A Comparative Study of ICS Honeypot Deployments

Preprint · September 2025

CITATIONS
0

READS
165

7 authors, including:

Frederik Ondrikov
Eindhoven University of Technology
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Denis Donadel
University of Verona
25 PUBLICATIONS **291** CITATIONS
SEE PROFILE

Francesco Lupia
University of Calabria
24 PUBLICATIONS **176** CITATIONS
SEE PROFILE

Massimo Merro
University of Verona
96 PUBLICATIONS **1,823** CITATIONS
SEE PROFILE

A Comparative Study of ICS Honeypot Deployments

Frederik Ondrikov[1], Denis Donadel[2], Francesco Lupia[3], Massimo Merro[2], Daniel dos Santos[4], Emmanuele Zambon[1], and Nicola Zannone[1]

[1] Eindhoven University of Technology
f.ondrikov@student.tue.nl,e.zambon@tue.nl,n.zannone@tue.nl
[2] Università degli Studi di Verona
denis.donadel@univr.it,massimo.merro@univr.it
[3] Università della Calabria
francesco.lupia@unical.it
[4] Forescout Technologies
daniel.dossantos@forescout.com

Abstract. Honeypots are increasingly used in Industrial Control Systems (ICS) to divert attacks from critical assets and study malicious behavior. While prior work has examined specific aspects of ICS honeypot design, a comprehensive understanding of cost-effective deployment strategies is still lacking. This work investigates how interaction level, network type, and geographic location affect the attractiveness of ICS honeypots. We deploy both low- and high-interaction honeypots, alongside a physical device, across corporate and cloud networks in various geographic regions. We collect and analyze network interactions involving HTTP, S7Comm, and Modbus protocols from 16 honeypots with diverse configurations over a three-month period. Our results show that network type has the largest impact on ICS honeypot traffic, while interaction level and geographic location play a minor role. We also find that low-interaction honeypots capture traffic comparable to high-interaction setups, supporting their use for general threat intelligence.

1 Introduction

Industrial Control Systems (ICSs) are physical and engineered systems whose operations are monitored, coordinated, and controlled by interconnected computing and communication components [25]. ICSs include Operational Technology (OT), such as Supervisory Control and Data Acquisition (SCADA), and embedded devices, such as Programmable Logic Controllers (PLCs), which form the backbone of critical infrastructures.

Modern ICSs are increasingly integrating Information Technology (IT) capabilities into legacy OT environments. This integration enhances connectivity and remote access but also creates a more complex and exposed attack surface. ICSs often have long operational lifespans, making them vulnerable to emerging cyber threats. Notable incidents such as the Stuxnet worm targeting Iran's nuclear program [6] and the Industroyer malware used in the Ukraine power grid attack [15] demonstrate the real-world impact of ICS vulnerabilities.

To better understand and mitigate these threats, honeypots are increasingly deployed as decoy systems designed to attract attackers, allowing analysts to observe and analyze malicious behavior. They serve as early warning systems and deception mechanisms that

divert attacks from critical assets [24]. Honeypots vary in complexity based on (among others) their interaction level. Low-interaction honeypots expose limited functionality, require less effort to deploy, and pose minimal risk of system compromise, but are often easily fingerprinted and dismissed by sophisticated attackers or scanners like Shodan [16, 21, 26, 29, 32]. High-interaction honeypots, by contrast, more closely resemble real systems, making them harder to detect and better suited for capturing complex attacker behavior [14]. However, they entail higher operational costs and increased risk of compromise.

Beyond the level of interaction, factors such as deployment environment and geographic location can also influence the effectiveness of a honeypot [3, 5, 35]. While ICSs are traditionally deployed on-premise within corporate networks, cloud-based honeypots are increasingly being considered to avoid exposing real infrastructure. Yet, attackers may regard ICS honeypots in cloud environments as less credible targets, reducing their willingness to engage. On the other hand, Shodan scans show that ICS protocols (e.g., Modbus, S7Comm) are widely used in cloud environments, although attacker behavior toward such protocols in cloud environments is not yet well understood. Similarly, the geographic location of deployments can influence traffic volume and behavior [5, 12, 28]. As ICS devices are unevenly distributed, attacker interest may vary by region, focusing more on areas with a higher concentration of ICS devices, such as North America, Asia, and Europe.

However, key challenges remain underexplored in the literature. There is limited understanding of how specific honeypot characteristics–particularly interaction level, network type, and geographic location–impact the volume and nature of ICS interactions. Additionally, while high-interaction honeypots may generate richer and potentially more interesting threat intelligence, their complexity raises deployment and maintenance barriers. Understanding these trade-offs is essential for designing effective honeypot-based defenses for industrial environments.

Contributions. This work examines the impact of interaction level, type, and geographic region of the deployment network on ICS honeypot attractiveness. To this end, we deploy 16 ICS honeypots in collaboration with Forescout Technology, a cybersecurity company specialized in threat detection and operational technology security. Our setup includes a physical PLC (Siemens Simatic S7-1200) and both low- and high-interaction honeypots emulating the same device, distributed across two network types (corporate network vs. cloud network) and three geographic regions (Europe, North America, Asia). The honeypots are exposed to the Internet for three months, during which we collect HTTP, Modbus, and S7Comm traffic. We characterize attractiveness by traffic volume and complexity; due to space constraints, we omit a detailed analysis of traffic nature, which is part of ongoing work. The main contributions are as follows:

- Our findings show that, for ICS honeypots, network type has a stronger influence on attracting ICS traffic than geographic location or interaction level, highlighting the need to consider the deployment environment when designing honeypot studies.
- Our study shows that unsolicited ICS traffic is significantly less frequent than IT traffic, yet its presence may indicate reconnaissance activity and, thus, should be considered in threat detection efforts.

– Our study shows that low- and high-interaction honeypots receive comparable ICS traffic, suggesting that low-interaction setups are generally sufficient for generic threat intelligence gathering.

Outline. The remainder of this paper is organized as follows. Section 2 reviews relevant background and prior research on ICS honeypots. Section 3 introduces our research questions. Section 4 describes the deployed infrastructure and the methods used to address the research questions. Section 5 presents the results, and Section 6 discusses the key findings. Finally, Section 7 concludes the paper.

2 Background and Related Work

This section introduces ICS honeypots, reviews related work, and identifies research gaps.

2.1 ICS Honeypots

ICS honeypots serve multiple purposes, including diverting attackers from critical assets, studying adversary behavior, and gathering threat intelligence. Like traditional honeypots, they are categorized by interaction level. Low-interaction honeypots simulate basic network behavior without replicating the full device functionality, relying on scripted actions that attackers may eventually recognize [16]. Despite this, they remain popular for their ease of deployment, simplicity, and lower operational risk. High-interaction honeypots, on the other hand, offer richer emulation by supporting full process control and interaction with simulated or physical environments, though they require more complex setup and pose greater security risks. Recent frameworks like HoneyICS [17] have emerged to provide high-interaction capabilities by virtualizing PLCs and linking them to simulated industrial processes. Built on OpenPLC [2], a widely used open-source virtual PLC, HoneyICS supports Modbus natively and integrates Snap7 [22] to enable S7Comm communication. It allows interaction with a simulated industrial process, offering higher realism compared to low-interaction honeypots like Conpot [19]. Understanding the trade-offs between honeypot types is essential for designing effective experiments and cost-efficient deployment strategies.

