The key aim of this article is to identify how network scanners interact with SCADA devices and whether or not they cause significant disruption to the way these devices operate. Also, the results of this research aim to enhance the understanding of reconnaissance technologies when applied to SCADA networks. To do this, experiments need to be conducted in order to monitor how a range of network scanners execute their asset/service detection scans and to see if this causes the normal operation of SCADA networks to change or malfunction. Once this has been achieved, suggestions and a proof of concept will be made in order to provide an alternative method of scanning SCADA systems without damaging the network itself.

The following list details the main contributions of the article:

(1) Researching the different methods of detecting assets on a wide variety of different networks

(2) Evaluating the feasibility of performing scans on SCADA networks and how the results differ from IP networks

(3) Designing and developing a network scanner which facilitates the requirements of a SCADA network.

2. Related Work

The focus of this section is to explore and critically analyse the current research into the issues with conducting asset detection or network scans on SCADA systems with the same tools used on conventional IP networks. Emphasis will be on identifying the different types of network scanning methods and the tools which are currently available to security auditors, penetration testers, and black hat hackers. Reference will be made to the bespoke elements of SCADA systems, specifically the types of devices used to monitor and control field equipment such as sensors and valves. Discussion will then be targeted at how the current tools are used on these bespoke devices and whether they have a negative impact on how they operate. The intention is to identify how much knowledge there is about how these two technologies interact with each other and where the significant vulnerabilities may lie.

The analysis of sources within this document suggests that a better understanding is needed about how network scanners interact with SCADA networks. The lack of understanding of how SCADA devices react to being scanned and the subsequent consequences this may have is a significant factor which underlines the analysis in this document. It is clear that network scanners must be directly tested against nonoperational SCADA devices in order to report on how the two technologies interact and whether they are compatible. This will then allow the owners of these systems to better understand the consequences of using newer, IP-based tools on older SCADA networks. This knowledge will inform the users of SCADA how to adapt or develop new ways of performing asset detection without having damaging impacts on not only the devices themselves but the millions of civilians who rely on the integrity and consistency of these systems on a daily basis.

Reconnaissance, whether passive or active, lawful or malicious, remains one of the most important parts of any strategic cybersecurity operation [11]. Network scans help visualise the configuration of a communications infrastructure and help identify possible methods of entry or exploitation. Reconnaissance can be achieved through service detection and operating system fingerprinting, two key features of many network scanning tools [12]. Conducting reconnaissance within the cyberdomain has become even more vital as the CNIs of various countries are now governed and controlled using computer networks. These systems are responsible for the auditing and control of national grids, power stations, water treatment plants, and industrial production lines. As the technology and communication networks that run these systems have become outdated and consequently less secure, the question must be asked about how volatile are these devices when conducting network scans? Systems which have a direct impact on the wellbeing of human civilisation are falling victim to the same tools used to audit or attack corporate networks and Internet-based services. Unlike traditional networks which utilise TCP/IP technology, ICSs face numerous unique vulnerabilities due to the bespoke devices they use and the configuration of the services and functionality they provide [13]. IP-based networks can take advantage of Intrusion Detection Systems, firewalls, and anti-malware tools to identify and prevent snooping or open-port attacks that target a node or network. The operating systems which have been installed on SCADA/ICS devices such as programmable logic controllers (PLCs) and Remote Terminal Units (RTUs) may not have this capability. Furthermore, the ports which control the transfer of SCADA/ICS data run on insecure protocols [14], where even a single unexpected packet could cause a system overhaul and could stop the normal function of the equipment entirely. As these devices are the interface between networks and industrial assets such as pumps, turbines, and sensors, this could have significantly damaging consequences. The purpose of this study is to investigate the vulnerabilities which are created by the use of asset-detection tools on SCADA networks and whether they pose a significant threat to the integrity of these systems. Could the process of scanning a network for assets cause damage on a national scale? If so, what are the causes?

2.1. Methods of Network Scanning. Network reconnaissance is an essential stage in any cyberauditing or penetration testing operation. Whether using passive scanning systems or active probing tools, service discovery and asset detection are paramount towards assessing the overall vulnerability of a corporate network or industrial infrastructure [15]. The findings highlighted in [13] give a concise breakdown of the differences between these two methods of network reconnaissance. Details of how each method is executed and how different conditions may impact the monitoring process give an insight as to which is most beneficial within different political, technological, and time-sensitive environments. This information, however, fails to address how either of these techniques would perform on SCADA systems and gives little detail on the current tools available to facilitate the different network scans. Jaronim [16] focuses on outlining the current tools that are available within the public domain which can provide full network monitoring and scanning features. The key tools that are mentioned within this publication are Nmap and Nessus. Although the description and analysis of these tools are not as thorough as the information provided within Bartlett et al. [13], the crucial advantage is that the application and suitability of these technologies are directed towards SCADA systems. This information is highly advantageous as it helps highlight any significant pitfalls in the understanding of how SCADA reacts to network scans, as well as which technologies provided the best results. As this paper was published by the Air Force Institution of Technology in 2013, the technologies, tools, and scientific methods they used to conduct their research are more modern than those of Bartlett et al. [13]. A more modern approach to assessing the different methods of scanning is highlighted within Samtani et al. [9]. Like Bartlett et al. [13], the aim is towards evaluating and understanding scanning methodologies on SCADA systems. Although this source of information is far more modern than that of Bartlett et al. [13], there is a lack of detail when it comes to explaining how each method of scanning is achieved, as well as having a very limited scope when identifying the tools used to conduct scans. Bartlett et al. work [13], though older, is able to explain the technologies and processes behind scans in much greater detail. Collating the information from all the papers, focussing on the descriptive breakdown of both passive and active scanning methods, and with reference to the tools and technologies used within SCADA environments, the following deductions can be made about the two methods of network scanning.

2.1.1. Passive Scanning. Passive scanning methods use the monitoring of network traffic to identify services, hosts, and clients. An observation point is set up on the network, requiring assistance from network administrators or network engineers to configure these systems for optimum results. As referenced in Xu et al. [17] passive scanners can be run continuously for large periods of time without disrupting regular network traffic or interacting with the devices themselves, as the input data for passive scanning tools is a direct feed of the network's traffic. This means that algorithms can be created in order to dissect each protocol. This has the potential to extract important information and identifiers from each packet. An independent passive scanner designed by Gonzalez and Papa [18] demonstrates how a simple algorithm can be created to extract Modbus traffic from a network and gain information about master and slave devices as well as monitoring the status of Modbus transactions. Although the algorithms presented in this article demonstrate the versatility of passive scanners, the tools are still only limited to analysing a single SCADA protocol. The validity of the algorithms could also be challenged as this system was designed and implemented in 2007. There is a significant chance that changes may have been made to this particular protocol which makes the extraction and parsing system redundant [19]. Through inspection of these papers it is evident that passive systems seem to satisfy one of the main criteria of this research, compliance with regular network traffic and the avoidance of interacting with the volatile field devices.

2.1.2. Active Probing. The process of active probing has one significant difference to passive sniffing: live interaction with the devices. Bartlett et al. [13] define active probing as *"attempting to contact each service at each host. Sending packets to each host and monitoring the response."* This is then contradicted within Deraison and Gula [20], where it is stated that *"any use of a network scanner to find hosts, services and vulnerabilities is an active assessment."* When comparing the justification of active scanning from both papers, the comments provided within Deraison and Gula [20] seem biased and irrational on the basis that the organisation publishing this paper has a large investment in active scanning tools. However, both papers agree regarding the pitfalls of active techniques, this method produces data for the current state of the system. This information could become obsolete as time passes, or indeed when repeating the same scan at a later date.

In evaluating the information given in the previous sources, the process of passively scanning a network seems to be far more applicable to gaining information about devices on an ICS or SCADA network. As referenced in both Bartlett et al. [13] and Deraison and Gula [20] active methods require some form of interaction with the devices on the network, which could be one of the potential ramifications of using active tools against SCADA devices, as opposed to the passive methodologies discussed in Xu et al. [17] which run for a longer period at an *"observation point"* on the network, removing the need to send or receive data from any devices that are connected.

2.2. Existing Tools. From discussing the key advantages and disadvantages of each scanning methodology, attention can then be brought to the current technologies and tools available in the public domain.

2.2.1. Nmap. Bartlett et al. [13] discuss the use of Nmap as an example of active network probing. The conditions on which Nmap is used are confined to a very limited set of network technologies. The main focus seems to be standard corporate networks with services such as HTTP, SSL, MySQL, and SMTP. The application of Nmap against these services demonstrates how active probing works in a TCP/IP environment; however, it fails to address how Nmap is used on more bespoke networks such as SCADA and ICS. Bodenheim [10] gives a more relevant example of Nmap being used on the networks of interest. This paper provides explanations behind specific Nmap commands and how it achieves the desired output. There is, however, no reference to Nmap being an active and intrusive scanning type; therefore no information is supplied about how this could impact the operation of a SCADA or ICS network. Jaronim [16] supports the information presented in Bartlett et al. [13], enforcing the fact that Nmap is an active probing mechanism. Again it is evident that there is little understanding as to how probes such as Nmap impact the ordinary functions of SCADA and ICS networks.

2.2.2. Nessus. Nessus is a tool developed by Tenable Network Security. Peterson [21] discusses how Nessus can be used to scan for vulnerabilities within a control system environment with reference to *"a vulnerability scan that takes down a key control system server or component."* There is also reference to the damaging effect this could have. The general opinion is that SCADA systems should not be scanned. With this attitude presented at the beginning of the paper, Peterson goes on to explain how Nessus works and how it can be tailored to facilitate SCADA networks. The information that follows seems to disregard the damaging impact Nessus could have on an ICS/SCADA system by stating that, due to the number of plug-ins associated with the tool, some of the extended functionality may cause control systems to crash. This suggests that there is still a lack of understanding as to why these crashes happen, as the remedies in this paper suggest trial and error with the Nessus tool until the cause is found. Jaronim [16] acknowledges the Nessus tool and again highlights its potential to cause significant disruptions when used on SCADA networks. This paper still fails to specify why Nessus, or even the wider range of active probing tools, causes this disruption. However, Jaronim brings attention to a report justifying how active techniques can have damaging consequences. This report is one of the only research documents to directly relate the sensitivity of SCADA technology to a documented report of a damaging incident. Although the description of how scanning tools operate lacks in sophistication, Jaronim is able to link the pitfalls of active scanning to real-world examples of SCADA disruption, an area which has been neglected in previous sources.

2.2.3. Passive Vulnerability Scanner (PVS). Maintained by the same organisation responsible for Nessus, PVS is a passive accompaniment to the suite of network scanning tools provided by Tenable Network Security. Deraison and Gula [20] define a passive tool to be a mechanism which *"sniffs network traffic to deduce a list of active systems."* What is interesting within this paper is that PVS and passive scanning as a whole are associated with the *"sniffing of a network, as opposed to scanning."* Both Xu et al. [17] and Gonzalez and Papa [18] fail to elaborate on this underlying detail. Contrary to initial expectations, Deraison and Gula [20] fail to discuss how PVS or any other passive system achieves its goals as an unobtrusive scanner. No breakdown of technology is given and there is little evidence of PVS being used successfully on a range of networks. Seeing as this source is provided by Tenable, the validity of the claims in this paper could be considered biased, whereas Xu et al. [17] and Gonzalez and Papa [18] and Myers et al. [22] clearly identify how passive technology works and give examples of live experiments. From the information provided within these sources it seems that the use of passive network sniffers over a longer period of time is the most beneficial and nonintrusive way of performing reconnaissance on SCADA systems.

