An Analysis of Adversary-Centric Security Testing within Information and Operational Technology Environments

ALEXANDER STAVES, Lancaster University, United Kingdom
ANTONIOS GOUGLIDIS, Lancaster University, United Kingdom
DAVID HUTCHISON, Lancaster University, United Kingdom

Assurance techniques such as adversary-centric security testing are an essential part of the risk assessment process for improving risk mitigation and response capabilities against cyber attacks. While the use of these techniques, including vulnerability assessments, penetration tests, and red team engagements, is well established within Information Technology (IT) environments, there are challenges to conducting these within Operational Technology (OT) environments, often due to the critical nature of the OT system. In this paper, we provide an analysis of the technical differences between IT and OT from an asset management perspective. This analysis provides a base for identifying how these differences affect the phases of adversary-centric security tests within industrial environments. We then evaluate these findings by using adversary-centric security testing techniques on an industrial control system testbed. Results from this work demonstrate that while legacy OT is highly susceptible to disruption during adversary-centric security testing, modern OT that uses better hardware and more optimised software is significantly more resilient to tools and techniques used for security testing. Clear requirements can, therefore, be identified for ensuring appropriate adversary-centric security testing within OT environments by quantifying the risks that the tools and techniques used during such engagements present to the operational process.

CCS Concepts: • **Hardware → Hardware reliability**; • **Security and privacy → Penetration testing**; **Embedded systems security**.

Additional Key Words and Phrases: Industrial Control Systems, Operational Technology, Information Technology, Security Testing, Risk

ACM Reference Format:
Alexander Staves, Antonios Gouglidis, and David Hutchison. 2022. An Analysis of Adversary-Centric Security Testing within Information and Operational Technology Environments. *Digit. Threat. Res. Pract.* 1, 1, Article 1 (January 2022), 30 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

In recent years, there has been a global push to improve cyber security capabilities within organisations, primarily in response to the dramatic increase in targeted cyber attacks [49]. Increasingly, such attacks have started targeting networks of Critical National Infrastructures (CNIs), which are systems that are essential for the smooth operation of a country's economy and society [12]. Successful cyber attacks on a CNI can have serious consequences, as observed in the Stuxnet attack of 2010, which set back the Iranian Nuclear Programme by several years [62].

Authors' addresses: Alexander Staves, a.staves@lancaster.ac.uk, Lancaster University, United Kingdom, LA1 4WA; Antonios Gouglidis, a.gouglidis@lancaster.ac.uk, Lancaster University, United Kingdom, LA1 4WA; David Hutchison, d.hutchison@lancaster.ac.uk, Lancaster University, United Kingdom, LA1 4WA.

2576-5337/2022/1-ART1 $15.00
https://doi.org/XXXXXXX.XXXXXXX

Moreover, such attacks can also bring danger to civilian life by affecting critical environments such as electrical grids, emergency services and transportation services.

Despite the urgency to effectively defend a CNI against cyber attacks, the primary differences between Operational Technology (OT) systems often used in CNIs, and the more traditional Information Technology (IT) systems, make it difficult to transfer skills and techniques from one domain to the other [57]. As opposed to IT systems, which prioritise the handling of data or information, OT systems are used to ensure the successful operation of operational processes. Examples of OT include Programmable Logic Controllers (PLC), Supervisory Control and Data Acquisition Systems (SCADA), Distributed Control Systems (DCS), and Industrial Control Systems (ICS).

An increasingly popular method for evaluating and improving both cyber resilience and incident response capabilities is through adversary-based security testing [27]. These engagements use highly specialised teams to emulate the actions of genuine malicious actors. Conducting such engagements helps organisations understand both the psychological factors and the techniques employed during genuine cyber attacks. In doing so, underlying vulnerabilities can be detected and patched, and incident response teams can be trained by being kept updated about tools and techniques used by modern attackers [42].

While adversary-based security testing has become widely adopted within IT environments, this is not commonly the case for OT environments. Many training courses and certifications exist for IT penetration testing, such as the Offensive Security Certified Professional certification, whereas relatively little currently exists for OT penetration testing [65]. This presents several challenges, as not all tools and techniques used within IT environments apply to OT environments. For example, even simple actions such as active port scanning, often used during IT security tests, may result in system crashes within poorly configured OT environments [76]. Thus, it is essential to establish the similarities and differences in these two environments in order to facilitate more effective adversary-based OT security testing.

The aims of this paper are first to provide a comprehensive comparison of the differences between Operational and Information Technology systems from a general cyber security point of view and, second, to illustrate how these similarities and differences need to be considered when conducting adversary-based security tests. Finally, these differences are evaluated by employing active adversary-centric security testing techniques on ICS and assessing how these could disrupt the operational process. In this way, precise requirements can be identified for the scoping of adversary-centric security tests within OT environments, allowing for the development of a framework to ensure the appropriate use of security testing tools and techniques during such engagements.

The remainder of the paper is structured as follows: Section 2 provides a background of current practices and discusses related work; Section 3 provides a cyber security focused comparison between OT and IT systems; Section 4 illustrates how these differences affect adversary-based security testing engagements; Section 5 evaluates the findings from Section 4 by conducting IT-typical penetration testing techniques on both OT and IT systems; and Section 6 concludes the paper and presents future work including the development of a safety and operational risk-based framework for scoping of adversary-centric security tests on ICS/OT.

2 BACKGROUND AND RELATED WORK

Over the past decade, there has been a noticeable increase in allocated importance towards OT cyber security. Most researchers link this back to the Stuxnet attack of 2010 on the Iranian Nuclear Programme [62]. This attack is considered one of the first documented use of a cyber weapon with the aim to cause industrial damage to a nation state’s activities. The malware used in this attack targeted PLCs and caused centrifuge speed fluctuations within uranium enrichment facilities, causing them to fail and leading to operational shutdowns [43]. Since then, there has been an exponential rise in cyber attacks targeting ICS, often part of underlying critical infrastructure networks, with multiple attacks even occurring recently, such as the attack on a Florida town water supply in February of 2021 [69] or even the DarkSide attack on the US Colonial Pipeline infrastructure in May of 2021 [87].

This ever-growing increase in attacks targeting these systems has led governments and organisations to invest considerable resources into defending their systems against cyber attacks. For example, the European Union Agency for Cybersecurity (ENISA) adopted the EU Network and Information Security Directive (NIS Directive) in 2016 to enhance critical infrastructure cybersecurity across the European Union [17]. Similarly, individual countries have also produced their own strategies for defending against cyberattacks targeting critical infrastructure and, therefore, ICSs such as the UK's Cyber Assessment Framework [58] or the USA's NIST Framework for Improving Critical Infrastructure Cybersecurity [59].

Several surveys over the past decade, such as those by the US Government Accountability Office [88]or by Westby [91] on how board members and senior management within Critical Infrastructure govern the security of their organisation, have been conducted. Findings from these concluded that several security issues were missing at the time of the surveys, including an effective mechanism for sharing information on cyber security, general cyber security awareness, security features built into critical infrastructure networks, including OT, and metrics for measuring and assessing cyber security capabilities. While these surveys were conducted in 2011 and 2012, a recent survey on the use of standards and guidelines to aid in the development of cyber incident response and recovery capabilities found similar results [83]. This survey concluded that while there have been significant advances in developing standards and guidelines for ICS and CNI, their widespread adoption was minimal, resulting in a less than complete picture. Preparation for incidents, including security assessments such as penetration testing, was identified as a crucial phase for effectively improving cyber incident response and recovery capabilities. Despite this, the use of adversary-centric assurance techniques was limited due to both the skill gap between OT engineering and general penetration testing and the limitations imposed by the safety-critical nature of ICS. A survey conducted by the SANS Institute showed that the top initiatives demonstrated by OT stakeholders included both performing security assessments or audits of control systems and their networks as well as initiatives to bridge the IT/OT gap [18]. While component testing, through assessment engagements such as vulnerability scanning, was considered a strong positive for improving network resilience, only 41% of participants claimed that they used these due to the risk of disrupting the operational process. A survey by Green et al. details the approaches adopted by security practitioners during risk assessment within ICS environments [27]. In this study, penetration tests were considered a distinct phase within the risk assessment process and could provide additional risk validation prior to appropriate mitigation. Scoping, including that of penetration tests, was identified as both one of the most important and most challenging parts of the risk assessment process.

Several works discuss and propose solutions for the general concerns raised from the presented surveys [11, 27, 42, 57, 81]. Conklin, for example, discusses the issues linked with utilising IT-specific methodologies within an industrial context, especially concerning the Confidentiality, Integrity and Availability (CIA) Triad [11]. The author proposes the addition of Resilience as an additional factor to consider alongside the CIA Triad while referencing several standards adapted from IT-specific security controls for use in OT environments such as NIST SP 800-53. While Conklin does not directly reference adversary-centric security testing within an industrial context, the fact that the CIA triad alone needs to be reconsidered when discussing OT environments demonstrates that further engagements to test this, such as penetration tests, also need to be reconsidered. Song et al. discuss the cyber risk assessment process for the design of I&C systems within nuclear power plants [81]. The final phase of their methodology recommends penetration testing to validate the proposed security design and implementation. However, the authors note that potential for disruption is possible when simulating attacks on the systems under consideration. No specifics are given on how these disruptions occur and what remediations exist for them. Murray et al. discuss the convergence of IT and OT and how this affects cyber security for critical infrastructures [57]. Using Hofstede's Theory, the authors demonstrate the differing cultural values between IT and OT across several dimensions, such as the Power Distance Index or the Uncertainty Avoidance Index. While the analysis does not provide insight into the technical differences between IT and OT, the cultural differences observed show that substantial readjustment is required to ensure the smooth transition to the convergence of the two technologies. Finally, Knowles et al. discuss assurance techniques for ICS, including penetration testing [42]. In this study, simulated security assessments are identified as being able to generate demonstrable audit evidence to assess and improve risk posture. Usage of security assessments was observed to be lacking due to the general absence of a workforce with specialised skills when assessing OT environments, especially those that are safety-critical.

As we can see, current research on adversary-centric security testing discusses its benefits and the challenges faced when conducting such engagements within industrial environments; these are summarised in Table 1. However, little detail is provided on the considerations of the technical differences between IT and OT for safely conducting tests. The following sections provide, firstly, a technical analysis of required cyber security considerations within OT environments compared to traditional IT environments and, secondly, an analysis of how these differences affect the undertaking of engagements such as penetration tests.

Reference	**Motivation**	**Contribution**	**Challenges**
[11]	Challenges with using IT-specific methodologies for OT cyber security	Reformulation of the CIA Triad to include Resilience for OT	Testing of CIA Triad for OT requires reconsideration
[81]	Design of I&C systems cannot use traditional risk assessment	Unique risk assessment process for design of I&C systems	Penetration Testing recommended as part of Risk Assessment life-cycle but no solutions for enabling this
[57]	Convergence of IT and OT in CNI presents new challenges for the cyber security of these	Cultural differences between IT And OT demonstrate the need for readjustment for smooth convergence of the two technologies	Readjustment also needed due to technical differences between IT and OT
[42]	Unique assurance techniques required for ICS	Mapping of assurance techniques to ISO/IEC 27001:2013 with penetration tests identified as an important technique	While identified as an effective assurance techniques, penetration testing shown as lacking in practice due to lack of specialised workforce
[27]	Understanding practitioner's approaches to risk assessment for OT	Identification of key phases for OT risk assessment	Penetration testing identified as a key phase for OT risk assessment but is also identified as one of the most challenging due to additional constraints in OT environments

Table 1. Summary of Related Work

3 ANALYSIS OF INFORMATION AND OPERATIONAL TECHNOLOGY

3.1 Methodology

For our analysis, we have made use of standards and guidance which discuss asset management in detail. The scope of these sections of the articles is to guide stakeholders with asset management and concentrate on activities such as implementing a new asset within a network, transferring an existing asset to another network, and continuous hardware and software monitoring. As presented in these documents, asset management is considered a critical part of an organisation's cyber security lifecycle as mismanagement of this process can adversely affect other phases or categories such as resilience or incident response. We found that by selecting the categories discussed during asset management sections, distinct criteria can be identified for comparing OT and IT systems. While we identified several publications on asset management specifically, such as the National Institute of Standards and Technology (NIST) Special Publication 1800-5, which discusses IT Asset Management for large financial services organisations [60], most of these articles referenced the following two documents: The NIST Framework for Improving Critical Infrastructure Cybersecurity [59] and the ISO/IEC 27000-series [36, 37]. We, therefore, selected the sections from these documents detailing asset management as the basis for our comparison.

