ADVANCED CONTROL SYSTEMS IN INDUSTRIAL INSTRUMENTATION : A COMPREHENSIVE SURVEY

[1]Sejal Dilipkumar Patel, [2]Manoj D. Khediya
[1]Lecturer, [2]Assistant Professor
Instrumentation and Control Engineering
Government Polytechnic Gandhinagar
Vishwakarma Government Engineering College Chandkheda
Gujarat Technological University

Abstract

This paper presents a comprehensive survey of control systems in industrial instrumentation, examining developments in factory automation, process control, embedded systems, and emerging technologies from 2000 to early 2018. The study analyzes proportional-integral-derivative (PID) controllers, model predictive control (MPC), adaptive control techniques, industrial communication networks, Industrial Internet of Things (IIoT) integration, and cybersecurity frameworks. Through systematic analysis, we identify key technological advancements including IT/OT convergence, edge computing, wireless sensor networks, and energy efficiency optimization. The survey reveals that while classical PID control dominates with over 95% adoption in industrial loops, advanced techniques like MPC and adaptive fuzzy control are gaining traction in multivariable constrained systems. We examine the evolution from proprietary fieldbuses to industrial Ethernet and wireless standards (WIA-FA, Wireless HART), cybersecurity challenges addressed by IEC 62443, and energy management strategies achieving 10-15% efficiency improvements. This work provides a foundational reference for researchers and practitioners navigating the convergence of control theory, communication engineering, and cybersecurity in modern industrial automation.

Keywords: Control Systems, PID Control, Model Predictive Control, Industrial Automation, IIoT, Cybersecurity, Industrial Ethernet, Energy Efficiency, SCADA Systems, Embedded Control

1. INTRODUCTION

Control systems in instrumentation have undergone remarkable transformation over the past two decades, evolving from conventional standalone controllers to sophisticated networked cyber-physical systems[1]. The convergence of information technology (IT) and operational technology (OT) has redefined industrial automation paradigms, enabling unprecedented levels of connectivity, intelligence, and operational efficiency[2]. Modern industrial landscapes demand control systems that are precise, reliable, adaptive, secure, and energy-efficient [3], [4].

The rapid proliferation of embedded controllers, industrial communication protocols, and intelligent sensors has created a complex ecosystem requiring systematic analysis[5]. Factory automation, process industries, robotics, and motion control applications increasingly rely on advanced control algorithms integrated with cutting-edge sensing technologies, high-speed communication networks, and cloud-based analytics[6] . These developments have been accelerated by the emergence of the Industrial Internet of Things (IIoT), promising to revolutionize manufacturing through data-driven decision-making and predictive maintenance strategies[7], [8]. This survey aims to provide comprehensive coverage of control system technologies developed between 2000 and early 2018, compare various control strategies, analyze communication infrastructure evolution, examine cybersecurity challenges, investigate energy efficiency techniques, and identify future research directions.

2. EVOLUTION OF INDUSTRIAL CONTROLLERS AND EMBEDDED SYSTEMS

2.1 Controller Architecture Evolution

Industrial controllers have evolved from pneumatic and relay-based systems to sophisticated microprocessor-based platforms capable of executing complex algorithms in real-time[9]. The transition from Programmable Logic Controllers (PLCs) to Distributed Control Systems (DCS) and advanced embedded controllers represents a fundamental shift in automation architecture[10].

The evolution can be characterized by four key phases:

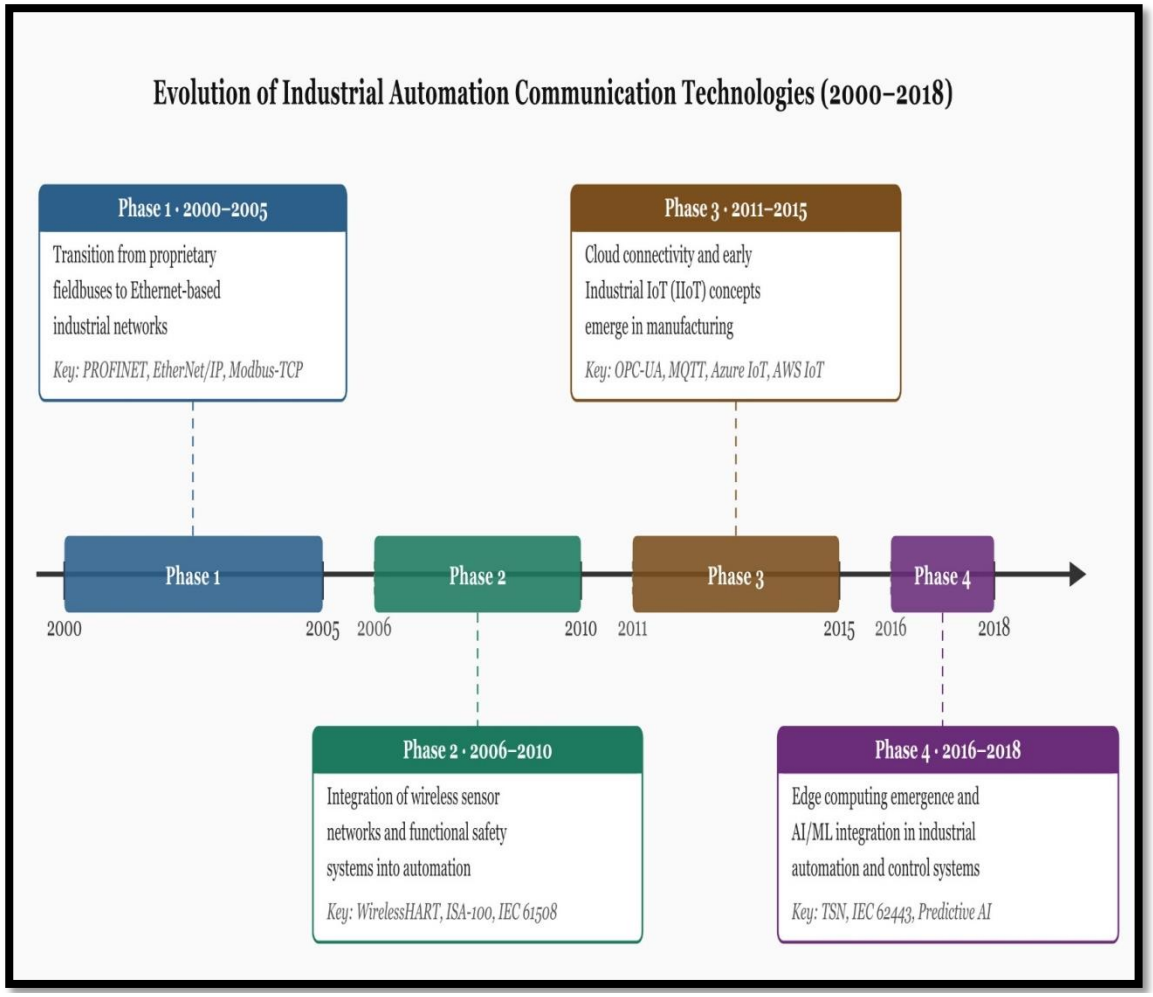

Figure 1 Controller Architecture Evolution

2.2 Embedded Control Architectures

Embedded control systems integrate sensing, computation, and actuation within compact, dedicated hardware platforms characterized by real-time performance requirements and resource constraints[11]. Key applications span factory automation control for manufacturing execution and assembly line operations, process control systems in chemical processing and power generation, motion control for servo systems and CNC machines, and robotics control integrating trajectory planning and sensor fusion[12].

Edge computing represents a paradigm shift where computational intelligence is distributed to field devices and controllers rather than centralized infrastructure, reducing latency to sub-millisecond response times while enhancing reliability through autonomous operation during network failures [13]. Edge computing had emerged as a critical enabler for time-critical industrial applications requiring deterministic performance[14].

3. ADVANCED CONTROL STRATEGIES

3.1 Proportional-Integral-Derivative Control

PID control remains the workhorse of industrial automation, accounting for more than 95% of all control loops in process industries as of today [15]. The enduring popularity stems from simplicity, robustness, and effectiveness across diverse applications.

The classical PID controller computes the control signal as:

$$u(t) = K_p e(t) + K_i \int_0^t e(\tau)d\tau + K_d \frac{de(t)}{dt}$$

where K_p, K_i, and K_d represent proportional, integral, and derivative gains respectively, and $e(t)$ is the error signal.

Several enhanced PID architectures addressed limitations of classical implementations including adaptive PID with self-tuning mechanisms, gain scheduling with multiple parameter sets, cascade PID for improved disturbance rejection, feedforward-feedback combinations, and fuzzy PID integration for nonlinear gain adaptation[16].

Method	Description
Ziegler-Nichols	Classical frequency-response method using ultimate gain and period
Cohen-Coon	Process reaction curve method for first-order plus dead-time models
Lambda Tuning	Specifies desired closed-loop time constant for systematic design
IMC Tuning	Internal Model Control approach providing robustness-performance tradeoff
Auto-tuning	Automated identification and tuning using relay feedback tests

Table 1: Common PID tuning methods in industrial practice

3.2 Model Predictive Control

Model Predictive Control emerged as a powerful advanced control technique particularly suited for multivariable constrained system [17] . MPC uses explicit process models to predict future behavior and optimize control actions over a finite horizon[18].

At each sampling instant, MPC solves an optimization problem:

$$\min_u \sum_{k=0}^{N_p} \|y(k) - r(k)\|_Q^2 + \sum_{k=0}^{N_c-1} \|u(k)\|_R^2 + \sum_{k=0}^{N_c-1} \|\Delta u(k)\|_S^2$$

subject to constraints on inputs, rate changes, and outputs, where N_p is the prediction horizon, N_c is the control horizon, and Q, R, S are weighting matrices[. This optimization yields a sequence of control moves, but only the first is implemented following the receding horizon principle.