2.2.4. ZMap. With similar functionality to Nmap, ZMap is an open-source active network prober designed to perform Internet-scale scans. The probing of Large Area Networks (LANs) is achieved using TCP-SYN and ICMP echo scans. This is addressed in Durumeric, Wustrow, and Halderman [23]. Not only is the active technology behind ZMap discussed in detail, but also each element of the ZMap functionality is dissected and explained at a substantial technical level, including its modular framework for dissecting different protocols. Amongst these pieces of information, reference is made to limitations of certain networks which may result in the tool not working correctly, particularly when the scan rate of the probing packets being sent is too high for the target infrastructure. Although an experiment was conducted to investigate whether there is a correlation between *"scan rate"* and *"hit rate"* when probing a network, the results are more concerned with the efficiency and success of the tool itself, not the potential damage this may cause to the target network. This is an issue when linking this research to ICS and SCADA systems, where the focus is on protecting the normal operation of the system rather than evaluating the success of the tool. No reference is made to the use of ZMap against SCADA or ICS systems. Li et al. [24] also make reference to ZMap and its ability to probe a multitude of different protocols through the use of plug-in modules. There is evidence to suggest that ZMap can be used to probe protocols such as DNP3, Modbus, and Siemens S7. Although

Table 1: A summary of the existing active and passive network scanning tools.

Tool	Summary
Nmap + ZMap	(i) Open source, active (ii) Uses a combination of ping sweeping, SYN scanning, and TCP connecting to determine which hosts reside on a network and which services they are operating. (iii) Version detection or full TCP connection could cause legacy systems to misbehave. (iv) Nmap Scripting Engine has allowed for bespoke modules to be created for SCADA protocols such as Modbus. (v) Could potentially threaten the operation of a ICS/SCADA system. (vi) ZMap has an almost identical capability but can scan Large Area Networks.
Nessus	(i) Commercial, active (ii) Working on a "policy" framework, Nessus allows users to conduct host discovery and vulnerability analysis in a similar way to Nmap, again using ICMP, TCP, and ARP scanning. (iii) Unlike Nmap, Nessus has the ability to actively probe each service to report on potential vulnerabilities, which could cause accidental DoS on SCADA systems.
Passive Vulnerability Scanner	(i) Commercial, passive (ii) Uses interface packet sniffing to dissect and analyse the data being sent over the network in order to gain information about the assets and services being deployed. (iii) Although it does not require any form of direct probing with nodes, PVS must be continuously ran in order to gain a better understanding of the network it is monitoring. (iv) It is not intrusive, but the time it takes to analyse traffic is significantly higher than the active alternatives.
Shodan	(i) Open source/membership based, active (ii) Uses similar techniques to Nmap, ZMap, and Nessus to find the services that are running on internet-facing devices. (iii) All results are then stored in a database for users of the Shodan search engine to query against. (iv) As this tool uses the same technology as other active scanners, it too poses the risk of affecting ICS/SCADA systems, especially as it has the capability to scan globally, meaning any CNI running legacy software could be at a significant risk. (v) Shodan has the potential to bring unwanted malicious attention to ICS/SCADA networks through the storing and reporting of information about ICS infrastructures.

this information shows that ZMap can be used on these networks, there is no evaluation of the success or the effects this tool has on the devices themselves. Unlike the paper by Durumeric et al. [23], there is no information present within this research which highlights potential performance issues that could be linked to the network type. On the other hand, neither paper addresses the potential impact this tool could have on the physical devices being probed.

2.2.5. Shodan. Shodan is a service which acts as a search engine to identify and index Internet-facing devices. Shodan has become of significant interest as many ICS and SCADA systems are identifiable via this tool. Bodenheim [10] directly explores how the technology behind Shodan impacts the devices connected to ICS. The level of detail supplied about how Shodan obtains its data is not as thorough as the previous sources discussing the other scanning tools. However, the general premise of the paper is different as it focuses on the possible harmful nature of network scanning techniques from its start. As the potential harms that scanners could cause are only briefly discussed in previous sources, Bodenheim [10] addresses research hypotheses relevant to the negative impact of using Shodan against ICS and SCADA systems. Where this paper draws significant differences in research is the type of negative impact that occurs after a Shodan scan. Whereas the key focus of this research is to find how the physical devices are affected, this source wishes to answer the question of whether or not an ICS or SCADA system will become more vulnerable because of their presence on the Shodan database, which in turn may convince malicious minds or state programs to attack these systems. The aim here is not to deduce the physical consequences to the field devices but rather does a Shodan scan encourage attacks? Jaronim's work [16] remains to be the only paper to directly acknowledge potential physical damage that can be done by active scanners such as Shodan. This paper, however, lacks the hypotheses and experimentation with active tools which run throughout Bodenheim [10].

This study provides a summary of each of these tools. Table 1 gives a concise breakdown of the key information about each of the tools referenced within this section.

2.3. The Impact on SCADA Systems. After consulting numerous sources to gain information about the current network scanners, their methods of execution, and whether they show any sign of harming the physical network devices, it is evident that minimal research has been conducted which emphasizes the potentially devastating consequences of an active scan and whether it causes disruption to ICS and SCADA field equipment. Although the information presented within the paper by Jaronim [16] does not conduct research or experiments into how network scanners affect physical devices, there is reference made to a report written by the Sandia National Laboratory which gives *"actual examples of negative behaviour in response to network scans."* Following the references made within both Jaronim [16] and Bodenheim [10], the report of Duggan et al. [7] discloses the details of multiple failed asset-detection operations performed on an active Process Control Systems (PCS) and SCADA systems. A ping sweep being used to gain information about the devices connected to the network caused a robotic arm to move 180 degrees, despite being in a standby state before the sweep was initiated. A similar ping sweep was conducted on a PCS network causing a circuit fabrication machine to hang on operation, resulting in £50k worth of damage to the production line. Lastly, a penetration test was conducted on a SCADA system responsible for gas utility. As a result of using penetration testing equipment, the system froze, meaning no gas could be distributed outside of the plant, causing a loss of service to the customers of the plant for 4 hours. This source then goes on to describe possible remedies for some of these failures. Despite suggesting alternate methods of gaining the same data as the failed network scans, the report does not elaborate on how these scanners affected the devices in great detail or whether there has been any successful deployment of the replacement methods. As the report was submitted in 2005, there may be the possibility that the technology once affected by scanning and probing tools may have been patched or secured since then. However, relating this report to the more modern sources referenced within this section, there is no evidence to suggest that there has been significant development within the area of cybersecurity and SCADA technology. It is clear from these documents that

(i) there exist a lot of related work that discuss how network scanners can be used for conducting vulnerability analysis in SCADA systems,

(ii) based on the analysis of the related work that was surveyed, it is evident that some have identified negative behaviours of physical devices that are caused from network scans,

(iii) there is still a lack of understanding as to exactly how scanners disrupt ICS and SCADA devices,

(iv) there is a lack of alternate methods of execution and examples of their success.

3. SCADA and ICS Technologies

This section identifies the technologies which are bespoke to ICS/SCADA systems and the potential vulnerabilities which could be exploited by the use of a network scanner.

3.1. SCADA Network Devices. In order to understand how penetration testing and network scanning interrogate ICS and SCADA devices, research must be conducted into the types of technologies which reside on these networks and how they differ to the more conventional IP-based systems. As most tools for security auditing or ethical/unethical hacking were developed for IP-based networks, it is vital to understand how an ICS or SCADA system differs in terms of the physical devices present on the network, what embedded or bespoke software is installed on those devices, and how that may cause defects or irregularities when faced with the existing scanning tools. Chromik et al. [25] give an extensive review as to how SCADA systems work on the physical layer of networking. programmable logic controllers (PLCs), Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IED) are all referenced within this paper, with details about how data from field devices is acquired or monitored by one of these physical machines. SCADA servers, historians, and Human Machine Interfaces (HMIs) are also mentioned as part of an informal system description, where the basic hierarchy and control flow of SCADA are outlined at a high level. Although this paper is able to highlight the main devices which are both unique and essential to SCADA and ICS, the amount of detail given as to how each device functions and communicates, in particular focussing on layers 3–7 of the Open Systems Interconnection (OSI) model, is significantly lacking in content and depth. Having knowledge of how each device utilises its data through each one of the OSI layers would be highly advantageous towards developing a clear understanding of how the process and services present on these SCADA nodes could potentially compromise the whole system. This paper fails to provide details in this area. National Communications System (2004) is much more descriptive about not only the physical devices which form a SCADA system but also the protocols they use. Here, SCADA data flow is explained using examples of the devices mentioned in Chromik et al. [25]. However, the description of each devices' responsibility is more elaborate, referring to how RTUs act as interfaces which convert electronic signals from the field devices into a protocol which can then be utilised by the extended network. This information is then extended to PLCs, demonstrating how the two technologies link together, and provides details about the history and evolution of these devices. The details this paper is providing about Distributed Network Protocol (DNP3) are very thorough and cover all areas of discussion around this protocol, for example, the relationship between DNP3 clients and servers, as well as showing a typical design diagram for a DNP3 network architecture. However, the paper fails to address the wider range of SCADA technologies and protocols which are still utilised in today's systems, that is, Modbus, Siemens S7, and so forth. The content of this paper seems to skip the details about the higher levels of the SCADA infrastructure, such as the HMIs and SCADA servers, something which was explained within Chromik et al. [25].

Complementing the information provided within the previous two sources is the work of Samtani et al. [9]. Although this paper is aimed at finding vulnerabilities within SCADA through the use of passive and active assessment techniques, the description of the SCADA specific devices supports the statements made in the previous papers. As this is a modern report, the information that is provided not only gives an up-to-date representation as to the devices that are used within SCADA networks but it also gives a brief comparison between old SCADA technology and how the Internet has caused changes to how SCADA and ICS are controlled and configured to facilitate the needs of a modern organisation or industry. Reflecting on the information provided from a range of different sources, the devices that are bespoke to ICS and SCADA systems should be the focal point of experimentation and research, which are Human Machine Interfaces (HMIs), programmable logic controllers (PLCs) [26], Remote Terminal Units (RTUs) [27], Intelligent Electronic Devices (IED) [26, 28, 29], and Master Terminal Units (MTUs) [9, 24, 25]. From this list it can be confirmed that the devices that are closest to the field are the ones which will need examining in more detail in respect of how network scanners could possibly affect them. Here, RTUs and PLCs appear to be the most critical devices to analyse. A diagram (see Figure 1) shows the typical configuration of a corporate and SCADA network, detailing where each of the devices operates in respect of the entire SCADA system.

3.2. The Fragility of SCADA Devices. Attention must be drawn to the vulnerabilities associated with the different SCADA devices listed above, as well as the constraints of each different type of SCADA network. Wood et al. [30] present a holistic end-to-end view of the requirements and medium-to-high severity risks and propose a generic security architectural pattern to address them. Wedgbury and Jones [31] identify that the components of a SCADA or ICS network could hold significant vulnerabilities when being targeted by a network scanner. This source explains that SCADA equipment, and the services they provide, has been designed and implemented with little attention having been paid to the operational security of these devices and their ability to handle errors or unexpected events. This has been referred to as having "poor network robustness." Wiberg [32] also identifies that SCADA devices are inherently vulnerable as they have not been designed or built to provide basic information security attributes of confidentiality, integrity, and availability (CIA). Wiberg also references the lack of standardisation within the automation manufacturing industry and implies that this may also be a significant reason why SCADA devices are vulnerable. A significant issue identified by Wiberg is that using active network scanners, such as Nmap, presents a weakness when attempting port recognition or service detection on SCADA devices. Wiberg states that active tools such as Nmap can use unusual TCP segment data to try and find available ports. Furthermore, they can open a massive amount of connections with a specific SCADA device but then fail to close them gracefully.

