International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Industrial Control Systems for Cyber-Security Networks in Data Science

Sushanth Chandra Addimulam

Submitted: 20/10/2023 **Revised:** 08/12/2023 **Accepted:** 12/12/2023

Abstract: Data science is the driving force behind the significant technological and operational changes that cyber security is going through in the computer world. Identifying trends or insights regarding security occurrences in cyber security data and creating a data-driven model that correlates with them are essential elements in creating an automated and intelligent safety system. This means gathering data from pertinent cyber security sources and applying analytics to improve the most recent trends based on data. The article also highlights important variables that affect the design choices made for the control, communication, redundancy, and reliability of ICS, as these aspects are crucial in figuring out the security requirements of the system. Network segmentation, access control, patches management, and security monitoring are just a few of the security countermeasures that are currently in place. Additionally, the paper investigates how machine learning methods might be integrated to improve ICS cyber security. Subsequently, we list the pros and cons of the available security solutions, talk about how to secure industrial control systems (ICSs) and implement additional security measures (like risk assessment methodologies), point out unresolved security research issues related to ICSs, and make recommendations for future directions in ICS security research.

Keywords: *Industrial control systems, threats, security, machine learning, Artificial Intelligence risk assessment.*

1. Introduction

Water treatment facilities, nuclear power reactors, and other essential infrastructures frequently use industrial control systems infrastructure, manufacturing of energy, heavy industries, and systems of distribution. The formal classification of control systems known as "ICS" encompasses a wide range of techniques, such as distributed management systems, management and data gathering systems, and other control system configurations such as PLC controllers. To achieve a range of industrial objectives (such as production and the movement of materials or energy), an ICS is a group of wireless and control elements that work together, such as mechanical, electrical, hydraulic, and pneumatic elements [1]. Many control loops, human-machine interfaces, and remote diagnostic and maintenance tools constructed using a variety of network protocols make up an ordinary industrial control system. From now on, all of its previously mentioned components shall together be collectively referred to as ICS.

SCADA systems track and regulate various components of industrial control systems by gathering data from and transmitting commands to field stations that are spread out geographically. DCS and SCADA frequently require networking in order to work together. Even though a DCS manages an industrial facility's operations, communication between the DCS and to maintain a balance between production output and the needs for delivery and distribution, the SCADA system is required. ICSs were kept off the Internet until fairly recently, a very long time ago. Numerous wireless technologies—Zigbee, Z-Wave, and Wi-Fi, as well as private networks and certain specifically created protocols like Modbus RTU and Modbus TCP, were used for communication between distant components. Other protocols for complete automation include Device Net, Actuator-sensor interface, Common Industrial Protocol, and Highway Addressable Remote Transducer Protocol. But lately, businesses have come to recognize the potential benefits associated with the Internet and the Information Technology landscape, including cloud computing.

Cloud providers provide a solution called infrastructure as a service (IaaS), which has been receiving a lot of attention lately. Such cloud-based services can be advantageous to several industries. IaaS allows for the implementation of SCADA and PLC controller instances as services using cloud-based infrastructure. For the sectors, this might result in considerable savings on infrastructure and hardware expenses. When ICSs have connections to the server and the web, they are vulnerable to the majority of cyber-attack scenarios. Furthermore, ICS equipment is not as resistant to sophisticated attacks as they are to more conventional ICS risks (such insider sabotage or catastrophic human error). Their distinctive qualities and complex threads are the reason for this.

Sr. Infrastructure and Security Engineer,
Applied Computer Techniques,
28345 Beck Road STE 308, Wixom, MI- 48393
Email: sushanth93@gmail.com