MPC had been successfully deployed in refineries, chemical plants, and power generation facilities, demonstrating measurable benefits including 3-8% reduction in energy consumption, 2-5% increase in throughput, 15-30% reduction in product quality variability, and improved constraint handling reducing safety incidents[19].

3.3 Adaptive and Fuzzy Logic Control

Adaptive control systems modify parameters in real-time to maintain optimal performance despite changing process dynamics [20]. Fuzzy Logic Systems provide an alternative approach capturing expert knowledge and handling nonlinear, uncertain systems without precise mathematical models[21].

Adaptive controllers typically consist of process identification for real-time parameter estimation, control design calculating parameters based on current models, and modification mechanisms adjusting controller structure. Common approaches include Model Reference Adaptive Control (MRAC), Self-Tuning Regulators (STR), and gain scheduling[22].

Fuzzy logic controllers use linguistic rules to implement control strategies of the form: IF error is A_i AND error rate is B_j THEN control output is C_{ij}, where fuzzy sets define membership functions for linguistic variables[16]. The integration of fuzzy logic with adaptive mechanisms creates hybrid controllers capable of handling significant uncertainties, finding applications in mobile robotics, process control, and motion systems during 2015-2018[23].

4. INDUSTRIAL COMMUNICATION TECHNOLOGIES

4.1 Industrial Ethernet Protocols

Industrial Ethernet protocols including PROFINET, EtherNet/IP, EtherCAT, and Modbus TCP had become dominant communication standards, providing deterministic, high-bandwidth connectivity suitable for real-time control applications[24].

Protocol	Organization	Standard	Applications
PROFINET	PROFIBUS International	IEC 61158	Factory automation, process control
EtherNet/IP	ODVA	IEC 61158	Discrete manufacturing, automotive
EtherCAT	EtherCAT Technology Group	IEC 61158	Motion control, robotics
Modbus TCP	Modbus Organization	Open	Process monitoring, building automation

Table 2: Major Industrial Ethernet protocols and their characteristics

Industrial Ethernet protocols achieve deterministic performance through various mechanisms. PROFINET uses Isochronous Real-Time (IRT) with time slicing for deterministic cycles, EtherNet/IP employs Common Industrial Protocol with scheduled messaging, EtherCAT implements on-the-fly processing with logical ring topology, and POWERLINK uses time-division multiple access for guaranteed cycles[25].

4.2 Wireless Industrial Communications

Wireless Industrial Communication Networks emerged as viable alternatives and complements to wired infrastructure[26]. Standardized as IEC 62948 in 2018, WIA-FA provides IEEE 802.11-based wireless communication specifically designed for factory automation with deterministic performance guarantees through frequency hopping for interference robustness, time-division scheduling for determinism, multi-channel support for scalability, and redundancy mechanisms for reliability[27].

Process automation applications adopted WirelessHART (IEC 62591) and WIA-PA (IEC 62601) based on IEEE 802.15.4 for sensor networking and field device connectivity, providing mesh networking for extended coverage, channel hopping for interference mitigation, time-synchronized operation, and self-organizing capabilities[28].

Application Domain	Latency	Reliability	Update Rate
Motion control	< 1 ms	99.999%	1-4 kHz
Discrete automation	< 10 ms	99.99%	10-100 Hz
Process control	< 100 ms	99.9%	1-10 Hz
Monitoring	< 1 s	99%	0.1-1 Hz

Table 3: Communication performance requirements for industrial applications [3]

4.3 Time-Sensitive Networking

IEEE 802.1 Time-Sensitive Networking standards were under development to enable converged networks supporting both real-time control and IT traffic on shared Ethernet infrastructure. Key TSN features include IEEE 802.1AS for precise time synchronization, IEEE 802.1Qbv for deterministic traffic scheduling, IEEE 802.1Qbu for frame preemption enabling low-latency traffic, and IEEE 802.1CB for seamless redundancy failover [29].

5. Industrial Internet of Things Integration

5.1 IIoT Architecture and IT/OT Convergence

The Industrial Internet Consortium, formed in 2014, established frameworks and guidelines for IIoT deployment, publishing comprehensive security frameworks and networking guidelines by 2016-2018[14]. The IIC Reference Architecture defines a standards-based open architecture comprising business, usage, functional, and implementation viewpoints.

The convergence of Information Technology and Operational Technology represents one of the most significant trends in industrial automation, enabling seamless data flow from field devices to enterprise systems, cloud-based analytics for process optimization, remote monitoring and predictive maintenance, and real-time performance visibility across organizational hierarchies[11].

Key challenges in IT/OT convergence include cultural differences where IT focuses on information security while OT prioritizes safety and availability, lifecycle mismatches with IT systems refreshing every 3-5 years versus OT assets operating 15-30 years, technology gaps where legacy protocols lack security features, skill shortages with few professionals understanding both domains, and OT requirements for deterministic real-time performance[30].