The first document selected for our comparison is the NIST Framework for Improving Critical Infrastructure Cybersecurity [59]. This document was created following the Cybersecurity Enhancement act of 2014, which tasked NIST with developing a cyber security risk framework for operators and owners of Critical Infrastructures [89]. The framework scope is to guide operators and owners of Critical Infrastructure to improve their cyber security activities and help implement resilient cyber security strategies within an organisation's larger risk management process. A large portion of this framework provides guidance on effectively managing assets of critical infrastructures as part of the cyber security lifecycle. As ICS are often found within critical infrastructure networks, this document can mostly be extended to include any operators or owners of OT assets.

The second document used for this comparison is the ISO/IEC 27000-series. This series of standards, mainly ISO/IEC 27001 and 27002, provide best practice guidance for information security management [36, 37]. Having a broad scope, these standards can be used by all types of organisations. While generally IT-focused, the sections of these standards that do not go into technical detail can still mostly be used by operators and owners of ICS. However, it is recommended that more OT-focused standards such as ISO/IEC 27019 be consulted as well, especially for the energy industry [38].

Section Title	ISO/IEC 27001/2	NIST Framework
Asset Management	A.8	ID.AM
Physical Security	A.11	PR.AC
Software Management	A.12.5	ID.AM
Communications Security	A.13	ID.AM, PR.AC, PR.DS
Security Policies	A.5	ID.GV
Awareness and Training	A.7.2.2	PR.AT

Table 2. Equivalent Sections from the NIST Framework and ISO/IEC 27001/2

To begin with the comparison, all relevant sections from the NIST Framework for Improving CI Cybersecurity and ISO/IEC 27001/2 on Asset Management were extracted. These sections allowed us to categorise different aspects of IT and OT systems for our comparison. However, despite these two documents catering towards OT and IT, respectively, the topics related to Asset Management are identical in content, as shown in Table 2. From this, we, therefore, extracted the following categories to use in our analysis:

- Hardware: function, manufacturing etc.
- Software: underlying programming, patching etc.
- Network: network topology, communication protocols etc.
- Socio-Technical: governance, policies, education, training etc.

3.2 Hardware

One of the most fundamental differences between OT and IT-based systems is their hardware. This is due to, essentially, their function within their respective environments. As per the name, Information Technology exists to store, retrieve and manipulate information or data, whereas Operational Technology is mainly used to detect and cause changes in an operational process.

Throughout the years, Information-based systems have seen significant technological advances in speed and energy efficiency, as observed by Moore [56]. Typically an enterprise network will be comprised of systems such as personal workstations, various servers and peripheral devices such as printers. Due to their tasks of processing, transferring and modifying data, these require hardware that can perform tasks at efficient speeds. Memory-based hardware components such as storage drives, RAM, CPUs, and GPUs are, therefore, often heavily invested in to allow for larger resource loads. This flexibility allows IT hardware to withstand resource-intensive actions such as aggressive port scanning or vulnerability scanning in an adversary-centric security test.

Many devices are categorised under OT based on their specific role within the industrial process. Their function, which is to view, monitor, and control physical processes, directly impacts their hardware design and implementation. For example, PLCs are devices designed to operate reliably within harsh environments (high temperature, wet conditions) for extended time frames (several decades). As they are often designed with specific tasks in mind, their hardware architecture reflects this; being composed of a processor unit, power supply, an I/O interface, a communication interface and dynamic memory only, in most cases. Because of this, their hardware capability is often designed with durability and reliability in mind, meaning that components such as their processor units are often designed to operate at minimal power without interruption. The CPU resources, therefore, reflect this; for example, the SIEMENS S7-1200 PLC specifications indicate that its power consumption is 1.2A at 24V [78]. Consequently, the S7-1200's CPU processing time ranges between 0.085μs and 2.5μs per instruction depending on the operation type (bit, word or floating-point arithmetic), and its total available memory is 50kbyte and 1Mbyte for work and load memory, respectively. As we can see, the specifications for OT equipment differ significantly from the terms used for typical IT products, primarily because these are targeted toward automation engineers. Because of this, however, difficulties arise when comparing these two system types directly, further demonstrating the IT and OT gap.

To summarise, due to the differences in functionality between IT and OT, the hardware specifications between these two system types also differ significantly, illustrated in Table 3. OT is designed to withstand harsh environmental factors for an extended time, whereas IT processes information as efficiently as possible. As such, OT is often considered more fragile than IT. When conducting an adversary-centric security test on these, additional care must be taken when performing aggressive actions on OT, requiring a thorough understanding of these prior to any security engagement.

3.3 Software/Firmware

Similarly to the differences in hardware between OT and IT systems, there are many differences pertaining to software. This is also due to the underlying purpose of these devices. As IT systems are designed around data storage and manipulation, this is reflected in the software they run, which is both efficient and straightforward enough for mainstream use. Many IT devices such as personal computers or servers run commercially available or open-source Operating Systems (OS) such as Microsoft Windows, Apple's macOS, and GNU/Linux distributions,

	Information Technology	Operational Technology
Design Philosophy	Data Processing	Operational Control
Physical Design	Temperature-Oriented	Environment-Oriented
Power Requirement	Low-to-High	Low
Computation Power	Flexible	Limited to Intended Tasks
Uptime Requirement	Low-to-High	High

Table 3. Hardware differences between IT and OT systems

to name a few. These OSs offer an easy-to-understand Graphical User Interface (GUI) for everyday work projects or personal use. Specialised versions of these have also been developed with OSs explicitly designed for servers, such as Microsoft Windows Server [48]. Over the years, these OSs have seen heavy investment in security with regular security patches and the development of built-in tools including proprietary anti-viruses or even a shift towards using biometric access control such as facial recognition or fingerprint readers instead of passwords [47]. Due to the popularity of these systems, new vulnerabilities and exploits are discovered regularly, resulting in the constant threat that machines are not updated regularly enough to keep up with newly discovered exploits despite vendors such as Microsoft being able to provide timely patches for newly discovered vulnerabilities. This was the case, for example, with the Wannacry attack on the UK National Health Service (NHS) in May 2017, where 80 out of 236 hospital trusts were affected due to having not made the appropriate updates to their Operating Systems, which was issued in March 2017 and advised by NHS Digital's CareCERT bulletin in April 2017 [80].

Unlike IT systems, OT systems are designed to be used by specialised groups such as automation engineers. As such, industrial software also reflects this. PLCs, for example, are commonly programmed using Ladder Logic [7]. This specialised programming language represents written programs through graphical diagrams based on logic circuitry. Since its conception, other similar languages have been designed and standardised in IEC 61131-3 [32]. Ladder Logic provides a simple yet optimal method for controlling PLCs. When programmed correctly, it is improbable to cause software or hardware crashes, which is critical when running inside environments that require near-total uptime, such as water supply stations or power plants [66]. Due to the critical aspect of ICS, engineers require quick and easy access to these if operational actions need to be modified or halted. Because of this, devices such as PLCs often run as root by default [67]. This has cause for several security concerns, especially considering that such PLCs are used as part of Critical Infrastructure networks. If an attacker were to gain access to these PLCs, they would have direct access to all of their functionalities, resulting in severe operational impact.

In recent years, there has also been a push toward using Real-Time Operating Systems (RTOS) for various embedded systems within OT networks. These specialised OSs serve real-time applications and process data without little or no buffering delay. This allows for the smooth operation of time-sensitive processes, which is often required within industrial networks [28]. However, a study on the security of RTOSs conducted by Yu et al. concluded that despite the advantages gained by using these, security against cyber attacks is still a significant concern in systems that use these specialised OSs [92].

Due to the criticality of requiring high uptime within OT environments, updating software for these can be challenging. For example, a study presented at Black Hat USA found that the average time between disclosure of a vulnerability and detection of that same vulnerability within an OT network was 331 days at the time of the study [41]. Allowing attackers such an extensive time frame to develop exploits increases the risk associated with unpatched vulnerabilities and increases the potential impact that could be caused. Additionally, while IT systems can allow for timely security patches, not all OT systems can do the same, depending on their functions.

Power plants, for example, could schedule patching during the Summer, when not all systems are required for operations. However, providing software updates during the Winter could prove more challenging as the demand for electricity during that time is considerably higher [20, 83].

To summarise, the software differences between IT and OT, implemented based on their respective function, leads to a significant disparity in their security capabilities, as illustrated in Table 4. Furthermore, critical security features are often overlooked due to the only recent implementation of security features in OT software, leading to significant exposure to external threats.

	Information Technology	**Operational Technology**
Operating System	Open-Source, Commercially Available	RTOS, Ladder-Logic, Function Block Diagrams
Target Audience	Everyday Users	Specialised Engineers
Security Design	Security by-design	Operational Function by-design
Patching/Updates	Regular and Easy	Rare and Difficult

Table 4. Software differences between IT and OT systems

3.4 Network Architecture and Protocols

A common theme present throughout our comparison is that the difference in purpose between IT and OT systems undoubtedly leads to a difference in the characteristics of these systems. This also holds true for OT or IT network architecture and protocols. As IT networks were very early in their adoption of Internet Protocols, this naturally led to a need to defend these systems against remote attacks [2]. Over the years, techniques and models have been developed to ensure that IT networks are highly resilient against both external and internal attacks. Many network security reference architectures have since been developed and widely adopted, such as the Fortinet Network Security Reference Architecture [71] or through guidance provided by IBM [82]. The main objective of these architectures is to allow for good network flexibility while being resilient to threats. While network reference architectures exist for OT environments, such as the Purdue Enterprise Reference Architecture [14], these focus more on the segmentation of network zones based on hierarchical function. Figure 1 illustrates the zones described in the Purdue Model. While there is little detail on how each layer can be secured at an individual level, the model uses a Demilitarized Zone (DMZ) to address security risks between the IT and OT zones. One such recommendation detailed by Cisco is to design the DMZ so that no traffic traverses directly through it, meaning that traffic must either terminate or originate in the DMZ. Historically, ICS security also relied on the use of "air gapping" networks, making it so that external threats could not attack networks remotely. While this may have been a viable security policy a couple of decades ago, the introduction and implementation of smart networks through IoT make it very difficult to truly have an air gap anymore [10].