2.2 Related Work

Research on ICS honeypots spans several dimensions, including the comparison of interaction levels and the influence of network type and geographic location. Table 1 summarizes the literature in this domain.

Level of Interaction. The attractiveness of honeypots with different interaction levels has been explored primarily in IT and IoT environments. Early IT honeypot studies [1, 23] found that high-interaction setups complemented low-interaction ones by validating configurations, with most intrusions attributed to inexperienced attackers using automated tools. However, these findings may not reflect recent advances in attack automation [33] and honeypot technologies. Recent work [14] highlights the richer data collected with high-interaction honeypots, though Guarnizo et al. [9] found similar attack patterns

Table 1. Summary of related work

	Domain	Level of Interaction				Deployment Environment	
		Low-Interaction Honeypot	High-Interaction Honeypot	Physical PLC	Level of Interaction Comparison	Network Type Comparison	Region Comparison
Pouget et al. [23]	IT	◐	●	○	◐	○	○
Alata et al. [1]	IT	◐	●	○	◐	○	○
Bloomfield et al. [4]	IT	◐	●	○	◐	●	○
Sochor et al. [27]	IT	●	○	○	○	●	○
Bove et al. [5]	IT	●	○	○	○	●	●
Kelly et al. [12]	IT	●	○	○	○	◐	●
Kocaogullar et al. [14]	IT	●	●	○	●	○	○
Zou et al. [35]	IT	●	○	○	○	◐	◐
Guarnizo et al. [9]	IoT	●	●	○	●	◐	◐
Tambe et al. [30]	IoT	○	●	○	○	◐	◐
Jicha et al. [11]	ICS	●	○	○	○	○	○
Dodson et al. [7]	ICS	○	●	○	○	○	◐
You et al. [34]	ICS	◐	●	●	●	○	◐
Bieker et al. [3]	ICS	●	○	○	○	●	●
Maesschalck et al. [19]	ICS	●	○	●	◐	○	○
Lupia et al. [18]	ICS	○	●	○	○	○	○
Srinivasa et al. [28]	IoT/ICS	●	●	○	●	●	●
This work	ICS	●	●	●	●	●	●

Legend: ○= Not Discussed, ◐= Partially Discussed, ●= Fully Discussed.

across interaction levels, suggesting realism does not always boost engagement. Some studies focus specifically on ICS honeypots. Jicha et al. [11] and Bieker et al. [3] deploy Conpot and GridPot variants, but offer limited traffic analysis. Dodson et al. [7] conduct a large-scale high-interaction deployment, capturing rare yet significant ICS-specific attacks. Srinivasa et al. [28] compare RioTPot and Conpot, observing that high-interaction honeypots attract more interactions, although differences in protocol support complicate the comparison. Only a few studies compare honeypots to physical PLCs. Maesschalck et al. [19] highlight limitations of low-interaction simulations, though their physical PLC is not exposed to the Internet. Similarly, You et al. [34] deploy a physical Siemens S7-300 PLC and compare its function code coverage with Conpot, but their setup lacks a physical process, limiting realism. Overall, research involving physical ICS honeypots remains limited. Prior work rarely includes online deployments of physical devices, and systematic comparisons between physical, high-, and low-interaction honeypots are lacking. As a result, the relative effectiveness of these honeypots remains underexplored.

Network Type. Several studies have examined how network type influences IT honeypot interactions. Bloomfield et al. [4] find that high-interaction IT honeynets in corporate environments attract more attacks than those in small- to medium-sized enterprises, likely due to public IPs and greater visibility. Sochor et al. [27] show that attackers differentiate between academic and commercial IP ranges. Kelly et al. [12] observe higher attack volumes on Google Cloud compared to AWS and Azure, though the use of different cloud locations may have influenced the results. Other studies deploy honeypots across network types without analyzing the effect. For instance, Guarnizo et al. [9] and Tambe et al. [30] deploy IoT honeypots in local networks with cloud-based forwarders but do not evaluate environmental differences. Bove et al. [5] find minimal variation in SSH intrusions between cloud and internet-connected hosts. Bieker et al. [3] observe lower ICS traffic in cloud honeypots than academic networks, attributing this to the scarcity of ICS devices in the cloud, although their sequential deployment limits confidence in their findings. In contrast, Srinivasa et al. [28] conduct a parallel deployment in corporate and

cloud networks, detecting more ICS traffic in the cloud. Although these studies suggest network type may influence attacker behavior, systematic evaluations in ICS remain scarce. Most prior work focuses on IT systems and rarely includes controlled, parallel deployments that isolate network effects.

Region. Prior research highlights the importance of deploying honeypots across diverse locations to uncover regional variations in attacker tactics. For instance, Dodson et al. [7] advocate geographically distributed honeypots to capture a broader spectrum of attack strategies. Building on this, Zou et al. [35] deploy high-interaction IT honeypots in East Asia, Western Europe, and US East via Azure, observing notable differences in traffic volume and unique IPs across regions. Similar trends are also reported in [5, 12]. Srinivasa et al. [28] report Europe attracted the most malicious IoT/ICS traffic, followed by the US and Asia, while Bieker et al. [3] record more ICS traffic in Asia than in the US. Most of these findings, however, are based on IT honeypots, leaving geographic influences on ICS honeypot attractiveness underexplored. In addition, inconsistent experimental setups between locations make it difficult to isolate geographic effects from other variables.

2.3 Research Gaps

To the best of our knowledge, there is no systematic comparison of interaction levels—low and high—in ICS environments. Existing studies often use inconsistent setups or overlook how these configurations influence honeypot attractiveness. This limits our ability to assess the trade-off between deployment cost and effectiveness. Moreover, the impact of the deployment environment is still unclear. While some studies suggest differences in traffic between cloud and corporate networks, these findings often rely on sequential deployments or vague threat classifications. Without controlled, concurrent experiments, the true impact of network context on honeypot attractiveness remains unclear. Geographic location is another underexplored factor. While IT-focused research highlights regional differences, ICS studies are limited in scope and often inconsistent in results. A broader and systematic evaluation across locations is needed to assess how the deployment region influences the attractiveness of ICS targets. Finally, interactions between factors—such as network type and geographic location—are rarely investigated. This lack of multi-dimensional analysis restricts our understanding of how ICS honeypots are perceived in practice. Addressing these gaps through systematic evaluations would enhance our understanding and offer clearer guidance for honeypot deployment.

3 Research Questions

Previous studies have examined various honeypot types and configurations, often focusing on isolated aspects (cf. Section 2.2). However, honeypot attractiveness may depend on a broader, potentially interdependent set of factors, including interaction level, network type, and geographic location. This work systematically investigates how these factors influence the attractiveness of ICS honeypots. Our first research question investigates the role of interaction level. High-interaction honeypots, including those involving physical PLCs, can capture more sophisticated behavior, but they are also

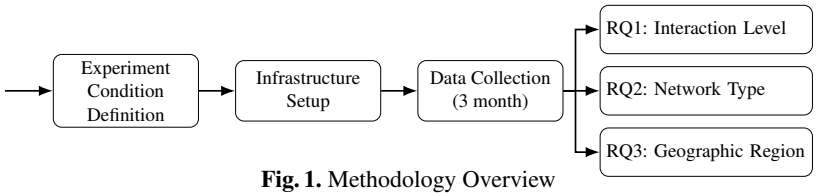

Fig. 1. Methodology Overview

more complex to deploy and operate. Understanding their impact helps assess when the added complexity is justified.