5.2 IIoT Communication Protocols

Protocol	Transport	Application	Characteristics
OPC UA	TCP/IP	Industrial automation	Security, information modeling, interoperability
MQTT	TCP/IP	IoT messaging	Publish-subscribe, lightweight, QoS levels
CoAP	UDP/IP	Constrained devices	RESTful, low overhead, resource discovery
DDS	UDP/IP	Real-time systems	Data-centric, QoS policies, discovery

Table 4: IIoT communication protocols and characteristics

Cloud platforms provided industrial applications with access to artificial intelligence and machine learning for pattern recognition and anomaly detection, big data analytics for historical analysis across multiple plants, digital twin technologies as virtual replicas of physical assets, collaborative platforms for engineering tools, and scalable computing resources for computational-intensive tasks[31].

The optimal IIoT architecture distributes computing across the edge-cloud continuum with field edge handling real-time control and safety functions, plant edge performing aggregation and local analytics, enterprise edge enabling multi-plant coordination, and public cloud supporting AI/ML training and long-term analytics[32].

6. Cybersecurity in Industrial Control Systems

6.1 Threat Landscape and Major Incidents

Industrial Control Systems and SCADA networks face increasing cybersecurity threats as connectivity expands[1]. The convergence of IT and OT networks exposes previously isolated control systems to malware designed to disrupt processes, unauthorized access through compromised connections, denial of service attacks, software vulnerability exploitation in legacy systems, man-in-the-middle attacks on insecure protocols, and insider threats.

Incident	Year	Impact
Stuxnet[33]	2010	Damaged Iranian nuclear centrifuges via PLC exploitation
Havex[34]	2013	Targeted energy sector with ICS-specific reconnaissance
BlackEnergy[35]	2015	Ukrainian power grid attack causing blackouts
Industroyer[36]	2016	Directly controlled electrical substation switches
TRITON/TRISIS[37]	2017	Targeted safety instrumented systems in petrochemical plant

Table 5: Major ICS cybersecurity incidents prior to 2018

6.2 Security Frameworks and Standards

The IIC Security Framework, published in draft form in 2016, provided comprehensive guidelines for securing IIoT and industrial control systems. IEC 62443 (formerly ISA-99) addresses protection of critical infrastructure through four main categories: General (concepts, terminology, metrics), Policies and

Procedures (security program requirements), System (security requirements, zones and conduits), and Component (product development requirements)[38].

IEC 62443 defines four security levels: SL 1 for protection against casual violation, SL 2 against intentional violation using simple means, SL 3 against sophisticated means with moderate resources, and SL 4 against sophisticated means with extended resources[39].

Essential cybersecurity measures include network segmentation isolating ICS networks from IT environments, DMZ implementation for controlled data exchange, defense in depth with multiple security layers, identity and access management with multi-factor authentication, intrusion detection systems for network and host-based detection, security information and event management for unified visibility, and application whitelisting allowing only authorized applications to execute[40].

6.3 Emerging Security Technologies

Emerging technologies for ICS cybersecurity included AI/ML-based threat detection using behavioral analysis for anomalous activities, software-defined perimeters with micro-segmentation, advanced packet inspection analyzing industrial protocol traffic, blockchain for tamper-proof audit trails, and security by design with embedded features in new ICS products[40].

7. ENERGY EFFICIENCY IN INDUSTRIAL CONTROL SYSTEMS

7.1 Energy Monitoring and Measurement

Energy efficiency emerged as a critical concern in industrial automation, with monitoring systems enabling measurement, analysis, and optimization of energy consumption[41]. Advanced energy monitoring systems integrated with SCADA platforms provided real-time visibility into energy usage across manufacturing facilities.

Comprehensive energy management systems include smart meters and sensors for device-level measurement, data acquisition systems with PLCs and RTUs, communication infrastructure for data transmission, analytics platforms for real-time analysis and predictive modeling, visualization dashboards showing consumption and efficiency metrics, and automated control for load scheduling and demand response[42].

7.2 Control Strategies for Energy Optimization

Energy-efficient control strategies implemented till date included load management through scheduling equipment during off-peak periods, load shedding curtailing non-critical loads during peaks, load balancing distributing consumption evenly, and peak shaving using on-site generation or storage[43].

Equipment optimization employed variable speed drives adjusting motor speeds to match load requirements typically saving 20-50% energy, compressor control optimizing compressed air systems, HVAC optimization adjusting based on occupancy and process needs, and pump optimization coordinating multiple pumps for efficiency[43].

Process optimization utilized predictive control using forecasts to optimize energy usage, multi-objective optimization balancing production, quality, and energy objectives, heat recovery capturing and reusing waste heat, and batch optimization scheduling operations for energy efficiency[44].

Indicator	Definition
Specific Energy Consumption (SEC)	Energy consumed per unit of production
Energy Intensity	Energy consumption relative to output value
Power Factor	Ratio of real power to apparent power
Overall Equipment Effectiveness (OEE)	Composite of availability, performance, and quality
Energy Cost per Unit	Total energy cost divided by production quantity

Table 6: Common energy performance indicators in industrial settings

Smart grid initiatives enabled industrial facilities to participate in demand response programs where control systems automatically adjusted consumption in response to price signals from electricity markets, grid frequency deviations, capacity shortage alerts, and renewable energy availability peaks[45].