However, the security capabilities of individual protocols used within OT networks are also worth noting. As most of these protocols were created when security was not a primary concern, most of these have inherent vulnerabilities that can be exploited [22]. Attack vectors such as ARP spoofing, DNS cache poisoning or generally poor encryption need to, therefore, either be mitigated internally through firewall ruling or by implementing the secure version of the protocols under consideration, by using SSL/TLS, for example [9]. However, this shift toward using more secure protocols is not yet widespread within OT networks [6]. Despite some of the standardised protocols being updated to use TLS, such as Modbus TLS or OPC UA, a significant number of these protocols still do not use proper encryption or authentication, such as PROFINET or CAN [90]. Modbus, as an example, is a protocol created by Modicon (now Schneider Electric) in the late 1970s and is a widely adopted OT protocol, mainly because of its simplicity and robustness. The Protocol Data Unit of the Modbus packet frame contains

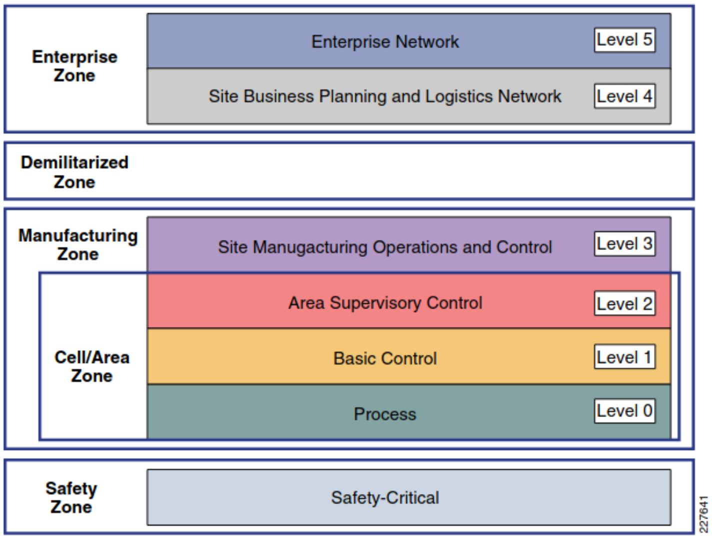


Fig. 1. Purdue Enterprise Reference Architecture [14]

Function Code	Function Description
1	Read Coils
4	Read Input Registers
5	Write Single Coil
6	Write Single Holding Register
14	Read Device Identification
15	Write Multiple Coils
16	Write Multiple Holding Registers
17	Report Slave ID

Table 5. Example Modbus Functions

a function code and data payload. Packets can be handcrafted within any programming language to perform specific actions that could benefit an adversary, such as reading the device identification or reading/writing directly to coils or registers. Table 5 provides several examples of Modbus Functions and their respective codes that could be identified during an adversary-centric security test as a security risk. This is mainly because, as an older protocol, Modbus lacks modern security features that would prevent attacks such as unauthenticated commands or replay attacks. This means that an adversary could control an operational process, such as through a traffic light system, while making it appear from a connected HMI that the system under consideration was never altered. Similar Security weaknesses exist within most ICS protocols, standard and proprietary alike. DNP3, for example, supports the use of a Direct Operation Function, which means that target devices can be actuated directly by the output points specified in the object of the received packet [1]. This can be done by anyone with access to the network or remotely communicating with a device using DNP3 due to the lack of authorisation control.

The documentation of these industrial protocols can be jarring at best, meaning that operators may be reluctant to upgrade implemented protocols to their more secure versions. For example, the complete documentation available for the Common Industrial Protocol is over 1500 pages long [64]. Another challenge that industrial networks face is that many of these still make use of proprietary protocols such as S7COMM (Siemens) or Melsec/TCP (Mitsubishi Electrics) [50, 55]. While some have been updated to provide encryption and authentication, these protocols rely on their vendors for updates meaning that operators can be left with substantial delays between security updates.

In General, three mitigation techniques can be implemented to reduce the inherent risk of using OT protocols [6]. While it can be challenging to do so within a production environment, keeping firmware up to date can mitigate known network-based attack vectors such as arbitrary code execution or replay attacks. This, however, does not reduce the risk originating from undiscovered vulnerabilities (otherwise known as zero-days) but can help minimise their discovery. Most importantly, the implementation of proper network topology and segmentation, such as through using the Purdue Reference Architecture Model, can help reduce unauthorised access to industrial systems through means of layered defense [14]. Finally, incorporating Intrusion Detection Systems should also be done. However, as opposed to IT, Intrusion Prevention Systems are discouraged for OT networks as their use could halt critical traffic within the process network due to false positives.

To summarise, due to the only recent requirements of implementing proper security control within OT networks, many gaps in security capabilities can be identified, as illustrated in Table 6. Despite a push to use more secure protocols, this is not yet comprehensive in practice, leaving industrial networks exposed to simple attack vectors due to the lack of security within communication protocols.

	Information Technology	**Operational Technology**
Network Architecture	Secure-by-Design	Safe-by-Design
Protocol Priority	Confidentiality	Availability
Protocol Security	Inherent	Optional
Authentication	Required	Little-to-None
Detection Systems	IDS/IPS	IDS

Table 6. Network and Protocol differences between IT and OT systems

3.5 Socio-Technical Considerations

While the previous sections discussed technical differences between IT and OT, socio-technical aspects also play an essential part in the overall strategy for effectively securing assets against malicious actors. However, how these are implemented can differ between IT and OT.

One of the most well-known concepts for implementing cyber security controls and policies, for example, is the Confidentiality-Integrity-Availability (CIA) triad. In most cases, an organisation's primary goal is to maintain the confidentiality, integrity and availability of information, ensuring complete coverage of cyber security capabilities. The ordering of this model reflects the prioritisation of these attributes, primarily for IT. As such, the preservation of confidentiality is overall allocated more priority over integrity and availability. This means that, in the event of a cyber attack, IT organisations will allocate more resources to ensuring the preservation of confidentiality than availability. This, however, is not the case for OT environments. Due to their time-critical nature, any change in availability can have detrimental consequences. For example, if the availability of a Safety PLC (part of a Safety Instrumented System) were to be compromised, this could most likely lead to an overall loss of safety. For this reason, OT security controls and policies prioritise the conservation of availability (and consequently integrity), whereas IT security controls and policies prioritise the conservation of confidentiality.

An observation noted during several of the surveys discussed in Section 2 was the apparent lack of cross-disciplinary skills and communication between OT and cyber security. OT engineers, historically, were not required to be knowledgeable in security. However, with the rapid technological changes introduced to this domain, this is no longer the case. Because of this, senior engineers have been required to review their practices from the ground up, leading to a significant disparity in skill and a shake-up in standard practices. To this day, an OT engineer is likely to firstly view a cyber incident as a technical fault before considering the event as a cyber attack, leading to a delay in appropriate response and recovery actions [83].

The use of standards and guidelines was also found to be more mature for IT than for OT. While a plethora of guidance is available for aiding OT operators in assessing and improving their cyber security capabilities, the disparity of topics discussed within these could leave operators with a less than complete picture, resulting in a potential gap in the implementation of security controls and policies [83]. To this end, existing standards and guidelines often lack the required tooling and frameworks for proper implementation within OT environments, instead applying information-based strategies as opposed to function.

This discrepancy can also be observed for certifications related to cyber security, especially security testing. Currently, no accreditations exist to certify that an individual meets a specific level of understanding and expertise when conducting security engagements within industrial environments. Many of these exist for traditional IT, such as the Offensive Security Certified Professional, the Certified Ethical Hacker or the GIAC Penetration Tester certifications, but little currently exists for OT/ICS Penetration Testing [16, 21, 65]. The SANS Institute and ISA used to both offer SCADA and ICS penetration testing courses [35, 72]. However, these are short in length, are not recognised by governing bodies, and are currently unavailable for enrolment. Instead, high-level courses are listed which provide a general overview of OT cyber security [34, 73]. Because of these challenges, only a small set of individuals are officially qualified to provide adversary-centric security tests for operators of OT, especially CNI.

To summarise, socio-technical aspects of security for OT have been observed to be significantly less mature than within IT, as illustrated in Table 7. Because of this, a significant knowledge gap exists between essential cyber security concepts and OT engineering, leading to a disparity in cyber security capabilities between IT and OT.

	Information Technology	**Operational Technology**
CIA Triad Prioritisation	Confidentiality	Availability and Safety
Security Culture	Mature	In-Progress
Use of Standards and Guidelines	Comprehensive	Limited
Certifications	Widely Available	Little-to-None

Table 7. Socio-Technical differences between IT and OT

4 ADVERSARY-CENTRIC SECURITY TESTING CONSIDERATIONS

An essential aspect of an organisation's cyber security lifecycle, including defence and response, is preparation [27, 81, 83]. If organisations are not prepared to effectively defend and respond to cyber-attacks, whether targeting IT or OT, the impact of these can be disastrous and even possibly life-threatening in the case of most critical infrastructure environments [49]. Security testing, especially adversary-based such as red teaming, can provide significant benefits to ensuring that organisations are sufficiently prepared to defend and respond to cyber-attacks.

Firstly, these types of engagement test current non-human-based defence and response capabilities by discovering vulnerabilities and weaknesses in existing protective measures such as firewalls and detection mechanisms. Secondly, they also test, train and improve human-based defence and response capabilities such as the incident response team or the general security culture of the organisation. While adversary emulation can prove to be more complex and costly than other engagements such as vulnerability scanning or training/exercising, since these engagements aim to be as close to reality as actual cyber attacks, this often results in a more thorough and in-depth understanding of current defence and response capabilities and ultimately leads to better improvement of these [42].

While conducting adversary-centric security tests has gained significant traction within IT environments, this is yet to be the case for OT [18]. The first reason for this is the only recent evolution of technologies within industrial environments. For example, the transformation of electrical grids into smart grids means that they now rely much more on both IT and ICS infrastructure than before [29]. Secondly, since OT systems are often found as part of underlying critical infrastructures, the critical nature of these environments means that teams conducting any adversary-centric security test within these need to be highly specialised and vetted thoroughly, such as through the NCSC CHECK accreditation, for example [61]. This section extends the comparison made in section 3 by detailing how the differences and similarities between IT and OT systems affect decision-making and actions taken during adversary-centric security tests within these environments.

4.1 Methodology

As adversary-based security testing aims to emulate actual cyber-attacks to test, train and improve an organisation's resilience, response, and recovery capabilities, the Tools, Techniques and Procedures (TTPs) used during these engagements closely mirror those of actual cyber-attacks. Although many of the cyber-attacks that have occurred over the years are somewhat unique, the adversaries behind them all follow, to some degree, the same steps for achieving their goals. Lockheed Martin mapped these steps to a framework titled the Cyber Kill Chain (CKC) [30]. As part of the Intelligence Driven Defense model, the framework identifies and details what adversaries must complete to ensure their objectives. The aim of this is for defenders to better understand the TTPs behind cyber-attacks to defend more effectively against them. The CKC is made up of seven steps; these are as follows:

(1) Reconnaissance: Gain information on the target system by identifying and harvesting information that can be used to gain an initial foothold within the network.
(2) Weaponisation: Create a payload to exploit the vulnerabilities found through reconnaissance.
(3) Delivery: Deliver the payload to the target.
(4) Exploitation: Gain access to the target by executing the payload to exploit vulnerabilities found through reconnaissance.
(5) Installation: Establish a backdoor within the target to maintain access.
(6) Command & Control: Open a command channel to be able to remotely manipulate the target system.
(7) Actions on Objectives: Accomplish the attack's objectives.

It is worth noting that although the CKC contains phases similar to a linear process flow framework, it represents a dependency-based process flow. This means that the further an attacker advances through the kill chain, the more their subsequent actions depend on previously taken actions. Therefore, revisiting previous steps within the framework is extremely common and often essential, defining the CKC as more of a circular and non-linear process. For example, if an attacker has reached the Delivery stage (stage 3) of the CKC after crafting a payload to exploit a discovered vulnerability in the target network, they may need to conduct additional reconnaissance (stage 1) in order to discover how to deliver the payload as effectively as possible.

While the Lockheed Martin CKC provides a complete overview of the steps most adversaries take to conduct cyber-attacks, attacks on ICS require more depth and sophistication to succeed. Because of this, the SANS Institute developed the Industrial Control System Cyber Kill Chain [4]. This model, based on Lockheed Martin's original model, describes the steps taken by attackers to conduct a cyber-attack on ICS specifically. While simple ICS attacks such as industrial espionage or ICS disruption might not follow each stage of the ICS CKC, The steps described in this kill chain help defenders gain knowledge on how to better combat in-depth cyber-physical attacks, such as those originating from nation-state-sponsored groups. The ICS CKC is composed of two stages, each containing multiple phases; these are as follows:

- STAGE 1: Cyber Intrusion Preparation and Execution

(1) Planning: Reconnaissance.
(2) Preparation: weaponisation and Targeting.
(3) Cyber Intrusion: Delivery, Exploitation, and Installation/Modification.
(4) Management and Enablement: Command & Control.
(5) Sustainment, Entrenchment, Development and Execution.

- STAGE 2: ICS Attack Development and Execution

(1) Attack Development and Tuning.
(2) Validation and Testing.
(3) ICS Attack: Deliver, Install/Modify, and Execute.

As we can see, the first stage of the ICS CKC closely resembles the Lockheed Martin CKC. The two models start to differ after this, however. The ICS CKC contains an additional stage because successful attacks on ICS with re-attack options require extremely high levels of confidence to execute.