RQ1: *To what extent does the level of interaction supported by an ICS honeypot influence the attractiveness of the honeypot?*

Realistic IP addresses are key for honeypots to avoid detection [7]. While cloud setups offer convenience and isolation, ICS devices are typically tied to physical infrastructure, making corporate deployments appear more authentic. This raises the question whether corporate-based ICS honeypots are more attractive than cloud-hosted ones.

RQ2: *To what extent does the network type on which an ICS honeypot is deployed influence the attractiveness of the honeypot?*

Prior work suggests that attacks can vary by region, motivating the geographic distribution of ICS honeypots [7]. To investigate this, ICS honeypots should be deployed in diverse locations to assess whether geographic location affects attractiveness and reveals potential regional differences in traffic captured.

RQ3: *To what extent does the geographic location of an ICS honeypot influence the attractiveness of the honeypot?*

4 Methodology

An overview of our methodology is shown in Fig. 1. After defining the experiment conditions (Section 4.1), we deploy the data collection infrastructure and collect data over a 90-day period (Section 4.2). To answer the research questions, we evaluate protocol-specific attractiveness across honeypots by comparing the captured traffic based on interaction level (RQ1), network type (RQ2), and geographic region (RQ3).

4.1 Experiment Conditions

We define 12 experiment conditions in our study (Fig. 2). Each condition corresponds to a specific configuration of the honeypot, determined by three variables: the *interaction level* it supports, the *type of network* in which it is deployed, and the *geographic region* of deployment. We now discuss the choices made for each of these variables.

Interaction Levels. To assess how interaction level affects honeypot attractiveness (RQ1), we deploy three setups: a *low-interaction ICS honeypot*, a *high-interaction ICS honeypot*, and a *physical ICS device*. To allow meaningful comparison, all honeypots simulate the same device type and expose the same ICS protocols. Specifically, we choose the Modbus and S7Comm protocols due to their high diffusion in the wild [20, 26]. We select the S7-1200 as the physical PLC due to native protocol support and wide ICS

adoption. We use Conpot [19] for low interaction and HoneyICS [17] for high interaction. Both can simulate a Siemens S7-1200 PLC, support Modbus and S7Comm, and host a static web server. All setups appear similar externally but differ in interaction level: Conpot gives static responses, HoneyICS offers process interaction via Modbus only, and the PLC offers process interaction via both protocols and full device configuration via S7Comm. The interaction levels of the three setups are detailed in Appendix A.

Network Types. To assess whether network type affects honeypot attractiveness (RQ2), we consider a *corporate network* and a *cloud-based network*. The corporate network reflects a realistic ICS setup, with on-premise devices accessible via public IPs. In contrast, cloud networks are commonly used only for honeypot deployments [3, 5, 12]. By comparing the two, we aim to determine whether they are perceived differently in terms of attractiveness. To control for geographic bias, one cloud deployment is placed in the same region as the corporate network (Europe); see Section 4.2 for details.

Geographic Regions. To assess the influence of geographic region (RQ3), we consider three global regions: *Europe*, *North America*, and *Asia*. This selection follows prior research and Shodan scans showing these areas host the most publicly accessible ICS devices. According to Shodan, the US has the highest number of exposed ICS devices using Modbus and S7Comm, making it the best representative for North America. While China ranks second, infrastructure restrictions prevent server deployment there; thus, we choose Singapore, ranked third, to represent Asia. The choice for Europe reflects the location of the corporate network available for our study (see Section 4.2).

4.2 Data Collection

Infrastructure. Based on our experiment conditions (Section 4.1), we set up the infrastructure to enable data collection (Fig. 2). The infrastructure encompasses 16 ICS honeypots[5]. All honeypots expose HTTP, S7Comm, and Modbus services. They are deployed on a corporate network and exposed on the cloud network using proxies. This ensures consistent behavior across network types and regions. We now describe key details of the infrastructure.

Honeypots. We deploy Conpot as a Docker container and customize it to mimic a Siemens S7-1200 PLC. Customization involves modifying Conpot's default templates to update its web interface and the scripted S7Comm and Modbus responses. We deploy two HoneyICS instances in a Docker environment that simulates a production process controlled by virtualized S7-1200 PLCs. Each virtualized PLC exposes the same services (Modbus and S7Comm) and a web interface. The physical Siemens S7-1200 PLC interacts with HoneyICS via Modbus and controls part of the same (simulated) physical process. To this end, its ladder logic is built and loaded using Siemens TIA Portal software. To ensure continuous operation under attack, an automated script monitors the PLC integrity and restarts it when needed (e.g., if forced into STOP mode).

Deployment. We deployed our honeypots using the infrastructure and resources of Forescout Technologies, including a subscription to Amazon Web Services (AWS). The four honeypots are hosted on a corporate network in the Netherlands, each with a unique

[5] Note that we deploy two instances of HoneyICS, resulting in 16 honeypots across the 12 experiment conditions in Section 4.1. This allows us to estimate variability in the collected traffic.

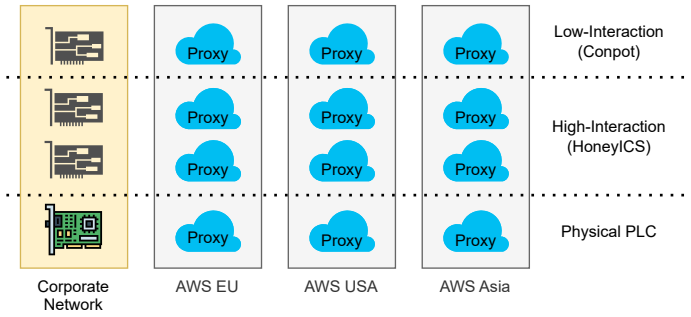

Fig. 2. Architecture of the honeypots and AWS proxies

IPv4 address leased from a Dutch ISP that supports enterprise and ICS environments, to guarantee realism. For the cloud instances, we leverage Forescout's subscription to AWS. Based on our experiment conditions (Section 4.1), we selected three AWS regions: US East (North Virginia), Asia Pacific (Singapore), and EU Central (Frankfurt), which is the AWS region closest to the corporate network. Instead of duplicating instances, we deploy lightweight proxies on AWS that forward traffic to the corporate-hosted honeypots. Each proxy has a dedicated Elastic IP to ensure stable public access across reboots.

Packet Capture and Storage. All traffic to and from the honeypots on ports 80 (HTTP), 102 (S7Comm), and 502 (Modbus) is captured as PCAP files using tcpdump [31]. The packet capture setup varies depending on the network environment. In the corporate network, it integrates with the existing infrastructure, which includes a pre-configured mirroring system. All traffic is mirrored to an external analysis system and stored in an AWS S3 bucket using tcpdump. For AWS deployments, a challenge arises as requests are proxied, so honeypots log correct payloads but proxy IPs. To address this, we capture traffic on the proxies. Tcpdump filters ensure proxy traffic is excluded from honeypot captures and vice versa, so each system records only its own interactions. PCAP files are saved on separate virtual drives for each honeypot and proxy to protect against system failures. File sizes are limited to 100 MB to reduce data loss in case of corruption.