8. COMPARATIVE ANALYSIS AND TECHNOLOGY MATURITY

8.1 Control Strategy Comparison

Strategy	Complexity	Multi-variable	Computation	Adoption
Classical PID	Low	Poor	Very Low	Very High (>95%)
Adaptive PID	Moderate	Limited	Low	Moderate
Cascade PID	Moderate	Good	Low	High
MPC	High	Excellent	High	Growing
Fuzzy Logic	Moderate	Good	Moderate	Niche
Adaptive Fuzzy	High	Good	Moderate-High	Limited

Table 7: Comparative analysis of control strategies[46]

Different control architectures suit specific application domains. Discrete manufacturing benefits from PLCs with fast scan cycles and industrial Ethernet due to proven reliability. Process industries utilize DCS with advanced control including MPC for superior multivariable performance. Motion control requires specialized controllers with EtherCAT or SERCOS III for deterministic performance. Batch processing benefits from ISA-88 compliant systems with flexible PID and logic control. Robotics employs embedded controllers with real-time operating systems and specialized motion planning algorithms[47].

8.2 Technology Maturity Assessment

Technologies can be categorized by maturity level with diverse advancements. Mature technologies with widespread deployment include PID control, PLCs, DCS, Industrial Ethernet, and HMI/SCADA systems. Maturing technologies with growing adoption include MPC, wireless sensors (WirelessHART), OPC UA, variable speed drives, and energy monitoring. Emerging technologies with pilots and early deployments include IIoT platforms, edge analytics, digital twins in concept stage, and predictive maintenance. Early stage technologies in research and development include edge AI, TSN standards development, 5G industrial trials, and blockchain for supply chain[48].

9. FUTURE DIRECTIONS AND RESEARCH CHALLENGES

9.1 Advanced Control Algorithms

Integration of machine learning algorithms with classical control approaches promises adaptive systems learning optimal policies from operational data[48]. Reinforcement learning, neural network-based controllers, and hybrid approaches combining model-based and data-driven techniques represent promising research avenues. Key directions include deep reinforcement learning for complex tasks, neural networks for nonlinear system identification, transfer learning for rapid adaptation, federated learning for multi-plant optimization, and explainable AI for transparent control decisions[49].

Distributed control architectures where multiple controllers coordinate without centralized supervision will gain importance as manufacturing systems become more modular and reconfigurable[50]. Multi-agent systems and consensus-based control algorithms provide theoretical foundations, with research challenges including scalability to large numbers of agents, convergence guarantees under communication constraints, resilience to agent failures, plug-and-play integration, and coordination under conflicting objectives[51].

9.2 Communication Infrastructure Evolution

Future communication systems must address ultra-low latency with sub-millisecond deterministic communication, massive connectivity supporting thousands of sensors per cell, reliability exceeding 99.999% availability even under interference, security by design with integrated cryptographic protection, and Time-Sensitive Networking converged infrastructure[52].

Fifth-generation cellular technology promises to address industrial wireless requirements through Ultra-Reliable Low-Latency Communication (URLLC) providing 1ms latency with 99.999% reliability, Massive Machine-Type Communication supporting up to 1 million devices per km², network slicing for virtual dedicated networks, edge computing integration, and private enterprise-owned networks for factories.

9.3 Cybersecurity Advances

Critical cybersecurity research directions include ICS-specific intrusion detection systems designed for industrial protocols, AI-based anomaly detection trained on normal operational patterns, physical process monitoring detecting cyber-attacks through physical manifestations, and threat intelligence sharing for collaborative defense.

Secure-by-design controllers incorporating hardware security modules, trusted execution environments, secure boot, and firmware signing will become essential. Resilient control algorithms maintaining safe operation even under attack, graceful degradation under sensor/actuator compromise, attack detection through control-theoretic methods, and game-theoretic approaches represent important research directions[53].

9.4 Energy Efficiency and Sustainability

Future developments will focus on predictive energy management using forecasts of production schedules, energy prices, and renewable generation to optimize consumption through stochastic optimization under uncertainty and integration with battery storage systems. Multi-objective optimization balancing production, quality, and energy objectives in real-time control with Pareto-optimal solutions for conflicting goals and hierarchical optimization will become standard.

Grid integration enabling bidirectional interaction between industrial facilities and smart grids for demand response and distributed generation, virtual power plants aggregating flexible loads, ancillary services provision, and transactive energy markets represents a critical evolution[54].

10. CONCLUSION

This comprehensive survey examined the state-of-the-art in control systems for instrumentation as of early 2018, covering factory automation, process control, advanced algorithms, industrial communications, IIoT integration, cybersecurity, and energy efficiency. The analysis reveals clear trends shaping industrial automation's future. Classical PID control remains dominant due to simplicity and effectiveness, controlling over 95% of industrial loops, yet advanced techniques including MPC, adaptive control, and fuzzy logic gain traction in applications requiring sophisticated multivariable coordination or explicit constraint handling. The evolution from proprietary fieldbuses to industrial Ethernet and wireless standards created flexible, high-performance communication infrastructure supporting increasingly complex automation architectures, with WIA-FA standardization marking a significant milestone.