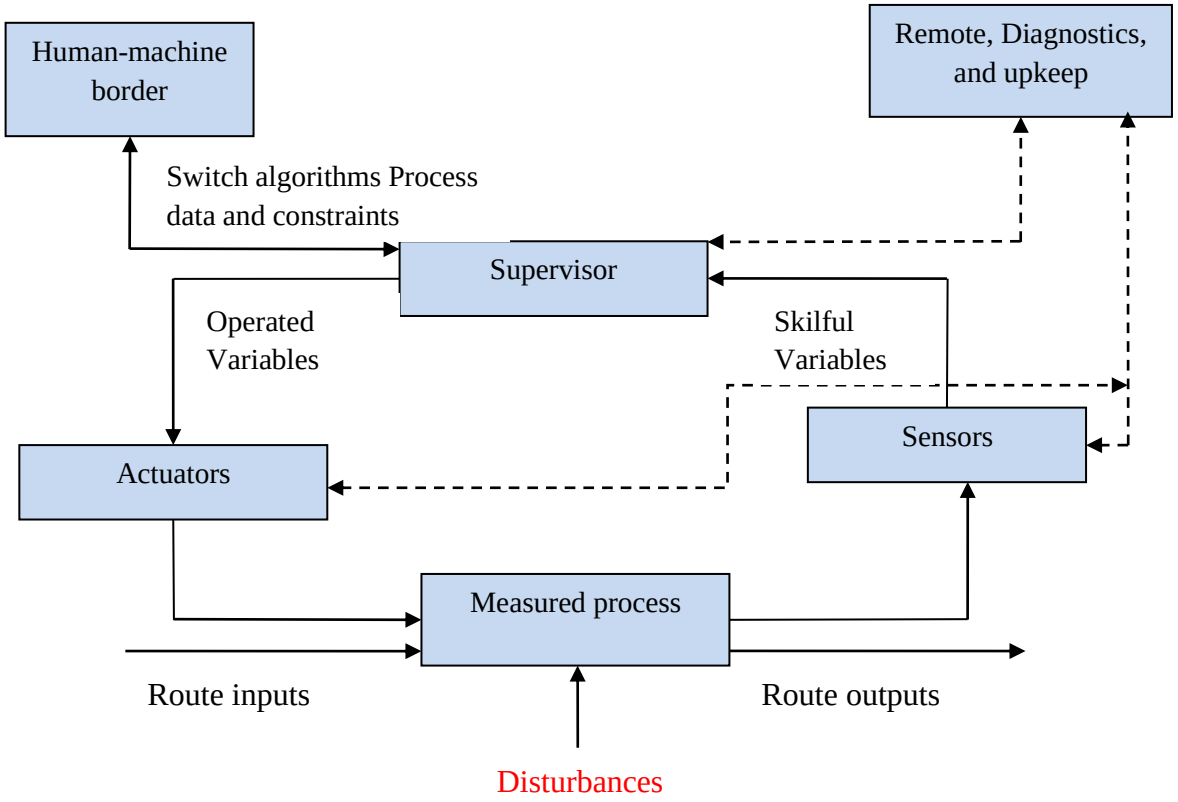

Fig. 1.1. Components of an ICS

Potential ICS-related dangers include the following:

- Advanced Persistent Threats
- The unintentional compromising of the company network
- Delay in phone and data network services
- Physical and cyber-attacks that are coordinated
- Hacktivist attacks
- Disruption or compromise in the supply chain
- Distributed Denial of Service

Scalability, affordability, and flexibility are just a few benefits of moving ICSs to the cloud. ICSs could be vulnerable to fresh attacks and weaknesses, though, if they move to the cloud in Figure 1.1. The initial goal of this paper is to demonstrate, via a few related works and the introduction of these technologies, the efficacy of using honeypots and machine learning to address the cyber security issue. The second objective of the paper is to discuss a machine learning and honeypot-based cyber security system. Our main goal is to create a smart tool that, through automatically assessing the information obtained via the honeypot and applying a variety of machine learning methods, can predict new attack profiles [2]. By combining various algorithms, the goal is to produce a predictive agent for cyber security that is accurate in representing the data and can forecast future and zero-day assaults.

The following is the arrangement of this paper. In Section 2, preliminary information and the problem statement are provided. The main conclusions drawn from the stability analysis and control syntheses are given in Section 3. A numerical example is shown in Section 4 to illustrate the effectiveness of the proposed methodology. Section 5 presents a few conclusions and ideas for further study.

2. Literature Review

Wu, J., Xing, X., et.al [3] A grid-connected system model and several solar power generation units make up a photovoltaic grid-connected system model. Following their parallel connection, active electricity is transferred to the collection station after the solar power producing units have been boosted by a step-up transformer by the system via the 110 kV gathering line. The design and simultaneous transfer of several solar power production collection branches constitute the constituents of a photovoltaic grid-connected network.

Yan, Z., Zhang, Y., et.al [4] The authors are able to examine the fault spread and cumulative effects through the use of a sequence technique, a sophisticated network model, and induced and dependent interactions between function nodes. The software complex network's function node security features are also defined and quantified. To acquire security metrics of the frequently used paths, frequent programme execution pathways are weighed and mined to comprehend software design patterns and manage the process of developing and maintaining them.

Yin, X., Zhang, S., et.al [5] Ethernet technology, currently the most extensively used network technology for communication in both the industrial and railway sectors, has been evolving at the fastest rate in recent years. A few major manufacturers of network equipment have been regularly releasing their network redundancy self-healing approaches, which aim to diminish the financial harm produced by an unexpected network failure and enhance the requirement for industrial Internet for data transmission network reliability.

Shi, D., Kou, L., et.al [6] Every node connected to the CAN bus can actively transmit and receive messages. The bus implements an arbitration method to prevent disputes when numerous nodes send messages to it simultaneously. After reading the messages on the bus, each node compares the bits from the adjudication field with the information it sent. When the invisible bit is set to 1, arbitration is lost, and the bus moves from the next bit to the receiving state until it is once again free to send messages. In the event that the dominant bit is 0, it will maintain control over the bus.

Junejo, A. K., et.al [7] Furthermore, symmetric key methods are suggested by certain studies for devices with limited resources. However, the symmetric key management procedure gets extremely intricate and complex in large-scale Fog-CPS systems. A distinct protocol must be used for session key creation and agreement in symmetric schemes. Additionally, if a symmetric key is used to encrypt short-length data, any information that is disclosed about the key could be crucial for a ciphertext-only

assault. Additionally, the confidentiality of communications between the sender and recipient may be in danger due to the compromise of CA.