Dataset. Data collection took place over 90 days, between December 21, 2024, and March 21, 2025. In this period, all incoming and outgoing packets for each honeypot are captured and stored as PCAP files. This format allows us to extract all relevant traffic details, such as source and destination addresses, protocols and payload content (e.g., Modbus function codes). As a preliminary step, we removed all traffic generated from IPs under our control to remove any bias in the data. Table 2 summarizes the distribution of HTTP, Modbus, and S7Comm requests across honeypots.

4.3 Data Analysis

To answer our research questions, we characterize and compare interactions across different honeypot deployments. To this end, we first introduce the notion of interaction and define the metrics for assessing honeypot attractiveness.

Interactions. We adapt the definition of interaction in [18]: a sequence of requests that (1) originate from the same IP, (2) target the same destination IP and port, and (3) occur

Table 2. Observed requests per honeypot

Honeypot	Network	Region	HTTP	Modbus	S7Comm
Conpot	Corporate	EU	27032	1172	1336
HoneyICS1	Corporate	EU	26307	776	1682
HoneyICS2	Corporate	EU	25829	643	1632
Physical PLC	Corporate	EU	15329	695	1658
Conpot	Cloud	EU	123332	403	761
HoneyICS1	Cloud	EU	119915	453	845
HoneyICS2	Cloud	EU	117983	460	904
Physical PLC	Cloud	EU	60915	411	901
Conpot	Cloud	US	73377	415	811
HoneyICS1	Cloud	US	77890	429	875
HoneyICS2	Cloud	US	84779	475	920
Physical PLC	Cloud	US	77429	441	889
Conpot	Cloud	Asia	87613	450	810
HoneyICS1	Cloud	Asia	105403	466	979
HoneyICS2	Cloud	Asia	84149	425	961
Physical PLC	Cloud	Asia	67718	436	841
Total			1175000	8550	16805

within a specified maximum time interval. We exclude the source port to account for tools that use multiple TCP connections for a single logical task. Following [18], we analyze inter-request intervals to define appropriate time thresholds, considering potential proxy-induced delays, particularly in HTTP traffic. For HTTP, we select a 30-second threshold, which captures 95% of HTTP follow-up requests (from the same IP). For S7Comm and Modbus, we inspect packet sequences, ensuring continuity of TCP connections. Based on this analysis, we apply a 15-second threshold across all deployments for both S7Comm and Modbus, which captures 99.96% and 100% of subsequent requests, respectively.

Attractiveness. We assess attractiveness by interaction volume and complexity. The complexity is measured as the number of requests per interaction, providing an indication of their sophistication. A honeypot is deemed more attractive if it receives a larger number of interactions with higher complexity.

Analysis Methods. We aggregate the data according to experiment conditions to assess attractiveness across different interaction levels (RQ1), network types (RQ2), and geographic regions (RQ3), analyzing interaction volume and complexity in each case. To address RQ1, we aggregate interactions by honeypot type (Conpot, HoneyICS1, HoneyICS2, and the physical PLC) across all deployment environments (corporate network, AWS EU, AWS US, and AWS Asia). To address RQ2, we separately aggregate interactions from the honeypots on the corporate network and on the AWS EU cloud. To address RQ3, we focus on cloud deployments and aggregate interactions for each region (AWS EU, AWS US, AWS Asia). Additionally, we analyze the geographic origin of IP addresses interacting with the honeypots using GreyNoise [8] and, where necessary, IP-API [10]. Grouping IP origins by continent helps assess whether the deployment region influences the geographic distribution of interactions.

5 Results

This section presents our results, structured around the research questions; we refer to Appendix B for the complete results.

Table 3. Interaction level: volume and complexity

Honeypot	Protocol	Min	Q1	Median	Q3	Max	Count
Conpot	HTTP	1	1	1	2	19994	42321
	S7Comm	1	3	3	3	8	1318
	Modbus	1	1	1	1	241	1487
HoneyICS1	HTTP	1	1	1	2	12534	40408
	S7Comm	1	3	3	3	16	1535
	Modbus	1	1	1	1	10	1393
HoneyICS2	HTTP	1	1	1	2	8021	41870
	S7Comm	1	3	3	3	16	1529
	Modbus	1	1	1	1	16	1348
Physical PLC	HTTP	1	1	1	2	7365	38381
	S7Comm	1	3	3	3	4	1484
	Modbus	1	1	1	1	10	1314

RQ1: To what extent does the level of interaction supported by an ICS honeypot influence the attractiveness of the honeypot? Table 3 reports the number of interactions (Count) and their complexity (Min, Q1, Median, Q3, and Max) for each protocol across different levels of interaction (Conpot, HoneyICS, and physical PLC). The table shows notable differences between protocols. We now discuss the results for each protocol.

HTTP. Fig. 3 (left) shows the number of HTTP interactions per day for each level of interaction. For a large portion of the data collection period, we observe no notable differences between the honeypots. However, we observe a sharp increase in March for Conpot and both HoneyICS instances, while the physical PLC maintains a stable trend. This shift may be attributed to differences in the web server technologies used by the honeypots. Conpot and HoneyICS both employ Lighttpd, whereas the physical PLC uses a jQuery-based server. A detailed analysis shows that a single IP address is responsible for the shift (on both Conpot and HoneyICS), repeatedly issuing HTTP GET requests to `/login.cgi/cgi_main.cgi` with admin/admin credentials. The Lighttpd servers generate responses that appear to encourage repeated attempts, while the jQuery-based server returns responses that did not trigger further activity. This suggests that the observed increase in interactions is primarily driven by server behavior rather than by the honeypot's interaction level. Considering the overall number of interactions (see Table 3), the physical PLC receives the fewest interactions, followed by HoneyICS, while Conpot receives the most. Even among honeypots with the same interaction level (HoneyICS1 vs. HoneyICS2), we observe a noticeable variation in the number of interactions, further suggesting that interaction level alone does not determine HTTP attractiveness. Moreover, Table 3 shows that the Min, Q1, Median, and Q3 values are identical across honeypots, indicating that at least 75% of interactions have similar complexity regardless of the honeypot's interaction level. The main difference lies in the maximum complexity: Conpot exhibits the most complex interaction, followed by HoneyICS and then the physical PLC. Again, notable variation between the two HoneyICS instances reinforces the conclusion that interaction level does not consistently influence the attractiveness or complexity of HTTP interactions in ICS honeypots.

S7Comm. Fig. 3 (center) reports the S7Comm interactions per day for each interaction level. The curves are closely aligned, indicating minor differences in interaction frequency across levels. Conpot consistently receives the fewest interactions. HoneyICS shows the highest activity, with its two instances differing by only six interactions

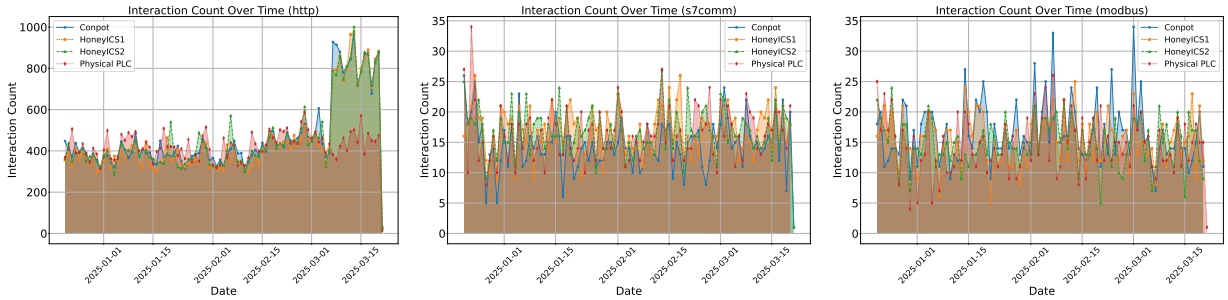

Fig. 3. Interactions per interaction level for HTTP (left), S7Comm (center), and Modbus (right)

(Table 3). The physical PLC follows, with approximately 50 fewer interactions (3%), indicating a comparable level of engagement. The distribution of interaction complexity is nearly identical across all honeypots (Table 3). Outliers are scarce for Conpot and both HoneyICS instances, while absent for the physical PLC.