Identifying the fatal flaws between the network scanning tools and the devices themselves and being able to present a technical example is where Wiberg [32] triumphs over Wedgbury and Jones [31]. Although both sources acknowledge that SCADA devices could compromise a system due to the bespoke or legacy services they run, Wiberg [32] provides an explanation as to how the network scanning technologies conflict with these devices and the possible consequences. However, the level of technical detail provided by Wiberg [32] still lacks depth and only gives a high-level overview of both the technologies underlying one particular network scanner (Nmap). Later on in the paper, Wiberg goes on to describe some of the false-positives generated when executing a network scan on SCADA systems. Although this shows how fingerprinting SCADA devices can be difficult as some of the "commonly known" ports are used for bespoke protocols, no examples have been given to show a network scanner interfering with an old or volatile service causing the device to crash.

In order to protect SCADA systems a lot of methods and mechanisms were recently proposed [33, 34], including Intrusion Detection Systems (IDS) for embedded platforms or Distributed IDS for SCADA, device-level anomaly detection [35] and classification [36], IDS solutions combining network traces and physical process control data [37], and detection based on traffic and protocol models or approaches based on semantic analysis [38]. Cruz et al. [39] present a distributed intrusion detection system (DIDS) for Supervisory Control and Data Acquisition (SCADA) Industrial Control Systems. In [40] Cook et al. conduct a thorough analysis of IT security methods and how they could be applied within an ICS. All scan methods may induce additional privacy issues that must be addressed [41] when designing secure SCADA systems.

3.3. Differences between SCADA and Commercial IP Networks. After developing an understanding of the unique devices and protocols used within an ICS/SCADA system, key distinctions can be made between SCADA and TCP/IP-based networks, such as corporate infrastructures and the infrastructures which provide the underlying technology and functionality behind ICS and SCADA systems. Galloway and Hancke [42] review the key differences between *"industrial and conventional networks,"* detailing areas in SCADA such as implementation, real-time requirements, failure severity, and ruggedness. This source seems to suggest that the most notable differences between the two network types are as follows:

(i) The implementation of the network
(ii) The architecture which structures each node and subnet
(iii) The severity of the consequences if the network fails.

These attitudes are shared within Stouffer et al. [43]. However, this source highlights the significant difference in system operation and resource constrains. Here, information is given about how SCADA and ICS devices run on legacy systems (defined as an old method, technology, or an outdated computer system), meaning they are prone to vulnerabilities such as *"resource unavailability and timing disruptions."* This is then supported by the research within Duggan et al. [7], referring to the collateral damage caused by the ping sweep of an operational ICS network. Although this source of information predates the research of Galloway and Hancke, [42], it is able to answer two significant questions in support of the research into the potential volatility of SCADA devices when being scanned: the use of legacy systems correlates with the idea that legitimate system resources could be directly

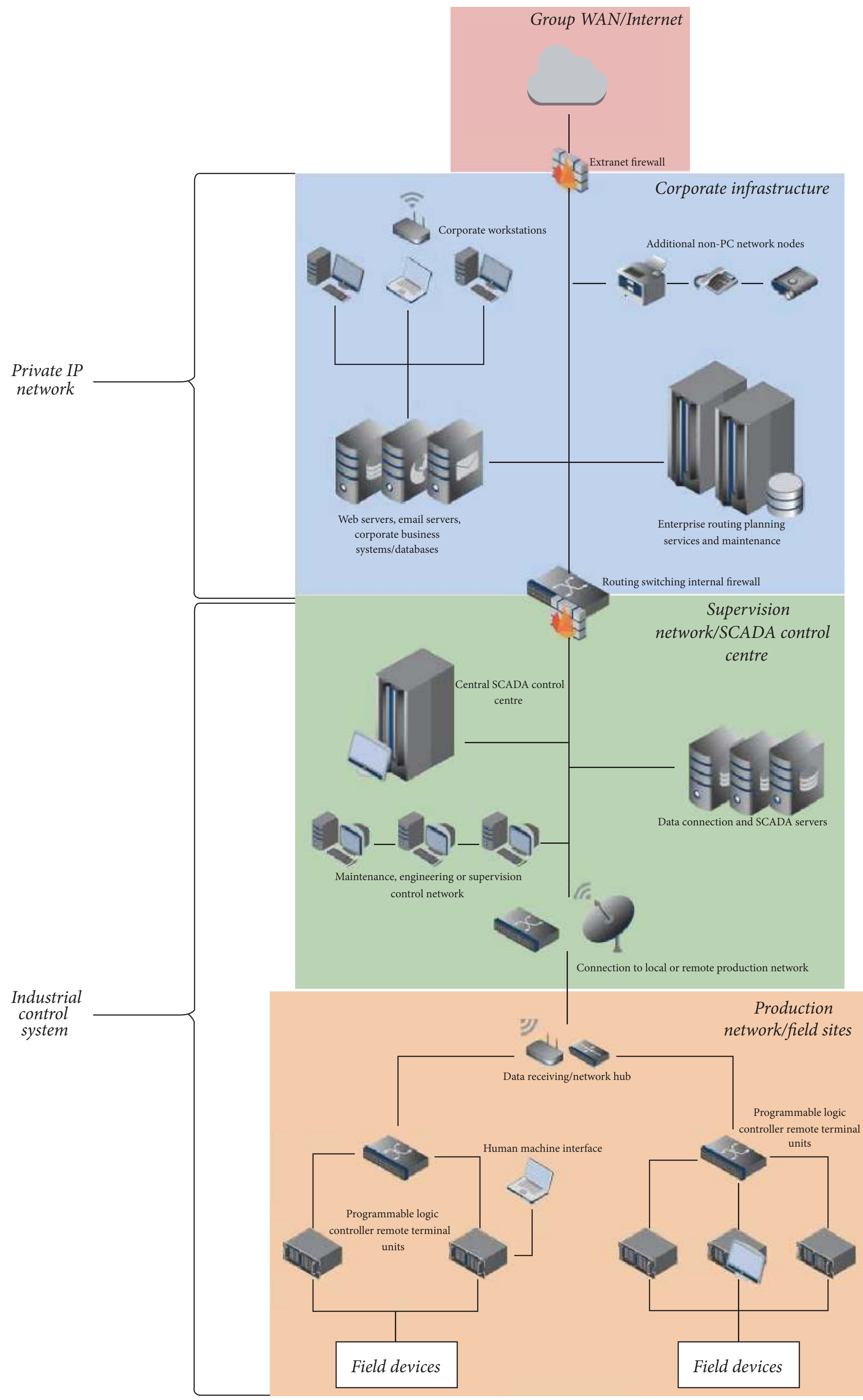


Figure 1: A network diagram showing the link between corporate and SCADA networks.

impacted by the use of conventional network auditing/pen-testing tools. This is supported by referencing the work of Franz [44]. Within this source, an experiment is conducted to survey vulnerabilities in Ethernet-enabled ICS devices. This experiment was conducted using active TCP/UDP scans and OS fingerprinting. The information within this source could be seen as irrelevant, not only because of the date it was published but also because of the fact that it is directly stated that an objective of the experiment is to *"Avoid automation protocols such as Modbus/TCP, Ethernet/IP, Fieldbus HSE, etc."* and to only focus on TCP/IP protocols. Although this was stated, the results of the experiment seemed to compliment the attitudes displayed by Jaronim [16], Bodenheim [10], and Duggan et al. [7], stating that *"Simple"* port scans (of 200–300) ports did cause some devices and applications to become unresponsive. Although this report may be outdated and tailored towards the research and development of Cisco's technologies, it provides evidence to support previous speculations or ideas portrayed in the previous sources. On the other hand, even though the experiment bared results which supported the hypotheses made by others, the protocols that are of particular interest were not the centre of Franz's research, meaning that further investigation must be done to determine the potential vulnerabilities these services could hold.

There is evidence to suggest that although network scanners have the ability to disrupt SCADA equipment, this having been acknowledged in many of the papers referenced, there is still a lack of understanding as to what aspect of the scanning process causes these devices to malfunction or behave erratically. The information which has been presented has helped identify where more research needs to be conducted, as well as how to formulate experimentation on nonoperational SCADA devices. Throughout the analysis of papers and reports, it became evident that although the awareness of potential vulnerabilities is there, few have gone to elaborate on why vulnerability scans may be unsuitable for use on SCADA networks, meaning there is a limited technical explanation as to why exactly these systems fail or malfunction. This coupled with the fact that most papers failed to enforce their opinions or claims due to having a lack of examples or references. This meant that proving the direct correlation between the use of network scanning tools and the damage of SCADA services or devices is difficult. A small subset of the sources within this document referenced a real-life example of an asset-detection incident that caused significant disruption to a couple of ICS networks. This was very insightful as it was able to detail what type of technology was used and what the consequences were. Although this part of the research benefited the understanding that ICS/SCADA systems can react negatively to scans, the research failed to directly satisfy a majority of the question areas, such as why a device or service behaved differently when a certain action was performed. Overall technical detail was hard to obtain. However, this did allude to further discussion which could potentially commend the reasoning for the current research.

As most of the sources simply implied that network scanners would have a negative impact on SCADA devices, this suggests that the reason for the lack of technical detail when investigating is because a large majority of SCADA systems are fully operational, meaning either reverse-engineering these incidents or testing tools against these systems is not practical as it could cause severe disruptions to the wellbeing of citizens on a national or global scale. This proves that, in order to understand and protect against possible network scanning vulnerabilities, the tools mentioned within this document need to be directly tested against nonoperational SCADA devices. With this taken into consideration, the sources highlighted the significant threat of using reconnaissance tools on these types of systems as they cannot be tested in the current environment.

Despite this there is very little information to suggest how active scans can be tailored to better facilitate the needs of SCADA networks. It is apparent that adjusting the current method of asset detection or creating a bespoke piece of software will be a more beneficial solution to reducing the risk of damaging networks with sniffers or probers, rather than trying to restructure or redesign the current systems and devices implemented across the globe. Much information has been provided about the different types of network scanning tools and techniques. From the information within each of the sources, it can be concluded that, from the two methods of network scanning, active probing has the potential to pose a much greater threat to ICS/SCADA devices rather than the passive sniffing alternatives. This research also provided thorough detail about the current tools available to pen-testers and how they can be applied to a range of different networks, but there has been little discussion on how successful these methods are against SCADA systems and whether they are an appropriate way of conducting vulnerability analysis on ICS/SCADA systems.

4. Method of Research

SCADA devices will continue to become integrated within IP networks regardless of the evident security vulnerabilities and the significant differences between the two communications technologies. The difficulty with replacing every ICS/SCADA device with a newer, more secure alternative is not a feasible option as these types of devices are responsible for controlling CNIs of countries around the globe. This in turn means that in order to ensure that these devices can be monitored and secured, whilst being connected to, and accessible by corporate IP networks, the current security tools must be compatible with both SCADA and IP. Research and experimentation are needed in order to evaluate the effects of using existing network scanning tools on ICS and SCADA equipment in order to justify the suitability and potential dangers on doing so.