Although both the Lockheed Martin CKC and the ICS CKC provide a holistic overview of the steps used during an adversary-centric security test, due to the high-level nature of these models, they provide little technical detail on the TTPs used during each phase of the CKC. To provide more technical depth to our analysis, we have, therefore, selected both the MITRE ATT&CK and MITRE ICS ATT&CK Frameworks for this [51, 52]. These frameworks provide a knowledge base of adversary tactics and techniques based on real-world observations. Each TTP is categorised by attack types such as reconnaissance or lateral movement. These frameworks aim to provide defenders with knowledge on the TTPs used by attackers to understand them better and, consequently, better defend against them. As demonstrated in section 3, there are distinct differences that need to be considered when attacking ICS networks compared to traditional IT networks. The following sections will detail these differences when conducting an adversary-based security test on IT and OT systems. While the phases of the CKC and TTPs detailed within the ATT&CK frameworks are often leveraged during an adversary-centric security test to emulate real-world adversaries, a specific subset of these TTPS and phases may be utilised depending on the type of engagement being done. For example, a red team engagement is likely to leverage all phases of the CKC, while a typical vulnerability scan may make use of the reconnaissance phase and part of the weaponisation phase only.

4.2 Reconnaissance

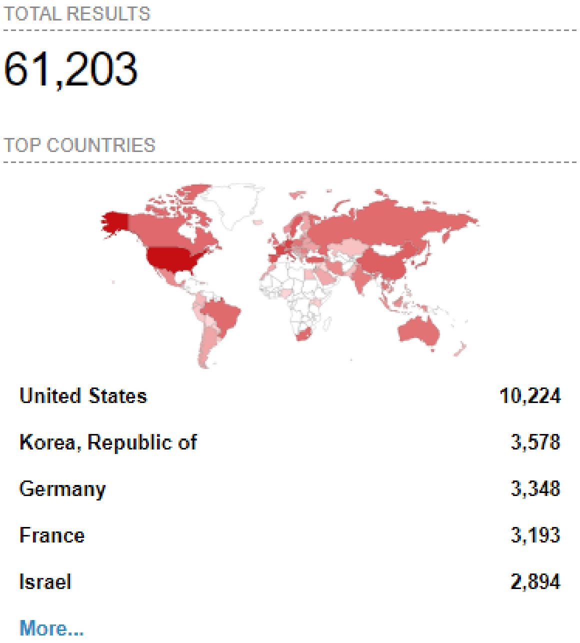
At the beginning of any adversary-based security test, reconnaissance must be conducted to gain the information required to exploit the target systems. Two types of reconnaissance exist: passive reconnaissance and active reconnaissance. Passive reconnaissance refers to conducting reconnaissance that does not directly interact with the target system. This can either correspond to using non-technical reconnaissance such as Open-Source Intelligence (OSINT) through search engine searches (google, Shodan) and tools such as Netcraft or using passive tools and methodologies such as network sniffing. Active reconnaissance, on the contrary, directly interacts with the target system to obtain information on it. This corresponds to using techniques and tools such as vulnerability scanners, port and service scanners, fingerprinting, banner grabbing, etc. While reconnaissance is integral to any cyber intrusion exercise, only the MITRE ATT&CK Framework provides specific TTPs for this phase. This is because the ICS ATT&CK framework is defined as a "knowledge base [that] can be used to better characterise and describe post-compromise adversary behaviour" rather than a framework encompassing the whole CKC. Despite the TTPs described in the ATT&CK framework being meant for IT networks, most of them can also be applicable for OT networks. The MITRE ATT&CK framework details four different types of goals when conducting general reconnaissance: Gathering victim host (T1592), identity (T1589), network (T1590) and organisation (T1591) information. Once enough actionable information is acquired on these, teams can proceed to the next step of the CKC, the weaponisation of a payload. The following sections discuss the characteristics of passive and active reconnaissance techniques and TTPs, and how they differ between IT and OT environments.

4.2.1 Passive Reconnaissance. As mentioned, passive reconnaissance is a means of acquiring actionable information on a target system or network without directly interacting with it. While it often takes considerably longer to obtain valuable information through this method, the fact that no direct interaction with the target is required means that detection is infrequent. This presents several opportunities for attackers and red teams alike, including the freedom of evading detection, gaining considerable time to develop exploits and more. While the advantages of conducting passive reconnaissance are plentiful, this information can be somewhat limited depending on the context. IT-based targets often have a plethora of public-facing information available for attackers to use through tools such as email harvesters, domain lookup, search engine dorking and more. The MITRE ATT&CK framework details several TTPs associated with conducting passive reconnaissance. This includes the use of searching through closed sources (T1597), such as searching through or purchasing private data, including technical data from threat intelligence vendors and other private sources; and searching through open sources such as technical databases (T1596), open websites and domains (T1593), and victim-owned websites (T1594).

While it is also possible to use these methods to conduct passive reconnaissance on OT-based networks, these often mean that much of the information that is of value to an attacker is hidden from the public domain. In recent years, many ICS networks have started integrating IoT to improve automation, data collection and more. Despite the benefits this provides, this has also significantly increased the potential attack surface for these by, in several cases, making these networks public-facing. For example, a simple search using the Shodan search engine shows that over 61 000 public-facing devices are running with port 502 open, which commonly uses the Modbus TCP/IP protocol [46]. Figure 2 illustrates the results of using Shodan to search for devices with port 502 open. If operators do not correctly setup their Modbus TCP/IP connections, this can be exploited by attackers with relative ease due to the large number of vulnerabilities that exist within the default version of Modbus TCP/IP, including the use of clear text, the lack of integrity checks, and the lack of authentication [5].

Overall, while the amount of actionable intelligence gained from performing passive reconnaissance can vary from organisation to organisation, the primary objective is to gain information while preventing detection. As such, engagements that include the participation of a red team can benefit greatly from this. However, publicly available information on industrial networks, such as those within critical infrastructures, is often and should be relatively limited compared to what could be gained from an IT-based organisation. These findings are summarised in Table 8.

4.2.2 Active Reconnaissance. As opposed to passive reconnaissance, active reconnaissance is used to obtain information on a target system through direct interaction. The most common way of conducting this type of reconnaissance is through port and vulnerability scanning (T1595) using manual tools such as Nmap or automated scanners such as Nessus [45, 84]. While such tools can help attackers and red teams obtain valuable information for discovering vulnerabilities and weaknesses within target systems, misusing them can lead to an extremely high risk of detection. This includes, for port scanners, using TCP connect scans, aggressive scan timings, and aggressive scripts, which are all often detected by IDSs and IPSs. It is, however, possible to configure scans to minimise detection risk using techniques such as packet fragmentation, decoy scanning, source IP address



TOTAL RESULTS

61,203

TOP COUNTRIES

United States	10,224
Korea, Republic of	3,578
Germany	3,348
France	3,193
Israel	2,894

More...

Fig. 2. Shodan "port:502" search results

	Information Technology	Operational Technology
Detectability	Low	Low
Disruptability	Low	Low
Potential Gathered Information	High	Low
Ease of Information Gathering	High	Low-to-High

Table 8. Passive Reconnaissance Summary

spoofing, source port spoofing, and lowering scan timing. A difference between IT and OT systems is the risk that active reconnaissance can have on OT systems, especially if they are legacy devices. Due to how these systems are programmed, as discussed in Section 3, any form of unrecognised or heavy network traffic could cause software crashes, resulting in significant operational impact; as demonstrated when a ping sweep on an active ICS network to identify all hosts caused a fabrication plant to hang, destroying $50 000 worth of equipment [15]. As such, additional care must be taken when performing active scanning on OT systems, such as reducing scanning speed to minimise network traffic, performing the correct scan type for the target system (i.e. avoiding UDP scans on devices using TCP ports), and manually selecting scripts to run. Many standards and guidelines, such as the IEC 62443 series, recommend including subject specialists such as OT engineers when performing any cyber security activity, including adversary-centric security testing [31, 33]. In recent years, custom scanners, like PLCSCAN and SIMATICSCAN, have been designed to facilitate performing active reconnaissance on devices such as PLCs [3, 23]. While these allow for better and easier scanning of specific ICS types such as Simatic PLCs, these solutions are not comprehensive. Because of this, teams conducting reconnaissance will often resort to primarily using passive reconnaissance or more generalised tools like the ones discussed here.

Another form of active reconnaissance is using social engineering (T1598) to obtain information such as credentials or private information on networks or systems. Similar to active scanning, properly conducting social engineering is crucial for evading detection. Any indication that a third-party message, such as an email, is being used as social engineering can be detected by both automated methods and potential victims. Messages need to, therefore, be carefully crafted to avoid such detection, often done using social-engineering tools such as the TrustedSec Social-Engineer Toolkit [40].

Overall, while active reconnaissance can obtain a large amount of actionable information in little time, if not used properly, it can easily be detected and, in some cases, even cause accidental operational impact to systems. To prevent this, time needs to be taken to fully understand the tools being used, and a near-comprehensive understanding of the targeted devices is required, making black-box testing considerably more difficult, albeit not impossible. These findings are summarised in Table 9.

	Information Technology	**Operational Technology**
Detectability	High	High
Disruptability	Low	High
Potential Gathered Information	High	High
Ease of Information Gathering	High	Low

Table 9. Active Reconnaissance Summary

4.3 Weaponisation

Once enough actionable information has been acquired from reconnaissance, the weaponisation of a payload to exploit the target system can begin. While it is entirely possible to craft a payload manually, attackers often make use of automated tools such as the Metasploit framework [68] or vulnerability databases such as NIST NVD [63] or MITRE CVE [53] to then obtain Proof of Concept code to modify. During this stage, attackers will often combine a Remote Access Trojan (RAT) for Command & Control post-exploitation and the malicious code used to exploit vulnerabilities discovered during reconnaissance into a deliverable such as client data application files (PDF, Word, etc.).

The weaponisation of a payload often depends on the attacker's primary goal, which is often associated with the desired impact of the attack. Both the MITRE ATT&CK and ICS ATT&CK Frameworks categorise four main impact types of cyber-attacks: Denial, Sabotage, Collection, and Control. For adversary-centric security testing, distinguishing how different exploits can impact systems is essential for calculating risk and identifying relevant mitigation strategies.

Denial is often the most common type of attack impact due to its ease of execution. These attacks aim to deny the target of either view, access, or control to their own environment. Such attacks that cause denial include Denial of Service (DoS) attacks (T1499, T1498), encryption attacks (T1486), account access removal (T1531), service stops (T1489) and system shutdowns (T1529). While these attacks cause operational downtime, they often only have a short-term impact on IT systems since, in most cases, there is no destruction of data or hardware. However, for OT systems, even slight downtime can be detrimental for time-sensitive environments such as power plants.

While a consequence of sabotage can also be denial, the act of sabotage involves the deliberate destruction or obstruction of regular operation. Such attacks that cause sabotage include the destruction of data (T1485) through wiping disks (T1561), for example; corrupting firmware (T1495); damage to property (T0879); and, in extreme cases, a loss of protection or safety (T0837, T0880). Similar to denial, the consequences of attacks causing sabotage are vastly different between IT and OT systems. Sabotage attacks can have severe economic and social consequences for IT systems if proper recovery steps are not implemented. For example, the corruption of a database containing customer data could lead to a complete halt in operations, leading to potential severe economic loss and the potential loss of existing customers due to dissatisfaction or distrust. While sabotage attacks on OT systems can also have economic and social consequences on future operations, the potential for loss of protection or safety makes it critical to effectively respond and recover from such attacks, as such consequences could lead to a danger to life.

Any attack involving collection corresponds to actions where information or data is extracted from the target system. The goal of such an attack can include further reconnaissance (see section 4.2), the theft of data to sell on black markets or use for blackmail. The ATT&CK Framework categories 17 different collection techniques, including capture-based techniques such as screen (T1113), video (T1125), audio (T1123), clipboard (T1115), and input capture (T1056); direct data extraction techniques from various sources such as cloud storage (T1530), configuration repositories (T1602), information repositories (T1213), local systems (T1005), network shared drives (T1039), removable media (T1025), and mail servers (T1114). While collection attacks do not have a direct operational impact on either IT or OT systems, it leaves the target organisation open to further action from adversaries. These can be especially devastating for national critical infrastructures when they are the victim of industrial espionage from other nation-states, for example.

