IJCRL

International Journal of Contemporary Research and Literacy works (IJCRL)

Are Mechatronic Devices Failing in Industry 4.0

Tariq Al-Zoubi, Rami Al-Qudah
Mechatronics Engineering Department, German Jordanian University, Amman 11180, Jordan
ramialqud@gju.edu.jo

Abstract:

Industry 4.0 promises remarkable efficiency gains, with potential energy consumption and greenhouse gas emission reductions of 30% to 40% in manufacturing processes. While this digital transformation offers significant benefits through the integration of mechatronic devices, we're witnessing an increasing number of system failures that threaten these advantages. Despite the potential for enhanced operational efficiency and production flexibility, mechatronic systems face serious challenges in the Industry 4.0 environment. The lack of standardization in IoT devices creates security vulnerabilities, while cyber-physical systems expose critical infrastructure to new threats. Additionally, the rapid pace of technological change has created a significant skills gap, where existing workforce struggles to operate and maintain these advanced systems effectively. We're seeing these challenges manifest across various industries, as the complexity of integrating Industry 4.0 technologies demands continuous investment in infrastructure and workforce development. In this article, we'll examine why these failures occur and provide practical solutions to ensure your mechatronic devices can reliably support your Industry 4.0 initiatives.

Article History:

Received: 02 May 2024 Revised: 19 November 2024
Accepted: 18 December 2024 Published Online: 10 January 2025

Keywords:

Cyber-Physical Systems; Industry 4.0 Challenges; Mechatronic Device Failures; Operational Reliability; Workforce Skills Gap

1. The Widening Gap Between Legacy Mechatronic Systems and Industry 4.0 Requirements

Legacy mechatronic systems face mounting challenges as Industry 4.0 revolutionizes manufacturing environments. These outdated systems, characterized by technology in the later stages of its useful life, increasingly limit efficiency, increase downtime, and jeopardize long-term factory vitality. The disconnect between older mechatronic infrastructure and modern digital requirements creates a technological gap that threatens production capabilities across industries [1]-[3].

Compatibility issues with modern communication protocols

The transition from tethered machines to autonomous, mobile mechatronic devices introduces distinct communication challenges that older systems simply weren't designed to handle. Modern robotic communication requires wireless capabilities for fleet interaction and equipment connectivity. Nevertheless, many legacy mechatronic systems rely on outdated communication standards, making integration with Industry 4.0 technologies nearly impossible without significant modifications [4]-[7].

For effective Industry 4.0 implementation, mechatronic devices must support diverse networking and communication options including Ethernet (wired or wireless), serial networks, OPC, Modbus, Profibus, and other control standards. Furthermore, modern protocols like TCP/IP, SMTP, SNMP, and FTP become essential for integration with corporate networks. The reality, however, is that many legacy systems lack these capabilities entirely.

The ROS (Robot Operating System) framework - commonly used in advanced mechatronic devices - exemplifies these challenges. Although ROS 2 improves upon ROS 1 by eliminating single-point failures, it introduces new obstacles such as scalability issues with peer-to-peer communications, resource-intensive discovery protocols, and complex security configurations. Consequently, older mechatronic systems struggle to interface with this modern framework.

Processing limitations of older mechatronic controllers

The computational capacity of legacy mechatronic controllers presents another critical barrier. As control applications grow increasingly complex, there's a shift from general-purpose processors to high-performance targeted embedded controllers. Older mechatronic systems typically lack the processing power needed for these advanced control strategies.

One fundamental issue stems from the sequential design approach traditionally used in mechatronic development, where control specialists design and tune controllers only after mechanical prototypes are fabricated. This approach fails to account for interactions between mechanical and control systems, resulting in conservative design parameters that significantly downgrade achievable performance.

Older controllers often struggle with the computational demands of modern control algorithms. In fact, many legacy systems require translation from floating-point algorithms to fixed-point algorithms to function at all, introducing performance risks. The controllers in these systems frequently can't handle the mathematical complexity required for tasks like self-adaptation, real-time simulation, and parametric identification from control signals [8]-[11].

Data storage and management constraints

The data demands of Industry 4.0 overwhelm most legacy mechatronic systems. Modern manufacturing environments generate vast amounts of data that requires robust management and cybersecurity measures. Older mechatronic devices typically lack sufficient memory for acquiring and storing this volume of data, let alone the capability to share it directly with corporate databases over network connections.

In addition, Industry 4.0 environments require mechatronic devices to provide continuous self-diagnostic information, performance assessment, and condition monitoring - capabilities rarely found in legacy systems. This limitation prevents integration with predictive production planning layers and enterprise resource planning systems.

The technical debt accumulated in legacy mechatronic systems - manifested as confusing code, missing wiring diagrams, and an abundance of disparate networks - creates significant friction against efficiency improvements. Accordingly, these data management constraints represent perhaps the most fundamental barrier to successful Industry 4.0 implementation.

To overcome these limitations, manufacturers must consider the compatibility of new programmable automation controllers (PACs) with all legacy systems, including networks and protocols. This approach consolidates separate systems and links them with company computers to exchange control, production, and monitoring data - the core requirement for effective Industry 4.0 implementation that most legacy mechatronic systems simply cannot fulfill without substantial modernization.

2. Common Failure Points in Mechatronic Production Systems

Mechatronic production systems encounter various failure points that impede optimal performance in modern manufacturing environments. These breakdowns don't happen randomly but follow distinctive patterns across four critical areas that warrant close examination for anyone maintaining these systems.