Modbus. Fig. 3 (right) reports the Modbus interactions per day for each interaction level. All levels of interaction show similar daily trends, but Conpot exhibits the most frequent and highest peaks, while HoneyICS and the physical PLC follow a comparable but lower pattern. This trend is consistent with the total interaction counts shown in Table 3, where Conpot receives approximately 100 more interactions (7%) than HoneyICS and about 170 more than the physical PLC (12%). These findings suggest that Conpot attracts more Modbus interactions compared to the higher-interaction counterparts. Across all interaction levels, most Modbus interactions have a complexity of 1. For HoneyICS and the physical PLC, the few interactions with higher complexity comprise 6 and 10 requests, while for Conpot, they mostly comprise 2 or 3 requests (Table 3). An in-depth analysis shows that this difference in complexity is influenced by how Conpot responds to a tool used by Crowdstrike. This suggests that interactions with low-interaction honeypots tend to be less complex than those with high-interaction honeypots or physical PLCs. However, Conpot was involved in one interaction comprising 241 requests, while they were at most 10 and 16 for HoneyICS and 10 for the physical PLC. This suggests that while Conpot typically attracts simpler interactions, it can also elicit highly complex behavior.

Answer to RQ1. The interaction level does not consistently determine the attractiveness of an ICS honeypot. For HTTP, server configuration had a greater impact on interaction patterns than interaction level. In the case of S7Comm, HoneyICS was slightly more attractive, while for Modbus, Conpot drew more interactions. Overall, attractiveness appears to depend more on protocol-specific factors than on interaction level alone.

RQ2: To what extent does the network type on which an ICS honeypot is deployed influence the attractiveness of the honeypot? Table 4 reports the number of interactions (Count) and their complexity (Min, Q1, Median, Q3, and Max) for each protocol across network types (corporate vs. cloud). We now discuss the results for each protocol.

HTTP. Fig. 4 (left) shows the HTTP interactions per day for both the corporate network and the cloud network (AWS EU). Across the entire observation period, the cloud

Table 4. Network type: volume and complexity

Network	Protocol	Min	Q1	Median	Q3	Max	Count
Corporate	HTTP	1	1	1	2	8021	30700
	S7Comm	1	3	3	3	7	2258
	Modbus	1	1	1	1	241	1585
Cloud	HTTP	1	1	1	2	7269	44365
	S7Comm	1	3	3	3	8	1183
	Modbus	1	1	1	1	10	1313

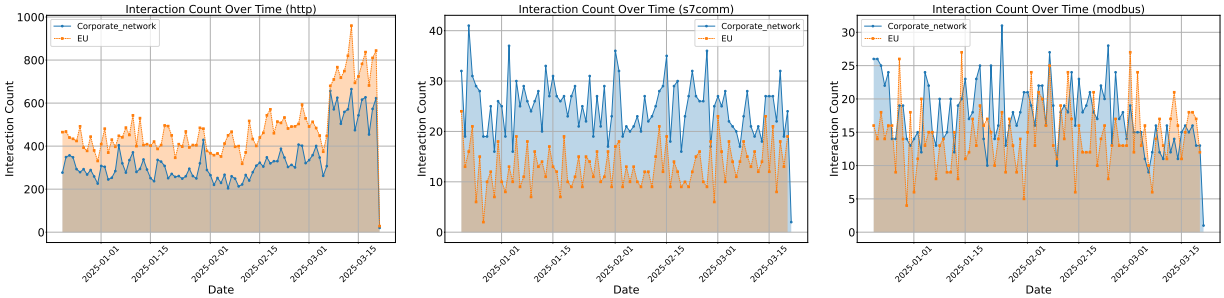

Fig. 4. Interactions per network type for HTTP (left), S7Comm (center), and Modbus (right)

network consistently receives more HTTP interactions than the corporate network (45%), suggesting that it is more attractive for HTTP-based activity. The distribution of HTTP interaction complexity is largely consistent across both networks, with only minor differences. As shown in Table 4, the Min, Q1, Median, and Q3 values are identical, indicating similar interaction patterns regardless of network type. The only notable distinction is in the maximum observed complexity, which is approximately 750 higher on the corporate network. This suggests that while HTTP interactions are largely comparable across networks, the corporate network occasionally attracts more complex requests.

S7Comm. Fig. 4 (center) reports the S7Comm interactions per day for both the corporate and cloud networks. Over the entire observation period, the corporate network consistently receives more S7Comm interactions than the cloud network. This trend is confirmed by Table 4, which shows that the corporate network records approximately twice as many S7Comm interactions (91%), suggesting it is more attractive for this protocol. The overall complexity is almost constant in the two networks, which shows a maximum complexity of 7 and 8 requests for the corporate and cloud networks, respectively.

Modbus. Fig. 4 (right) shows the Modbus interactions per day for the corporate and cloud networks. While both exhibit fluctuations, the corporate network consistently receives more interactions. Table 4 confirms this trend, showing that the corporate network receives approximately 270 more interactions (21%), suggesting it is a more attractive target for Modbus traffic. Table 4 shows that the overall distribution is largely the same on both networks, with most interactions having a complexity of 1. The difference in maximum complexity is due to a single outlier from Conpot on the corporate network, as noted in the RQ1 analysis. The maximum complexity for all other honeypots on the corporate network is 10, matching that of the cloud network. This suggests that, overall, interaction complexity for Modbus does not meaningfully differ between network types.

Table 5. Geographic region: volume and complexity

Location	Protocol	Min	Q1	Median	Q3	Max	Count
EU	HTTP	1	1	1	2	7269	44365
	S7Comm	1	3	3	3	8	1183
	Modbus	1	1	1	1	10	1313
US	HTTP	1	1	1	2	19994	41386
	S7Comm	1	3	3	3	16	1182
	Modbus	1	1	1	1	16	1303
Asia	HTTP	1	1	1	2	12534	46529
	S7Comm	1	3	3	3	16	1243
	Modbus	1	1	1	1	10	1341

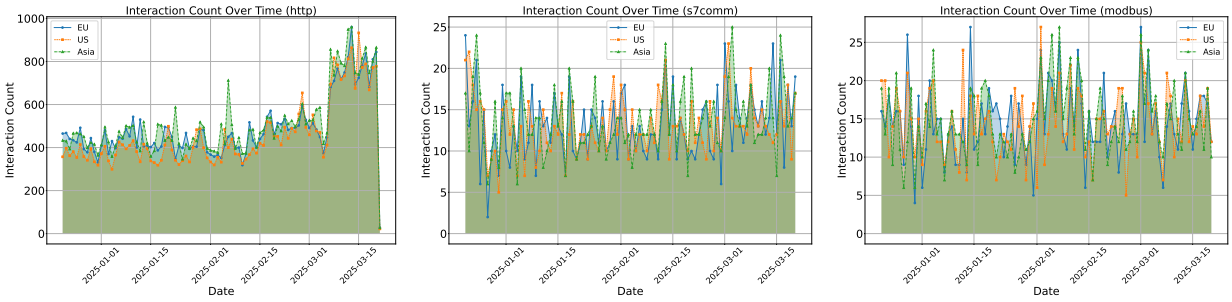

Fig. 5. Interactions per region for HTTP (left), S7Comm (center), and Modbus (right)

Answer to RQ2. Network type affects the volume of interactions for specific protocols but not their overall complexity. HTTP traffic is more frequent in the cloud environment, whereas S7Comm and Modbus interactions are more common on the corporate network. This suggests that while network type influences protocol-specific attractiveness, it has a limited impact on the sophistication of interactions.