When conducting a network audit or security scan or during the process of a malicious cyberattack, network scanners and sniffers are used in order to gain information about the devices present on the target network, as well as gathering data about the types of services they offer. These tools have been successful in gathering information about IP systems in numerous cybersecurity cases; however, this technology has not been adapted to facilitate scans on

SCADA networks. Experimentation and testing are needed in order to fully understand how network scanners and sniffers function and how these technologies could impact SCADA in a negative way. Being able to identify exactly how these two technologies interact will educate people on how to properly perform asset discovery or vulnerability scans on networks which hold ICS and SCADA devices. Research into the networking technologies present on both IP and SCADA networks is needed in order to understand the differences between them. The focus here was to dissect and analyse the way data is carried across each network so that when the IP and SCADA experiments commence, any anomalies or significant results can then be cross-referenced with the facts drawn from the research.

Alongside the research into the different network protocols and technologies, the network scanning tools also need to be executed and analysed in order to determine how they use specially configured protocols and packets in order to gain information about a network. The tools should be run on an IP network initially, before they are deployed against a SCADA environment. This will ensure that each scan is deployed, and they will all be executed successfully, meaning that the entirety of the scanning process can be witnessed and analysed without unexpected errors. This in turn will help broaden the understanding of how the technologies operate in order to gain information, and this can then be combined with the previous network technologies research in order to make assumptions and hypothesise about the application of scanners on SCADA systems such as SCADA. In order to achieve this, a Netkit lab was created in order to provide a virtual testing environment which replicated a small IP network. Once a Netkit network had been created, a series of passive and active network scanners were executed against the virtual machines which resided on that network. The packets sent between the scanning system and the virtual machines were captured and saved into a packet capture (.pcap) file format. Here, the traffic could be analysed and explained in detail, allowing for statements to be made about the suitability of running these scans on SCADA equipment/systems.

The same tools must then be executed against SCADA devices following the premise set by the previous research and experiments. These experiments will test the hypothesis *"Does the use of current active or passive IP network probers and sniffers have a negative effect on the normal behaviour of SCADA specific devices?"* This demonstrates how the network scanners and sniffers function on SCADA networks, how they interact with each of the devices, and what impact this has on the overall function of the SCADA network. The technical research and testing of each scanning tool accompany the data obtained from the SCADA experiments with the purpose of highlighting the risks associated with running network scanning tools on networks which do not run via an IP-based system and also highlighting the potential threat to the wellbeing of citizens and businesses when operational field devices are impacted by these scans. To facilitate this aspect, two SCADA networks were constructed which contained two different PLCs, as well as different sets of field devices. A host machine was then connected to the PLCs via an Ethernet cable and would conduct active scans against the SCADA equipment. The network and equipment were observed in order to identify any changes in activity. Similar to the IP experiments, the traffic between the SCADA system and the host machine was captured so that the scanners packets could be analysed and discussed.

During the SCADA experiments, another hypothesis was formed as a result of the data being provided by the execution of active network scanners; *Do adding more devices to the PLC and thus executing more complex code have a significant impact in the systems behaviour when being targeted by a network scanner?* To investigate this hypothesis, the active scans were repeated against a new SCADA system which held a larger amount of field devices and subsequently had to run a more complex set of logic codes.

All the data obtained throughout aim to help highlight the dangers of using globally renowned security tools on the networks responsible for the production of goods and the regulation of our CNI. Understanding the technologies behind network scanners, as well as the differences between IP and SCADA networks, forms a platform on which new network scanning technologies can be created which do not damage the functionality of ICS/SCADA networks but also deliver the same verbose and security-critical data generated by the existing tools used today. This data also aims to provide alternate methods of performing asset detection on SCADA systems, as well as enhancing knowledge on the subject.

5. Research into SCADA Protocols and Networks

This section explores the different protocols used by SCADA networks in order to transmit data between its bespoke devices. Using the information provided by the literature review, 3 common SCADA/ICS protocols have been dissected and explained in order to fully understand the technology which controls SCADA communication. Each one of the protocols has been explained and compared against each other; a discussion highlights the potential issues which may arise when scanning these networks with an IP-based tool.

In order to understand the differences between the technologies used on IP-based networks and SCADA networks, research was conducted into the protocols used by SCADA and IP systems. As a result of the information provided by the literature review, Ethernet, Modbus, and DNP3 appeared to be the most commonly used protocols in both IP and SCADA networks. The data yielded from this research aims to highlight the dissimilarities between each network protocol which could impact the way the SCADA devices react when subject to a network scanning or sniffing tool. The results of this research will help evaluate the feasibility of performing network scans on SCADA devices and how the results differ from IP networks.

When considering the use of IP scanning tools on SCADA networks, the main area of concern is the type of packets the scanning tools use in order to gain information from each device. Tools such as Nmap, ZMap, and Tenable Nessus all use Ethernet frames to transfer data between the host machine and the target devices. This is referenced within Bartlett et al. [13] and supported by Samtani et al. [9]. As stated within Galloway and Hancke [42] (see Section 3.3), the protocols used to transmit data on IP networks and SCADA networks have a varying amount of differences. These differences could prove to be an influencing factor when discussing the impact of executing some of the aforementioned IP scanners.

The research shows that Ethernet and traditional TCP/IP protocols focus on embedding data within the payload of multiple frames so that Internet technologies such as routers, web servers, proxies, and email servers can correctly send, receive, and utilise that data. DNP3 and Modbus have very few data abstraction mechanisms as they are strictly master/slave communications channels. This means that Ethernet packets are far larger and more sophisticated than the SCADA/ICS protocols discussed above. Scans targeted at SCADA must be a lot more specific to the technologies present on those types of network, meaning the data being sent across the wire must be the same length, the same data structure, and the same frequency as the existing traffic. The commands within each message must be adapted to match each specific slave device which resides on the network in order to gain valid responses or successful data transfer. Using this method of scanning has a greater chance of providing information relevant to a reconnaissance scan or asset-detection sweep of a SCADA/ICS network.

As Ethernet frames are the underlining mechanism used by network scanners, any device with an Ethernet interface should experience little to no changes when being scanned, unless the data being received is too great for the processing power of that device. As SCADA devices are often set up on older, legacy systems, the rate at which Ethernet packets are processed may be too great for SCADA and ICS devices. The most crucial aspect of these protocols is the way that they distinguish between individual packets. Whereas Ethernet uses a block of data to separate packets, Modbus uses physical breaks in time in order to achieve the same result. If connected to a Modbus RTU network, the Ethernet delimiter will not be valid. Therefore, if the traffic from the scan is received directly after a legitimate Modbus message, the receiving device may drop the data packet or continue to try and process the data as if it is a continuation of the last packet it received. This could result in bottlenecks being formed at specific parts of the network, meaning none of the data destined for the SCADA devices will be received and the data flowing from multiple devices or subnets could be disrupted.

Running foreign protocols on networks such as Modbus or DNP3 may be completely dropped and disregarded before being received by intended device. The way asynchronous packets are formed and sent across the network means that if an Ethernet packet were to be sent through a serial connection, the data would not correspond to the agreed transfer speed and would not be encapsulated correctly. Although this means that the devices themselves will not get compromised, attempting to send large Ethernet packets through a DNP3 or Modbus serial port could obstruct the legitimate SCADA traffic from reaching its destination. This would be an example of a denial-of-service attack achieved through overloading the network connections with incompatible data.

The most notable discoveries made from the protocols and networks research can be summarised as follows:

(i) The data held within the different protocols may not correspond with the instruction-set of the recipient device. Although an Ethernet packet may successfully reach a Modbus or DNP3 device, the information present within each packet may not solicit a correct response from the SCADA device. This means that any information transmitted back to the scanning device may not be useful in managing assets or diagnosing security vulnerabilities on the network.

(ii) The differences between how Ethernet, Modbus, and DNP3 synchronise and delimit the data traveling across the network could impact the operation of SCADA devices. If the data being received is too large or is being received too quickly, the on-board CPUs within SCADA equipment may struggle to parse the incoming data, meaning less time is spent performing their original, logical tasks.

(iii) The data being transmitted by the scanning tool may not be able to travel through that particular medium being used by the network. Although this may not have an impact on the devices themselves, the scan will return with no results. If used incorrectly, executing IP scanners on serial networks could either cause a denial of service, connection disruption, or false negative scan results.

All the information provided by this research has helped aid the understanding of how IP and SCADA networks could behave when subject to a network scan, as well as evaluating the feasibility of performing scans on SCADA networks.

6. Testing the Network Scanning Tools: IP Network Experiments

This section provides details about the network scanning experiments conducted against the virtual IP network. A list of the equipment used and an overview of the methodology used in order to test both passive and active network scanners are all contained within this section. In addition to covering the prerequisites and processes of the IP experiments, this section also analyses the results provided within the networks and protocols report. Each tool is critically analysed and reviewed against their suitability to conduct scans on a SCADA network.

Once a thorough understanding of the common SCADA and IP protocols had been established, the next phase was to analyse how network scanners function on a familiar network hosting machines and services typically found on an IP system. In order to do this, a set of experiments were conducted, on which each network scanning/sniffing tool was executed. The decision to run a series of both active and passive network reconnaissance tools on an IP network was made in order to give a clear indication as to how

Table 2: Table of Tools Executed against the IP Network.

Network scanning tool	Method of information gathering	Scan type
Nmap 7.40	Active	TCP-SYN Scan, Service Detection Scan, HTTP Banner Grab
Zmap 2.1.0	Active	ICMP Ping Sweep, TCP SYN Scan, NTP Scan
Tshark 2.0.5	Passive	Promiscuous-mode Packet Capture
Ettercap 0.8.2	Passive	Man-in-the-middle Traffic Intercept

these technologies function in a controlled environment. Observing and analysing the tools in this environment allow assessments to be made about the types of data the tools send and receive and how this could possibly translate on a SCADA network. Once all the network scans have been completed and all the data has been captured and analysed, a discussion of the results is done in order to evaluate the potential discrepancies between IP scans and SCADA scans.

6.1. Materials and Methodology. To conduct the IP scanning experiments a virtual network was created and configured in order to simulate the functionality of a common IP network. Details on the design, setup, and configuration of this network can be found within the Supplementary Materials (available here). The tools and equipment used within these sets of experiments were as follows:

(i) Ubuntu 16.04 LTS virtual machine: it is a Linux-based virtual machine capable of running the Netkit network simulator in an isolated and repeatable environment.

(ii) Netkit 2.8: it is a lightweight virtual IP network simulator used for training and academic purposes.

(iii) Tcpdump 4.7.3: it is a command line packet analyser which comes preinstalled with Unix-based operating systems. It is used for capturing traffic from a network interface card and saving the data in the.pcap format.

(iv) Nmap 7.40: it is a "network mapper," an open-source network scanning tool used for asset discovery, service detection, and security auditing.

(v) ZMap 2.1.0: it is an open-source network scanning tool optimised for conducting Internet-wide scans quickly and efficiently.

(vi) Tshark 2.0.5: Tshark is the command line interface provided by Wireshark. It is a packet analyser used to capture traffic from any network interface present on a machine.