Sensor degradation and calibration drift

Sensors form the nervous system of mechatronic devices, yet they frequently become unreliable through gradual degradation. Over time, sensors drift from their calibrated state, producing

increasingly inaccurate readings even when the measured input remains constant. This drift isn't merely a theoretical concern—uncalibrated sensors directly compromise product quality, data credibility, and overall system reliability. Exposure to harsh environments, continuous operation, and physical wear accelerate this degradation process.

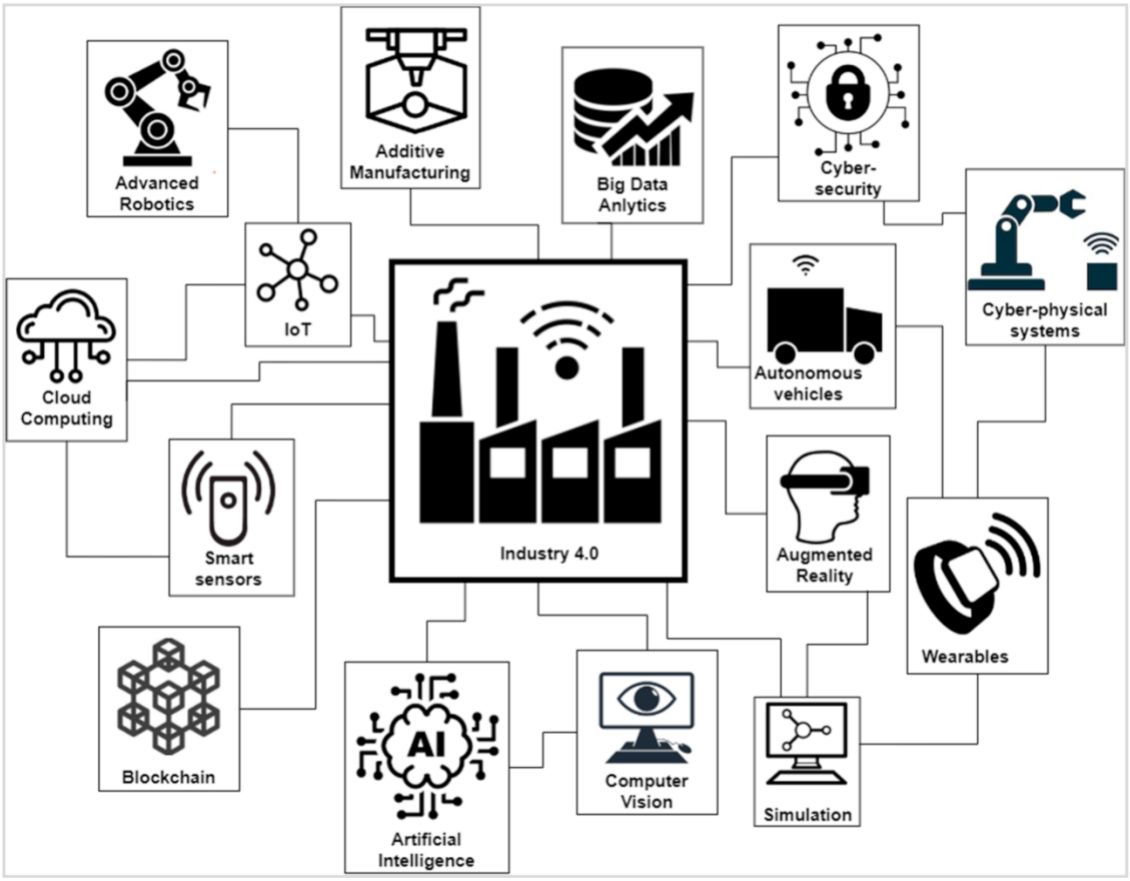

Figure 1. Sensor degradation and calibration drift

Sensor calibration drift manifests through several mechanisms. Mechanical problems or degradation of filling fluid within the sensor itself commonly cause calibration shifts. Moreover, electrical noise from nearby equipment introduces additional errors in sensor outputs. For pharmaceutical industry monitoring, the consequences of sensor drift can be particularly severe, potentially leading to inaccurate readings and compromised product quality.

The type of sensor significantly influences drift susceptibility. NTC sensors, though cost-effective and suitable for wide temperature ranges, prove more prone to drift compared to RTD sensors, which demonstrate higher accuracy and stability. Digital sensors typically offer superior accuracy with minimal drift over time, making them preferable for critical applications.

Actuator response limitations

Actuators in mechatronic production systems face several mechanical constraints that limit their performance. One fundamental issue involves the relationship between accuracy and repeatability. An actuator may maintain high repeatability without achieving high accuracy, meaning it consistently reaches the same position even if that position deviates from the intended target.

Resolution—the smallest positional increment a motion system can achieve—faces practical limitations from mechanical factors like friction and nut backlash. Furthermore, when actuators

reach their maximum output capability regardless of input demand, they exhibit nonlinear behavior once crossing this saturation point.

Static and Coulomb friction present particular challenges for actuator positioning. Unlike the assumption that friction is directly proportional to velocity, real systems exhibit static friction that must be overcome before movement begins. Subsequently, as an actuator approaches its final position, velocity approaches zero and the actuator force balances frictional load, potentially stopping slightly off the desired position and compromising repeatability [12]-[14].

Control system latency issues

Latency represents a critical yet often misunderstood concern in mechatronic systems. Missing control deadlines results in unwanted "jerky" movements that compromise precision operations. Most concerning are latency outliers—even if a system performs as expected 99% of the time, the remaining 1% can cause more damage than all other measurements combined.