RQ3: To what extent does the geographic location of an ICS honeypot influence its attractiveness? Table 4 reports the number of interactions (Count) and their complexity (Min, Q1, Median, Q3, and Max) for each protocol across regions. We now discuss the results for each protocol, along with the origin of iterations per region.

HTTP. Fig. 5 (left) reports the HTTP interactions per day across different regions. The trends are relatively similar across regions, although Asia exhibits the highest peaks, followed by the EU and then the US. Table 5 confirms this pattern, showing that Asia receives over 2000 more HTTP interactions than the EU (5%) and over 5000 more than the US (12%). This suggests that Asia is the most attractive region for HTTP interactions. The complexity is consistent across all regions, with identical Min, Q1, Median, and Q3 values, as shown in Table 5. The only notable variation lies in the maximum values: the US records the highest at 19,994, followed by Asia (12,534) and the EU (7,269). These, however, appear to be outliers; most complex interactions for the US and Asia typically fall between 7,100 and 7,400. Overall, these findings suggest that HTTP interaction complexity is not strongly influenced by geographic region.

S7Comm. Fig. 5 (center) reports the S7Comm interactions per day across different regions. The trends are relatively similar, with no substantial differences in the number of S7Comm interactions. As shown in Table 5, Asia receives approximately 60 more

Table 6. Origin of HTTP interactions

Region	Africa	Asia	Europe	North America	Oceania	South America	Total
EU	86 (0.19%)	8045 (18.13%)	**24201 (54.55%)**	11424 (25.75%)	170 (0.38%)	439 (0.99%)	44365 (100%)
US	84 (0.20%)	5868 (14.18%)	23403 (56.55%)	**11455 (27.68%)**	154 (0.37%)	422 (1.02%)	41386 (100%)
Asia	313 (0.67%)	**8852 (19.02%)**	24539 (52.74%)	12185 (26.19%)	169 (0.36%)	471 (1.01%)	46529 (100%)
Total	483 (0.37%)	22765 (17.21%)	72143 (54.54%)	35064 (26.51%)	493 (0.37%)	1332 (1.01%)	132280 (100%)

Table 7. Origin of S7Comm interactions

Region	Africa	Asia	Europe	North America	Oceania	South America	Total
EU	0 (0.00%)	92 (7.78%)	**227 (19.19%)**	817 (69.06%)	0 (0.00%)	47 (3.97%)	1183 (100%)
US	0 (0.00%)	115 (9.73%)	183 (15.48%)	**817 (69.12%)**	0 (0.00%)	67 (5.67%)	1182 (100%)
Asia	0 (0.00%)	**136 (10.94%)**	214 (17.22%)	847 (68.14%)	0 (0.00%)	46 (3.70%)	1243 (100%)
Total	0 (0.00%)	343 (9.51%)	624 (17.29%)	2481 (68.76%)	0 (0.00%)	160 (4.43%)	3608 (100%)

interactions than both the EU and the US (5%), while the difference between the EU and US is minimal, just one interaction. This may indicate that Asia is marginally more attractive for S7Comm interactions, though the variation is minor. The distribution of interaction complexity is nearly identical across all regions, as shown in Table 5. The only notable difference is in the maximum complexity, with both the US and Asia showing interaction values roughly twice as complex as those observed in the EU.

Modbus. Fig. 5 (right) reports the Modbus interactions per day across different regions. The trends are relatively similar across all regions, with no substantial differences observed. Table 5 supports this observation, indicating that Asia receives approximately 30 more Modbus interactions than the EU (2%) and 40 more than the US (3%). Similarly, the distribution of interaction complexity is nearly identical across regions as shown in Table 5. The only notable deviation is the slightly higher maximum complexity observed in the US compared to the other regions.

Origin of Interactions. Tables 6, 7, and 8 present the geographic origin of interactions for each protocol, with bold values indicating the regions where the honeypots were deployed. Across all protocols, we observe only minor differences in the distribution of interaction origins based on deployment region. While the region in which a honeypot is hosted tends to show a slightly higher share of interactions for that protocol, the difference is minimal, never exceeding 2.7%. These results suggest that geographic deployment has limited influence on the origin of incoming interactions, indicating that honeypot attractiveness is largely independent of deployment region.

Answer to RQ3. Geographic location has limited impact on honeypot attractiveness. For each protocol, volume and complexity are mostly consistent across regions, with only minor differences. The origin of interacting IPs also appears unaffected by deployment region, suggesting ICS honeypots are not systematically targeted based on location.

6 Discussion

The results of this study offer valuable insights into ICS honeypot deployments, providing key considerations for improving their design and effectiveness in future research.

Table 8. Origin of Modbus interactions

Region	Africa	Asia	Europe	North America	Oceania	South America	Total
EU	2 (0.15%)	163 (12.41%)	**218 (16.60%)**	887 (67.56%)	0 (0.00%)	43 (3.27%)	1313 (100%)
US	3 (0.23%)	147 (11.28%)	200 (15.35%)	**903 (69.30%)**	0 (0.00%)	50 (3.84%)	1303 (100%)
Asia	5 (0.37%)	**162 (12.08%)**	229 (17.08%)	900 (67.11%)	0 (0.00%)	45 (3.36%)	1341 (100%)
Total	10 (0.25%)	472 (11.93%)	647 (16.35%)	2690 (67.98%)	0 (0.00%)	138 (3.49%)	3957 (100%)

For ICS honeypots, network type matters more than geographic region and interaction level. Our results show that the interaction level (RQ1) and geographic location (RQ3) of ICS honeypots have minimal impact on the volume or complexity of traffic across protocols. In contrast, the network type affects the amount of ICS traffic (RQ2): honeypots in the corporate network received 91% more S7Comm traffic than the cloud-host honeypots (Table 4). This suggests that IPs associated with cloud infrastructure may be excluded when targeting ICS systems, though retained when scanning for exposed web applications. Our results partially align with prior work. Zou et al. [35], using an IT honeypot, found more IT traffic in certain regions, especially Asia. While we found similar results for our IT traffic (HTTP), the same behavior cannot be seen in the OT world (Modbus and S7Comm protocols), where geographical differences are negligible. This contrasts with Bieker et al. [3] and Srinivasa et al. [28], who reported higher ICS traffic in Asia and Europe, respectively. This discrepancy likely stems from methodological choices in prior work, such as aggregating results across protocols and interpreting scanning behavior as inherently malicious. In contrast, our protocol-specific analysis avoids strong assumptions about attacker intent, offering a more cautious interpretation that may more accurately reflect the nature of unsolicited ICS traffic. Our findings have two key implications. First, they highlight the importance of protocol-level analysis when designing honeypot studies or interpreting their results, as the received traffic may be influenced by the specific services exposed. Second, they suggest that to attract more ICS-relevant interactions, honeypot deployments should prioritize corporate environments and expose an HTTP-based HMI alongside ICS protocols. Future work should analyze how different combinations of ICS and IT services influence honeypot attractiveness, to guide the design of more effective and targeted honeypot deployments.

