2023 IEEE Symposium Series on Computational Intelligence (SSCI)
Mexico City, Mexico. December 5-8, 2023

Challenges and Opportunities of Computational Intelligence in Industrial Control System (ICS)

Sunzida Siddique
Daffodil International University
Dhaka, Bangladesh

Mohd Ariful haque
Clark Atlanta University
Atlanta, GA

Rakib Hossain Rifat
BRAC University
Dhaka, Bangladesh

Laxmi Rani Das
Noakhali S&T University
Noakhali, Bangladesh

Sajedul Talukder
Southern Illinois University
Illinois, USA

Syed Bahauddin Alam
University of Illinois at Urbana-Champaign
Illinois, USA

Kishor Datta Gupta
Clark Atlanta University
Atlanta, GA

***Abstract*—Artificial intelligence (AI) is not a fancy term anymore, or not limited to only researchers and academia. AI is currently becoming a part and parcel of our daily life, we are using AI/ intelligent systems by knowing or without knowing. Event product manufacturers are also trying to incorporate AI with their products to make it more preferable to consumers and trying to get the full benefit of using AI in their production and control units even for business decisions. Therefore, In our paper, we give a comprehensive survey of recent advances in Computational intelligence in industrial Control Systems and cover many usages of how industrial Control Systems are getting benefits from using Computational intelligence. We covered multiple domains like Manufacturing, Energy Management, Transportation, Food and Beverage Industry, and Pharmaceutical Industry, how these industries are utilizing multiple CI-based control systems like Programmable Logic Controllers, Distributed Control Systems, Supervisory Control and Data Acquisition, Industrial Automation, and Control Systems, Intelligent Electronic Devices and found benefits in their operations and manufacturing which helping them to focus more in innovation and improvement of their products. We believe that this survey shall be valuable to researchers across academia and industry.**

***Index Terms*—Programmable Logic Controllers, Distributed Control Systems, SCDA, Industrial Automation and Control Systems**

I. INTRODUCTION

AI is merging with industrial control systems to change various sectors. It could change and optimize manufacturing and industrial processes. The term ”Industrial Control Systems” refers to the mix of hardware and software that is used to monitor and control the operation of industrial processes and machinery [22]. Traditionally, these systems relied on pre-programmed logic and human intervention for decision-making. However, the introduction of AI technologies opens up new possibilities for automation, predictive maintenance, real-time data analysis, and overall process improvement [27]. Industrial Control Systems, which include technologies such as SCADA, DCS, and PLC, have formed the backbone of industrial automation, allowing complicated processes to be monitored and controlled [4]. AI opens up a world of new possibilities and benefits for these systems. The main reason ICS uses AI is to move from rule-based, deterministic control to data-driven, adaptive decision-making. Real-time sensor data, historical records, and other contextual information can be used by AI algorithms to optimize operations, detect possible faults, and enable autonomous decision-making [2]. This revolutionary synergy improves the operational agility and competitiveness of enterprises in a variety of industries [3].AI can predict equipment failures by analyzing sensor data and performance, enabling proactive maintenance, minimized downtime, and improved asset reliability. AI-driven anomaly detection offers real-time monitoring, enabling early deviation detection and prompt corrective steps to prevent significant failures. Furthermore, AI augments human expertise through cognitive automation, which handles difficult tasks such as natural language processing, data analysis, and decision-making with unparalleled speed and precision [14]. This human-machine collaboration provides vital insights to industrial operators, engineers, and decision-makers, allowing them to make better-educated decisions. These developments, however, bring with them new obstacles. To protect critical infrastructures from potential risks and attacks, the integration of AI in ICS demands sophisticated cybersecurity measures. Addressing ethical concerns, maintaining openness, and encouraging responsible AI use are all critical to sustaining public trust and confidence in the technologyThis comprehensive overview of Industrial Control System (ICS) Computational Intelligence advancements offers new perspectives. It emphasises industrial applications and benefits outside academic boundaries. New concepts, methods, and research areas improve knowledge of AI integration in industrial control and motivate continued research in this dynamic issue.