The emergence of IIoT represents a paradigm shift toward connected, intelligent manufacturing with IT/OT convergence enabling unprecedented access to cloud-based analytics and optimization. Edge computing complements cloud resources by providing local intelligence for real-time control while leveraging cloud capabilities for computationally intensive analytics and machine learning.Connectivity introduces significant cybersecurity challenges requiring comprehensive frameworks addressing network segmentation, access control, threat detection, and resilient control design, with IEC 62443 providing structured security requirements. Notable attacks including Stuxnet, BlackEnergy, and TRITON demonstrated that ICS systems face sophisticated, targeted threats requiring defense-in-depth strategies.

Energy efficiency has become a critical performance dimension, with advanced monitoring and optimization systems essential for sustainable manufacturing. Statistical process control applied to energy consumption enables identification of inefficiencies, while integration with demand response programs provides both economic and grid stability benefits. Looking forward, the future of control systems lies in integrating machine learning with physics-based models, distributed cooperative control architectures, ultra-reliable low-latency communications, comprehensive digital twin platforms, and holistic approaches to cybersecurity and energy efficiency. Realizing this vision requires continued advances in control theory, communication protocols, embedded platforms, standardization, and workforce development.

The convergence of control theory, computing, and communication technologies positions industrial automation for continued innovation and impact on industrial productivity and sustainability. As manufacturing enters an era of unprecedented connectivity and intelligence, control systems will continue serving as the foundation, translating digital insights into physical actions while ensuring safety, reliability, and optimization across multiple objectives.

REFERENCES

[1] S. McLaughlin *et al.*, "The cybersecurity landscape in industrial control systems," *Proc. IEEE*, vol. 104, no. 5, pp. 1039–1057, 2016.
[2] Y. Lu, "Industry 4.0: A survey on technologies, applications and open research issues," *J. Ind. Inf. Integr.*, vol. 6, pp. 1–10, 2017.
[3] J. Qi, Y. Kim, C. Chen, X. Lu, and J. Wang, "Demand Response and Smart Buildings: A Survey of Control, Communication, and Cyber-Physical Security," *ACM Trans. Cyber-Phys. Syst.*, vol. 1, no. 4, pp. 1–25, Oct. 2017, doi: 10.1145/3009972.
[4] T. Yang, D. Clements-Croome, and M. Marson, "Building energy management systems," *Encycl. Sustain. Technol.*, vol. 36, pp. 291–309, 2017.
[5] G. K. Moinudeen, F. Ahmad, D. Kumar, Y. Al-Douri, and S. Ahmad, "IoT applications in future foreseen guided by engineered nanomaterials and printed intelligence technologies a technology review," *Int. J. Internet Things*, vol. 6, no. 3, pp. 106–148, 2017.