While HTTP traffic is more common, unsolicited ICS scans might reveal insights into industrial system vulnerabilities. We observed a substantially higher volume of HTTP requests compared to ICS-specific traffic (i.e., Modbus, S7Comm) across our honeypot deployments. This discrepancy is likely due to the prevalence of broad, automated scanning activities that primarily target common IT protocols such as HTTP. Although scanning traffic using ICS protocols was also observed, it occurred at a significantly lower frequency. These findings indicate that ICS protocols are probed less frequently than standard IT services, but the presence of unsolicited scans still reflects a degree of exposure. This has important implications for threat detection: ICS protocol activity, even when not clearly targeted, may signal reconnaissance behavior directed at operational technology environments and should be monitored accordingly.

For general threat intelligence, realistic ICS honeypots offer insights similar to simpler setups but can reveal more about occasional complex and targeted interactions. Our analysis indicates that both low- and high-interaction honeypots capture similar ICS

traffic, regardless of deployment environment (cloud vs. corporate) or geographic region. This suggests that for gathering general threat intelligence, the added realism of high-interaction honeypots offers limited benefit. For this purpose, low-interaction honeypots provide a more cost-effective and operationally simpler choice. However, the occasional appearance of more complex interactions–even on low-interaction honeypots as seen with Modbus in our study–indicates that high-interaction honeypots may still play a role in capturing and analyzing rare but potentially insightful behavior as they are better suited for targeted investigations of attack methodologies and post-exploitation behaviors. This finding underscores the importance of aligning the honeypot type with its intended purpose, as advocated in [13]. Future work should aim to identify concrete criteria for when high-interaction honeypots are justified, enabling more informed trade-offs between realism, resource investment, and threat intelligence insights.

Threats to Validity. *Internal Validity:* Anonymization methods (e.g., VPNs, TOR) and dynamic IP address reassignment by service providers can affect the accuracy of interaction origin. Misattribution of interaction origin may bias regional comparisons, introducing confounding factors that limit causal interpretations. *External validity:* Our study spans a three-month collection period. While a longer period might have captured additional behaviors, the stability of the observed traffic suggests our findings would remain unchanged. Our deployments account for a single PLC model and cloud provider and support Modbus and S7Comm, which may limit generalizability. Although prior work reports differences in honeypot traffic across cloud providers [12], these findings are based on IT environments; it remains unclear if similar patterns apply to ICS settings. Future research should examine a broader range of PLCs, ICS protocols, and cloud platforms.

7 Conclusion

In this study, we investigated how different ICS honeypot configurations influence their attractiveness, focusing on interaction level (low vs. high), network type (corporate vs. cloud), and geographic region (Europe, North America, Asia). Our infrastructure included emulated low- and high-interaction Siemens Simatic S7-1200 PLCs and a physical device, deployed across 16 setups and monitored over three months. Results show that interaction level and geographic location have minimal impact on traffic, while corporate deployments attract significantly more ICS activity, especially S7Comm. These findings highlight the importance of protocol-level analysis and suggest that low-interaction honeypots are generally sufficient for broad threat intelligence. Future work should define criteria for selecting honeypot types based on deployment goals and investigate how combining ICS and IT services influences honeypot attractiveness. We also plan to further analyze traffic and payloads to uncover attacker patterns and characterize interaction nature.

Acknowledgments This work has been partially supported by the INTERSECT project, Grant No. NWA.1162.18.301, funded by the Netherlands Organization for Scientific Research (NWO). Denis Donadel, Francesco Lupia and Massimo Merro have been partially supported by the SERICS project (PE00000014) under the *MUR National Recovery and Resilience Plan*, funded by the EU - NextGenerationEU.

References

1. E. Alata, V. Nicomette, M. Kaâniche, M. Dacier, and M. Herrb. Lessons learned from the deployment of a high-interaction honeypot. In *European Dependable Computing Conference*, pages 39–46. IEEE, 2006.
2. AUTONOMY. `https://autonomylogic.com/`. Accessed: 2025-06-07.
3. M. C. Bieker and D. Pilkington. Deploying an ics honeypot in a cloud computing environment and comparatively analyzing results against physical network deployment. Master's thesis, Naval Postgraduate School, Monterey, CA, 2020.
4. R. Bloomfield, I. Gashi, A. Povyakalo, and V. Stankovic. Comparison of empirical data from two honeynets and a distributed honeypot network. In *International Symposium on Software Reliability Engineering*, pages 219–228. IEEE, 2008.
5. D. Bove. Using honeypots to detect and analyze attack patterns on cloud infrastructures. Master's thesis, Friedrich-Alexander University, 2018.
6. T. M. Chen and S. Abu-Nimeh. Lessons from stuxnet. *Computer*, 44(4):91–93, 2011.
7. M. Dodson, A. R. Beresford, and M. Vingaard. Using global honeypot networks to detect targeted ICS attacks. In *International Conference on Cyber Conflict*, pages 275–291. IEEE, 2020.
8. GreyNoise. `https://www.greynoise.io`. Accessed: 2025-06-07.
9. J. D. Guarnizo, A. Tambe, S. S. Bhunia, M. Ochoa, N. O. Tippenhauer, A. Shabtai, and Y. Elovici. Siphon: Towards scalable high-interaction physical honeypots. In *Workshop on Cyber-Physical System Security*, pages 57–68, 2017.
10. ip-api. IP Geolocation API. `https://ip-api.com`. Accessed: 2025-06-07.
11. A. Jicha, M. Patton, and H. Chen. Scada honeypots: An in-depth analysis of conpot. In *Conference on Intelligence and Security Informatics*, pages 196–198. IEEE, 2016.
12. C. Kelly, N. Pitropakis, A. Mylonas, S. McKeown, and W. J. Buchanan. A comparative analysis of honeypots on different cloud platforms. *Sensors*, 21(7):2433, 2021.
13. S. Kempinski, S. Ichaarine, S. Sciancalepore, and E. Zambon. Icsvertase: A framework for purpose-based design and classification of ics honeypots. In *International Conference on Availability, Reliability and Security*, pages 1–10. ACM, 2023.
14. Y. Kocaogullar, O. Cetin, B. Arief, C. Brierley, J. Pont, and J. Hernandez-Castro. Hunting high or low: Evaluating the effectiveness of high-interaction and low-interaction honeypots. In *Socio-Technical Aspects in Security*, page 14–30. Springer-Verlag, 2025.
15. P. Kozak, I. Klaban, and T. Šlajs. Industroyer cyber-attacks on Ukraine's critical infrastructure. In *International Conference on Military Technologies (ICMT)*, pages 1–6. IEEE, 2023.
16. E. López-Morales, C. Rubio-Medrano, A. Doupé, Y. Shoshitaishvili, R. Wang, T. Bao, and G.-J. Ahn. Honeyplc: A next-generation honeypot for industrial control systems. In *SIGSAC Conference on Computer and Communications Security*, pages 279–291. ACM, 2020.
17. M. Lucchese, F. Lupia, M. Merro, F. Paci, N. Zannone, and A. Furfaro. HoneyICS: A high-interaction physics-aware honeynet for industrial control systems. In *International Conference on Availability, Reliability and Security*. ACM, 2023.
18. F. Lupia, M. Lucchese, M. Merro, and N. Zannone. ICS Honeypot Interactions: A Latitudinal Study. In *IEEE International Conference on Big Data*, pages 3025–3034. IEEE, 2023.
19. S. Maesschalck, V. Giotsas, and N. Race. World wide ICS honeypots: A study into the deployment of Conpot honeypots. In *Industrial Control System Security Workshop*, 2021.
20. M. Mladenov, L. Erdodi, and G. Smaragdakis. All that glitters is not gold: Uncovering exposed industrial control systems and honeypots in the wild. In *European Symposium on Security and Privacy*. IEEE, 2025.
21. S. Morishita, T. Hoizumi, W. Ueno, R. Tanabe, C. Gañán, M. J. Van Eeten, K. Yoshioka, and T. Matsumoto. Detect me if you… oh wait. an internet-wide view of self-revealing honeypots. In *Symposium on Integrated Network and Service Management*, pages 134–143. IEEE, 2019.