The common assumption that latency follows a Gaussian distribution leads to reporting only mean and standard deviation values. Yet, latency typically demonstrates multi-modal patterns where outliers dramatically impact system determinism. For accurate assessment, examining latency through histograms and percentile plots (e.g., "99.9% of measurements below X milliseconds") provides more practical insight.

Operating system choice fundamentally constrains responsiveness. The effectiveness of feedback from sensors and the control system largely determines dynamic response characteristics. Mechatronic professionals increasingly implement low-level control (PID loops, motor control, safety features) on a per-actuator level with dedicated RTOS, making the system independent of user code and less sensitive to latency.

Power supply instabilities in connected environments

Power supply reliability fundamentally impacts the performance and lifespan of mechatronic production systems. Unstable power supplies cause severe system issues, including audible noise from passive components, unexpected jittering in switching frequency, extreme oscillations in output voltage during load transients, and semiconductor switch failures.

Voltage instabilities take various forms—interruptions, fluctuations, unbalance, sag, swell, and transients—each detrimentally affecting operating costs and power supply reliability. For reliable operations, mechatronic systems require power supplies that maintain stability under all circumstances, particularly challenging in the connected environments characteristic of modern production systems.

Importantly, un-tuned compensation networks account for most instability issues in switching power supplies. Power supply transient performance depends primarily on bandwidth (BW) and phase margin (PM), with higher BW resulting in faster response and higher PM indicating better stability. Effective system design must balance these competing requirements while accounting for increased power demands in connected environments.

3. Data Integration Challenges Causing Mechatronic Device Failures

Integrating diverse engineering disciplines creates fundamental challenges in mechatronic systems that directly contribute to device failures in Industry 4.0 environments. The multidisciplinary nature of mechatronics—combining mechanical, electronic, and computational components—introduces complexity that grows exponentially as these systems evolve. This integration demands not merely connecting physical components but ensuring sophisticated software systems can effectively communicate with hardware to perform complex tasks accurately and efficiently.

Incompatible data formats between systems

The coordination between specialists from different engineering disciplines represents a significant integration hurdle, as each discipline brings its unique language, tools, and

methodologies. This disciplinary fragmentation manifests most visibly in incompatible data formats that prevent seamless information exchange between system components. Without standardized data exchange formats, mechatronic systems struggle to move information reliably between software tools or maintain system-independent archives.

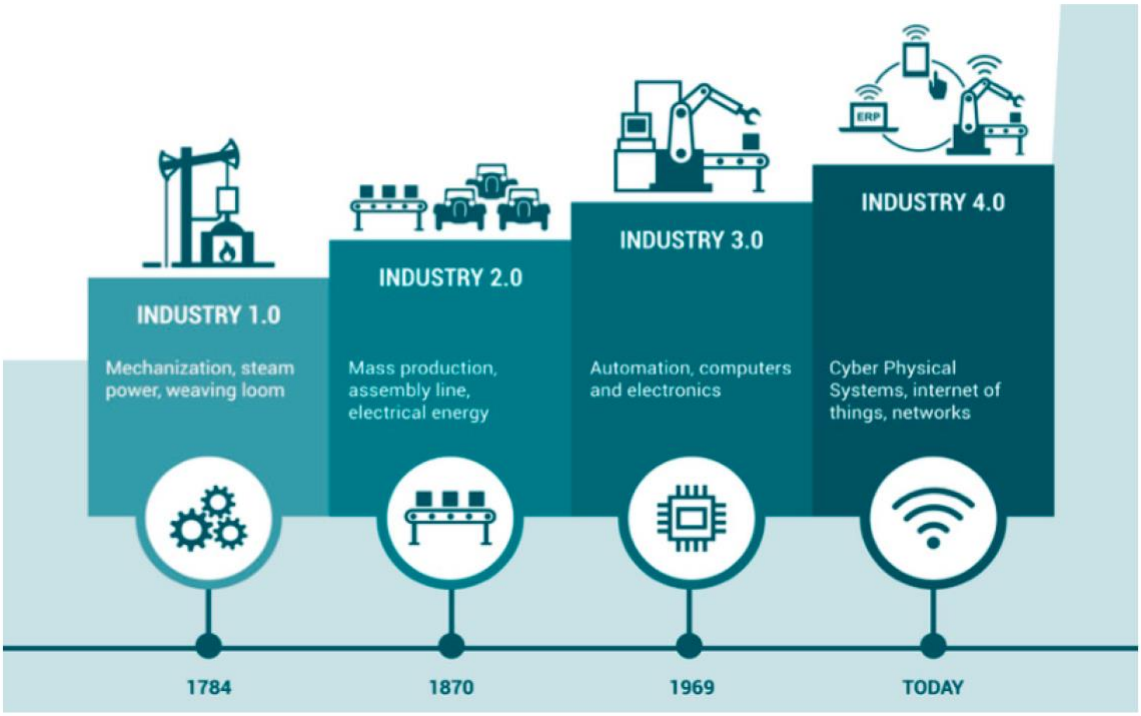

Figure 2. Incompatible data formats between systems

Data integration—the process of combining information from different sources into a unified view—becomes exceptionally difficult when mechatronic components employ incompatible formats, structures, schemas, or semantics. For instance, older mechatronic devices often generate data in proprietary formats incompatible with newer systems or industry standards. Essentially, these incompatibilities create communication barriers that prevent components from sharing critical operational information.