(vii) Ettercap 0.8.2: it is a tool which allows users to perform man-in-the-middle attacks on local area networks. This allows for the sniffing, interception, and logging of network traffic.

(viii) Wireshark 2.0.5: it is a full graphical interface which allows users to dissect and analyse network traffic contained within .pcap files.

The decision to use these tools was based on both the information presented by the literature review and the results obtained from the networks and protocols research task. Both Nmap and ZMap rely on the TCP/IP protocol suite in order to gain information about networked devices. As the main underlying technology of TCP/IP is Ethernet, either this could cause the SCADA devices to become overloaded with foreign traffic or the serial system may drop or freeze because of the inability to process the Ethernet traffic. Although there are other technologies which can facilitate TCP/IP communication such as WiFi 802.11 and mobile 3G telecommunication, these fall out of the scope of the current research and will not be assessed. The passive tools were selected because of their ability to capture network traffic in order to deduce a list of active systems. As Tenable's Passive Vulnerability Scanner (PVS) was unavailable for these experiments, using a combination of both Tshark and Ettercap would ensure that the full functionally of such tool could be replicated and analysed on the IP network.

Executing these experiments required a virtual network to be created on the Ubuntu virtual machine. The choice to run a virtual network was based on the ability to restore and run the network from a clean install each time a new experiment was conducted. This ensured that each tool was exposed to the exact same environment and that any changes made by the previous experiment would not jeopardise future results. A virtual network can provide the same functionality as a physical IP network; however, setup and administration are simpler and the ability to reset the network was highly advantageous. These features made the IP experiments both repeatable and reproducible. Once the virtual network had been created, a series of active and passive network scanners were executed against each virtual host. Table 2 details the scans which were conducted against the network in order to understand the technologies behind them.

These methods of network scanning and traffic sniffing were selected based on several factors, the first being that both Nmap and ZMap are tools currently being used against both SCADA and IP networks. The combined capability of these two tools covers a range of scanning and reconnaissance methods used against modern SCADA systems. Being able to replicate the functionality of SCADA specific threats such as Shodan and intrusive network scanners is crucial towards understanding how these tools work and how they could pose a potential threat to SCADA and ICS systems. Being able to test each of the scans provided data which was used to evaluate the feasibility of performing the active and passive scans on a SCADA network. The data obtained from the IP experiments allows comparisons to be made once data has been generated from the SCADA experiments.

Each scan was executed against the individual subnets present on the network. For each active scan run against the virtual network, several observation points were set up in order to capture both the probing traffic as well as the host's responses. The tool responsible for capturing this traffic was Tcpdump. Once each scan had been executed, the network capture files were opened and analysed in Wireshark, a packet analyser, which gave an insight into how the different tools obtained information from the remote targets.

For the passive sniffing experiments, the Tcpdump tool was replaced by Tshark. On executing each passive tool, traffic would then be generated between the IP machines in order to test whether the tool was able to capture the data. When testing Ettercap, a MITM intercept tool, the previously referenced Tshark observation points were removed and two additional machines were added to the network. These new machines allowed for traffic to be intercepted between two endpoints. The data was then captured and relayed onto its original destination. The results from these experiments were displayed in the form of packet capture (.pcap) files, as well as the output displayed on the physical machines.

6.2. Results and Discussion. As a result of the experiments conducted against the virtual IP network, as well as the data provided through the use of packet captures taken throughout both the active and passive experimentation, the following conclusions can be made with reference to the future experiments to be performed on a SCADA network.

Firstly, running a series of different asset discovery and service detection scans using Nmap revealed a number of facts to take into consideration when discussing using scanners on SCADA systems, the first being that Nmap utilises the TCP protocol in a variety of different ways in order to gain different amounts of information from the target networks. An unexpected result from these experiments was that Nmap uses TCP-SYN and ACK packets in order to establish whether a particular address is active on a network. A standard ICMP echo request (or ping) is used to send a small amount of data addressed to a raw socket, meaning that ICMP bypasses TCP and communicated directly with IP. This could prove as both an advantage and a disadvantage when replicating this scan on the SCADA devices. Although Nmap does not open raw sockets when using TCP pings, which could cause the target machine to behave unexpectedly, the method of using TCP requires the utilisation of the TCP protocol.

The data from both the Nmap and ZMap experiments shows that host discovery can be achieved using both ICMP echo requests as well as sending solitary TCP-SYN packets to all the ports on target machines. The issue with both of these methods is that they have been tailored to work specifically with IP devices. ICMP works directly above the IP layer, relying on raw sockets being opened in order for data to be sent back and forth between hosts without the need for a TCP connection. The ability to open and communicate with raw sockets may not be possible when applying the same approach to SCADA devices which reside on SCADA networks. Issues also arise from the payload of the Ethernet frames themselves. If these active scanners do not support other types of serial frames, the ports receiving the scan data may not be able to interpret or handle the IP headers or Ethernet frames. The same issues are presented when using TCP-SYN scans. Unless the SCADA device supports TCP connections through select ports, there is no guarantee that when the active tools send data to each port on that device, the data will be accepted and parsed. ZMap may be the more advantageous scanner to use in this scenario, as it offers minimal interaction with the target devices and requires users to be specific about the services, addresses, or ports that they wish to interrogate.

Active scanners appear to reveal more details about the network than the passive alternatives. Throughout all the experiments conducted on the IP network, none of the passive scanners or packet capture devices were able to prove the identity of the gateway machines which connected between each subnet. From analysing the packet capture files, it could be suggested that the observation points for each passive tool could have been adjusted in order to give a broader perspective on the entire network. However, when considering the ramifications of modern SCADA networks, it is not practical to have passive scanners placed at every significant point of the network. This is due to both the devices inability to run such software as Tcpdump or Tshark and also the fact that as physical field devices can be located at sights which are huge distances from the central control units, it then becomes very difficult to coordinate and synchronise a passive scan. It could be suggested that, given more time, the passive scanners would be able to obtain as much data as the active alternatives; however the results obtained from these experiments, under the specified circumstances, do not support this statement.

As the active tools require interaction with the target network and rely on sending data to each machine, the choice to use a MITM machine could be beneficial towards gaining information about a network, specifically networks containing SCADA/SCADA devices. There are however two concerns with this methodology, the first being that it suffers from the same practicality issues as the other passive scanners. MITM requires machines to be placed around the network which, as discussed in the previous statement, is impractical on a SCADA system. Another significant factor is being able to replicate the functionality of ARP poisoning on systems which do not use the Address Resolution Protocol.

Combining the results from the networks and protocols research, as well as executing both active and passive networks scanners on an IP network, it appears that the type of network a SCADA system is running may not be the predominant issue when being scanned by the tools referenced within the previous section. It has been identified that the type of packets used by network scanners are not suited towards devices communicating via a serial protocol. However, there is no data present to suggest that the active scanning tools are able to send data through any other interface besides Ethernet. This has significant influence on the direction of the current research as SCADA and ICS systems being used today continue to run serial protocols. This implies that if active scanners are unable to communicate with SCADA devices through serial ports, the issues facing SCADA and

ICS may be through the adoption and utilisation of Ethernet communications. Both Nmap and ZMap were successful in identifying hosts on the virtual network, through the use of mass port scanning and applying probes which are specific to services found on common IP devices. This implies that if a SCADA device has been configured to use Ethernet but does not offer any of the services used within the IP experiments, the device may not be able to parse the data correctly or elicit a valid response. This could potentially cause the SCADA device to crash or behave unexpectedly, not because of the unfamiliar traffic that its receiving but from being unable to process unfamiliar requests for services it does not provide.

The data provided by the Ettercap and Tshark experiments shows that passive scanners do not directly interact with the hosts connected to a network. This in turn suggests that running passive tools at multiple points on a network could provide a stable method of gaining information about a SCADA network. The issue with passive tools is that data about each host on the network is not immediately accessible, as the packets captured need to be analysed in order to identify hosts and services. Another issue with passive scanners is compatibility. Ettercap requires the target hosts to utilise the ARP protocol. If the SCADA device in question is running on a serial network, this method of information gathering would not function correctly. As the hosts used in these experiments communicated via IP, Ettercap was successful in obtaining data from the network. The last significant drawback to passive tools is the need to distribute them across the network in order to gain a wide coverage. Modern SCADA systems can span across multiple sites located across continents, therefore being unable to remotely execute asset and service detection scans would not be suitable in that scenario.

Understanding how each of these asset discovery and network reconnaissance tools function within an idealistic environment has been a key exercise which helped identify the ramifications and the possible consequences of using these tools on SCADA networks. The findings from these experiments assisted in understanding how each of these tools performs its scans, and it has helped to create hypotheses which will create an all-encompassing platform on which to conduct the SCADA experiments. Without the results supplied by these tests, any significant findings or datasets which may appear in the forthcoming SCADA experiments would lack a comprehensive justification as to why that result has occurred. Furthermore, setting up and executing these experiments have satisfied two of the core objectives of the current article: an IP network has been replicated using the Netkit environment and the Netkit machines have been used to conduct extensive tests on network scanning tools in order to analyse their functionality.

The IP experiments provided insightful data which helped enhance the understanding of both active and passive network scanners. The use of a virtual network and packet capture software was successful in facilitating the network scanning tests as well as capturing the data in a form which could be easily analysed and presented. Improvements could have been made to the setup and execution of these experiments which would have allowed for more time and resources to be directed at the SCADA testing phase. The main issue was the amount of time spent designing and configuring the virtual network. A preconfigured Netkit lab could have been downloaded and executed in order to minimise the amount of time spent improving and adjusting the virtual network. However, choosing to install a virtual network from beginning to end meant that the nodes, services, and scale of the network could be tailored to suit the objectives of the research. Knowing the configuration in great detail allowed for a better analysis of the network scanners and their ability to obtain crucial information about the network. This however did not warrant the time spent creating the test environment and should be reevaluated for future experiments.

7. Testing the Network Scanning Tools: SCADA Network

The following section provides an overview of the experiments conducted against a SCADA system. Details about the equipment used as well as an explanation of the methods used to test the active scanning tools are also contained within this section. Once all the specific details about the SCADA experiments have been presented and explained, the results obtained from the SCADA tests are then discussed and analysed against the main objective of the current article; does the execution of an active network scan have a negative effect on SCADA systems, and if so, what caused it and why? Each of the tools is critically analysed and reviewed against their suitability to conduct scans on a SCADA network. A critical analysis of this part of the research has also been provided which aims to address strengths and weaknesses. Following the testing of both passive and active network scanners on the virtual IP network, the active scanning tools are needed to be executed against devices exclusive to SCADA networks. These experiments allowed for assessments to be made about the impact of using the network scanning tools against devices found within modern ICS/SCADA systems. Executing the active scanners on a SCADA network will help determine whether the conclusions formed from the IP experiments were correct, as well as determining whether executing scans against SCADA equipment causes them to crash or divert from their normal operations.