22. D. Nardella. Snap7. https://snap7.sourceforge.net/. Accessed: 2025-06-07.
23. F. Pouget and T. Holz. A pointillist approach for comparing honeypots. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 51–68. Springer, 2005.
24. N. Provos. A virtual honeypot framework. In *USENIX Security Symposium*, pages 1–14, 2004.
25. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic. Cyber-physical systems: The next computing revolution. In *Design Automation Conference*, pages 731–736, 2010.
26. Shodan. https://www.shodan.io/. Accessed: 2025-06-07.
27. T. Sochor and M. Zuzcak. Attractiveness study of honeypots and honeynets in internet threat detection. In *International Conference on Computer Networks*, pages 69–81. Springer, 2015.
28. S. Srinivasa, J. Pedersen, and E. Vasilomanolakis. Interaction matters: a comprehensive analysis and a dataset of hybrid IoT/OT honeypots. In *Annual Computer Security Applications Conference*, pages 742–755. ACM, 2022.
29. S. Srinivasa, J. Pedersen, and E. Vasilomanolakis. Gotta catch'em all: a multistage framework for honeypot fingerprinting. *Digital Threats: Research and Practice*, 4(3):1–28, 2023.
30. A. Tambe, Y. L. Aung, R. Sridharan, M. Ochoa, N. O. Tippenhauer, A. Shabtai, and Y. Elovici. Detection of threats to IoT devices using scalable VPN-forwarded honeypots. In *Conference on Data and Application Security and Privacy*, pages 85–96. ACM, 2019.
31. Tcpdump. https://www.tcpdump.org. Accessed: 2025-06-07.
32. A. Vetterl and R. Clayton. Bitter Harvest: Systematically Fingerprinting Low- and Medium-interaction Honeypots at Internet Scale. In *USENIX Workshop on Offensive Technologies*. USENIX Association, 2018.
33. S. Vyas, J. Hannay, A. Bolton, and P. P. Burnap. Automated cyber defence: A review. *arXiv preprint arXiv:2303.04926*, 2023.
34. J. You, S. Lv, L. Zhao, M. Niu, Z. Shi, and L. Sun. A scalable high-interaction physical honeypot framework for programmable logic controller. In *Vehicular Technology Conference*, pages 1–5. IEEE, 2020.
35. J. Zou, Z. Sun, C. Ku, X. Li, and A. Dahbura. WiP: Developing High-interaction Honeypots to Capture and Analyze Region-Specific Bot Behaviors. In *Hot Topics in the Science of Security Symposium*, 2024.

A Function coverage for S7Comm, Modbus, and HTTP

Table 9. Function coverage for S7Comm (left), Modbus (center), and HTTP (right)

S7Comm Function	Conpot	HoneyICS	PLC
Setup Communication	◐	◐	●
CPU Information	○	◐	●
CPU State	◐	◐	●
Start PLC	◐	◐	●
Stop PLC	◐	◐	●
Read Data Block	○	◐	●
Write Data Block	○	◐	●
Project Upload	○	○	●
Project Download	○	○	●

Modbus Function Code	Conpot	HoneyICS	PLC
01 (Read Coils)	◐	●	●
02 (Read Discrete Inputs)	◐	●	●
03 (Read Holding Registers)	◐	●	●
04 (Read Input Registers)	◐	●	●
05 (Write Single Coil)	◐	●	●
06 (Write Single Register)	◐	●	●
15 (Write Multiple Coils)	◐	●	●
16 (Write Multiple Registers)	◐	●	●
17 (Report Slave ID)	◐	○	○
43 (Report Device Information)	◐	○	○

HTTP Permission	Conpot	HoneyICS	PLC
CPU Diagnostics	◐	◐	●
Flash LEDs	○	○	●
Change Operating Mode	○	○	●
CPU Maintenance	○	○	●
Tag Access	○	○	●
User-Defined Web Pages	○	○	●
Filebrowser Access	○	○	●

Legend: ○= Not Supported, ◐= Partially Supported, ●= Fully Supported.

B Results

Table 10. Interactions and complexity

	Interactions	Conpot						HoneyICS1						HoneyICS2						Physical PLC					
		Min	Q1	Mdn	Q3	Max	Count	Min	Q1	Mdn	Q3	Max	Count	Min	Q1	Mdn	Q3	Max	Count	Min	Q1	Mdn	Q3	Max	Count
Corporate Network	HTTP	1	1	1	2	8003	8146	1	1	1	2	7926	7748	1	1	1	2	8021	7759	1	1	1	1	363	7047
	S7comm	1	3	3	3	4	490	1	3	3	3	4	594	1	3	3	3	7	580	1	3	3	3	4	594
	Modbus	1	1	1	1	241	510	1	1	1	2	10	382	1	1	1	2	10	339	1	1	1	1	10	354
EU	HTTP	1	1	1	2	7115	11090	1	1	1	2	7109	10620	1	1	1	2	7110	11734	1	1	1	2	7269	10921
	S7comm	1	3	3	3	8	256	1	3	3	3	4	301	1	3	3	3	4	317	1	3	3	3	4	309
	Modbus	1	1	1	1	5	314	1	1	1	1	10	334	1	1	1	1	10	345	1	1	1	1	10	320
US	HTTP	1	1	1	2	19994	10800	1	1	1	2	7112	10382	1	1	1	2	7112	10990	1	1	1	2	7365	9214
	S7comm	1	3	3	3	4	280	1	3	3	3	4	302	1	3	3	3	16	303	1	3	3	3	4	297
	Modbus	1	1	1	1	4	314	1	1	1	1	10	328	1	1	1	1	16	337	1	1	1	1	10	324
Asia	HTTP	1	1	1	2	7113	12285	1	1	1	2	12534	11658	1	1	1	2	7113	11387	1	1	1	2	7194	11199
	S7comm	1	3	3	3	4	292	1	3	3	3	16	338	1	3	3	3	4	329	1	3	3	3	4	284
	Modbus	1	1	1	1	5	349	1	1	1	1	10	349	1	1	1	1	10	327	1	1	1	1	10	316