Zhong, J., et.al [8] The suggested methodology, which optimises efficiency by combining cloud and edge computing, is founded on the "cloud-tube-edge-end" Internet of Things power distribution architecture used in cyber-physical energy systems. It implies a collaborative control mode that is cloud-edge. Due to the large number of delayed terminal data requests, the distribution cloud master station is unable to manage them. The Kademlia algorithm-based distributed data storage approach is advised to raise the edge intelligent terminal's data storage security. Next, we store and query all edge intelligent terminal data in the ciphertext using enhanced homomorphic encryption and secret-sharing algorithms.

Yan, S., et.al [9] an integral-based ETS, a closed-loop system with gain fluctuations, and cyberattacks are built. The stochastic cyberattacks are described by a Bernoulli variable. Legendre polynomials serve as the foundation for the construction of a novel augmented Lyapunov–Krasovskii functional. The integral term produced by integral-based ETS is handled without approximation error by the innovative Bessel-Legendre inequality and LKF.

Park, S., et.al [10] The "framework, definitions, system, hardware, and software requirements" chapter is the first. "Guidelines for the application of IEC 61511-1" is the second chapter. "Guidance for the determination of the required safety integrity levels" is the third chapter. IEC 61511 breaks down the safety standards into five distinct safety sections.

Attuluri et al. [11] has studied the privacy preservation in cloud data centres using discrete harmony search algorithm.

Attuluri et al.[12] has studied the security in cloud environment using optimized key generation using swarm intelligence.

The creation, distribution, planning, implementation, verification, testing, running, adjusting, and dismantling of an intelligent control system are some of these components. The safety requirements in IEC 61511 are comprised of 15 sections and a total of 215 controls.

3. Methods and Materials

The goal of this section is to build solutions for the design of current ICS by extending the classic ICS network design problem with security considerations.

3.1 ICS Key mechanisms

The fundamental components of ICS designs and implementations are covered in this part; these components can be applied to either DCS or SCADA alone, or to both. A later section of the chapter will cover other ICS designs.

- **Control elements:** The Control Server is the controller configuration software; it houses every application related to control logic device network installations, and various real-time monitoring services. A control network connects the control server to the control devices directly.
- **SCADA Server:** The object model for process-related facilities is known as MTU in academic works. It serves as the primary SCADA device, housing all data, control operations, and monitoring functions.
- **Remote Terminal Units:** Field devices that are commonly utilised in telemetry installations for SCADA systems. Telemetry is a highly automated communication process that allows data collection and measurement to be done remotely in locations without wired connections. RTUs transmit collected telemetry data and carry out logic operations for fundamental object control to connect items to SCADA or DCS systems in industrial facilities.
- **Programmable Logic Controller:** A PLC is described by the National Institute of Standards and Technology as "a smaller industrial computer originally utilized to perform logic functions performed by electrical hardware," it has to do with the first PLCs, which were introduced in the middle of the 1960s. These days, PLCs can handle intricate tasks in SCADA and DCS systems alike. PLCs may solve complex logic problems to regulate data produced by the control server as well as process functions. PLCs are typically connected to lower-level components like sensors and actuators in real-world installations.
- **Intelligent Electronic Procedures:** Sensitive and actuator industrial devices are capable of gathering data and sending it to PLCs, RTUs, and other monitoring services because they are intelligent enough [13]. IEDs interact with the field component of the process, where analogue communication features are necessary for IEDs to perform both local control and data acquisition.
- **Human Machine Interface:** Software that enables users to manually override control actions, modify control settings, and monitor the process on computers or specialised devices. HMIs can be directly connected to the management network or they can be SCADA server clients.
- **Data Historian:** All process records and events are collected in a single database that is connected to one or more MTUs. Some big data services let users to access a collection of information kept by historians for data analysis and enterprise-level communication.
- **Input/output Server:** To provide process data received by control devices to SCADA and control servers, IO servers are software components that collect, buffer, and grant access to the data.

3.2 Network Mechanisms:

The Enterprise, Control, and Field networks comprise the three network levels of an ICS. It is possible to create both SCADA and DCS systems with a few of the components that we previously discussed by the ICS components that were previously discussed. These components interact at different tiers. Depending upon the context of use and the topology, they are interconnected via network components. IT network components have to be modified in order to satisfy ICS criteria like as availability, performance, and so on. This is because control system components were developed to support IT-based protocols [14]. Additional explanations include integrating company networks with control networks and allowing engineers to oversee and monitor process control remotely from outside the structure for employing IT-based network solutions. The primary network elements used in ICS systems at each tier are listed below.

- **Fieldbus System:** IEDs like as actuators, sensors, and other outside devices are connected to a PLC or other controllers using the fled bus system. Sensors and field devices cannot be directly connected to PLCs when an outdoor device network is used. Devices and controllers, as well as devices themselves, communicate with each other via a variety of communication protocols.
- **Control Network:** Control servers, supervisory control, and monitoring services are connected to the controllers and RTUs through the control network.
- **Remote Access Points:** When it comes to remotely configuring, monitoring, and accessing remote equipment like RTUs and IEDs, radio-based communication devices, or RAPs is widely used in highly distributed SCADA systems.

3.3 ICS Architectures

The components of ICS implementations interact differently due to the functional context that underpins each implementation; this interaction is dictated by the communications protocols that are heavily utilised in the ICS.