II. LITERATURE REVIEW

This paper [12] describes an improved intrusion detection approach for IoT-driven smart building control systems. Combining an ensemble AE-OCSVM model yields a 99.6% F1 score, resulting in an excellent intrusion detection system. However, false alarms in the OCSVM model and sporadic anomaly identification in the AE model necessitate more investigation. Future studies will try to improve model accuracy, investigate novel methodologies, and integrate ensemble methods with other unsupervised ML models to

978-0-7381-4408-5/23/$31.00 ©2023 IEEE

improve system performance. This work [8] uses machine learning to predict cardiac issues using BRFSS survey data from 400k US adults. Xgboost achieves the highest accuracy of 91.30% when tested against six models: Bagging, Random Forest, Decision Tree, K-Nearest Neighbor, and Naive Bayes. The paper, however, recognizes the limitations of relying simply on accuracy for model evaluation. Future studies will try to enhance prediction accuracy by using larger datasets and relevant features, as well as investigating additional categorization techniques such as deep learning. This article [6] presents a blockchain-based smart grid energy storage unit (ESU) charge coordination system that enhances transparency, reliability, and privacy while ensuring efficient power delivery to ESUs. It advocates for a decentralized charge coordination system with smart contracts, emphasizing the importance of a cryptocurrency-independent blockchain for widespread adoption. Future implementation will focus on utilizing blockchain technology suitable for larger smart grid applications. The paper [2] presents a voice-activated, push-button-controlled intelligent wheelchair for elderly, disabled, and patients. It increases user independence and mobility with forward, backward, left, right, and stop capabilities. The proposed model includes Arduino Mega, battery, motor driver, Bluetooth module, button switch, and car chassis. Future work involves testing, improvement, implementation, production research, and real-world deployment to enhance user mobility and freedom. The study [15] introduces FedeX, a federated anomaly detection system for Industrial Control Systems (ICS) in Smart Manufacturing (SM) based on Federated Learning (FL), achieving high performance and lightweight deployment on edge devices. FedeX outperforms existing algorithms on various criteria using liquid storage and SWAT datasets, incorporating Explainable Artificial Intelligence (XAI) for interpretable reasons. The research [3] presents an AI-powered IIoT framework for optimizing Caterpillar generator set (genset) operations, using real-time data from Modbus RTU and ML.Net. The platform aims to improve fuel efficiency, predict maintenance, and promote sustainability. Future work will explore advanced optimization algorithms for enhanced industrial efficiency. The study showcases the potential of IIoT and AI to revolutionize genset operations and boost economic rewards. The study [5] proposes a signaling game-based defense using Moving Target Defense (MTD) to combat Stealthy Link Flooding Attacks (SLFAs). The technique dynamically modifies network settings to effectively protect with minimal overhead. Testing in a Mininet-based network shows comparable SLFA protection to complex MTD systems but with less overhead.Future work will focus on extending the architecture to protect against new DDoS-based threats. [17] introduces a novel deep learning-based technique for detecting smart meter fraud and identifying possibly suspect Advanced Metering Infrastructure (AMI) relay nodes. By analyzing a large dataset of 1 million smart meter recordings, the suggested technique achieves an outstanding accuracy of 85.7% while maintaining a remarkably low false positive rate of only 5.7%. Future efforts will focus on improving the method's security capabilities and addressing dataset imbalance to improve the accuracy of detecting abnormalities and rogue nodes inside the AMI network. [16] proposes a unique automated approach for detecting paddy leaf illness in the context of Advanced Metering Infrastructure (AMI). Surprisingly, the Inception-ResNet-V2 model obtains a great accuracy of 92.68%, demonstrating its use in this application. However, it is worth noting that the model's performance may be influenced by dataset imbalance, demanding changes to maintain robustness in complicated settings. In the future, the study intends to investigate a broader range of disease types, fine-tune convolutional neural network (CNN) models, assess the efficacy of detection criteria, and conduct comparative analyses pitting Inception-ResNet-V2 against other CNN models designed for detecting plant leaf diseases. [18] proposes a unique multi-agent reinforcement learning technique for optimal UAV work distribution. The technique models the path planning problem as a multi-agent economic game, allowing for cooperative and competitive resource allocation (POIs). UAVs make judgments on movement and POI trading using Q-learning and a greedy strategy, resulting in successful work allocation. REPLANNER outperforms commonly used RL-based trajectory search techniques. Future work will concentrate on improving the training process, resolving problematic tactics, and suggesting new enhancements. [22] provides a comprehensive security architecture for Smart Healthcare Systems (SHS) based on IoT, ubiquitous computing, and machine learning. HealthGuard identifies harmful activities such as interference, fraudulent data insertion, and device manipulation. The dataset includes vital sign data from eight medical devices for both healthy and diseased people. HealthGuard incorporates four machine learning approaches (ANN, Decision Tree, Random Forest, and k-nearest Neighbor). The results demonstrate 91% accuracy and a 90% F1 score for detecting harmful activities in the Smart Healthcare System.