[6] K. Hwang, J. Dongarra, and G. C. Fox, *Distributed and cloud computing: from parallel processing to the internet of things*. Morgan kaufmann, 2013.
[7] R. Akerkar, "Analytics on Big Aviation Data: Turning Data into Insights.," *Int. J. Comput. Sci. Appl.*, vol. 11, no. 3, 2014
[8] P. Tadejko, "Application of Internet of Things in logistics–current challenges," *Ekon. Zarządzanie*, vol. 7, no. 4, pp. 54–64, 2015.
[9] Y. Zhang, "Development of an intelligent inspection system for detecting and classifying garment defects," 2013, Available: https://theses.lib.polyu.edu.hk/handle/200/7399
[10] E. R. Alphonsus and M. O. Abdullah, "A review on the applications of programmable logic controllers (PLCs)," *Renew. Sustain. Energy Rev.*, vol. 60, pp. 1185–1205, 2016.
[11] A. Malinowski and H. Yu, "Comparison of embedded system design for industrial applications," *IEEE Trans. Ind. Inform.*, vol. 7, no. 2, pp. 244–254, 2011.
[12] D. Li, "Perspective for smart factory in petrochemical industry," *Comput. Chem. Eng.*, vol. 91, pp. 136–148, 2016.
[13] T. V. Lakshman, K. Sparks, and M. Thottan, "The future of wide area networks," *Future X Netw. Bell Labs Perspect.*, p. 113, 2016.
[14] C. Khona, "Key attributes of an intelligent IIoT edge platform," *Xilinx White Pap. Program. Devices WP493 V1 0 Sept.*, vol. 6, 2017, Available: https://fpga.eetrend.com/files-eetrend-xilinx/download/201711/12163-33327-wp493-iiot-edge-platforms.pdf
[15] H. L. Wade, *Basic and advanced regulatory control: system design and application*. John Wiley & Sons, 2017.
[16] F. Santoso, M. A. Garratt, and S. G. Anavatti, "State-of-the-art intelligent flight control systems in unmanned aerial vehicles," *IEEE Trans. Autom. Sci. Eng.*, vol. 15, no. 2, pp. 613–627, 2017.
[17] B. Kouvaritakis and M. Cannon, *Model Predictive Control*. in Advanced Textbooks in Control and Signal Processing. Cham: Springer International Publishing, 2016. doi: 10.1007/978-3-319-24853-0.
[18] M. N. Zeilinger, C. N. Jones, and M. Morari, "Real-time suboptimal model predictive control using a combination of explicit MPC and online optimization," *IEEE Trans. Autom. Control*, vol. 56, no. 7, pp. 1524–1534, 2011.
[19] T. Blevins and J. J. Downs, "Process Control in the Chemical Industry," in *Handbook of Industrial Chemistry and Biotechnology*, J. A. Kent, T. V. Bommaraju, and S. D. Barnicki, Eds., Cham: Springer International Publishing, 2017, pp. 2069–2115. doi: 10.1007/978-3-319-52287-6_39.
[20] P. Swarnkar, S. K. Jain, and R. K. Nema, "Adaptive Control Schemes for Improving the Control System Dynamics: A Review," *IETE Tech. Rev.*, vol. 31, no. 1, pp. 17–33, Jan. 2014, doi: 10.1080/02564602.2014.890838.
[21] M. Hanss and S. Turrin, "A fuzzy-based approach to comprehensive modeling and analysis of systems with epistemic uncertainties," *Struct. Saf.*, vol. 32, no. 6, pp. 433–441, 2010.
[22] D. Xu, B. Jiang, and P. Shi, "Adaptive observer based data-driven control for nonlinear discrete-time processes," *IEEE Trans. Autom. Sci. Eng.*, vol. 11, no. 4, pp. 1037–1045, 2013.
[23] K. Zeb, Z. Ali, K. Saleem, W. Uddin, M. A. Javed, and N. Christofides, "Indirect field-oriented control of induction motor drive based on adaptive fuzzy logic controller," *Electr. Eng.*, vol. 99, no. 3, pp. 803–815, Sep. 2017, doi: 10.1007/s00202-016-0447-5.

[24] C. Xin and L. Di, "A survey on real-time Ethernet," *Int. J. Auton. Adapt. Commun. Syst.*, vol. 10, no. 4, p. 409, 2017, doi: 10.1504/IJAACS.2017.088776.
[25] X. Wu, L. Xie, and F. Lim, "Network delay analysis of EtherCAT and PROFINET IRT protocols," in *IECON 2014-40th Annual Conference of the IEEE Industrial Electronics Society*, IEEE, 2014, pp. 2597–2603. Available: https://ieeexplore.ieee.org/abstract/document/7048872/
[26] Rashid, Bushra & Rehmani, Mubashir Husain. (2015). Applications of wireless sensor networks for urban areas: A survey. Journal of Network and Computer Applications. 60. 10.1016/j.jnca.2015.09.008.
[27] Z. Pang, M. Luvisotto, and D. Dzung, "Wireless high-performance communications: The challenges and opportunities of a new target," *IEEE Ind. Electron. Mag.*, vol. 11, no. 3, pp. 20–25, 2017.
[28] M. Zheng, W. Liang, H. Yu, and Y. Xiao, "Performance Analysis of the Industrial Wireless Networks Standard: WIA-PA," *Mob. Netw. Appl.*, vol. 22, no. 1, pp. 139–150, Feb. 2017, doi: 10.1007/s11036-015-0647-7.
[29] R. Hummen, S. Kehrer, and O. Kleineberg, "Tsn–time sensitive networking," *Hirschmann USA WP00027*, 2016, Available: https://resources.ipd.com.au/documents/white-papers/tsn-time-sensitive-networking.pdf
[30] G. Murray, M. N. Johnstone, and C. Valli, "The convergence of IT and OT in critical infrastructure," 2017, Available: https://ro.ecu.edu.au/ism/217/
[31] Y. Liu and X. Xu, "Industry 4.0 and cloud manufacturing: A comparative analysis," *J. Manuf. Sci. Eng.*, vol. 139, no. 3, p. 034701, 2017.
[32] N. M. Gonzalez *et al.*, "Fog computing: Data analytics and cloud distributed processing on the network edges," in *2016 35th International Conference of the Chilean Computer Science Society (SCCC)*, IEEE, 2016, pp. 1–9. Available: https://ieeexplore.ieee.org/abstract/document/7836028/
[33] M. Baezner and P. Robin, "Stuxnet," ETH Zurich, 2017. Available: https://www.research-collection.ethz.ch/entities/publication/d059a54b-bcc0-41a1-a7f9-c9f71bc799b7
[34] J. Rrushi, H. Farhangi, C. Howey, K. Carmichael, and J. Dabell, "A quantitative evaluation of the target selection of havex ics malware plugin," in *Industrial control system security (ICSS) workshop*, ICSS, 2015, pp. 1–5. Available: https://www.acsac.org/2015/workshops/icss/Julian.Rrushi%20et%20al-%20Manuscript.pdf
[35] R. Khan, P. Maynard, K. McLaughlin, D. Laverty, and S. Sezer, "Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid," in *4th International Symposium for ICS & SCADA Cyber Security Research 2016*, BCS, 2016, pp. 53–63. Available: https://pure.qub.ac.uk/en/publications/threat-analysis-of-blackenergy-malware-for-synchrophasor-based-re/
[36] N. Kshetri and J. Voas, "Hacking power grids: A current problem," *Computer*, vol. 50, no. 12, pp. 91–95, 2017.
[37] M. Bakuei, R. Flores, V. Kropotov, and F. Yarochkin, "Securing smart factories," *Trend Micro Httpsdocuments Trendmicro Comassetswhitepaperswp-Threats--Manuf.-Environ.---Era--Ind.-4 Pdf*, 2017, Available: http://documents.trendmicro.com/assets/white_papers/wp-threats-to-manufacturing-environments-in-the-era-of-industry-4.pdf