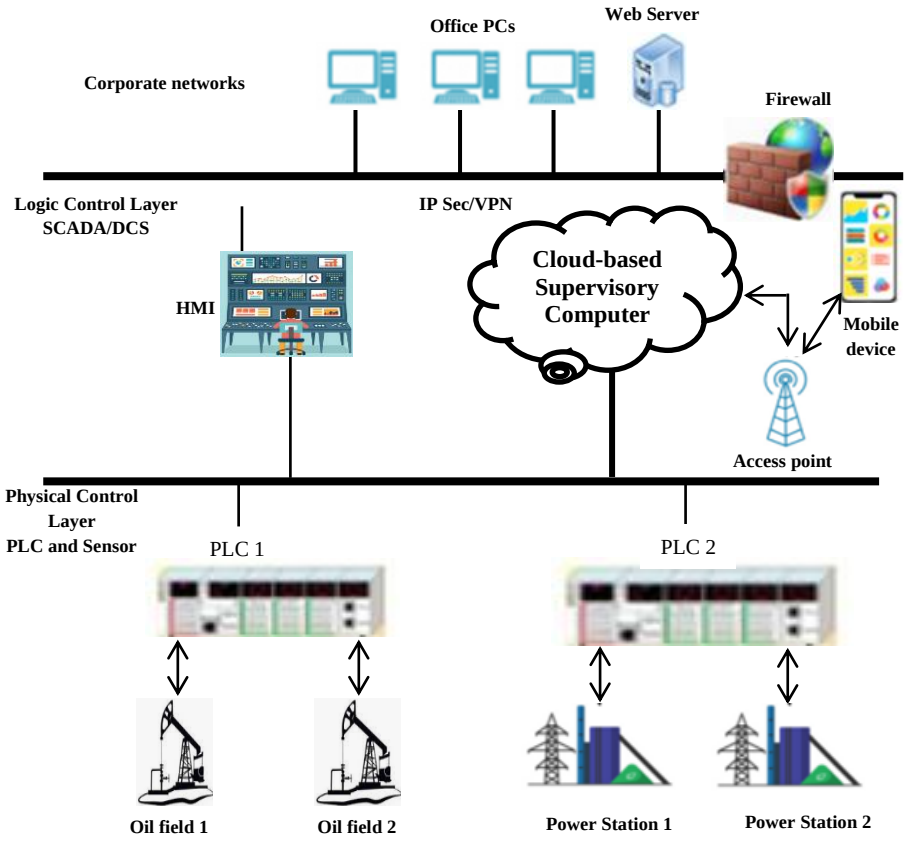

Fig. 3.1. The industrial control system

In Figure 3.1, a two-layer ICS is shown. First, the knowledge of high-level process logic needed to carry out process supervisory management is included in the logical layer. The second layer, known as the physical control layer, is made up of various sensor kinds and the control protocols that go along with them. These are utilized to provide the communication interface between sensors and actuators.

Regrettably, in recent years, threats to intrusion detection systems have grown. One such threat is social engineering, which describes malicious behaviours aimed at tricking a user into divulging private keys or passwords. With the use of the stolen data, hackers may be able to enter the intended system and perform several actions aimed at taking it down. The components of various ICS system types, devices, and communication protocols will be described in this section along with any possible security concerns.

3.1.1. Objective Function

The following is an impartial function that reduces the price of ICS connection:

$$min\left(\sum_{i\epsilon I} v_i^R g_i + \sum_{i.k\epsilon I j\epsilon J} v_{il}^B t_{il}^j d_j + \sum_{i\epsilon I j\epsilon J} \left(v_{ji}^A x_{ji} + v_{ij}^F w_{ij}\right) d_j + \sum_{i\epsilon k, r\epsilon R} v_{ir}^Z y_{ir} + \sum_{i,k\epsilon i} v_{ik}^V e_{ik}\right) \quad (1)$$

The goal function (1) takes into consideration the entire installation price of security zones and concentrators, lines of message between CSs, and security conduits. The word $\sum_{i\epsilon I} v_i^R g_i$ refers to the overall cost of installing all chosen CSs; the phrase $v_{il}^B t_{il}^j d_j$ refers to the total bandwidth expenditure incurred by TD routing between CSs, and $\left(v_{ji}^A x_{ji} + v_{ij}^F w_{ij}\right) d_j$ refers to the overall bandwidth price of terminals connected to CSs that are used for entry and outflow.

The final two factors take the cost of installing security measures into consideration: $v_{ir}^Z y_{ir}$ is the total expense of putting in security zones in CS i premises, and $v_{ik}^V e_{ik}$ is the entire cost of putting in safety conduits between CSs i and k.

3.1.2. Limitations

The following restraints are defined.

1) Access/Egress Endpoint Constraints:

$$\sum_{i\in I} x_{ji} = 1, \sum_{i\in I} w_{ij} = 1 \qquad \forall j \in J \quad (2)$$

$$x_{ji} \le a_{ji} g_i, w_{ij} \le f_{ij} g_i \quad \forall\, j \in J, i \in I. \quad (3)$$

Because of these limits, the amount of connection between access/egress request endpoints and CSs is strictly limited to one.