III. BASIC OF ICS

Complex networks with control loops, human interfaces, and remote diagnostics and maintenance tools make up Industrial Control Systems (ICS). Control loops use sensors, actuators, and controllers (PLCs) to regulate a process. The controller evaluates sensor data and generates manipulated variables for actuators to operate on [28]. Engineers and operators employ human interfaces to monitor, configure set points, control algorithms, and change controller parameters. The interfaces give real-time process status and historical data. Maintenance and diagnostics help avoid, detect, and recover from aberrant operations and breakdowns. Nested or cascade control loops have set points that depend on process variables. Continuous control loops with millisecond to minute cycle times operate throughout the operation. Figure 1 shows the fundamental operation of an ICS.

TABLE I
SUMMARY OF SELECTED STUDIES

Reference	Key Findings	Model and Accuracy	Future Work
[1]	SCADA RTU improves automation in low voltage networks by providing fault control and data gathering.The master function of	RTU, employing Ethernet controllers, ensures stable communication with digital modules.	Improve fault isolation and communication resilience, and broaden SCADA with real-time analytics for improved distribution network performance.
[2]	Voice-activated intelligent wheelchair for the aged, disabled, and patients using Arduino Mega, Bluetooth module, and other components.	Improves user movement and independence.	testing, improvement, implementation, production research, and real-world deployment.
[3]	AI-powered IIoT framework for Caterpillar genset operational optimization.	Machine Learning.Net (ML.Net)	Future research will investigate advanced optimization algorithms.
[6]	a smart grid energy storage unit charge coordination system based on blockchain.	Blockchain-based decentralized charge coordination.	Improves openness, dependability, and privacy.
[7]	Biotechnological fermentation is vital in food and beverage production, yet intelligent control faces challenges from living organisms and changing conditions.	Fuzzy logic and neural fuzzy hybrids	Enhance precision and reliability.
[8]	Machine learning-based cardiac problem prediction	Xgboost achieves 91.30% accuracy.	Utilize larger datasets.
[9]	Pipeline leakage concerns need immediate response; real-time DCS and CAO-SCADA monitoring successfully mitigates losses.	models using z-test, verifying assumptions on pipeline failure, system variations, and industrial control.	Focusing on compliance, ICT, and SCADA policies will optimize operations and reduce losses in the future.
[10]	The hybrid intelligent-classic control technique in nonlinear cyber-physical and IoT systems.	Neural network (NN)	Improving the flexibility of the intelligent estimator and evaluating performance and real-world applications.
[11]	Adaptive load-shedding solution for under-frequency load shedding in energy systems.	Iranian grid method.	try in other conditions, experimenting with modifications for improved performance.
[12]	Improved intrusion detection for IoT-driven smart buildings	AE-OCSVM model achieving 99.6% F1 score.	False alarms in OCSVM and intermittent anomaly identification.
[13]	IEDs with distributed intrusion detection improve cybersecurity in IEC 61850 networks	Proposed IEDs efficiently monitor anomalies in systems and communication (GOOSE, SV), accurately mitigating cyber threats.	Research should focus on improving simultaneous assault detection, expanding protocol coverage, and testing IEDs against sophisticated incursions on numerous devices.
[15]	Anomaly detection solution for Industrial Control Systems (ICS)	Federated Learning (FL) methods.	Will employ XAI for interpretable reasons.
[16]	Automated deep-learning algorithm for paddy leaf sickness diagnosis	Inception-ResNet-V2 achieves 92.68% accuracy.	explore more illness kinds, fine-tune models, and compare to other CNN models.
[17]	Deep learning-based technique for detecting smart meter fraud and identifying questionable AMI relay nodes.	Achieves 85.7% accuracy with a low false positive rate.	increase security capabilities, as well as address dataset imbalance.
[18]	Multi-agent reinforcement learning technique for optimal labor allocation among UAVs using Q-learning.	REPLANNER.	improve training, address difficult techniques, and suggest improvements.
[21]	Manufacturing embraces extensive network integration for control, diagnostics, safety, and e-manufacturing over the internet.	Network performance in control, diagnostics, and safety is evaluated and shown on a reconfigurable industrial testbed.	wireless network usage, integration in control and safety, changing industrial protocols, with Ethernet and wireless becoming prominent for cost-effectiveness and flexibility.
[22]	Comprehensive security architecture for Smart Healthcare Systems (SHS) based on IoT, ubiquitous computing, and machine learning.	In detecting dangerous activities, HealthGuard obtains 91% accuracy and a 90% F1 score.	boost precision.
[24]	ICS confront IoT security issues; honeypots deceive attackers while collecting data.	ICS honeypot proof-of-concept with real-time traffic, Conpot.	Hydro power plant test to validate honeypot assess attack data.
[27]	Highlights complicated industrial automation by emphasizing safety, reliability, determinism, distributed structures, explicit timing, event-triggered computation, and enhanced security.	PLC approaches support deterministic, distributed models with an emphasis on innovation	look into new programming paradigms, promoting safety, validating proposed models, and encouraging practical implementation.