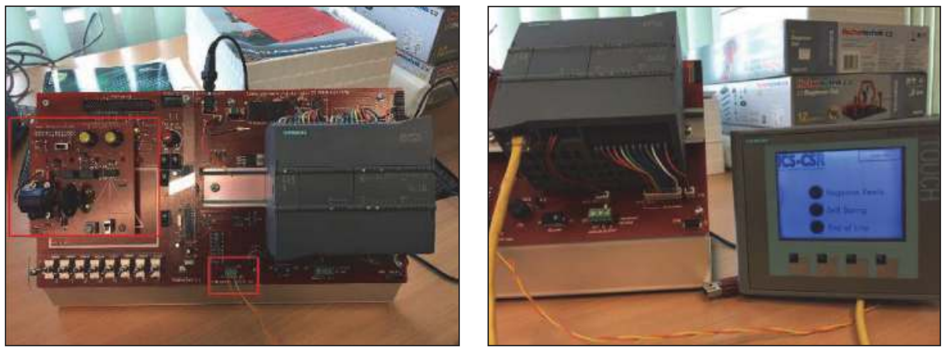
7.1. Materials and Methodology. In order to observe and assess the impact of running a network scanning operation against SCADA devices, a small SCADA system was constructed and configured to replicate the functionality of a PLC, HMI, and operational field devices. To achieve this, the following tools were acquired and configured to provide a SCADA testing environment:

(i) Siemens SIMATIC S7-1200 PLC: it is a compact programmable logic controller with an Ethernet-enabled interface.

(ii) Siemens SIMATIC KTP400 basic HMI: it is a 4-inch touchscreen device which can be used to control and monitor devices connected to the S7-1200 PLC.

Table 3: A table showing the types of tools and scans to be run against the SCADA system.

Network scanning tool	Method of information gathering	Scan type
Nmap 7.40	Active	TCP-SYN scan, service detection scan, UDP, and script scan
Zmap 2.1.0	Active	ICMP ping sweep
Python UDP_DoS.py	Active	UDP denial-of-service attack



(a) The Siemens S7-1200 PLC with the motor and HMI connection outlined

(b) The S7 PLC and HMI screen

Figure 2: The Siemens S7-1200 PLC and HMI setup.

(iii) ASEA brown boveri (ABB) PM564 PLC: it is a compact programmable logic controller produced by ABB. This PLC has both Ethernet and Serial interfaces as standard.

(iv) IKH didactic systems PLC trainer 1200: it is a custom PCB with components which allow PLCs to be connected to small, modular field devices.

(v) On-board modular motor: it is a bidirectional motor attached to the IKH Didactic Systems PLC Trainer 1200.

(vi) Compact flexible process line: it is a small replica of a conveyor-driven production line which can be connected to the aforementioned PLC Trainer.

(vii) Windows 7 64 bits with Siemens totally integrated automation (TIA): a software suite which allows code to be created and ran on Siemens S7 devices.

(viii) Windows 7 64 bits with ABB control builder plus and CoDeSys 2.2.0: it is a software suite which allows code to be created and ran on ABB Automation devices.

(ix) A laptop running a Linux-based operating system (Ubuntu 16.04 LTS): it is a platform which supports the ZMap active scanning tool.

(x) Nmap 7.40 and ZMap 2.1.0: see Section 6.1.

(xi) Tshark 2.0.5: see Section 6.1.

(xii) UDP_DoS.py: it is a custom-written Python script which sends large UDP packets to each port available on a target IP address.

Both of the two PLCs being tested come with on-board Ethernet interfaces. As referenced within the Supplementary Materials, the active network scanners used within these experiments send data via Ethernet communications. This suggested that once each active scanner has been deployed, there will be no connectivity issues and that the network scanners will be able to probe the PLCs as desired. As a result of this, the activity of both the PLC and the field devices will be monitored in order to deduce whether the process of scanning had caused the SCADA system to divert from its original functions.

Table 3 details the different scans which were executed against the SCADA system.

These types of active network scanning were chosen because of the results provided from the IP experiments. Firstly, the range of Nmap scans covers asset discovery, service detection, and UDP probing. These three methods of scanning utilise different techniques in order to gain information about a target. To facilitate the execution of each of these scans, the PLCs stated above were connected to the host machine. This machine was running Windows 7 as well as the two software suites needed to interact with each device. Once this connection had been made, the logic code corresponding with each PLC was downloaded and run. Once the code had been downloaded and run, each scan was executed against the network. During each scan, a packet capture was taken on the host machine using Tshark. In addition to the packet captures, each SCADA system was physically observed in order to determine whether the operation of the PLC or the connected field devices changed during each scan.

Firstly, each Nmap scan was executed against the Siemens S7 PLC (see Figures 2 and 3) with a singular motor connected. After all of the Nmap scans had been executed against this smaller setup, the Compact Flexible Process Line was added to the SCADA system. This was done in order to test an additional factor which is associated with the scanning of

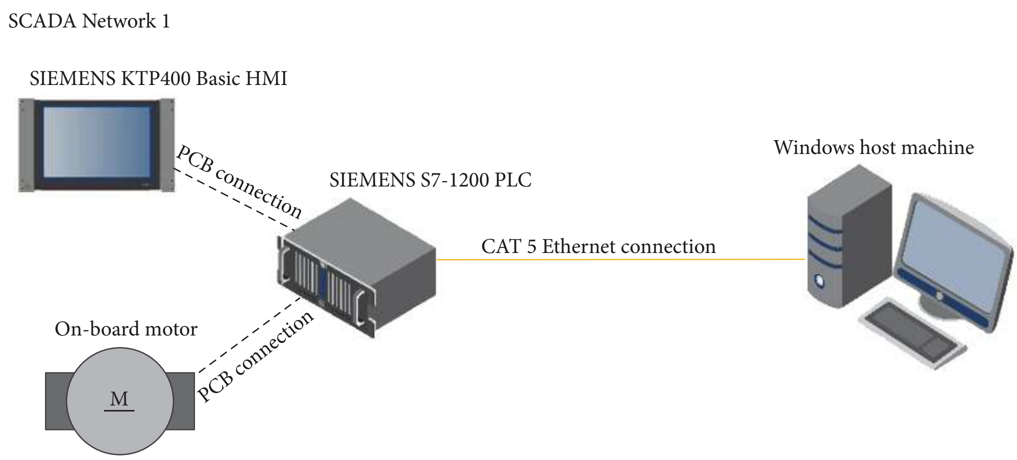
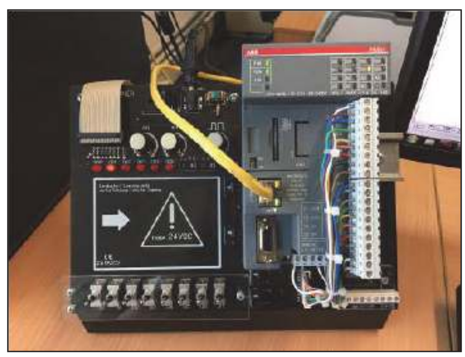
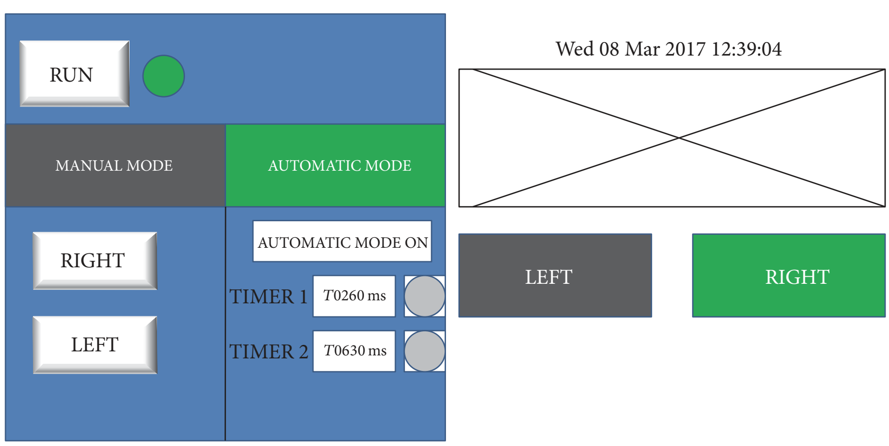


Figure 3: A topology showing the Siemens S7-1200 PLC network setup.



(a) The ABB PM564 PLC with an Ethernet connection



(b) The HMI interface configured to run on the host machine

Figure 4: The ABB PLC and HMI setup.

SCADA equipment: *Do adding more devices to the PLC and thus executing more complex code have a significant impact in the systems behaviour when being targeted by a network scanner?* Once each network scan had been executed against this larger system, the host machine was disconnected and reconnected to the ABB PM564 PLC (see Figures 4 and 5). Once connected, the same scans were then executed against this new PLC setup.

Two methods of network scanning were added to the SCADA experiments which were not executed on the IP network. These are Nmap's "UDP and Script Scan" and the "Python UDP_DoS.py Attack." These scans utilise the User Datagram Protocol (UDP), rather than TCP and ICMP which were present in the previous IP experiments. The reason for running these scans on the SCADA network was because these methods of network scanning were neglected during

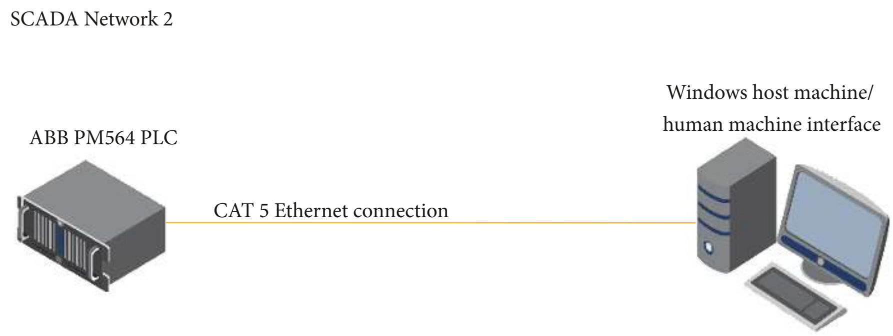


Figure 5: A topology showing the ABB PLC network setup.

the IP experiments. Throughout the process of conducting the IP scans, the ability to use the UDP protocol was present; however, due to the services configured to run on the virtual network, there was no requirement to run UDP scans as all of the services used TCP. On executing multiple TCP-based scans on the SCADA devices, the behaviour of the SCADA system did not change. Therefore the need to experiment using another scanning vector became paramount.

Although the passive scanning tools were deployed against the virtual IP network, they will not be used within the SCADA experiments. The decision to exclude these tools from the SCADA experiments was made because of the results provided by the previous IP experiments. Although the passive tools were able to successfully obtain data about the hosts and services present on the IP network, the testing of these tools would not give a valid representation of the data traveling across a large SCADA system. The SCADA environment used to facilitate the network scanning experiments contains only a singular Ethernet-enabled PLC with a single HMI. As a result of this, the environment used within this set of experiments would be unable to thoroughly test the functionality and capability of the passive tools used within the IP experiments. More information regarding the tests that were conducted can be found in the Supplementary Materials.

8. Discussion

From the experiments conducted on both the Siemens S7-1200 PLC and the ABB PM564 PLC, the following results contain information which details how SCADA equipment behaves when subject to a range of active network scanners. The information within this section focusses on evaluating the effect of using active scanners on SCADA systems, as well as identifying potential methods of network scanning which will facilitate the requirements of a SCADA network and successfully perform asset detection without disturbing normal network functionality.