2) Flow Preservation Restraints:

$$x_{ji} - w_{ij} - \sum_{k\in I} \left(t_{ik}^j - t_{ik}^j\right) = 0 \quad \forall i \in I, j \in J. \quad (4)$$

These are traditional multicommodity flow conservation limitations.

3) Concentrator Capacity Constraints:

$$\sum_{i\in J} d_j \left(x_{ji} + w_{ij}\right) \le c_i \quad \forall i \in I. \quad (5)$$

These limits require that served the connection capacity of each concentrator's ingress and egress TDs must not be exceeded. Concentrator Link Capacity Constraints:

$$\sum_{j\in J} d_j t_{ik}^j \le u_{ij} b_{ij} g_i, \sum_{j\in J} d_j t_{ik}^j \le u_{ij} b_{ij} g_k \forall i, k \in I. \quad (6)$$

4) Security Zone Constraints:

$$y_{ir} \le \sum_{j\in J} \left(s_{jr}^A x_{ji} + s_{jr}^F w_{ij}\right) \forall\, i \in I, r \in R \quad (7)$$

$$\alpha^z y_{ir} \le \sum_{j\in J} \left(s_{jr}^A x_{ji} + s_{jr}^F w_{ij}\right) \forall\, i \in I, r \in R \quad (8)$$

Due to these restrictions, the aim function (1) will only take into consideration the expense of setting up a level r security zone at CS i in the event that at least one request involving an endpoint connected to i has been made and for which designers have set up a level r security zone. More precisely, the initial disparity

requires y_{ir} = 0 if $\left(s_{jr}^{A}x_{ji} + s_{jr}^{F}w_{ij}\right)$=0, whereas the next inequality needs y_{ir} to equal 1 if $\left(s_{jr}^{A}x_{ji} + s_{jr}^{F}w_{ij}\right)$ = 1. Z is a huge integer limit whose value is larger than $\max\sum_{j\in Jr\in R}\left(s_{jr}^{A}x_{ji} + s_{jr}^{F}w_{ij}\right), \forall\, i \in I$. As a result, the following limits guarantee the capacity of safety zones, i.e., safety equipment, is not exceeded, i.e.,

$$\sum_{j\in J}\left(s_{jr}^{A}x_{ji} + s_{jr}^{F}w_{ij}\right)d_j \le z_r \;\forall\, i \in I, r \in R. \quad (9)$$

6) Security Conduit Constraints:

$$e_{ik} \ge p_j t_{ik}^{j}, e_{ik} \le \alpha^{v} b_{ik} \forall\; i,l \in I, j \in J. \quad (10)$$

Because of these limits, the highest possible safety conduit level between CSs i and k must be chosen. Because requests with a given conduit level can only be sent on a connection that implements a minimum of the same degree of safety conduit, these restrictions necessitate that all requests sent on the connection (i, k) meet security conduit standards. The first inequality, in particular, sets the lower constraint of e_{ik}, which must obtain at least the greatest amount from all conduit levels p_j sent on the connection (i, k) [15]. However, the second inequality requires upper limitations for e_{ik} of the highest conduit level if b_{ik} = 1, and zero otherwise. $\alpha^{v}$is an integer limit that represents the highest degree of security conduit, i.e. α^{v} = max $p_j, j \in J$.

7) Real-Time Traffic Constraints:

$$\sum_{i\in I}\left(q_{ji}^{A}x_{ji} + qw_{ij}\right) + \sum_{i,k\in I} t_{ik}^{j}\left(q_{ik}^{K} + q_i^{V}\right) + \sum_{i\in I} q_i^{v} w_{ij} \le q_j^{N} \quad \forall\, j \in J. \quad (11)$$

The routing paths that satisfy the latency requirements provided for every demand are selected based on these constraints. Regarding each request j, the phrase $\left(q_{ji}^{A}x_{ji} + qw_{ij}\right)$ is the total of latencies for both access and egress connections, the term $\sum t_{ik}^{j}\left(q_{ik}^{K} + q_i^{V}\right)$ is the total of the latencies caused by the links between the CSs and the term $\sum q_i^{v} w_{ij}$ is the egress CS latency. These are written so that the true efficacy of the objective function results from their removal from the problem. This is a very important feature of designing networks since, in real-life situations, particularly early in the design process; it might not be possible to determine all parameter values precisely. These should therefore be considered an additional set of constraints that are applied once all latency statistics have been accurately recorded.

4. Implementation and Experimental Results

Here, we assess the suggested ICS network design approach's sensitivity to several factors, including the cost of installation, demand amount, candidate CS number, and demand and endpoint security configuration. To demonstrate the higher performance of the strategy presented in this research and the significance of control loops, we conduct an experimental comparison between the CAIA procedure and related CAIA procedures. We scheduled meetings with representatives from the local electrical grid operator and ISP to guarantee a realistic evaluation of the requirements. Talks showed that industrial networking solutions lag much behind the QoS provided by ISPs, at least when it comes to Romania. As a result, industrial operators frequently choose the cutting-edge and dependable networking solutions provided by ISPs; other businesses tend to follow this trend.