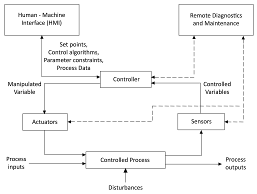
Human - Machine Interface (HMI)
Remote Diagnostics and Maintenance
Set points, Control algorithms, Parameter constraints, Process Data
Controller
Manipulated Variable
Controlled Variables
Actuators
Sensors
Process inputs
Controlled Process
Process outputs
Disturbances

Fig. 1. ICS operation

Sensors feed real-time physical parameter data to industry control systems (ICS), and actuators follow directions. To achieve objectives, the core controller processes sensor data with control algorithms. HMIs display real-time data and allow user control. Communication networks link parts. Safety systems will act immediately after data analysis stored historical monitoring data. For uninterrupted operations, ICS combines redundancy and security. These are the basic control ICS components. Several of these SCADA, DCS, and PLC components are system-specific. Feedback control system fundamental control equation:

$$e(t) = SP - PV(t) \tag{1}$$

where: $e(t)$ is the error at time t, SP is the setpoint (desired value), $PV(t)$ is the process variable (actual value) at time t.

The controller algorithm processes the error signal to calculate the controller output $CO(t)$:

$$CO(t) = f(e(t)) \tag{2}$$

where $f(e(t))$ is the control algorithm function that determines the appropriate control action based on the error.

After receiving the controller output $CO(t)$, the feedback loop ends when the actuators adjust the process variable to reach the setpoint. This basic feedback control system is the cornerstone for more advanced control methods used in industrial applications.

IV. TYPES OF ICS

Industrial Control Systems (ICS) have many varieties to handle different control tasks and functions. The following section describes the most typical industrial control systems:

1) **Programmable Logic Controllers (PLCs):** PLCs are highly advanced solid-state control systems [27] equipped with user-programmable memory. Within these memory modules, specific instructions are stored to facilitate a wide range of functions, including I/O control, logic operations, precise timing, counting, PID (Proportional-Integral-Derivative) control, communication protocols, arithmetic operations, as well as data and file processing. Figure 2 depicts the PLC Control System.
2) **Distributed Control Systems (DCS):** DCS represents a sophisticated industrial control system specifically designed for distributed operations [14]. In this approach, multiple control systems or processes operate autonomously, offering a departure from traditional centralized units. DCS relies on decentralized intelligence, allowing for efficient control and coordination of industrial processes.
3) **Supervisory Control and Data Acquisition (SCADA):** SCADA refers to computerized systems capable of acquiring and processing data, enabling operational control over vast geographical distances. SCADA [1] finds extensive applications in critical sectors like power transmission, distribution, and pipeline systems. It effectively addresses communication challenges presented by diverse media such as phone lines,

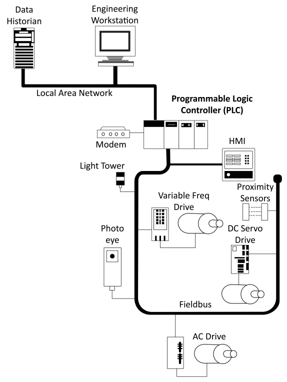

Fig. 2. PLC control System

microwaves, and satellites, ensuring seamless and reliable data exchange. Figure 3 depicts the SCADA system's General Layout.