In most cases, control attacks are considered the most dangerous attack types to affect target systems for both IT and OT. For these attacks, adversaries gain remote code execution (RCE) on their target. While crafting the payload to gain RCE on a target is done during the weaponisation phase, Command & Control is detailed in a separate phase of the CKC and is therefore discussed more in-depth in section 4.6.

Table 10 summarises the different impact types and their consequences on IT and OT, respectively.

	Information Technology	**Operational Technology**
Denial	Loss of Availability/Revenue	Loss of Availability/Control/Safety
Sabotage	Loss of Revenue/Data	Loss of Data/Safety
Collection	Theft of Data	Theft of Operational Information
Control	Manipulation of Control	Manipulation of Control/Loss of Safety

Table 10. Impact differences between IT and OT systems

4.4 Delivery

Once a suitable payload has been created for exploiting the target system, it needs to be delivered to the victim so that it can be executed. Two main techniques exist for doing this: adversary-controlled delivery and adversary-released delivery.

Delivery of a payload classified as adversary-controlled corresponds to a payload that executes through direct execution of an adversary. This is often done when remote access to the target is possible through open ports. For example, adversaries may access a system by exploiting public-facing applications (T1190) such as websites, databases, and standard services. Physical delivery of payloads is also possible using replication through removable media (T1091), such as by taking advantage of the autorun feature of most devices when inserting a USB drive. While this method may seem less viable due to strict physical security measures implemented within critical infrastructures such as power facilities, it is still possible through a trusted user, for example, as demonstrated in the Stuxnet attack of 2010 [62].

When attackers cannot directly access the target system, they may resort to delivering their payload through adversary-released means. When using this technique, adversaries often use social engineering to trick unsuspecting users into executing a payload. This can either be done through drive-by-compromise (T1189) by compromising a website that a user visits throughout normal browsing, for example; through direct phishing tactics (T1566) such as providing malicious links or attachments in emails or messages; or even through supply chain compromise (T1195) by inserting malicious code into tools used by the target organisation. Supply change compromise, in particular, has gained much attention recently due to the 2020 global supply chain cyber attack, which affected around 18,000 different organisations using software distributed by SolarWinds, including the United States National Nuclear Security Administration [13, 39, 93]. Such an attack demonstrates that even though the initial attack targeted IT systems, a wide variety of critical infrastructures, with some being comprised of OT, were affected.

Despite both IT and OT environments being vastly different in function and architecture, the techniques used to deliver malicious payloads for execution are often similar, as demonstrated by the listed techniques under "Initial Access" in both the MITRE ATT&CK and ATT&CK ICS frameworks. Some techniques do differ for OT-specific systems such as Data Historian Compromise (T0810) in the case of the ICS framework; however, general techniques such as the ones discussed here (drive-by-compromise, phishing, etc.) and summarised in Table 11 apply to both IT and OT environments and often require little to no modification in terms of methodology.

Technique	**ATT&CK Technique**
Adversary-Controlled Delivery	Public-Facing Applications (T1190), Replication through Removable Media (T1091)
Adversary-Released Delivery	Drive-by-Compromise (T1189), Phishing (T1566), Supply Chain Compromise (T1195)

Table 11. Summary of Delivery Techniques

4.5 Exploitation

Once the malicious payload has been successfully delivered onto the target network or system, execution of the code to exploit the target can begin. This phase of the CKC uses the weaponised payload discussed in Section 4.3. While the weaponisation stage of the CKC is difficult to detect and mitigate due to the activities during that stage being entirely separate from the target systems, if a malicious actor has reached the exploitation stage of the CKC, this should be reported as an incident, and appropriate response and recovery actions need to be taken, including during a red team engagement.

While, ultimately, the goal of conducting response and recovery is to return to a state of normal operation, different methods to achieve this outcome are required depending on the environment. For IT systems, the conservation of the CIA Triad is considered a high priority when responding to a cyber incident [19]. Confidentiality is vital for IT-based organisations to recover, as the unauthorised sharing of private data can have severe economic consequences and damage public relations. Violating the General Data Protection Regulation (GDPR), for example, can bring about severe fines of up to 20 million euro or 4% of worldwide turnover for the preceding financial year regardless of cause, including data breaches caused by cyber attacks [85]. This was the case for British Airways, which had to pay a fine of 20 million pounds sterling in 2020 due to a data breach in 2018 where malicious actors obtained private information such as log-in details, payment card information, and customer addresses [86].

Integrity also plays an important part when responding to IT cyber incidents, as data tampering is likely during such an event. Recent findings have reported that cyber attacks with the sole intention of manipulating data have increased significantly since 2020, leading to the spread of disinformation [79]. Compromising data integrity can also serve as a method of detection and defence evasion through techniques such as manipulating indicators (T1070) which can prevent defenders from properly using event collection and reporting. Similarly, data is often rendered useless without availability as it cannot be shared with intended users. Attacks that cause denial or sabotage, as discussed in Section 4.3, can affect the availability of systems.

While the CIA triad is considered a staple model for developing IT security policies and, consequently, something that should be tested thoroughly when conducting adversary-based tests, this is not always the case for OT-based systems. Due to the time-critical nature of these environments, availability is allocated considerably more priority than confidentiality and integrity (however, availability can be dependent on integrity). Furthermore, due to the operational nature of these environments, safety considerations also play a critical part when testing for security resilience. For example, during an attack on a German steel mill in 2014, adversaries gained access to a blast furnace control mechanism, preventing it from shutting down and causing significant damage to the machine itself and the surrounding environment [8, 44]. While there were no human casualties, a loss of safety was observed. Therefore, these differences, summarised in Table 12, need to be considered when conducting an adversary-centric security test to identify appropriate risk mitigation techniques. This table provides relative priority for each category of the CIA triad. This signifies that, for IT, while Availability could be considered a high priority for specific applications such as streaming services, the financial impact of having confidentiality compromised is still considered higher than if availability were to be compromised. Therefore, in general, confidentiality is allocated higher priority than availability within IT environments. This same reasoning is applied for the prioritisation of the CIA triad within OT environments.

CIA Triad Category	Priority for IT	Priority for OT
Confidentiality	High	Low (Medium/High for manufacturing processes that include corporate secrets such as chemical recipes)
Integrity	Medium	High (Due to effect of Integrity on Availability)
Availability	Low	High (Due to potential in reduction in Safety)

Table 12. CIA Triad Prioritisation Summary

4.6 Installation, Command and Control, and Actions on Objectives

Once a discovered vulnerability has been exploited, an adversary, depending on their goal, will then seek to install further capabilities such as persistent remote access or an escalation of privileges. This will often involve revisiting previous steps, such as reconnaissance, to obtain further information on how this can be done. A phenomenon often observed with attacks targeting ICS includes malicious actors gaining access to the industrial zone by pivoting from the enterprise zone. While this phase of the CKC is often not required for traditional penetration testing, demonstrating further capabilities provides additional depth for advanced security testing such as red team engagements.

To this day, achieving RCE on ICS has only been observed in highly advanced attacks [49]. For this reason, minimal detail is given on the TTPs provided by the MITRE ICS ATT&CK Framework. The framework details three techniques for this which are Commonly Used Ports (T0885), Connection Proxy (T0884), and Standard Application Layer Protocol (T0869). In contrast, the enterprise framework details 16 different categories of TTPs used in Command and Control activities, illustrating that knowledge of Command and Control in ICS is still relatively limited to this day. Recent research on Process Comprehension at a Distance has demonstrated the possibility of RCE by leveraging unused memory within PLCs, effectively creating a covert Command and Control channel for realising further actions on objectives [25]. However, more traditional methods for remotely controlling OT exist due to legacy design decisions in PLCs. For example, as discussed in Section 3, simply gaining network access could lead to RCE by leveraging the poor use of access control within standard industrial protocols and directly interfacing with PLCs.

4.7 Stage 2: Development and Execution (ICS only)

Due to the high confidence required for conducting precise cyber attacks and thorough adversary-centric security tests on ICS, the ICS CKC contains an additional stage to the traditional CKC. During this stage, attackers use the knowledge they gained from the previous stage to develop and test their capabilities so that a high-confidence attack on ICS can be carried out. If an impact is observed during the first stage of the ICS CKC, this is unintended and often caused by equipment failing due to its sensitivity. During this phase, several TTPs can be used to further increase the impact and precision of an attack by inhibiting response functions or impairing process control. For example, attackers may block or spoof reporting messages (T0804 & T0856) to delay response and recovery actions. Because of the precise requirements for this stage, the overall timeline for developing an attack of this capability is often greatly extended compared to low-confidence or imprecise attacks. This development time requirement can be directly translated to the time required for conducting an adversary-centric security test, often being a red team engagement at this stage based on scoping constraints such as cost and time.

4.8 Security Testing Software and Tools

As demonstrated from previous subsections, the differences between IT and OT fundamentally affect how adversary-centric security tests are performed within these environments. Because of this, the tools and techniques employed throughout the different phases of the security testing life-cycle also need to be considered. For example, during reconnaissance (discussed in section 4.2) blind scanning in an IT environment may be used for discovering running services on devices, but doing so within an industrial environment could lead to disruption due to unknown protocol compatibility issues. Because of this, specialised tools for security testing within OT environments have been developed. For example, the ControlThings Platform is a specialised penetration testing distribution for ICS [74]; similarly, Kali Linux is a penetration testing distribution for traditional IT [75].

Due to the often proprietary nature of software and protocols used within OT environments, security testing tools for OT are designed for the testing of specific protocols or products. For example, PLCScan is a tool developed by Dmitry Efanov for retrieving information on PLCs that use Modbus or S7comm [23]. Similarly, SIMATICScan, developed by Antrobus et al., can only scan Siemens-based PLCs but offers more depth of testing by also being able to scan for known vulnerabilities and perform fuzzing to discover unknown vulnerabilities [3]. To contrast the differences in functionality of specialised tools for ICS security testing, Samanis et al. developed a taxonomy for categorising ICS Asset Discovery Tools [70]. This covers security testing tools for asset discovery only, and the significant disparity in functionality and practicality between these tools demonstrates the challenges in the development and useability of software used for security testing within ICS environments.

Overall, the most noticeable difference between IT and OT security testing tools/software is that those developed for enterprise security testing often offer extensive functionality for specific tasks, whereas OT-specific tools also need to consider the compatibility of non-standard software or protocols, which often limits their applicability. To summarise, Table 13 presents an example list of tools used for security testing in IT and OT environments and comments on the challenges involved.

Functionality	IT Tools	OT Tools	Comments
Security Testing OSs	Kali Linux, ParrotOS	ControlThings	While traditional security testing distributions can be used for OT environments, a thorough understanding of the effect of tools available from these is required to prevent disruption
Port Scanning	Nmap, Netcat, Zenmap	Nmap, Netcat, Zenmap	Port scanning often unsuitable for OT environments due to potential compatibility issues
Passive Network Enumeration	Wireshark, TCPDump	Wireshark, TCPDump, NSA GRASSMARLIN	While less precise as active scanning, passive enumeration is preferred for OT due to low risk of disruption
Vulnerability Scanning	Nessus, OpenVAS	PLCScan, SIMATICScan	OT vulnerability scanners are often very limited in what devices they can be used on
Exploitation Frameworks	Metasploit, CORE IMPACT, Immunity CANVAS	Industrial Exploitation Framework, ICSSPLOIT	Custom exploitation in OT environments often favoured to increase precision and stealthiness of attack
C2 Frameworks	Empire, Covenant	Custom Capabilities	C2 still in infancy for OT but is possible as shown by recent research [25]
Adversary Emulation Frameworks	Cobalt Strike, CALDERA	OT CALDERA	Adversary Emulation Frameworks for OT still in development and not open source due security concerns

Table 13. Example Software/Tools used for Security Testing IT and OT

5 EXPERIMENTS

5.1 Methodology

Throughout Sections 3 and 4, the observed differences between IT and OT demonstrated that these need to be carefully considered prior to conducting any active form of adversary-centric security test within industrial networks. To evaluate these findings, we have conducted several experiments on our ICS testbed, for which its design and development closely aligns with the model proposed by Green, et al. [24, 26]. As such, the testbed has been built using physical, real-world hardware and software produced by major ICS vendors, including Siemens, Schneider, Allen Bradley, and ABB, and is actively being used to support the development and evaluation of industry-driven tools. This, therefore, affords us a high degree of realism for experimentation.