The results yielded from the Nmap scans showed that both of the PLCs used within these experiments remained stable during a TCP-SYN scan. However, the network traffic captured from the host machine during that scan shows that Nmap does not use the same method of asset detection as shown within the IP experiments. The differences are that when conducting the scan against both the Siemens and ABB PLCs, Nmap utilised the ARP protocol in order to determine which hosts were active, rather than sending TCP-SYN packets to common services ports such as web server ports (80) or SSL ports (443). Although this method of scan proved to be successful against this SCADA environment, it cannot be stated that the same level of success would be achieved on other SCADA devices or networks. The first reason for this is that both of the PLCs used within these experiments communicated with the host machine via an Ethernet connection. As a result of this, each interface has a MAC address. The ARP protocol is used to associate an IP address with these MAC addresses. If this same scan was executed against another Ethernet-enabled device, the embedded Ethernet interface will be able to handle the ARP traffic being sent from the scanning tool. However, the data obtained from this experiment does not clarify whether this method of scan would be stable on a serial-enabled device.

Executing Nmap's service detection scan against both the Siemens and ABB PLCs did not alter the behaviour of the SCADA system. This shows that if communicating with a remote component using Ethernet, the TCP-SYN traffic used to obtain information about the two PLCs did not have a negative impact on the operation of the system. This was supported by the creation of two output files which contained correct information about both devices. A notable aspect of both of the aforementioned output files was a line stating that 1000 ports on each device were filtered. This could have had an impact on the stability of both the SCADA devices during each active scan. However, further research needs to be conducted into how ports can be filtered on a SCADA device and how Nmap can be configured to avoid such obstacles in the future.

When performing a UDP scan using Nmap, neither of the two PLCs tested showed any indication that the active scan was being performed, as normal operation was maintained throughout the duration of the scan. On analysis of the data provided within the Nmap output file for the Siemens PLC, the UDP scan appeared to provide more in-depth data about the device than the previously executed TCP scans. However, replicating the same UDP scan on the ABB machine yielded different results. The UDP scan was unable to reveal the same information, such as CPU model and firmware version, as gained from scanning the Siemens PLC. This means that, as a result of the scan being able to execute and complete without altering the behaviour of the SCADA system, service detection scans must be specifically tailored to facilitate the unique setup of each individual PLC in order to gain specific details about a device. However, although it can be seen from the results obtained from the SCADA experiments that running a UDP scan against a Siemens S7-1200 can reveal device specification information, evaluating the risks associated with gaining this information is out of the scope of this research, and therefore no comment can be passed about how significant this data is or whether it exposes another attack vector towards the Siemens PLC.

On attempting to run an ICMP ping sweep against both the Siemens and ABB PLCs, the packets were unable to reach their intended destinations. The tool ZMap was used in order to facilitate these scans. The reason for this was due to how ZMap conducts asset-discovery scans. As seen within the IP experiments, ZMap utilises ICMP echo requests which run on top of IP packets, rather than the ARP broadcast method used by Nmap. In order to assess why the ICMP scan failed to run against both SCADA devices, the output packet capture file was opened and analysed. The data held within this file was unable to diagnose why the ICMP packets failed to gain a response from the SCADA devices. As a result of this, no safe conclusions can be made about the impact ICMP packets may have on SCADA systems.

From the results of the TCP, UDP, and ICMP scans, it was evident that running active tools against the SCADA networks did not have an impact on the operation of either the PLCs or field devices used within these experiments. When comparing these results to the outcomes of the IP experiments, there appears to be little difference between scanning on a SCADA network. Although the PLCs displayed different sets of data to the machines used on the IP network, the PLC devices were able to respond to a range of scans as well as remaining to maintain normal operation throughout the entire duration of the scan. The information displayed within the literature review suggests that these results do not correspond with previous cases involving network scanners and SCADA equipment. In order to understand why these results had occurred, more research had to be done into the fragility of SCADA equipment as well as the network constraints which are exploited by active scanners. This further research implies that the traffic being sent across a SCADA network must be carefully controlled to ensure that the network does not become congested with unused data. In order to test this, a Python script was created which would send a higher volume of network traffic to each port on the target PLCs.

On execution of the Python script, the Siemens PLC remained stable and continued to function as normal. However, on executing the same script against the ABB PLC, the connection between the host HMI and the PLC was prematurely terminated. On analysis of the packet capture taken during that scan, it appears that, due to the mass amount of UDP packets being sent from the host machine, the latency of the traffic containing the status of the field devices caused the HMI to terminate the connection and present an error to the user. Although retesting the ABB PLC with the Python script supports the claim that SCADA devices may alter when congested with massive amounts of network traffic, the Python UDP scanner does not represent a usable network scanner. The tool was created in order to send a large amount of UDP data across a network, whereas network scanners use a variety of protocols to gain information about the devices connected to a network. Therefore, the results of this scan prove that SCADA systems can be affected by mass amount of data flooding the network, and it does not prove that the same result could be achieved with any of the aforementioned network scanners. Furthermore, the Python script was only successful against one of the two PLCs tested. Therefore, the data from these experiments cannot suggest that running the same scans or scripts on a variety of other SCADA devices would yield the same results.

From the information presented by Duggan et al. [7] as well as the results of the SCADA experiments it is suggested that although network scanners may be a viable option on some types of SCADA systems or devices, there is no universal solution to performing asset discovery or service detection on SCADA systems. Every device and network are unique; therefore scanning technology must be adapted to facilitate the configuration of each unique device. Performing a network scan on a SCADA system with an all-purpose tool such as Nmap or ZMap is not feasible. However, conducting research into all SCADA devices and how they function would allow for a tool or framework which could provide a solution to the issue of bespoke technologies and the uniqueness of devices.

From the results generated by the SCADA experiments, the following conclusions can be made: if executing either an asset-discovery scan or service detection scan against an Ethernet-connected Siemens S7-1200 or ABB PM564 PLC using Nmap, the traffic generated by the scan does not have a negative effect on the operation of any of the SCADA devices present on the network. Using such protocols as ARP, TCP, and UDP, Nmap was able to locate both of the PLCs on the small SCADA network. On scanning the Siemens S7 PLC using UDP, Nmap was able to gain information about the system's specification, such as the model of the CPU and the current firmware being run as well as the manufacturer and IP address. Nmap was able to detect both PLCs using the ARP protocol. Although this method of asset detection did not affect the normal operation of the target system, the ARP technology can only be used against devices communicating via Ethernet. This is because the underlying concept of ARP uses MAC addresses, which are only contained within Ethernet frames. This means that although this method of scan was successful within these experiments, there is no guarantee that running the same scan against another type of PLC would produce the same results.

On attempting an asset-discovery scan, ZMap was unable to provide any information about either of the two PLCs tested in these experiments. Although ZMap was unable to disclose the hosts connected to the target network, there was no data to suggest that the SCADA devices had been affected by the scan or that they had received the data from the host machine. This was an unexpected result for a number of reasons. Firstly, from the research conducted within the literature review, there has been an example on which a similar method of asset detection had caused a SCADA system to malfunction. Secondly, as both the PLCs were connected to the host machine via Ethernet cable and had been configured to have a local IP address, there were no discrepancies with the setup of the network which would result in ZMap not functioning correctly. Lastly, in order to check that the network had been configured correctly, a singular ICMP packet was sent to each PLC from the host machine. This method of ICMP communication was able to identify each PLC on the network, despite using the same technology as ZMap. On the other hand, these results are not substantial enough to comment on the suitability of using ZMap to scan for hosts on a SCADA system. As referenced earlier in this section, the setup and configuration as well as the tools used within these particular experiments cannot be applied unanimously to all SCADA devices available today. Although ZMap was unable to gain information about any devices connected to the SCADA network, it did not cause the PLC or the field devices to malfunction, opposing the information provided within the literature review. In addition to this, if the ZMap scan conducted within these experiments had succeeded in identifying hosts on the network, there is no data present which suggests the results could be repeated on a different SCADA system.

Performing multiple experiments using the UDP protocol to conduct scans against each PLC has emphasized how unique each SCADA device is and how scans must be carefully targeted and controlled in order to gain the correct information without disturbing the operation of the network. When executing Nmap's UDP scan against both of the PLCs tested within these experiments, both scans were able to gain information about each device without compromising or disturbing the network. However, despite the success of using Nmap to perform UDP scans, the same protocol could pose a serious threat to the integrity of a SCADA system if ill-configured or misused. This was demonstrated through the use of the Python UDP script. This script demonstrated how the two PLCs coped when faced with a large number of UDP packets carrying a large amount of data. The most significant data came from the execution of the Python script against the ABB PLC. As a result of the script being executed, the ABB PLC lost connection with the HMI, which in this case was an interface present on the host machine. Although the Python script had not been designed to gather information about networked devices, it demonstrated that SCADA networks can suffer a DoS attack from one host running a single Python script. Not only does this emphasize the ideas drawn from the revisited literature review, but these results also suggest that if configured incorrectly, or if there are multiple remote users scanning the same network, active scanning tools could possibly replicate the same results as the Python script.

On the other hand, despite the results obtained from running the UDP DoS experiment against the ABB PLC, the Python script appeared to have no effect on the SCADA network controlled by the Siemens S7 PLC. From analysing the packet capture files from both experiments, it can be stated that the script used the same protocol equipped with the same payload when sending traffic to each PLC. This again highlights how unique each SCADA device can be. The data from these experiments show that when conducting either an asset discovery or service detection scan on a SCADA system, each device must be targeted on a case-by-case basis. As only two different types and manufacturers of SCADA equipment were tested during the course of these experiments, the data obtained from this research cannot suggest that it is feasible to scan a SCADA system with any of the active tools which were tested, despite the successes and failures of certain tests. The resources required to conduct active scanning experiments against all possible SCADA devices are beyond the scope of this article; however, it does emphasize a key point when assessing the suitability of using active scanners on SCADA networks. From the select range of tools and devices used within these experiments, there were differences when being scanned. The two PLCs provided different information when subject to the same scan as well as reacting differently when attacked by the Python UDP script. This means that there is not a universal solution which can facilitate the requirements of every SCADA system being used within modern society. Further research would be needed in order to detect similarities between bespoke SCADA protocols and manufacturers in order to fully understand the most effective way of conducting remote scans without compromising the integrity of the system.

The experiments conducted against the SCADA systems provided a set of results which identified that, using the network scanning tools and SCADA devices selected for these experiments, executing an active scan against a SCADA system does not affect the normal operation of the system. This suggests that, for the devices used within these experiments, it would be feasible to run all of the asset discovery and service detection scans against SCADA devices. The results obtained from conducting these experiments did not answer a range of questions which still apply to the use of scanners on SCADA networks.

Firstly, the SCADA experiments only focused on two different types of PLC, both of which communicated using the same networking technology, Ethernet. Choosing to conduct the network scanning tools on an Ethernet-enabled network would ensure that the packets sent from the scanning tools would reach the target devices, meaning any changes made to the system would most likely be a result of vulnerabilities within the individual devices, rather than through constraints of the network. Although this gave a good insight into the capability of the scanning tools and the type of information that can be gained from PLCs, the experiments did not address the issues of scanning on a serial network, therefore leaving a large ICS/SCADA demographic unaccounted for.

The complexity of the SCADA systems used within these experiments did not give a true representation of the critical operation of a modern SCADA system. Also the amount of time-critical processes loaded onto the PLC did not match that of a true SCADA system. Having the opportunity to experiment on larger, more complex networks would be beneficial towards validating the results and conclusions drawn from this research.