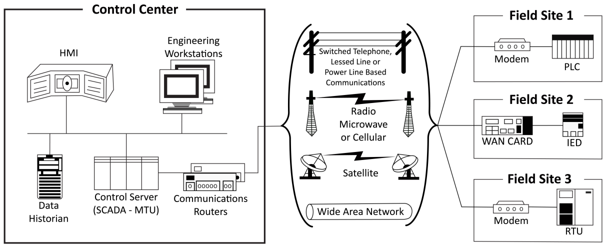

Fig. 3. SCADA System General Layout

4) **Remote Terminal Units (RTUs):** RTUs are essential microprocessor-based electronic devices integrated into Industrial Control Systems (ICS). They play a crucial role in establishing seamless connections between various hardware components and Distributed Control Systems (DCS) or SCADA [1]. Functioning as remote telemetry units, RTUs are responsible for gathering sensor data from control loops and transmitting this information to the central command of the ICS.
5) **Industrial Automation and Control Systems (IACS):** IACS solutions are characterized by their secure infrastructure, facilitating seamless information transfers and communications [26]. These systems also employ smart devices, such as sensors installed on machinery, to effectively collect data. The integration of hardware, software, and communication alternatives ensures the transformation of sensor data into actionable information for optimized decision-making.
6) **Programmable Automation Controllers (PACs):** PACs represent versatile automation controllers that encompass higher-level instructions for control and automation processes. Their application spans diverse sectors, including critical infrastructure and various industrial control systems (ICS) applications [29], making them valuable assets in enhancing efficiency and performance.
7) **Intelligent Electronic Devices (IEDs):** IEDs are electronic components equipped with integrated microprocessors, enabling digital communication through various protocols like Fieldbus and real-time Ethernet. These intelligent devices play a pivotal role [13] in enabling seamless and efficient data exchange within complex industrial control systems.

V. APPLICATION OF ICS

1) **Manufacturing Automation:** The integration of Industrial Control Systems (ICS) has revolutionized manufacturing automation [21]. This paper explores various critical aspects, including distributed control, diagnostics, and safety processes, while evaluating network performance characteristics and strategic implementation of cutting-edge network technologies within a reconfigurable factory testbed. The study also discusses emerging networking trends and challenges for future advancements.
2) **Energy Management:** Industrial Control Systems (ICS) are vital in monitoring, controlling, and optimizing energy processes in various sectors, including power plants, renewables, and smart grids. SCADA systems [19] play a crucial role in collecting real-time data, identifying inefficiencies, and ensuring reliable power supply, while smart grids integrated with ICS enable dynamic balancing and effective load management. The seamless integration empowers operators to optimize energy utilization and promote sustainability.
3) **Oil and Gas Industry:** In the oil and gas industry, ICS (Industrial Control System) plays a crucial role, with SCADA being instrumental in detecting pipeline leakages through real-time monitoring, which includes DCS and CAO-ICS Technology, minimizing losses effectively. The study conducted in Nigeria implemented [9] SCADA technology, along with DCS and CAO-ICS systems, in a specific oil and gas terminal, obtaining data through validated questionnaires and conducting z-test hypotheses. This integration of SCADA, DCS, and CAO-ICS ensures efficient pipeline monitoring, reducing leakage risks, and optimizing oil transportation, thereby enhancing overall system effectiveness and safety.
4) **Water Treatment and Distribution:** Water treatment and distribution systems rely on efficient and reliable operation, facilitated by Industrial Control Systems (ICS) integrating components like SCADA, Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), and Remote Terminal Units (RTU) [20]. These ICS components provide various advantages for water treatment and distribution:
   - **Real-Time Monitoring:** SCADA systems collect real-time data from sensors, enabling informed decisions, and optimizing efficiency, and response times.
   - **Process Optimization:** DCS and PLCs allow precise control over processes like chemical dosing, enhancing water quality and treatment efficiency.
   - **Data Analytics and Predictive Maintenance:** ICSs capture extensive data for proactive equipment maintenance, reducing downtime and ensuring uninterrupted water supply.
   - **Smart Water Management:** Integrating ICS with IoT and AI optimizes water usage, detects leakages and promotes water conservation.
5) **Transportation and Infrastructure:** Industrial Control Systems (ICS) play a vital role in transportation

and infrastructure, where their implementation ensures efficient and reliable operations. The paper [24] ”A Novel and Interactive Industrial Control System” introduces a novel ICS honeypot based on the Conpot framework, which is designed to emulate physical ICS devices and attract potential attackers for security analysis.