To identify to what extent active penetration testing techniques affect OT operations, several tools with varying degrees of risk in terms of affecting availability were selected. While these techniques may not necessarily be used for all types of adversary-centric security tests, they were selected based on their potential to disrupt operational processes within an industrial network by affecting network traffic or endpoint resource usage. The techniques used in our experiment are as follows:

- Default Ping Sweep: control test.
- Ping Flood: medium network traffic test.
- Hping3 Flood: heavy network traffic test.
- Malformed Packet Ping: abnormally large packet size test.
- Low-Risk Nmap Scan: TCP connect scan with 1 second delay between probes on top 1000 ports.
- Medium-Risk Nmap Scan: connect scan on all TCP ports, default speed and no probe parallelisation.
- High-Risk Nmap Scan: scan on all TCP/UDP ports, fastest speed, OS detection, version detection, script scanning, and traceroute.
- Nessus Scan: commonly used vulnerability scanner test.

All of the selected techniques are primarily used during the reconnaissance phase of an adversary-centric security test. Although techniques used during subsequent phases of the CKC, such as exploitation, can also adversely affect the operational process, the tools used for this depend greatly on identified vulnerabilities that can be unique to each device. Therefore, using reconnaissance techniques and their subsequent tools provides consistency when testing on distinct targets.

Four devices were selected for experimentation to identify how these techniques' usage could affect operational processes within an industrial environment. Firstly, to test legacy OT, we selected a Siemens SIMATIC ET-200S, which is, to this day, still commonly used in industry [77]. These PLCs started production in 1994 and are currently in product phase-out as of the 1st of October 2020, with a total phase-out planned for 2023. Next, to test more recent PLC lines, the Siemens SIMATIC S7-1200 was selected. Initially released for delivery in 2009, the S7-1200 currently has no announced phase-out date and has improved system properties over the older S7-300 and 400 series PLCs to meet the requirements of modern OT environments. To understand the effect of the selected tools on different PLC brands, we also selected an Allen-Bradley Logix5561 for the experiment. Finally, to demonstrate how these techniques could affect OT devices compared to IT devices, we also tested the tools and techniques on an IT workstation used to modify and upload code to the PLCs within our testbed.

Due to the significant differences in uses between the selected OT and IT devices, their technical specifications conform to the requirements of their end-users and are therefore described in vastly different terms. For example, the product details of the selected PLCs focus more on environmental resilience, such as interference immunity, maximum air pressure operation, relative humidity operation etc., as opposed to the traditional and more IT-focused description of the capabilities of a device's components such as power usage, CPU clock rate, RAM clock speed etc. To this end, limited information can be inferred when directly comparing hardware specifications between IT and OT. This is shown in Table 14, which provides technical specifications for each of the selected devices used in the experiment based on data sheets provided by their respective vendors and internal system information. Not only is the terminology between IT and OT vastly different, but cross-OT vendor terminology also presents significant challenges for conducting a direct comparison. For example, while the work memory in SIMATIC PLCs can be defined as equivalent to RAM for an IT Workstation, the CPU details of each of the selected devices make it difficult to make a quantitative comparison between their respective speed and efficiency; further amplifying the IT/OT gap demonstrated in Sections 3 and 4.

	ET200S	**S7-1200**	**AB Logix5561**	**IT Workstation**
Power/Current Draw	320mA @ 24V DC	1.2A @ 24V DC	14mA @ 24V DC	290W
Memory	128KB (work) + optional load	50KB (work) + 1MB (load)	478KB (I/O) + 2MB (user)	16.0GB (RAM)
CPU Speed	3μs/instruction (float)	2.5μs/instruction (float)	100 programs/task (32 concurrent max)	1 core @ 3.30GHz
OS/Firmware	IM151-8 PN/DP V2.7.1	1212C V3.0.2	1756-L61S V10.007	Windows 7 Enterprise V6.1.7601

Table 14. Device Hardware Specifications

To evaluate how these techniques could adversely affect availability, two metrics were selected, each split into sub-metrics:

- Network Delay:
  - Maximum Round-Trip Time - the maximum possible effect on availability.
  - Average Round-Trip Time - the average effect on availability.
  - Packet Loss - the amount of total availability loss.
- CPU Resource Usage:
  - Maximum CPU Job Execution Time or Usage - the maximum load increase on the CPU.
  - Average CPU Job Execution Time or Usage - the average load increase on the CPU.
  - CPU Response - the response rate of the CPU.

A default ping scan was conducted in parallel with running the selected tools to collect data on network delay. For collecting data on the CPU usage of each tested endpoint, custom python (for the PLCs) and Powershell (for the IT workstation) scripts leveraging the protocols used by these (S7comm, HTTP, Ethernet/IP) were utilised.

5.2 Results

	Max RTT	**Avg RTT**	**Packet Loss**	**Max CPU Time**	**Avg CPU Time**	**CPU Response**
Default Ping	13.203ms	5.133ms	0%	27ms	18.13ms	100%
Ping Flood	20.382ms	8.898ms	0%	38ms	25.41ms	100%
Hping3 Flood	1397.1ms	424.140ms	82.6087%	N/A	N/A	0%
Malformed Ping	7.444ms	4.629ms	0%	28ms	19.38ms	100%
Low-Risk nmap	11.276ms	4.331ms	0%	32ms	19.12ms	100%
Medium-Risk nmap	11.617ms	4.345ms	0%	49ms	27.74ms	100%
High-Risk nmap	227.995ms	33.658ms	CRASH	813ms	90.83ms	CRASH
Nessus Scan	283.754	49.950ms	CRASH	919ms	46.94ms	CRASH

Table 15. SIMATIC ET-200S Experiment Results

The results from running the selected tools on the four targets can be found in tables 15, 16, 17 and 18. During the entirety of the test, the ET-200S' availability was greatly affected by the more aggressive tools such as the hping3 flood, the high-risk Nmap scan, and the Nessus scan; resulting in a near-total loss of availability through resource overload in the case of the hping3 test or full system crashes for both the high-risk Nmap scan and the Nessus scan. All three of these techniques generated significant network traffic, resulting in the PLC being unable to reply to these on time. During the Nmap and Nessus scan, vulnerability and network enumeration scripts were performed, resulting in the PLC crashing due to its inability to handle these correctly. While the ping flood did not result in a total loss of availability, it caused significant network delay and an increase in CPU response time. Based on an organisation's requirements for availability, including system dependencies, this can cause adverse consequences on the overall network. For example, in a time-sensitive environment such as

	Max RTT	**Avg RTT**	**Packet Loss**	**Max CPU Time**	**Avg CPU Time**	**CPU Response**
Default Ping	2.018ms	0.958ms	0%	13ms	11.04ms	100%
Ping Flood	1.586ms	0.680ms	0%	22ms	19.36ms	100%
Hping3 Flood	1.463ms	1.088ms	95.45%	14ms	12.67	26.32%
Malformed Ping	2.216ms	0.933ms	0%	14ms	11.32ms	100%
Low-Risk nmap	2.312ms	1.056ms	0%	14ms	11.13ms	100%
Medium-Risk nmap	2.052ms	0.643ms	0%	14ms	10.98ms	100%
High-Risk nmap	2.326ms	0.846ms	0%	20ms	11.68ms	98.86%
Nessus Scan	2.649ms	0.766ms	0%	28ms	12.15ms	100%

Table 16. SIMATIC S7-1200 Experiment Results

	Max RTT	**Avg RTT**	**Packet Loss**	**Max CPU Load**	**Avg CPU Load**	**CPU Response**
Default Ping	1.790ms	0.750ms	0%	1.1%	0.81%	100%
Ping Flood	0.558ms	0.381ms	93.18%	1.8%	1.55%	100%
Hping3 Flood	823.89ms	813.78ms	98.53%	N/A	N/A	0%
Malformed Ping	1.797ms	0.786ms	0%	1.1%	0.81%	100%
Low-Risk nmap	1.792ms	0.714ms	0%	1.2%	0.92%	100%
Medium-Risk nmap	0.688ms	0.440ms	0%	7.9%	5.65%	100%
High-Risk nmap	1.798ms	0.653ms	0%	12.7%	3.25%	100%
Nessus Scan	0.676ms	0.418ms	0%	31.1%	1.11%	100%

Table 17. Allen-Bradley Logix5561 Experiment Results

	Max RTT	**Avg RTT**	**Packet Loss**	**Avg CPU Load**	**CPU Response**
Default Ping	1.212ms	0.735ms	0%	18.8%	100%
Ping Flood	0.809ms	0.501ms	0%	24.85%	100%
Hping3 Flood	5.442ms	2.585ms	8.08%	40%	100%
Malformed Ping	1.172ms	0.747ms	0%	18.68%	100%
Low-Risk nmap	1.189ms	0.715ms	0%	18.71%	100%
Medium-Risk nmap	1.573ms	0.707ms	0%	14.38%	100%
High-Risk nmap	1.226ms	0.664ms	0%	14.78%	100%
Nessus Scan	3.658ms	0.684ms	0%	14.23%	100%

Table 18. Windows 7 Workstation Experiment Results

the safety systems within a nuclear power plant, this decrease in availability would be undesirable. However, in less time-critical environments, tools with similar throughput may be acceptable for use. While no increase in network latency was observed for the medium-risk Nmap scan, the CPU response time did increase by 50%, which, similar to the high-risk Nmap scan, could be undesirable depending on the environment. No significant increase in network delay nor CPU response time was observed for the remaining tests.

Due to the more-recent hardware and firmware in the S7-1200, less impact on its availability was observed during the experiment than on the ET-200S. A significant decrease in availability was observed when performing an hping3 flood. However, a negligible decrease or no change in availability was observed for the seven other tests, including the Nessus and the high-risk Nmap tests. While these two tests did not increase network latency, an increase from 13ms to 20ms and 28ms respectively in CPU response time was observed, which may be undesirable for specific environments. This demonstrates that, apart from the most aggressive techniques, most tools generally present less risk to the availability of the S7-1200 than the ET-200S.

Despite the Logix5561 having more hardware resources than the S7-1200 and the ET-200S, it performed considerably worse than these when running heavy network generating tools such as ping and hping3. Both the ping flood and the hping3 flood saw a near-total loss of availability as opposed to the S7-1200 and ET-200S, which only saw a considerable loss of availability when running the hping3 flood. Despite this, the six other tests, including the high-risk Nmap scan and the Nessus scan, resulted in a negligible increase in network delay. However, these two tests, in particular, did produce a noticeable increase in CPU usage (12.7% and 31.1%, respectively) for the Logix5561.

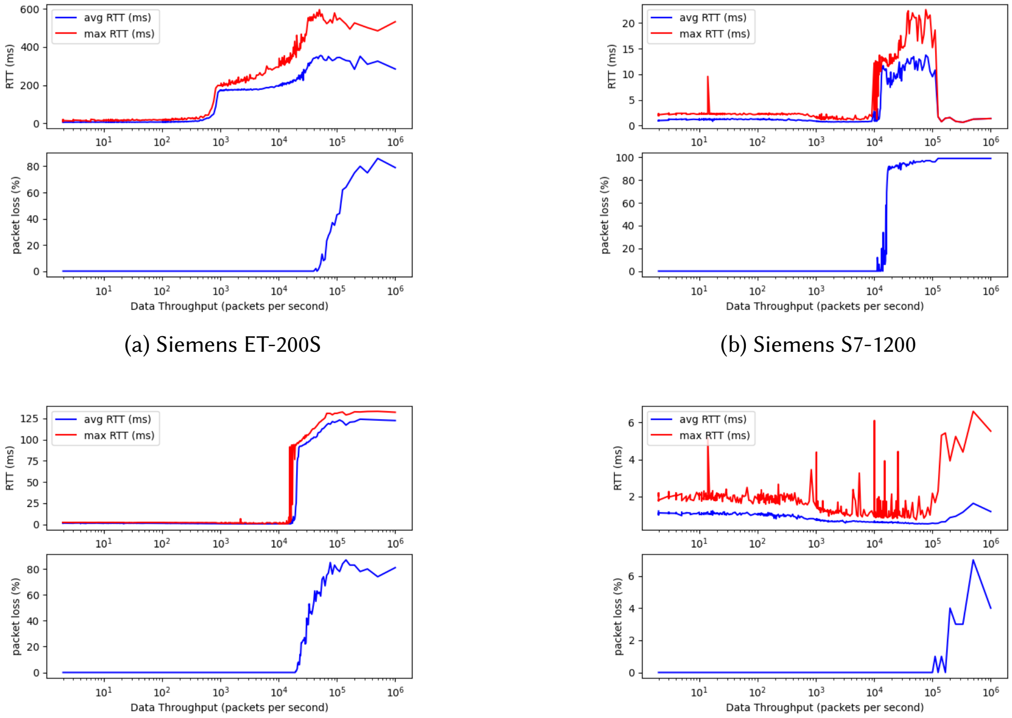
Findings from running the tools on the IT workstation show that it is generally more resilient than the tested PLCs. Only the hping3 flood resulted in a slight decrease in availability, although no total loss was observed. However, this is expected as an hping3 flood can generate over 170,000 packets per second, affecting even the most resilient systems without proper DoS mitigation techniques. All seven other tests had a negligible effect on the workstation.