The complexity extends beyond simple format differences. Many legacy mechatronic systems require intricate translation layers to convert between floating-point algorithms and fixed-point algorithms, introducing additional performance risks. Likewise, standardized input and output with mechatronic devices (SIOMS) must encapsulate I/O complexities while presenting users with simple interfaces that allow concurrent access from multiple processes—a delicate balance that many systems fail to achieve.

Model interpretability presents yet another dimension of the data integration challenge. As mechatronic systems increasingly incorporate deep learning techniques, their data structures must support advanced capabilities like multimodal sensor fusion, system identification, and domain adaptation to enhance model interpretability and robustness. Unfortunately, many existing mechatronic systems lack the architectural foundations to support these capabilities [15].

Bandwidth limitations for real-time operations

Real-time operation represents a core requirement for most mechatronic applications, yet bandwidth limitations frequently undermine this capability. For applications demanding real-time responses, mechatronic systems must integrate data processing and control mechanisms to

function within extremely narrow time constraints. Obviously, this requires sufficient bandwidth between components—a requirement many systems cannot satisfy.

Serial interfaces exemplify this challenge perfectly. Due to their inherently low bandwidth, serial interfaces make exact motion synchronization extremely difficult. Similarly, device drivers for mechatronic systems must allow efficient processor use with minimal overhead for interfacing to devices, typically at rates less than 100Hz. These limitations create significant constraints for real-time control applications.

The bandwidth challenges extend to deep learning integration as well. Mechatronic systems incorporating advanced automation and control techniques face significant real-time processing hurdles. The computational demands of deep learning models often exceed available bandwidth, especially when systems must process multiple data streams simultaneously.

Importantly, Bode's Integral Theorem introduces additional complexity, guaranteeing (under mild assumptions) the occurrence of error amplifications during feedback control loop shaping. This means disturbance amplifications from fundamental limits of feedback control must be flexibly managed with prescribed optimality and stability—a capability requiring substantial bandwidth that many systems lack.

Interface standardization presents another challenging dimension, as creating standards that don't require excessive overhead becomes increasingly difficult. The challenge arises primarily because real-time UNIX device drivers must encapsulate I/O complexities while maintaining simplicity and allowing concurrent device access—requirements that strain available bandwidth.

Indeed, these bandwidth limitations explain why high-performance operation beyond conventional closed-loop bandwidth remains exceptionally difficult to achieve. Without sufficient bandwidth, mechatronic systems cannot maintain the real-time responsiveness necessary for Industry 4.0 applications, ultimately leading to performance degradation or complete system failure [16]-[21].

4. Security Vulnerabilities in Connected Mechatronic Devices

Connected mechatronic devices increasingly face security threats that manufacturers and users often overlook as systems become more interconnected. As mechatronic systems evolve from isolated production tools to network-connected assets, their vulnerability surface expands dramatically, creating new attack vectors that traditional security approaches fail to address.

Outdated firmware and patch management issues

Patch management challenges plague mechatronic devices in industrial settings, primarily because these systems often run on outdated firmware with known vulnerabilities. Research from Microsoft found that between 70% to 80% of the top 10 malware infections could be prevented through proper system updates. Hence, unpatched mechatronic devices represent a significant security risk that compounds over time.

Many mechatronic production systems suffer from compatibility issues when applying patches, frequently resulting in instability that leaves systems exposed to threats. Third-party applications integrated with mechatronic devices often introduce additional security vulnerabilities that, without regular updates, make networks susceptible to malware injection, unauthorized access, and data breaches. At times, patches fail to apply successfully, leaving systems in unstable states that potentially cause data loss or corruption while requiring significant resources to identify and address.

The complexity of patch management increases with the shortage of IT professionals specializing in security and support sectors. This staffing gap affects managed service providers who have increasing workloads but lack personnel to deliver essential patching services. Given that mechatronic systems often operate in critical environments, the inability to meet compliance standards through timely, efficient patch management can have substantial financial implications if compliance audits fail.

Table 1. Key Causes of Mechatronic Device Failures in Industry 4.0 Environments

Failure Cause	Description	Industry 4.0 Impact	Observed Consequences
Lack of IoT Standardization	Devices use incompatible protocols and fragmented communication standards.	Weak interoperability between mechatronic, IoT, and cloud systems.	Data loss, unstable system performance, increased downtime.
Cybersecurity Vulnerabilities	Poorly protected networks and devices expose systems to cyberattacks.	High-risk exposure for cyber-physical infrastructures.	Unauthorized access, production halts, safety hazards.
Workforce Skills Gap	Workforce struggles with complex digital tools and advanced automation.	Inefficient operation and maintenance of mechatronic systems.	Incorrect configurations, delayed troubleshooting, frequent failures.
High System Complexity	Integration of robotics, sensors, digital twins, and AI increases system loads.	Harder diagnostics and maintenance requirements.	Unpredictable failures, performance drops.
Inadequate Predictive Maintenance	Reliance on reactive maintenance instead of AI-driven monitoring.	Reduced readiness in smart factories.	Increased wear, unexpected breakdowns, higher costs.

Network exposure risks

At present, the growing deployment of mechatronic devices for security-relevant applications creates significant network exposure challenges. According to cybersecurity research, tools like Shodan provide attackers with straightforward methods to identify exposed mechatronic systems connected to the internet. Once discovered, these systems often become targets for exploitation attempts, starting with simple password guessing and escalating to more sophisticated attacks.