- **Real-Time Monitoring and Control:** ICS enables real-time data collection from distributed sensors, facilitating informed decisions, operational efficiency, and system performance improvement.
- **Increased Security:** Honeypots can be used as countermeasures in ICS to attract potential attackers, gather information, and enhance security in transportation and infrastructure.
- **Automation and Process Optimization:** ICS with PLCs and RTUs enable automation and process optimization, controlling traffic signals, water flow, and energy distribution.
- **Remote Monitoring and Management:** RTUs allow remote monitoring and issue resolution, reducing downtime and improving maintenance efficiency.

6) **Building Automation:** Industrial Control Systems (ICS) play a crucial role in building automation for climate control, lighting, and access management. Advancements in ICS technologies like BACnet and KNX enable better integration with IT networks and remote management [23]. The adoption of IP-connected and IoT-like devices expands automation in smart homes, improving operational efficiency with distributed sensors.
7) **Food and Beverage Industry:** Intelligent control systems, such as fuzzy logic [7] and neural networks, offer promising solutions for controlling and monitoring biotechnological processes like fermentation in the food and beverage sector. Neural networks estimate data in real-time, improving process performance, while fuzzy logic-based systems handle uncertainty and improve decision-making. Intelligent soft sensing and unique sensor arrays create cost-effective monitoring networks and reliable processes, boosting food and beverage product quality and efficiency.
8) **Pharmaceutical Industry:** Industrial Control Systems (ICS) play a crucial role in continuous pharmaceutical manufacturing, ensuring high-quality drug products by managing critical quality attributes (CQAs) and addressing disturbances, uncertainties, and nonlinearities. Effective start-up and shutdown procedures impact economic operation, while traceability can be achieved through residence time distributions. Employing various approaches, such as direct measurement, first principles, empirical models, and design space, enables achieving CQA specifications [25].

VI. AI BASED ICS

AI in industrial control systems combines AI concepts and technology to improve and automate industrial operations, hence improving efficiency, productivity, and safety in a variety of industries. It uses AI algorithms to evaluate data, make choices, and automate processes, resulting in enhanced performance and streamlined operations [10]. AI is able to forecast equipment failures by examining sensor data and maintenance logs, enabling proactive maintenance to cut downtime and increase overall equipment effectiveness. Real-time AI algorithms optimize resource allocation and control parameters in complicated industrial processes to boost productivity and lower energy use. AI-based control systems can detect abnormalities and departures from typical behavior, enabling prompt reactions to avert system failures or mishaps. By examining sensor data to satisfy predetermined standards, AI keeps an eye on and maintains product quality. AI permits the creation of autonomous industrial systems that can carry out operations and make decisions without the involvement of a direct human. By anticipating demand, controlling inventory levels, and streamlining logistics and transportation routes, AI improves supply chain operations [6].

VII. CHALLENGES AND OPPORTUNITIES OF ICS

Industrial Control Systems (ICS) are crucial in modern industries. However, ensuring their secure and efficient operation poses challenges due to insufficient security in current infrastructures. Common countermeasures are ineffective, leaving ICS facilities vulnerable to attacks. The complex nature of ICS further complicates the detection of known and unknown threats. Despite challenges, opportunities exist to improve ICS security. Architectures show repetitive communication patterns, aiding anomaly detection and pattern recognition. Analyzing application logs using pattern mining helps detect potential anomalies. Integrating ICS with public networks introduces new cybersecurity challenges, increasing vulnerability to attacks. Researchers propose advancements in architecture, policies, system scanning, authentication, access control, encryption, and intrusion detection. The integration of Information and Communication Systems (ICS) with advanced technologies such as the Internet of Things (IoT) presents opportunities for enhancing manufacturing processes. The criticality of maintaining a balance between opportunities and challenges in the realm of cybersecurity cannot be overstated. Ongoing investigation and advancement in the field of Industrial Control Systems (ICS) security are imperative in order to proactively address the ever-changing landscape of potential threats and guarantee the integrity and dependability of these systems. Enhancing the security of Industrial Control Systems (ICS) is achieved by a combination of comprehensive data analysis, the implementation of appropriate detection systems, and fostering collaboration within the sector.