It is our assumption that the architecture will resemble a three-sectioned, expansive display. The communication network in this scenario consists of the company's own fiber optic-based communication lines (secondary network) and the channels for communication that are rented from many national ISPs, which are built using a mix of wireless and wired networks [16]. Furthermore, we assume that in comparison to other regions, a mountainous region that corresponds to REGION 1 (R1) has higher maintenance costs for primary communication lines. However, national ISPs have othxer options for connections. According to Table 1, these features have a major impact on the volume of requests that are routed in the secondary network. Table 1 shows how much it costs for conduit and bandwidth (secondary network) to route requests through it (R1).

Table 1. Demands routed within the secondary network concerning bandwidth expenses and conduit expenses

	Conduit Cost [MU]				
Bandwidth cost [MU/Mb/s]	31	61	121	211	301
2	21	21	21	21	21
6	10	10	10	10	10
11	7	7	7	7	7
16	6	6	6	6	6
21	6	6	6	6	6
27	1	3	5	5	5
31	1	3	3	3	3
41	1	1	3	3	3
51	1	1	3	3	3
81	1	1	1	3	3
101	1	1	1	1	3
124	1	1	1	1	1

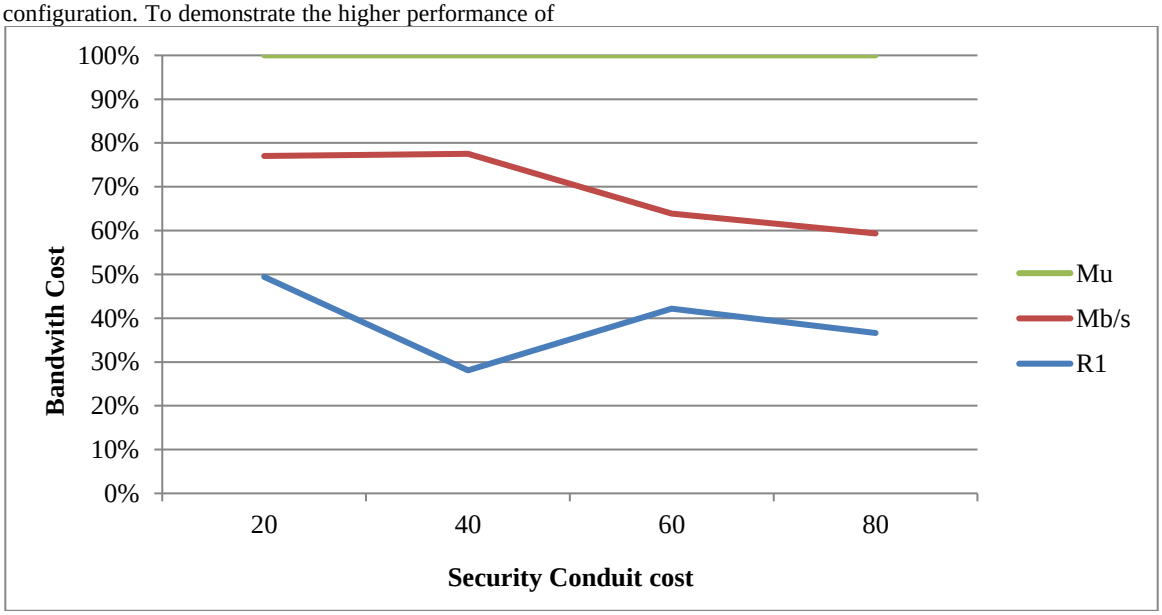

Fig. 4.1. Impact of link capacity fluctuations and security conduit expenses

The ILP model states that for cCjl = 300 MU, the removal of CSs from this network from the solution is contingent upon cBjl being at least 123 MU. This is determined by raising the cost of bandwidth units in the secondary network. However, in case cBjl is at least 26 MU, CSs from the secondary network are not included if cCjl = 30 MU in R1.Figure 4.1 shows the influence of costs on the solution, the lower bound of the needed bandwidth charges and the costs of security conduits have a linear relationship. Last but not least, it is critical to emphasise that, independent of costs or commonly chosen parameter standards, the suggested ILP paradigm makes sure that crucial real-time requirements, expressed in terms of communication delay, are met consistently.

Table 2. Impact of link volume changes on the cost of connection and the generated solution

u_{jl}[Mb/s]	N_L	N_L^A	N_S	S_B [Mb/s]	T_S [MU]
141	27	22	1	1	12281
131	28	22	1	1	12311
121	29	22	1	1	12341
111	30	22	1	1	12371
101	27	23	1	1	12551
91	26	23	1	1	12761
81	27	23	1	1	12801
71	32	24	1	1	13331
61	35	24	1	1	13741
56	36	25	5	21	16061
51	36	25	4	41	18041
46	38	25	9	81	22101
41	35	24	5	121	25741
36	51	27	12	176	32581

As Table 2 shows, the loss of capacity on all lines connecting CSs has a considerable effect on the ILP solution. The main way to solve the bandwidth shortage is to increase the number of communication lines from NL = 26 to NL = 34, starting at ujl = 140 Mb/s and going all the way down to ujl = 60 Mb/s ∀ j, l ∈ J. However, ILP model finds that, for ujl = 100 Mb/s, allocating an extra communication line with advanced conduit is more cost-effective than increasing the quantity of conduits for basic security that are used for transmission. The ILP model provides supplementary bandwidth from SB = 20 Mb/s for ujl = 55 Mb/s to SB = 176 Mb/s for ujl = 35 Mb/s, starting at ujl = 55 Mb/s ∀ j, l ∈ J. The penalties related to the additional bandwidth cost thereby raise the installation's total cost from T$ = 13 740 MU to T$ = 22.580 MU. This illustrates how the penalty fees for additional bandwidth allotments have a significant effect on the installation's overall cost.