Finally, the creation of the Python UDP scanner provided results which brought the focus of the experiments back to network constraints rather than device vulnerabilities. This in turn gave the experimentation phase a broader coverage of the possible ways network scanners could affect SCADA systems. The Python script used to perform the UDP DoS-style attack is not an official application or tool. Therefore, it could be argued that the results gained from the Python script experiments do not meet the criteria of the research, as it is not an official "scanning tool." Although this statement is correct, no research had been conducted into the tools capable of performing DoS attacks on a SCADA network. Instead, the Python script demonstrated two key facts about SCADA systems. Firstly, as the UDP attack was only successful on one of the PLCs, it proves that every SCADA device is different. Therefore, each device requires its own bespoke set of technologies in order to complete a network scan without causing a malfunction. Lastly, the UDP scanner shows that, without the correct configuration, a tool such as Nmap or ZMap could be misused or configured incorrectly and cause an accidental DoS on a SCADA network. This shows that SCADA scans must be specifically targeted and executed on a case-by-case basis, adapting and adjusting the scanning methodology as needed. These results would not have been revealed without the use of the Python script.

In order to fully understand how SCADA devices are fragile, rather than the constraints of SCADA networks, further research should be conducted into the internal workings of a wide range of different PLCs, RTUs, and HMIs. This research should elaborate on the information presented by Wedgbury and Jones [31] and Wiberg [32] (see Section 3.2). Focussing on the differences between the SCADA devices rather than the types of network would provide a deeper understanding about why certain scans succeed or fail when being executed against specific hardware.

The active network experiments conducted within this document were only executed against 2 different PLCs, both of which used Ethernet to communicate with the host machine, testing network scanners against a larger sample of PLCs, as well as other SCADA specific devices such RTUs and HMIs. This would provide more of an insight into the possible vulnerabilities present within modern SCADA systems. Testing a larger range of devices could inform the users of SCADA about the specific devices in their systems which could be vulnerable to a network scan and what collateral effects this may have on the rest of the network. This further research would also assist in the creation of a SCADA network scanner. This extra information could assist in the creation of a network scanner which can gain information from both serial and Ethernet devices.

Abbreviations

ARP: Address Resolution Protocol
CIA: Confidentiality, integrity, and availability
CNI: Critical National Infrastructure
CPNI: Centre for Protection of National Infrastructure
DNP3: Distributed Network Protocol Version 3
DoS: Denial of service
HMI: Human Machine Interface
ICS: Industrial Control System
IED: Intelligent Electronic Device
MITM: Man-in-the-middle
MTU: Master Terminal Unit
Nmap: Network mapper
PLC: Programmable logic controller
PVS: Passive Vulnerability Scanner
RTU: Remote Terminal Unit
SCADA: Supervisory Control and Data Acquisition
SSL: Secure Sockets Layer
ZMap: Internet-wide scanner.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Supplementary Materials

Information regarding the tests that were conducted can be found in the Supplementary Materials. This file includes the SCADA Network and Protocols Report, the Tests of Network Scanners Against IP Devices, and the Tests of Network Scanners Against SCADA Devices. *(Supplementary Materials)*

References

[1] D. Kalbfleisch, *SCADA Technologies and Vulnerabilities*, 2013, http://www.cs.tufts.edu/comp/116/archive/fall2013/dkalbfleisch.pdf.

[2] CPNI and Homeland Security. (2010) "Cyber Security Assessments of Industrial Control Systems", Control Systems Security Program & National Cyber Security Devision, https://scadahacker.com/library/Documents/Assessment_Guidance/DHS.

[3] A. Nickolson et al., "SCADA Security In The Light Of Cyber-Warfare," *Computers & Security*, vol. 31, no. 4, pp. 418–436, 2012.

[4] M. Franz, "Vulnerability Testing of Industrial Network Devices," in *ISA industrial network security conference, Critical Infrastructure Assurance Group (CIAG)*, Cisco Systems Inc., 2003.

[5] M. Evans, L. A. Maglaras, Y. He, and H. Janicke, "Human behaviour as an aspect of cybersecurity assurance," *Security and Communication Networks*, vol. 9, no. 17, pp. 4667–4679, 2016.

[6] N. Ayres and L. A. Maglaras, "Cyberterrorism targeting the general public through social media," *Security and Communication Networks*, vol. 9, no. 15, pp. 2864–2875, 2016.

[7] D. Duggan, M. Berg, J. Dillinger, and J. Stamp, *Penetration Testing of Industrial Control Systems*, Sandia National Laboratories, 2005.

[8] P. Kerr, J. Rollings, and C. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, Congressional Research Service, 7-5700, 2010, http://www.crs.gov.

[9] S. Samtani, S. Yu, H. Zhu, M. Patton, and H. Chen, "Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques," in *Proceedings of the 14th IEEE International Conference on Intelligence and Security Informatics, ISI 2015*, pp. 25–30, USA, September 2016.

[10] R. C. Bodenheim, *Impact of the Shodan Computer Search Engine on Internet-Facing Industrial Control System Devices*, Air Force Institute of Technology, 2014.

[11] N. R. Rodofile, K. Radke, and E. Foo, "DNP3 network scanning and reconnaissance for critical infrastructure," in *Proceedings*

of the Australasian Computer Science Week Multiconference, ACSW 2016, February 2016.

[12] E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*, Syngress, 2014.

[13] G. Bartlett, J. Heidemann, and C. Papadopoulos, "Understanding passive and active service discovery," in *Proceedings of the IMC'07: 2007 7th ACM SIGCOMM Internet Measurement Conference*, pp. 57–70, October 2007.

[14] C. K. Q. Nguyen, *Industrial control systems (ICS) & supervisory control & data acquisition (SCADA) cybersecurity of power grid systems: Simulation/modeling/cyber defense using open source and virtualization [Doctoral, thesis]*, Purdue University, 2014.

[15] A. Stefanov, C.-C. Liu, M. Govindarasu, and S.-S. Wu, "SCADA modeling for performance and vulnerability assessment of integrated cyber-physical systems," *International Transactions on Electrical Energy Systems*, vol. 25, no. 3, pp. 498–519, 2015.

[16] R. Jaronim, *Emulation of Industrial Control Field Device Protocols*, Air Force Institute of Technology, 2013.

[17] Y. Xu, M. Bailey et al., "Canvus: Contextaware network vulnerability scanning," in *In Proceedings of the 13th International Symposium on Recent Advances in Intrusion Detection (RAID)*, November 2010.

[18] J. Gonzalez and M. Papa, "Passive scanning in modbus networks," *International Federation for Information Processing*, vol. 253, pp. 175–187, 2007.

[19] N. R. Rodofile, K. Radke, and E. Foo, "DNP3 network scanning and reconnaissance for critical infrastructure," in *Proceedings of the the Australasian Computer Science Week Multiconference*, pp. 1–10, Canberra, Australia, Feburary 2016.

[20] R. Deraison and R. Gula, *Blended Security Assessment: Combining Active, Passive and Host Assessment Techniqiues*, Revison 10, Tenable Network Security Inc, 2011.

[21] D. Peterson, "Using the Nessus Vulnerability Scanner on Control Systems," *Digital Bond Inc*, 2006.

[22] D. Myers, E. Foo, and K. Radke, "Internet-wide scanning taxonomy and framework," in *Proceedings of the Australasian Information Security Conference (ACSW-AISC)*, Australian Computer Society, Inc., January 2015.

[23] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J. A. Halderman, "ZMap: Fast Internet-wide Scanning and Its Security Applications," in *Proceedings of the the 22nd ACM SIGSAC Conference*, pp. 542–553, Denver, Colorado, USA, October 2015.

[24] F. Li, Z. Durumeric et al., "Youve Got Vulnerability: Exploring Effective Vulnerability Notifications," in *25th USENIX Security Symposium (USENIX Security 16, USENIX*, Texas, USA, 2016.

[25] J. J. Chromik, A. Remke, and B. R. Haverkort, "What's under the hood? Improving SCADA security with process awareness," in *Proceedings of the 2016 IEEE Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids, CPSR-SG 2016*, Austria.

[26] National Communications System. (2004) "Supervisory Control and Data Acquisition (SCADA) Systems.", Technical Information Bulletin 04-1, October 2004.

[27] Motorolla INC, *White Paper: SCADA Systems*, Motorola, Illinois, USA, 2007.

[28] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Inclusion of SCADA Cyber Vulnerability in Power System Reliability Assessment Considering Optimal Resources Allocation," *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4379–4394, 2016.

[29] J. Vico, T. Smith, and R. Hunt, "Fully utilizing the intelligent electronic device capability to reduce wiring in industrial electric distribution substations," in *Proceedings of the 2010 IEEE Industry Applications Society Annual Meeting, IAS 2010*, USA, October 2010.

[30] A. Wood, Y. He, L. Maglaras, and H. Janicke, *A Security Architectural Pattern for Risk Management of Industry Control Systems within Critical National Infrastructure*, 2016.

[31] A. Wedgbury and K. Jones, *Automated Asset Discovery in Industrial Control Systems - Exploring the Problem*, Airbus Group Innovations Quadrant House Celtic Springs, Newport, NP10 8FZ, UK, 2015.

[32] K. Wiberg, *Identifying Supervisory Control And Data Acquisition (SCADA) Systems On A Network Via Remote Reconnaissance*, Naval Postgraduate School, Monterey, Calif, USA, 2005.

[33] A. Cook, H. Janicke, R. Smith, and L. Maglaras, "The industrial control system cyber defence triage process," *Computers & Security*, vol. 70, pp. 467–481, 2017.

[34] Y. Cherdantseva, P. Burnap, A. Blyth et al., "A review of cyber security risk assessment methods for SCADA systems," *Computers & Security*, vol. 56, pp. 1–27, 2016.

[35] J. Zaddach, L. Bruno, A. Francillon, and D. Balzarotti, *AVATAR: A Framework to Support Dynamic Security Analysis of Embedded Systems*, Firmwares. In NDSS, 2014.

[36] L. A. Maglaras, J. Jiang, and T. J. Cruz, "Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems," *Journal of Information Security and Applications*, vol. 30, pp. 15–26, 2016.

[37] W. Gao, T. Morris, B. Reaves, and D. Richey, "On SCADA control system command and response injection and intrusion detection," in *Proceedings of the 2010 Fall General Meeting and eCrime Researchers Summit, eCrime 2010*, October 2010.

[38] H. Lin, A. Slagell, Z. Kalbarczyk, P. Sauer, and R. Iyer, "Runtime semantic security analysis to detect and mitigate control-related attacks in power grids," *IEEE Transactions on Smart Grid*, 2016.

[39] T. Cruz, L. Rosa, J. Proença et al., "A Cybersecurity Detection Framework for Supervisory Control and Data Acquisition Systems," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 6, pp. 2236–2246, 2016.

[40] A. Cook, H. Janicke, L. Maglaras, and R. Smith, "An assessment of the application of IT security mechanisms to industrial control systems," *International Journal of Internet Technology and Secured Transactions*, vol. 7, no. 2, pp. 144–174, 2017.

[41] M. A. Ferrag, L. A. Maglaras, H. Janicke, and J. Jiang, "A survey on privacy-preserving schemes for smart grid communications," https://arxiv.org/abs/1611.07722.

[42] B. Galloway and G. P. Hancke, "Introduction to industrial control networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 860–880, 2013.

[43] K. Stouffer, J. Falco, and K. Scarfone, *Guide to Industrial Control Systems (ICS) Securit*, National Institute of Standards and Technology Special Publication, 2011.

[44] Ethernet - The Wireshark Wiki. Wiki.wireshark.org. N.p., 2017. Web. 16 Dec. 2016. https://wiki.wireshark.org/Ethernet.