VIII. CONCLUSION AND FUTURE WORK

The incorporation of AI in Industrial Control Systems (ICS) has opened unparalleled possibilities for industrialization, machine learning-based maintenance, and simultaneous data analysis, intensifying functioning resilience and competitiveness across industries. Predictive maintenance, AI-driven outlier identification, and AI-driven automation are among the crucial applications propelling this transformation. However, to effectively utilize the advantages of AI in ICS, executing cybersecurity measures, moral considerations, and accountable AI utilization is fundamental to ensure public faith and assurance in this technology. The limitation of the paper is not an applied AI Model. Future research could concentrate on creating different interpretable AI models and techniques based on ICS, contributing to further advancements in the field and enhancing the potential of AI in industrial control systems. Additional research could also explore the integration of AI with adaptive control strategies to enhance the adaptability and efficiency of ICS applications, making them more robust and effective in dynamic industrial environments.

IX. Acknowledgement

This research is funded in part by NSF Grants No. 2306109, and DOEd Grant P116Z220008 (1). Any opinions, findings, and conclusions expressed here are those of the author(s) and do not reflect the views of the sponsor(s).

References

[1] Musse Mohamed Ahmed and WL Soo. Supervisory control and data acquisition system (scada) based customized remote terminal unit (rtu) for distribution automation system. In *2008 IEEE 2nd International Power and Energy Conference*, pages 1655–1660. IEEE, 2008.

[2] Md Abdullah Al Rakib, Salah Uddin, Md Moklesur Rahman, Shantanu Chakraborty, and Fysol Ibna Abbas. Smart wheelchair with voice control for physically challenged people. *European Journal of Engineering and Technology Research*, 6(7):97–102, 2021.

[3] Ali S Allahloh, Mohammad Sarfraz, Atef M Ghaleb, Abdullrahman A Al-Shamma'a, Hassan M Hussein Farh, and Abdullah M Al-Shaalan. Revolutionizing ic genset operations with iiot and ai: A study on fuel savings and predictive maintenance. *Sustainability*, 15(11):8808, 2023.

[4] Mehmed asch Schaalan. *Air Supply for Industrial Process (PLC, SCADA DCS) - The Start of Industrial Automation Systems Evolution*, page 91. 01 2008.

[5] Abdullah Aydeger, Mohammad Hossein Manshaei, Mohammad Ashiqur Rahman, and Kemal Akkaya. Strategic defense against stealthy link flooding attacks: A signaling game approach. *IEEE Transactions on Network Science and Engineering*, 8(1):751–764, 2021.

[6] Mohamed Baza, Mahmoud Nabil, Muhammad Ismail, Mohamed Mahmoud, Erchin Serpedin, and Mohammad Ashiqur Rahman. Blockchain-based charging coordination mechanism for smart grid energy storage units. In *2019 IEEE international conference on blockchain (blockchain)*, pages 504–509. IEEE, 2019.

[7] S Birle, MA Hussein, and T Becker. Fuzzy logic control and soft sensing applications in food and beverage processes. *Food Control*, 29(1):254–269, 2013.

[8] Ranjit Chandra Das, Madhab Chandra Das, Md Amzad Hossain, Md Ashiqur Rahman, Md Helal Hossen, and Rakibul Hasan. Heart disease detection using ml. In *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0983–0987. IEEE, 2023.

[9] Akinwale Eso and Omorogiuwa Eseosa. Real-time effective monitoring and control in oil and gas industry using scada technology as a management tool. *Journal of Alternative and Renewable Energy Sources*, 8(2):22–38, 2022.

[10] Faezeh Farivar, Mohammad Sayad Haghighi, Alireza Jolfaei, and Mamoun Alazab. Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial iot. *IEEE Transactions on Industrial Informatics*, 16(4):2716–2725, 2020.

[11] Mohammad Hosein Fazaeli, Mohammad Mostafa Keramat, Hashem Alipour, et al. New adaptive decentralize under frequency load-shedding algorithm. In *2020 15th International Conference on Protection and Automation of Power Systems (IPAPS)*, pages 104–107. IEEE, 2020.

[12] Nur Imtiazul Haque and Mohammad Ashiqur Rahman. 287 artificial intelligence-assisted security analysis of smart healthcare systems. *AI, Machine Learning and Deep Learning: A Security Perspective*, pages 287–311, 2023.

[13] Junho Hong and Chen-Ching Liu. Intelligent electronic devices with collaborative intrusion detection systems. *IEEE Transactions on Smart Grid*, 10(1):271–281, 2017.