The interconnected nature of modern mechatronic systems—relying on intricate networks of sensors, actuators, and controllers—simultaneously enhances functionality and exposes these systems to cyber threats. Many IoT-based mechatronic systems operate without adequate protection, allowing attackers to gain access with minimal effort. Considering that mechatronic components handle increasingly sensitive operations from manufacturing plants to autonomous vehicles, unauthorized access can compromise system integrity with serious consequences.

As a consequence of rapid Industry 4.0 adoption, many organizations accept the inevitability of breaches rather than focusing on prevention. Security experts emphasize that proper defense requires effective risk management focused not merely on avoiding attacks but on developing robust response capabilities. Ultimately, connected mechatronic devices need protection strategies that acknowledge their unique cyber-physical characteristics rather than applying conventional IT security approaches.

Authentication and access control weaknesses

Broken access control represents one of the most prevalent vulnerabilities in mechatronic integrated devices, according to recent cybersecurity reports. Authentication weaknesses allow unauthorized individuals to manipulate mechatronic systems, potentially resulting in catastrophic failures or compromised operations in industrial automation environments. Even so, many systems lack robust authentication protocols, encryption methods, and access controls necessary to prevent unauthorized access.

Role-based Access Control (RBAC) implementation often suffers from inadequate management, making it easier for attackers to obtain access to low-level accounts and subsequently escalate privileges. Reviewing access logs frequently reveals users accessing data or functionality beyond their permissions—a clear indicator of access control problems. Correspondingly, web APIs have

become common points of broken access control vulnerabilities, where attackers manipulate endpoints or parameters to bypass restrictions.

The security requirements for mechatronic robot identification include uniqueness, provability, and technical impossibility of cloning without invasive attacks. Sessions in mechatronic systems require careful management through secure tokens, as weak implementation allows attackers to steal valid tokens and impersonate authorized users. In response to these challenges, security experts recommend implementing the Principle of Least Privilege, conducting regular access control audits, and incorporating comprehensive cybersecurity measures from the design phase.

5. Diagnostic Approaches for Failing Mechatronic Integrated Devices

Detecting potential failures before they occur represents the cornerstone of effective mechatronic maintenance strategies in the Industry 4.0 era. As mechatronic devices grow increasingly complex, traditional reactive maintenance approaches prove inadequate for preventing costly production stoppages and system failures. Fortunately, several diagnostic approaches offer solutions to identify and address potential issues before they cause significant disruption.

Implementing continuous monitoring systems

Continuous monitoring systems provide real-time surveillance of mechatronic devices, allowing for immediate detection of developing problems. These systems typically include sensors that track critical parameters like temperature, pressure, and humidity to ensure optimal operating conditions. Thermal imaging cameras have emerged as particularly effective tools for monitoring mechatronic systems, identifying heat buildup that often indicates poor equipment health and possible impending failure. These cameras can be fixed-mounted to eliminate reliance on periodic inspections, with alarms programmed to trigger once temperature thresholds are exceeded [22]-[23].

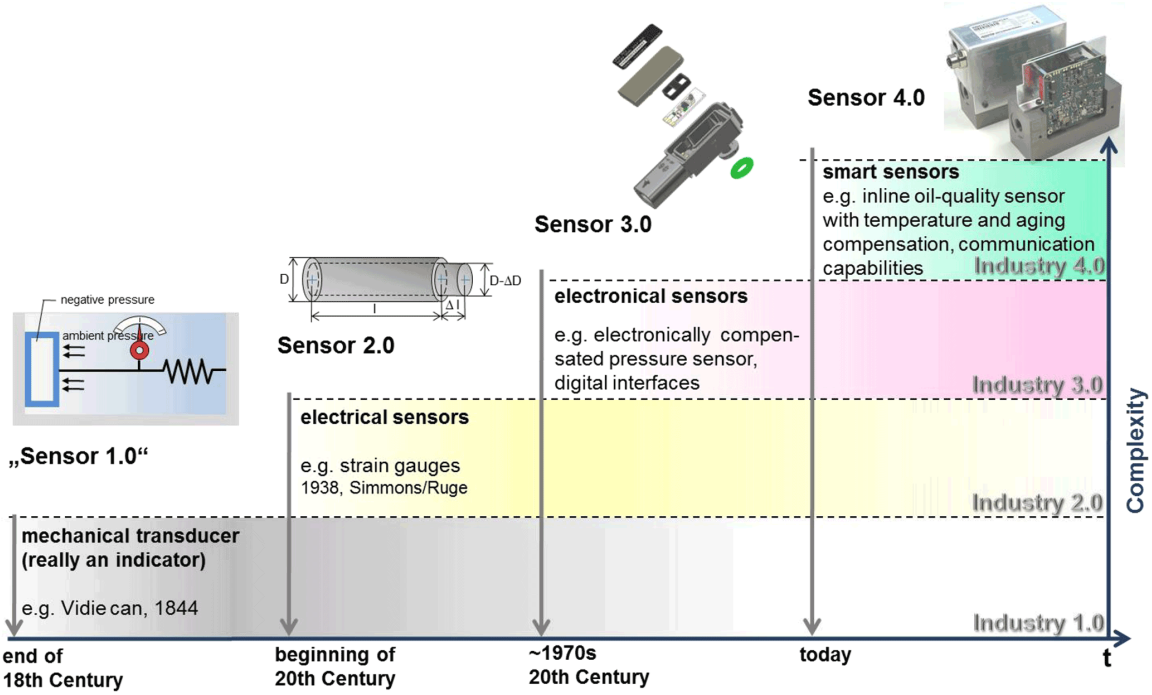

Figure 3. Implementing continuous monitoring systems

The implementation of continuous monitoring for mechatronic production systems offers numerous advantages beyond simple failure prevention. With thermal imaging cameras,

engineers can monitor everything from thermal gradients to production line consistency, providing 24/7 surveillance that protects equipment and prevents downtime. Currently, these systems allow full-time remote monitoring in virtually any weather condition, avoiding many technical and cost-related problems associated with alternative technologies like ultraviolet flame detectors, thermocouples, and pyrometers.