5.3 Discussion

Overall, the results from the experiment demonstrate that adversary-centric security testing techniques generally affect the availability of OT equipment more than IT. However, the extent to which these techniques affect OT is less than described by the findings from theory, discussed in sections 3, and 4. This, therefore, signifies that adversary-centric security testing is indeed possible within OT environments, following proper risk quantification of the effect on availability that techniques used have on the systems under consideration. Furthermore, while legacy OT equipment is more susceptible to having its availability affected by highly aggressive techniques, modern OT equipment generally allows for more flexible usage of testing tools.

Two primary factors were observed that could affect the availability of the tested OT devices. Firstly, the throughput of the data sent by the testing tools to the PLCs directly correlated to how much availability was affected. Despite the S7-1200 having similar hardware resources to the ET-200S in terms of capacity, it was more resilient to most of the selected tools. This is most likely due to both a combination of the hardware speed, which is not fully documented in the case of work memory for Siemens PLCs and optimisations provided by more recent firmware. In contrast, despite the Logix5561 having considerably better hardware than both Siemens PLCs, it performed worse during testing with a Ping Flood.

To further demonstrate the effect of network throughput on availability, a second experiment was conducted to determine the capability of these devices to operate appropriately under different network conditions. For this purpose, a custom script was written; it gradually increases the throughput of data being sent to the target devices to determine the thresholds at which each device could perform before observing both a non-negligible increase in latency and packet loss. The results are illustrated in Figure 3, and clear distinctions can be observed in how these devices handle different network throughputs. More specifically, for the Siemens ET-200S, an increase in latency can be observed at 400 packets per second (i.e. 25.6 KB/s due to each packet having a size of 64 bytes), and a start of packet loss occurs at 4000 packets per second (i.e. 2.56 MB/s). For the Siemens S7-1200, an increase in latency and a start of packet loss can be observed at 1000 packets per second (i.e. 640 KB/s). For the Allen-Bradley Logix5561, an increase in latency can be observed at 1000 packets per second (i.e. 640 KB/s), and a start of packet loss occurs at 1100 packets per second (i.e. 704 KB/s). For the Windows 7 workstation, no noticeable increase in latency is observed, and a slight increase in packet loss (6%) occurs at 100,000 packets per second (i.e. 6.5



(a) Siemens ET-200S

(b) Siemens S7-1200

(c) Allen-Bradley Logix5561

(d) Windows 7 Workstation

Fig. 3. Network Stress Test Results

MB/s). The results further reinforce the findings from the experiment detailed in section 5.2. These demonstrate that legacy OT (i.e. the Siemens ET-200S) is highly susceptible to disruption during security tests that employ aggressive tools and techniques but that modern OT (i.e. the AB logix5561 and Siemens S7-1200), while not as resilient as IT, can be tested with more flexibility.

The second factor that could affect the availability of the tested OT devices was the capability of these devices to process unexpected requests. For example, when vulnerability scripts were used on the ET-200S, it could not process these and resulted in a complete system crash, leading to a total loss of availability and requiring a manual reset. This, therefore, would have a detrimental effect on the environment, causing an adverse impact on the operational process. However, both the S7-1200 and the Logix5561 were able to process these by either handling such requests appropriately or ensuring proper exception handling if an error occurs, allowing for more flexible use of these tools.

Several requirements need to be defined when performing adversary-centric security tests on OT. First, both penetration testing and OT expert knowledge are required to understand precisely how specific tools interact with the system under consideration, as each endpoint will likely react differently to an identical set of tools depending on their hardware and software/firmware. Several factors, therefore, need to be considered concerning this, including determining which protocols the system can process, how errors are handled when encountering unknown requests, etc. The aggressiveness of the tools used during the engagement also needs to be considered to prevent disruption to the operational process, following availability reduction tolerance. An in-depth understanding is therefore required to understand precisely how specific tools could affect target endpoints which can be provided by both automation and safety engineers. From there, risk quantification can be performed to assess the full scope of the engagement while ensuring that the impact on the operational process is tolerable and that the engagement itself is as comprehensive as possible.

6 CONCLUSION AND FUTURE WORK

In this paper, we have extensively analysed the technical differences between Information Technology (IT) and Operational Technology (OT) from a general perspective and specifically within the context of adversary-centric security testing.

From an asset management point of view, the differences between IT and OT can be grouped into four distinct categories: hardware; software; network; and socio-technical differences. Summarised in Table 3, the design of both IT and OT hardware is directly correlated to their function within their environment. Because the goal of using IT is to store, process and exchange information, its hardware is designed to enable this as efficiently as possible, being flexible in processing tasks. In contrast, OT is designed for viewing, monitoring, and controlling operational processes, leading to their hardware design focusing on environmental resilience, high up-time, and cost-efficiency, often limited to processing highly specialised tasks. Similarly, the software of these system types is designed in consideration of their end-users, summarised in Table 4. Because IT is commonly used throughout different domains, its software is flexible and designed to be simple to understand. On the other hand, OT software is explicitly designed to be used by automation engineers, making skill transference difficult between the two domains. Additionally, a focus on safety is prioritised over security due to the critical nature of OT environments; this makes security updates challenging to implement and, therefore, uncommon due to the high up-time requirements of these systems. The critical nature of OT environments also affects the approach to their network architecture and the design of industrial protocols, summarised in Table 6. Because of the time and safety-critical aspects of OT networks, protocols used within them often lack fundamental security implementations, such as access control and encryption, despite being widely adopted in IT systems. These technical differences directly influence the sociological factors behind the implementation of security controls and the culture within IT and OT environments, further demonstrating the gap between IT and OT, as summarised in Table 7.

Considering the technical differences between IT and OT, several challenges were identified when conducting adversary-centric security tests within OT environments. The adversary-centric security testing process can be grouped into phases following the Lockheed Martin and the SANS ICS Cyber Kill Chain. Further analysis showed how the Tactics, Techniques and Procedures used during these phases need to be considered based on what systems or environments are being tested. During the reconnaissance phase, passive techniques, as shown in table 8, were found to have little to no impact on the operational process but provided less actionable intelligence for subsequent phases of the CKC. Despite the high probability of causing operational impact if not used properly, especially within OT environments, active reconnaissance techniques, as in table 9, were found to return significant actionable information allowing for more depth of testing to be made. The weaponisation stage of the CKC was identified as being closely correlated to the impact goals of adversaries, which can differ significantly between IT and OT targets, and are summarised in table 10. Further phases of the CKC found that the TTPs used during these were often similar in execution, albeit modified to suit targeted endpoints.

While commonly used tools for IT-centric engagements may not have any noticeable effect in these environments, it is possible that they can adversely disrupt the operational process within OT environments. This was validated by deploying tools with varying degrees of aggressiveness on industrial control systems. Findings from this exercise identified two factors that could adversely affect the operational process through a reduction or loss in availability. First, the network throughput of active tools was directly correlated to a loss of availability, the rate of which is unique to the system under consideration based on hardware and software capabilities. Second, the use of unexpected techniques such as vulnerability scans and scripts resulted in operational impact depending on the targets' capabilities for processing and handling errors.

Despite current approaches that limit the use of adversary-centric security testing tools to strictly passive ones during assessment engagements, employing active tools is possible subject to the resilience of the systems against more aggressive techniques, as demonstrated in section 5. While existing frameworks for adversary emulation for security testing exist, such as MITRE's Adversary Emulation Plans which provide techniques and tools for emulating specific threat actors [54], these do not take into consideration the safety and operational risks that security testing can present to OT environments. Therefore, future work needs to identify how to comprehensively quantify the risk that active adversary-centric security testing techniques have on ICS/OT and will allow for better scoping of these engagements. This will minimise the risks that these techniques present to safety and the operational process while ensuring the full depth of such an engagement as part of the overall cyber risk assessment life cycle.

REFERENCES

[1] 2010. IEEE Standard for Electric Power Systems Communications – Distributed Network Protocol (DNP3). *IEEE Std 1815-2010* (2010), 1–775. https://doi.org/10.1109/IEEESTD.2010.5518537

[2] AboutSSL. [n.d.]. History of the Internet – An Invention That Changed the World. https://aboutssl.org/history-of-the-internet/. Last Accessed: 30-06-2021.

[3] Rob Antrobus, Sylvain Frey, Benjamin Green, and Awais Rashid. 2016. *SimaticScan: Towards A Specialised Vulnerability Scanner for Industrial Control Systems.* Technical Report.

[4] Michael Assant and Robert Lee. 2015. *The Industrial Control System Cyber Kill Chain.* Technical Report. SANS Institute. Last Accessed: 03-21-2022.

[5] Liron Benbenishti. 2017. SCADA MODBUS Protocol Vulnerabilities. https://bit.ly/3nEeYy6. Last Accessed: 15-09-2021.

[6] Clint Bodungen, Bryan Singer, Aaron Shbeeb, Kyle Wilhoit, and Stephen Hilt. 2016. *Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions.* McGraw Hill Professional.

[7] William Bolton. 2015. *Programmable Logic Controllers* (sixth edition ed.). Elsevier Ltd.

[8] Eric Byres and Mark Fabro. 2014. RISI - The Repository of Industrial Security Incidents. https://www.risidata.com/Database. Last Accessed: 01-11-2021.

[9] Carnegie Mellon University. 2015. Network Security Protocols. https://bit.ly/3qNnxX7.

[10] Sanjay Chhillar. 2021. Common ICS Cybersecurity Myth 1: The Air Gap. https://bit.ly/39JCf9N. Last Accessed: 28-09-2021.

[11] Wm. Arthur Conklin. 2016. IT vs OT Security: A Time to Consider a Change in CIA to Include Resilience. In *2016 49th Hawaii International Conference on System Sciences (HICSS).* 2642–2647. https://doi.org/10.1109/HICSS.2016.331

[12] CPNI. 2021. Critical National Infrastructure. https://bit.ly/3ueRgu6. Last Accessed: 02-15-2022.

[13] Department of Homeland Security. 2020. Emergency Directive 21-01. https://cyber.dhs.gov/ed/21-01/. Last Accessed: 11-10-2021.

[14] Paul Didier, Fernando Macias, James Harstad, Rick Antholine, Scott A. Johnston, Sabina Piyevsky, Dan Zaniewski, Steve Zuponcic, Mark Schillace, and Gregory Wilcox. 2011. Converged Plantwide Ethernet (CPwE) Design and Implementation Guide. *Rockwell Automation* 9 (2011), 564.

[15] David P. Duggan. 2005. *Penetration Testing of Industrial Control Systems.* Technical Report. Last Accessed: 16-09-2021.

[16] EC-Council. 2021. Certified Ethical Hacker Certification. https://bit.ly/3cK7t23. Last Accessed: 24-11-2021.

[17] ENISA. 2018. The NIS Directive. https://bit.ly/3D0Bo27. Last Accessed: 15-06-2021.