[14] Arkadiusz Hulewicz, Zbigniew Krawiecki, and Krzysztof Dziarski. Distributed control system dcs using a plc controller. In *ITM Web of Conferences*, volume 28, page 01041. EDP Sciences, 2019.

[15] Truong Thu Huong, Ta Phuong Bac, Kieu Ngan Ha, Nguyen Viet Hoang, Nguyen Xuan Hoang, Nguyen Tai Hung, and Kim Phuc Tran. Federated learning-based explainable anomaly detection for industrial control systems. *IEEE Access*, 10:53854–53872, 2022.

[16] Md Ashiqul Islam, Md Nymur Rahman Shuvo, Muhammad Shamsojjaman, Shazid Hasan, Md Shahadat Hossain, and Tania Khatun. An automated convolutional neural network based approach for paddy leaf disease detection. *International Journal of Advanced Computer Science and Applications*, 12(1), 2021.

[17] AHM Jakaria, Mohammad Ashiqur Rahman, and Md Golam Moula Mehedi Hasan. Safety analysis of ami networks through smart fraud detection. In *2019 IEEE Conference on Communications and Network Security (CNS)*, pages 1–7. IEEE, 2019.

[18] Alvi Ataur Khalil, Alexander J Byrne, Mohammad Ashiqur Rahman, and Mohammad Hossein Manshaei. Replanner: Efficient uav trajectory-planning using economic reinforcement learning. In *2021 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 153–160. IEEE, 2021.

[19] Nitasha Khan, Zeeshan Shahid, Muhammad Mansoor Alam, Aznida Abu Bakar Sajak, MS Mazliham, Talha Ahmed Khan, Ali Rizvi, Syed Safdar, et al. Energy management systems using smart grids: An exhaustive parametric comprehensive analysis of existing trends, significance, opportunities, and challenges. *International Transactions on Electrical Energy Systems*, 2022, 2022.

[20] Aditya P Mathur and Nils Ole Tippenhauer. Swat: A water treatment testbed for research and training on ics security. In *2016 international workshop on cyber-physical systems for smart water networks (CySWater)*, pages 31–36. IEEE, 2016.

[21] James R Moyne and Dawn M Tilbury. The emergence of industrial control networks for manufacturing control, diagnostics, and safety data. *Proceedings of the IEEE*, 95(1):29–47, 2007.

[22] AKM Iqtidar Newaz, Amit Kumar Sikder, Mohammad Ashiqur Rahman, and A Selcuk Uluagac. Healthguard: A machine learning-based security framework for smart healthcare systems. In *2019 sixth international conference on social networks analysis, management and security (SNAMS)*, pages 389–396. IEEE, 2019.

[23] Thomas Novak and Andreas Gerstinger. Safety-and security-critical services in building automation and control systems. *IEEE Transactions on Industrial Electronics*, 57(11):3614–3621, 2009.

[24] Dimitrios Pliatsios, Panagiotis Sarigiannidis, Thanasis Liatifis, Konstantinos Rompolos, and Ilias Siniosoglou. A novel and interactive industrial control system honeypot for critical smart grid infrastructure. In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pages 1–6. IEEE, 2019.

[25] Jukka Rantanen and Johannes Khinast. The future of pharmaceutical manufacturing sciences. *Journal of pharmaceutical sciences*, 104(11):3612–3638, 2015.

[26] Luis Rosa, Tiago Cruz, Miguel Borges de Freitas, Pedro Quitério, João Henriques, Filipe Caldeira, Edmundo Monteiro, and Paulo Simões. Intrusion and anomaly detection for the next-generation of industrial automation and control systems. *Future Generation Computer Systems*, 119:50–67, 2021.

[27] Martin A Sehr, Marten Lohstroh, Matthew Weber, Ines Ugalde, Martin Witte, Joerg Neidig, Stephan Hoeme, Mehrdad Niknami, and Edward A Lee. Programmable logic controllers in the context of industry 4.0. *IEEE Transactions on Industrial Informatics*, 17(5):3523–3533, 2020.

[28] Keith Stouffer, Joe Falco, Karen Scarfone, et al. Guide to industrial control systems (ics) security. *NIST special publication*, 800(82):16–16, 2011.

[29] Tomasz Żabiński. Implementation of programmable automation controllers-promising perspective for intelligent manufacturing systems. *Management and Production Engineering Review*, 1(2):56–63, 2010.