Performance baseline establishment

Performance Measurement Baseline (PMB) establishment serves as a crucial foundation for diagnosing mechatronic integrated devices. A comprehensive PMB consists of three critical baselines: scope (defining what work needs to be done), schedule (outlining when work will be performed), and cost (determining the budget for completing the work). These three baselines work together to create a holistic view of planned performance, acting as a reference point for measuring actual progress against expectations.

For mechatronic systems specifically, performance baselines are essential for evaluating quality and reliability. They provide reference points for measuring the impact of design changes, environmental factors, and usage scenarios on system performance. Initially, establishing these baselines requires thorough documentation of normal operating parameters. Subsequently, deviations from these established norms can quickly signal developing problems before they manifest as complete failures.

The PMB approach, when combined with Earned Value Management (EVM), offers a powerful toolkit for diagnosing mechatronic device issues. Unlike traditional methods that treat scope, schedule, and cost separately, PMB incorporates these elements into a single, integrated plan that serves as an official benchmark for performance evaluation. This integration proves particularly valuable for complex mechatronic systems where interactions between components can create cascading failures.

Failure pattern recognition techniques

Modern diagnostic approaches increasingly rely on sophisticated pattern recognition techniques to identify potential failures in mechatronic integrated devices. Sliding mode observers have demonstrated remarkable effectiveness for fault detection and isolation in mechatronic systems. These observers excel at robust detection and reconstruction of both actuator and sensor faults, making them invaluable for complex mechanical-electrical systems.

Neural networks represent another powerful approach for failure pattern recognition. Fully connected cascade neural networks have proven especially effective for sensor failure detection, identification, and accommodation. By training these networks, specific fault patterns can be learned to accurately classify system conditions. Notably, recent advances have led to the integration of Graph Neural Networks (GNNs) with hierarchical attention mechanisms to enhance both performance and interpretability of data-driven fault detection models in complex mechatronic systems.

The implementation of artificial-intelligence-based, real-time diagnostic systems has fundamentally transformed mechatronic maintenance. These systems offer greater accuracy and robustness while enabling online operation. Presently, multiple fault diagnosis and classification—previously considered extremely difficult due to similar failure symptoms corresponding to different failures—has become increasingly feasible through machine learning models. Transfer learning applications have further extended these capabilities, addressing the common challenge of insufficient experimental data for training AI-based fault detectors and classifiers.

6. Hardware Upgrades to Modernize Existing Mechatronic Systems

Modernizing legacy mechatronic devices presents a viable alternative to complete system replacement, offering cost-effective pathways to Industry 4.0 compatibility. Targeted hardware upgrades can bridge technological gaps while preserving existing infrastructure investments.

Modular component replacement strategies

Modular design approaches revolutionize mechatronic system modernization by enabling independent replacement of outdated components without rebuilding entire systems. This modularity in specification management supports local analysis and verification of module design changes, enabling design teams to work in parallel without iteratively rebuilding system models to check fulfillment of specifications. Practically speaking, these "plug and produce" mechatronic solutions come preconfigured with all electronics, mechanical components, sensors, cabling, and control software delivered as single production tools. For manufacturers utilizing joining and pressing machines, this flexibility allows setup of new production lines in record time, as demonstrated by one sensor manufacturer that implemented a preconfigured package with minimal programming required.

Sensor network enhancements

Advanced sensing capabilities form the cornerstone of modern mechatronic systems, enabling real-time monitoring and adaptive performance. Flexible, large-scale sensor networks constructed using flexible printing circuits (FPC) considerably reduce weight while expanding coverage areas. Alternatively, stretchable sensor networks offer impressive versatility—manufactured at small scale then expanded for large-scale applications. IoT sensors installed on mechatronic production machines provide continuous data on machine health, part quality, and production status, enabling immediate corrective actions. These enhancements effectively transform conventional systems into intelligent networks capable of self-diagnosis and optimization.

Processing power augmentation options

Computational upgrades represent perhaps the most transformative hardware modernization strategy. Cloud robotics integration alleviates computational burdens by transferring demanding tasks to robust external processing systems, freeing up embedded processors and enabling smoother, more responsive performance. Artificial intelligence implementations analyze vast sensor data sets to identify optimal process parameters, resulting in improved part quality, reduced waste, and faster cycle times. In practice, manufacturers often enhance existing mechatronic devices through microcontroller upgrades that enable sophisticated sensing, processing, and actuation mechanisms for dynamic adjustment to varying conditions. These computational enhancements bridge the gap between older mechanical systems and today's advanced control requirements.

Ultimately, modernizing existing mechatronic systems through strategic hardware upgrades offers a pragmatic path to Industry 4.0 compatibility without the disruption and expense of complete system replacement. By focusing on modular components, enhanced sensing networks, and augmented processing capabilities, manufacturers can extend the useful life of valuable equipment while achieving new levels of performance.

7. Software Solutions for Extending Mechatronic Device Lifespan

Software offers powerful extensions for aging mechatronic devices facing obsolescence in the Industry 4.0 landscape. When complete hardware replacement isn't feasible, strategic software solutions can significantly extend operational lifespan while enhancing compatibility with modern systems.