4.1 The Quantitative Evaluation

We evaluated the CPU time performance of the ILP model using many ICS scenarios with 20, 50, and CSs can be connected to 10, 50, and 100 TDs as well as 1, 2, and 3 access/egress TD endpoints through CSs. After solving the network provisioning issue in AIMMS, we measured the execution time of CPLEX solver version 12.6. The testing was done on a Windows 7 PC with a 2.2 GHz dual-core CPU and 4.0 GB of physical RAM. The terms NI, NJ, and NT represent the number of TDs, viable CSs, and feasible TD–CS linkages, respectively, in the following. The size of the problem significantly increases the ILP model's computation time. NT has a major impact on the ILP model's performance. The fact that NT has an impact on the number of connections that are practical for admission and egress endpoints helps to explain this.

It is clear that all TD endpoints are fixed to specific CSs by enforcing NT = 1, meaning that there are no other options for connections. On the other hand, while the amount of CSs increases the calculating time, more CSs also present new connections for TDs, potentially reducing the total computing time. For instance, if NI = 60 and NT = 4, then NJ = 20 takes 46.4 seconds to compute, while NJ = 50 takes 19.52 seconds. This can be accounted for by the way ILP models behave, which is to provide new optimal solutions rather than a proportionate change in the problems' solution when parameters are changed.

Lastly, we examine how the resulting solutions are affected by gradually activating constraints. We assume that there are 30 CSs and 60 TDs in a randomly created network. Values for parameters are set up in Table 1. Originally; we were simply allowed restrictions on connectivity. Next, we progressively allow constraints related to capacity, security, and, lastly, real-time constraints. We evaluate the impact of connection features' uniform distribution on the final solution, considering their significance [17]. After testing each configuration 10 times, the average number of selected CSs is calculated, assuming that this number determines solutions. The connectivity parameters determine how many selected CSSs there are, as shown by the results in Figure 4.2. Fewer CSs are chosen when the connection probability approaches 100%.