[18] Barbara Filkins and Doug Wylie. 2019. SANS 2019 State of OT/ICS Cybersecurity Survey. https://bit.ly/3rP9amY.

[19] Fortinet. n.d.. The CIA Triad. https://bit.ly/3CDsEOK. Last Accessed: 01-11-21.

[20] Claire Gaving. 2014. Seasonal Variations in Electricity Demand. https://bit.ly/3qustQv.

[21] GIAC. 2021. GIAC Penetration Tester (GPEN). https://bit.ly/3G00Rt9. Last Accessed: 24-11-2021.

[22] Fernando Gont. 2008. *Security Assessment of the Internet Protocol.* Technical Report.

[23] Google. N.D. Google Code Archive: plcscan. https://bit.ly/3tMnJHw. Last Accessed: 16-09-2021.

[24] Benjamin Green, Richard Derbyshire, William Knowles, James Boorman, Pierre Ciholas, Daniel Prince, and David Hutchison. 2020. ICS Testbed Tetris: Practical Building Blocks Towards a Cyber Security Resource. In *13th USENIX Workshop on Cyber Security Experimentation and Test (CSET 20).*

[25] Benjamin Green, Richard Derbyshire, Marina Krotofil, William Knowles, Daniel Prince, and Neeraj Suri. 2021. PCaaD: Towards Automated Determination and Exploitation of Industrial Systems. *Computers & Security* 110 (2021), 102424.

[26] Benjamin Green, Anhtuan Lee, Rob Antrobus, Utz Roedig, David Hutchison, and Awais Rashid. 2017. Pains, Gains and PLCs: Ten Lessons from Building an Industrial Control Systems Testbed for Security Research. In *10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17)*.

[27] Benjamin Green, Daniel Prince, Jerry Busby, and David Hutchison. 2017. "How Long is a Piece of String": Defining Key Phases And Observed Challenges within ICS Risk Assessment. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3140241.3140251

[28] guru99. [n.d.]. Real-time operating system (RTOS): Components, Types, Examples. https://www.guru99.com/real-time-operating-system.html. Last Accessed: 28-06-2021.

[29] Mariana Hentea. 2021. *Building an Effective Security Program for Distributed Energy Resources and Systems.* John Wiley & Sons Inc.

[30] Eric Hutchins, Michael Cloppert, and Rohan Amin. [n.d.]. *Intelligence-Driven Computer Network Defense and Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.* Technical Report. Lockheed Martin. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

[31] IEC. 2011. *BS IEC 62443-2-1:2011.* Technical Report.

[32] IEC. 2013. *IEC 61131-3:2013.* Technical Report.

[33] IEC. 2019. *BS EN IEC 62443-4-2:2019.* Technical Report.

[34] International Society of Automation. 2021. ISA Courses. https://www.isa.org/store. Last Accessed: 24-11-2021.

[35] International Society of Automation. 2021. Overview of Penetration Testing for Industrial Control Systems (IC38C). https://bit.ly/2ZhvhqO. Last Accessed: 24-11-2021.

[36] ISO/IEC. 2017. BS EN ISO/IEC 27001:2017.

[37] ISO/IEC. 2017. BS EN ISO/IEC 27002:2017.

[38] ISO/IEC. 2017. BS EN ISO/IEC 27019:2017.

[39] Kevin Jornson and Mike Snider. 2020. Pompeo Says Russia "Pretty Clearly" Behind Cyberattack on US, but Trump Casts Doubts and Downplays Threat. https://bit.ly/2YGFg8k. Last Accessed: 11-10-2021.

[40] David Kennedy. 2020. The Social Engineer Toolkit. https://bit.ly/3CsnGDR. Last Accessed: 20-09-2021.

[41] Eric D. Knapp and Joel Thomas Langill. 2015. *Industrial Network Security.* Elsevier Ltd.

[42] William Knowles, Jose M. Such, Antonios Gouglidis, Gaurav Misra, and Awais Rashid. 2015. Assurance Techniques for Industrial Control Systems (ICS). Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/2808705.2808710

[43] Ralph Langner. 2011. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy* 9, 3 (2011), 49–51.

[44] Robert M Lee, Michael J Assante, and Tim Conway. 2014. German Steel Mill Cyber Attack. *Industrial Control Systems* 30 (2014), 62.

[45] Gordon Lyon. 1997. Nmap: the Network Mapper. https://nmap.org/. Last Accessed: 15-09-2021.

[46] John Matherly. 2009. Shodan Search Engine. https://www.shodan.io/. Last Accessed: 15-09-2021.

[47] Microsoft. [n.d.]. Windows Comprehensive Security. https://bit.ly/3qnouGx. Last Accessed: 26-06-2021.

[48] Microsoft. [n.d.]. Windows Server. https://bit.ly/3CXOspc. Last Accessed: 26-06-2021.

[49] Thomas Miller, Alexander Staves, Sam Maesschalck, Miriam Sturdee, and Benjamin Green. 2021. Looking Back to Look Forward: Lessons learnt from Cyber-Attacks on Industrial Control Systems. *International Journal of Critical Infrastructure Protection* 35 (2021), 100464. https://doi.org/10.1016/j.ijcip.2021.100464

[50] Gyorgy Miru. 2017. Siemens S7 Communication - Part 1 General Structure. http://gmiru.com/article/s7comm/. Last Accessed: 08-07-2021.

[51] MITRE. 2020. ATT&CK for Industrial Control Systems. https://collaborate.mitre.org/attackics/index.php/Main_Page.

[52] MITRE. 2021. ATT&CK Matrix for Enterprise. https://attack.mitre.org/. Last Accessed: 22-12-2021.

[53] MITRE. 2021. MITRE Common Vulnerability and Exposures. https://cve.mitre.org/. Last Accessed: 21-09-2021.

[54] MITRE. 2022. Adversary Emulation Plans. https://attack.mitre.org/resources/adversary-emulation-plans/ Last Accessed: 24-09-2022.

[55] Mitsubishi Electric. [n.d.]. *MELSEC Communication Protocol Reference Manual.* Technical Report. Last Accessed: 08-07-2021.

[56] Gordon E Moore et al. 1965. Cramming More Components onto Integrated Circuits.

[57] Glenn Murray, Michael N. Johnstone, and Craig Valli. 2017. The Convergence of IT and OT in Critical Infrastructure.

[58] National Cyber Security Centre. 2021. NCSC CAF Guidance. https://www.ncsc.gov.uk/collection/caf. Last Accessed: 15-06-2021.

[59] National Institute of Standards and Technology. 2018. *Framework for Improving Critical Infrastructure Cybersecurity.* Technical Report.

[60] National Institute of Standards and Technology. 2018. *NIST Special Publication 1800-5.* Technical Report.

[61] NCSC. 2019. CHECK - Penetration Testing. https://bit.ly/3xfOIx0.

[62] Falliere Nicolas, Liam Murchu, and Eric Chien. 2010. W32.Stuxnet Dossier Version 1.3. https://bit.ly/3aqefqg. Last Accessed: 14-06-2021.

[63] NIST. 2021. The National Vulnerability Database. https://nvd.nist.gov/. Last Accessed: 21-09-2021.

[64] ODVA. [n.d.]. *ODVA Specifications.* Technical Report. Last Accessed: 08-07-2021.

[65] Offensive Security. 2021. Courses and Certifications. https://www.offensive-security.com/courses-and-certifications/ Last Accessed: 14-06-2021.

[66] PenTestPartners. [n.d.]. Introduction to PLCs and Ladder Logic. https://bit.ly/3hoxXIv. Last Accessed: 26-06-2021.

[67] PenTestPartners. [n.d.]. Snakes and Ladder Logic. https://bit.ly/2U3sz5x. Last Accessed: 26-06-2021.

[68] Rapid7. 2003. The Metasploit Framework. https://bit.ly/3AFSVdW. Last Accessed: 21-09-2021.

[69] Frances Robles and Nicole Perlroth. 2021. "Dangerous Stuff": Hackers Tried to Poison Water Supply of Florida Town. https://nyti.ms/38PzNye. Last Accessed: 15-06-2021.

[70] Emmanouil Samanis, Joseph Gardiner, and Awais Rashid. 2022. A Taxonomy for Contrasting Industrial Control Systems Asset Discovery Tools. https://doi.org/10.48550/ARXIV.2202.01604

[71] Alex Samonte. [n.d.]. Network Security Reference Architecture. https://bit.ly/3Ahn5o7. Last Accessed: 30-06-2021.

[72] SANS Institute. 2021. Assessing and Exploiting Control Systems. https://bit.ly/3oVGhTM. Last Accessed: 24-11-2021.

[73] SANS Institute. 2021. Cybersecurity Courses & Certifications. https://bit.ly/3nLLZYQ. Last Accessed: 24-11-2021.

[74] Justine Searle. 2021. Control Things I/O. https://www.controlthings.io/home. Last Accessed: 27-06-2022.

[75] Offensive Security. 2022. Kali Linux. https://www.kali.org/. Last Accessed: 25-09-2022.

[76] Chris Sherry. 2020. Advantages and Disadvantages of Active vs. Passive Scanning in IT and OT Environments. https://bit.ly/3trOgLy Last Accessed: 14-06-2021.

[77] Siemens. 2020. SIMATIC S7-300 - Proven Multiple Times! https://sie.ag/3ol428k

[78] Siemens. 2022. SIMATIC S7-1200 CPU 1212C - Data Sheet. https://sie.ag/3MSWnIX. Last Accessed: 16-03-2022.

[79] Sebastian Klovig Skelton. 2021. Destruction and Integrity Cyber Attacks on the Rise. https://bit.ly/3ByOrWn. Last Accessed: 01-11-21.

[80] William Smart. 2018. Lessons Learned Review of the WannaCry Ransomware Cyber Attack. https://bit.ly/2UIg1AL.

[81] Jae-Gu Song, Jung-Woon Lee, Cheol-Kwon Lee, Kee-Choon Kwon, and Dong-Young Lee. 2012. A Cyber Security Risk Assessment for the Design of I&C Systems in Nuclear Power Plants. *Nuclear Engineering and Technology* 44 (12 2012). https://doi.org/10.5516/NET.04.2011.065

[82] Mike Spisak and James Darwin. [n.d.]. Network Security Architecture. https://ibm.co/3hBztHl. Last Accessed: 30-06-2021.

[83] Alexander Staves, Tom Anderson, Harry Balderstone, Benjamin Green, Antonios Gouglidis, and David Hutchison. 2022. A Cyber Incident Response and Recovery Framework to Support Operators of Industrial Control Systems. *International Journal of Critical Infrastructure Protection* (2022). https://doi.org/10.1016/j.ijcip.2021.100505

[84] Tenable. 2021. Nessus Vulnerability Scanner. https://bit.ly/399yave. Last Accessed: 16-09-2021.

[85] The European Parliament and Council. 2016. Regulation (EU) 2016/679. https://bit.ly/3bsAIpB. Last Accessed: 01-11-21.

[86] Joe Tidy. 2020. British Airways Fined 20m Pounds Sterling over Data Breach. https://bbc.in/3pRTejv. Last Accessed: 01-11-21.

[87] Joe Tidy. 2021. Colonial Hack: How Did Cyber-Attackers Shut Off Pipeline? https://bbc.in/3tClpod. Last Accessed: 15-06-2021.

[88] United States Government Accountability Office. 2011. Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use. https://www.gao.gov/assets/gao-12-92.pdf.

[89] U.S Government Publishing Office. 2014. S.1353 - Cybersecurity Enhancement Act of 2014. https://bit.ly/35JFUm3.

[90] Don C. Weber and Just Searle. 2021. Industrial Protocols Cheat Sheet v1.0. https://bit.ly/3IAHPKM. Last Accessed: 08-07-2021.

[91] Jody R. Westby. 2012. Governance of Enterprise Security: CyLab 2021 Report. https://bit.ly/3BdDefs.

[92] Weider D. Yu, Dipti Baheti, and Jeremy Wai. [n.d.]. Real-Time Operating System Security. https://bit.ly/3vZ3m9r.

[93] Christina Zhao. 2020. SolarWinds, Probably Hacked by Russia, Serves White House, Pentagon, NASA. https://bit.ly/3FB5U3H. Last Accessed: 11-10-2021.