Middleware implementation for legacy integration

Middleware functions as a critical bridge between outdated mechatronic systems and contemporary technologies, enabling seamless data exchange without radical infrastructure changes. This integration software creates a universal adapter that allows disparate technologies to communicate effectively, regardless of whether they're cloud-based or traditional on-premises systems. Enterprise Service Bus (ESB) implementations act as central communication hubs, while Integration Platform as a Service (iPaaS) solutions connect applications through standardized API integrations. Organizations implementing middleware report breaking down persistent data silos, with some systems maintaining functionality for thirty-plus years through strategic controller updates. Since middleware handles complex communication pathways between previously isolated systems, it effectively frees up developers to focus on core functionality improvements rather than struggling with incompatible interfaces.

Edge computing adaptations

Edge computing transforms legacy mechatronic devices by enabling data collection and analysis directly at the production source. This capability helps quickly identify and eliminate potential problems before they cause costly production downtime. At present, edge computing complements rather than replaces central computing resources, providing real-time decision capability where data originates. Complex algorithms—including artificial intelligence—can now execute on edge devices without compromising core functionality. For instance, one implementation enabled remarkable improvements in product lifetime through optimization applied to control schemes. Generally, the greatest challenge lies in heterogeneity when integrating edge computing into existing mechatronic systems, requiring multidisciplinary expertise spanning both information technology and traditional engineering domains.

Table 2. Comparison of Traditional Mechatronic Systems vs. Industry 4.0–Enabled Mechatronic Systems

Criteria	Traditional Mechatronic Systems	Industry 4.0–Enabled Mechatronic Systems	Resulting Challenges
Connectivity	Standalone or local network	Fully connected through IoT, cloud, and edge computing	Susceptibility to network outages, communication failures
Maintenance Approach	Reactive/preventive	Predictive, sensor-driven	Requires advanced analytics & skilled operators
Interoperability	Limited device-to-device integration	Multi-platform integration with cyber-physical systems	Protocol conflicts and integration errors
Security Level	Moderate; isolated risks	High-risk due to full connectivity	Increased attack surface and cyber threats
System Complexity	Lower, simpler components	High due to robotics, AI, automation	Increased probability of cascading failures

Firmware optimization techniques

Optimized firmware dramatically extends mechatronic device operational life through improved resource management. Test-driven development ensures thorough system testing, resulting in fewer bugs and more reliable performance. Creating modular, reusable code components simplifies maintenance while making systems easier to update as requirements evolve. Firmware

developers frequently implement power management techniques that extend battery life, using low-power modes during idle periods to minimize energy consumption. Algorithm optimization reduces computational complexity, with fixed-point arithmetic implementations substantially reducing processing overhead for resource-constrained controllers. These techniques collectively ensure mechatronic devices maintain peak performance even as demands increase.

8. Implementing Predictive Maintenance for Mechatronic Systems

Proactive failure prevention represents the ultimate goal for mechatronic system maintenance in Industry 4.0 environments. Forward-thinking organizations have already moved beyond traditional reactive approaches, adopting sophisticated techniques that anticipate problems before they occur.

Machine learning models for failure prediction

Advanced machine learning algorithms fundamentally transform maintenance practices for mechatronic systems. The XG Boost Classifier demonstrates remarkable effectiveness among traditional machine learning approaches, while Long Short-Term Memory (LSTM) networks provide superior accuracy compared to both conventional machine learning methods and Artificial Neural Networks (ANN). Practically speaking, these algorithms analyze vibration signatures—often the key indicator of machine condition—to detect faults in rotating machinery. Data-driven prognostic analysis approaches effectively predict mechanical component failures based on degradation paths, ultimately estimating remaining useful life with high accuracy. Supervised machine learning models, including accumulative neural networks, maintain the increasing trend and monotony of degradation paths, enabling accurate failure forecasting even for mechatronic devices with complex structures.

Condition-based maintenance scheduling

Condition-based maintenance (CBM) fundamentally differs from traditional time-based approaches. Instead of performing maintenance on a predetermined schedule, CBM relies on monitoring the actual condition of mechatronic equipment to determine precisely when intervention becomes necessary. This maintenance strategy employs sensors and monitoring equipment to collect performance data, currently analyzed through algorithms, machine learning, and AI to identify patterns indicating maintenance issues. Technically, CBM follows a structured lifecycle including planning, implementation, monitoring, analysis, and continuous improvement. Maintenance teams typically establish performance baselines—operating, historical, or manufacturer-specified parameters—as reference points for measuring equipment condition changes. Eventually, this approach minimizes unnecessary maintenance while focusing resources on truly needed interventions.

Digital twin implementation for system simulation

Digital twins effectively revolutionize mechatronic system maintenance through realistic virtual representations that reflect current conditions of physical assets. These dynamic models enable organizations to investigate how their mechatronic production systems perform under different circumstances without risking actual equipment. Directly enhancing control strategies, digital twins coupled with Smart Big Data (SBD) enable Smart Predictive Maintenance (SPM), undeniably a new frontier for mechatronic engineers. By evaluating individual component dynamics through simulation, maintenance professionals develop better control algorithms that extend equipment life. The digital twin concept has markedly evolved beyond simple modeling, now incorporating semantic technologies that generate new services—especially in operation and service phases—like Digital Plant Companions.

9. Conclusion

Mechatronic device failures present significant challenges for manufacturers transitioning to Industry 4.0, yet practical solutions exist through strategic modernization and maintenance approaches. Legacy systems face mounting pressure from compatibility issues, processing limitations, and data management constraints. These challenges, combined with security vulnerabilities and integration hurdles, threaten production capabilities across industries.