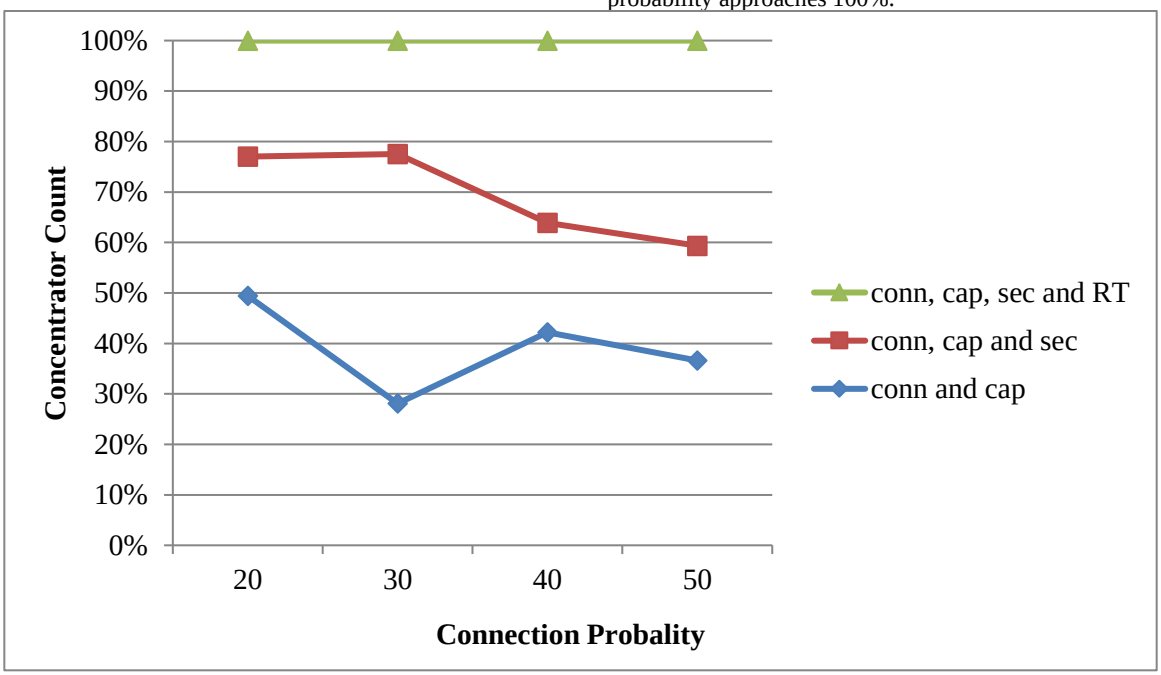

Fig. 4.2. Impact of progressively engaged limitations

Nevertheless, we find that when we activate capacity constraints—assuming 300 Mb/s of capacity—the number of CSs increases. Conversely, security constraints minimize the cost of SZC and have the opposite impact, leading to a modest drop in the number of CSs. Lastly, to guarantee that the maximum latency requirements are met, the number of chosen CSs is further reduced by turning on real-time communication limitations. These outcomes highlight the suggested ICS network design methodology's multiphase feature. In this way, after their values are accurately determined, constraints and the parameters that go along with them are triggered. However, the findings also highlight the significance of connectivity characteristics, which must be specified early in the design process. However, the precise installation features determine this information, which network designers can access in the form of device characteristics and location.

5. Conclusions

A critical strategic concern for the country's economy and people's way of life is industrial control system security. One of the primary challenges facing the ICS security arena is how to safeguard and stop malicious assaults and internal and external security threats. We examine the current state of industrial control systems both domestically and internationally in this research after learning more about the network architecture of industrial control systems. We briefly describe the prognosis for information security research in industrial control systems based on the current findings.

Customization should be expensive because security audit products cannot be harmonized for ICS. Thus it is imperative to have a uniform system for ICS security audits. This system incorporates methods to increase the industrial control system's safety level, including data collecting, anomaly detection, incident response, and troubleshooting.

Organizations possessing vital infrastructure to thwart insider threats ought to devise and execute a management system for personnel having elevated power over internal communications systems and other staff members. All workers who have a high probability of turning insiders should have their ICS activities tracked and documented. Remember that privileged account holders who are trusted with access to sensitive information could launch attacks on the ICS in addition to external sources.

References

[1] Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., &Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. *computers& security*, *89*, 101677.

[2] El Kamel, N., Eddabbah, M., Lmoumen, Y., &Touahni, R. (2020). A smart agent design for cyber security based on honeypot and machine learning. *Security and Communication Networks*, *2020*, 1-9.

[3] Wu, J., Xing, X., Wu, C., Li, B., Huang, W., Gan, P., & Zhou, H. (2020). Cyber-enabled intelligence control and security optimization for complex microgrid networks transient frequency stability analysis of power systems considering photovoltaic grid connection. *Complexity*, *2020*, 1-10.

[4] Yan, Z., Zhang, Y., Choo, K. K. R., & Xiang, Y. (2018). security measurements of cyber networks. *Security and Communication Networks*, *2018*.

[5] Yin, X., Zhang, S., Feng, L., &Xu, G. (2023). Ethernet Information Security Protocols Based on Industrial Control Wireless Sensor Networks. *Journal of Sensors*, *2023*.

[6] Shi, D., Kou, L., Huo, C., & Wu, T. (2022). A CAN Bus Security Testbed Framework for Automotive Cyber-Physical Systems. *Wireless Communications and Mobile Computing*, *2022*.

[7] Junejo, A. K., &Komninos, N. (2020). A lightweight Attribute-based security scheme for fog-enabled cyber physical systems. *Wireless Communications and Mobile Computing*, *2020*, 1-18.

[8] Zhong, J., &Xiong, X. (2021). Data security storage method for power distribution internet of things in cyber-physical energy systems. *Wireless Communications and Mobile Computing*, *2021*, 1-15.

[9] Yan, S., Nguang, S. K., & Zhang, L. (2019). Nonfragile Integral-Based Event-Triggered Control of Uncertain Cyber-Physical Systems under Cyber-Attacks. *Complexity*, *2019*, 1-14.

[10] Park, S., & Lee, K. (2014). Advanced approach to information security management system model for industrial control system. *The Scientific World Journal*, *2014*.

[11] Attuluri, S., & Ramesh, M. (2023). Multi-objective discrete harmony search algorithm for privacy preservation in cloud data centers. *International Journal of Information Technology*, 1-15.

[12] Attuluri, S., Bama, B. S., & Anand, K. (2023, June). Swarm Based Optimized Key Generation for Preserving the Privacy in Cloud Environment. In *2023 3rd International Conference on Intelligent Technologies (CONIT)* (pp. 1-5). IEEE.

[13] Asghar, M. R., Hu, Q., &Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks*, *165*, 106946.

[14] Genge, B., Haller, P., & Kiss, I. (2015). Cyber-security-aware network design of industrial control systems. *IEEE Systems Journal*, *11*(3), 1373-1384.

[15] Attaullah, H. M., Khan, R. A., & Mughal, S. (2021). Cyber security for Industrial Control System–A Survey. *iKSP Journal of Emerging Trends in Basic and Applied Sciences*, *1*(1), 15-21.

[16] Drias, Z., Serhrouchni, A., & Vogel, O. (2015, August). Analysis of cyber security for industrial control systems. In *2015 international conference on cyber security of smart cities, industrial control system and communications (ssic)* (pp. 1-8). IEEE.

[17] Yang, X., Yuan, J., Yang, H., Kong, Y., Zhang, H., & Zhao, J. (2023). A Highly Interactive Honeypot-Based Approach to Network Threat Management. *Future Internet*, *15*(4), 127.