[38] A. Gurtov, M. Liyanage, and D. Korzun, "Secure communication and data processing challenges in the Industrial Internet," 2016, Available: https://oulurepo.oulu.fi/handle/10024/21980
[39] J. Braband, "What's Security Level got to do with Safety Integrity Level?," in *8th European Congress on Embedded Real Time Software and Systems (ERTS 2016)*, 2016. Available: https://hal.science/hal-01289437/
[40] A. Wedgbury and K. Jones, "Cyber security architectures for ICS/supervisory control and data acquisition environments," *Eng. Technol. Ref.*, vol. 1, no. 1, Jan. 2012, doi: 10.1049/etr.2016.0055.
[41] D. C. Robinson, D. A. Sanders, and E. Mazharsolook, "Ambient intelligence for optimal manufacturing and energy efficiency," *Assem. Autom.*, vol. 35, no. 3, pp. 234–248, 2015.
[42] K. Bettagere, "Device monitoring and device management for smart meters," PhD Thesis, University of Oxford, 2012. Available: https://ora.ox.ac.uk/objects/uuid:3dbe5d49-7ec2-4204-aebb-23a8c92aab77
[43] K. H. Khan, C. Ryan, and E. Abebe, "Day ahead scheduling to optimize industrial HVAC energy cost based on peak/off-peak tariff and weather forecasting," *IEEE Access*, vol. 5, pp. 21684–21693, 2017.
[44] C. Wang and X.-B. Liu, "Integrated production planning and control: A multi-objective optimization model," *J. Ind. Eng. Manag. JIEM*, vol. 6, no. 4, pp. 815–830, 2013.
[45] T. Samad, E. Koch, and P. Stluka, "Automated demand response for smart buildings and microgrids: The state of the practice and research challenges," *Proc. IEEE*, vol. 104, no. 4, pp. 726–744, 2016.
[46] F. M. Salem, M. I. Mosaad, and M. A. Awadallah, "A comparative study of MPC and optimised PID control," *Int. J. Ind. Electron. Drives*, vol. 2, no. 4, p. 242, 2015, doi: 10.1504/IJIED.2015.076293.
[47] E. Wings, M. Müller, and M. Rochler, "Integration of real-time Ethernet in LinuxCNC: Using the example of Sercos III," *Int. J. Adv. Manuf. Technol.*, vol. 78, no. 9–12, pp. 1837–1846, Jun. 2015, doi: 10.1007/s00170-015-6786-y.
[48] D. Cearley, B. Burke, S. Searle, and M. J. Walker, "Top 10 strategic technology trends for 2018," *The Top*, vol. 10, pp. 1–246, 2016.
[49] M. P. Bonacina, "Automated reasoning for explainable artificial intelligence," *EASYCHAIR Proc. Comput.*, vol. 51, pp. 24–28, 2017.
[50] M. Khalgui and O. Mosbahi, "Intelligent distributed control systems," *Inf. Softw. Technol.*, vol. 52, no. 12, pp. 1259–1271, 2010.
[51] L. Meng *et al.*, "Review on control of DC microgrids and multiple microgrid clusters," *IEEE J. Emerg. Sel. Top. Power Electron.*, vol. 5, no. 3, pp. 928–948, 2017.
[52] P. Fleming, N. Vyas, S. Sanei, and K. Deb, "Emerging Trends in Electrical, Electronic and Communications Engineering: Proceedings of the First International Conference on Electrical, Electronic and Communications Engineering (ELECOM 2016), Bagatelle, Mauritius, November 25-27, 2016," 2017
[53] U. P. D. Ani, H. (Mary) He, and A. Tiwari, "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective," *J. Cyber Secur. Technol.*, vol. 1, no. 1, pp. 32–74, Jan. 2017, doi: 10.1080/23742917.2016.1252211.
[54] L. Bottaccioli *et al.*, "A flexible distributed infrastructure for real-time cosimulations in smart grids," *IEEE Trans. Ind. Inform.*, vol. 13, no. 6, pp. 3265–3274, 2017.