Smart implementation of diagnostic tools, hardware upgrades, and software solutions offers manufacturers viable paths forward. Continuous monitoring systems, performance baselines, and failure pattern recognition techniques help identify potential issues before they cause significant disruption. Strategic hardware modernization through modular components, enhanced sensor networks, and processing power upgrades extends equipment lifespan while maintaining compatibility with modern systems. Predictive maintenance, powered by machine learning and digital twin technology, represents the future of mechatronic system management. These advanced approaches enable manufacturers to anticipate and prevent failures before they occur, significantly reducing downtime and maintenance costs. Additionally, edge computing adaptations and middleware implementations help bridge the gap between legacy equipment and modern Industry 4.0 requirements. Success in the evolving manufacturing landscape requires a balanced approach to mechatronic system management. Through careful consideration of both technical requirements and practical constraints, manufacturers can effectively modernize their existing infrastructure while maintaining operational stability. This strategic evolution ensures continued competitiveness without sacrificing the reliability that modern production environments demand.

References:

[1] J. Lee, B. Bagheri, and H. Kao, "A cyber-physical systems architecture for Industry 4.0-based manufacturing systems," Manuf. Lett., vol. 3, pp. 18–23, 2015.

[2] F. Tao, Q. Qi, L. Wang, and A. Nee, "Digital twins and cyber–physical systems toward smart manufacturing," Engineering, vol. 5, no. 4, pp. 653–661, 2019.

[3] H. Kagermann, W. Wahlster, and J. Helbig, "Recommendations for implementing Industry 4.0," German National Academy of Science and Engineering (Acatech), 2013.

[4] A. Gilchrist, Industry 4.0: The Industrial Internet of Things. Springer, 2016.

[5] A. M. Madni and S. Jackson, "Towards a conceptual framework for resilience engineering," IEEE Syst. J., vol. 3, no. 2, pp. 181–191, 2011.

[6] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: Automation networks in the era of the Internet of Things," IEEE Ind. Electron. Mag., vol. 11, no. 1, pp. 17–27, 2017.

[7] L. Monostori, "Cyber–physical production systems: Roots, expectations and R&D challenges," Procedia CIRP, vol. 17, pp. 9–13, 2014.

[8] G. Qu, M. Potkonjak, and J. Hu, "Security challenges in IoT-enabled cyber-physical systems," IEEE Trans. Multi-Scale Comput. Syst., vol. 4, no. 1, pp. 1–13, 2018.

[9] S. Yin, X. Li, H. Gao, and O. Kaynak, "Data-based techniques focused on modern industrial systems: A review," IEEE Trans. Ind. Electron., vol. 62, no. 1, pp. 657–667, 2015.

[10] A. R. Al-Ali et al., "Internet of Things-enabled smart automation systems," IEEE Trans. Autom. Sci. Eng., vol. 17, no. 4, pp. 1617–1630, 2020.

[11] M. Brettel, N. Friederichsen, M. Keller, and M. Rosenberg, "How virtualization, decentralization and network building change the manufacturing landscape," Procedia CIRP, vol. 6, pp. 81–86, 2014.

[12] R. S. M. Goh, S. S. Goh, and A. K. Gupta, "Security in cyber-physical systems for Industry 4.0," IEEE Access, vol. 8, pp. 132084–132103, 2020.

[13] L. Ribeiro and A. Barata, "Lessons learned from maintenance failures in cyber-physical production systems," IFAC-PapersOnLine, vol. 51, no. 11, pp. 587–592, 2018.

[14] T. Stock and G. Seliger, "Opportunities of sustainable manufacturing in Industry 4.0," Procedia CIRP, vol. 40, pp. 536–541, 2016.

[15] P. Leitão, S. Karnouskos, and L. Ribeiro, "Industrial agents for cloud manufacturing and industrial IoT," IEEE Trans. Ind. Informat., vol. 14, no. 4, pp. 1890–1900, 2018.

[16] R. Y. Zhong et al., "Intelligent manufacturing in the context of Industry 4.0," Int. J. Prod. Res., vol. 56, no. 8, pp. 2941–2962, 2018.

[17] M. Hermann, T. Pentek, and B. Otto, "Design principles for Industrie 4.0 scenarios," Hawaii Int. Conf. Syst. Sci., pp. 3928–3937, 2016.

[18] S. Karnouskos, "Cyber-physical systems in the smart grid," IEEE Trans. Ind. Informat., vol. 14, no. 6, pp. 2700–2712, 2018.

[19] M. A. Cusumano and D. Yoffie, Competing in the Age of AI. Harvard Business Review Press, 2020.

[20] S. Wang, G. Wang, S. Liu, and J. Zhang, "Predictive maintenance modeling for Industry 4.0," IEEE Trans. Autom. Sci. Eng., vol. 17, no. 4, pp. 2064–2076, 2020.

[21] F. Almada-Lobo, "The Industry 4.0 revolution and the future of manufacturing execution systems," J. Innov. Manage., vol. 3, no. 4, pp. 16–21, 2015.

[22] S. H. Yang et al., "Industrial IoT and advanced automation: System integration challenges," IEEE Ind. Electron. Mag., vol. 14, no. 3, pp. 85–96, 2020.

[23] M. B. Erol, A. J. Levy, and P. B. Schönsleben, "Industry 4.0 workforce readiness: Skill gaps and training," Int. J. Adv. Manuf. Technol., vol. 97, pp. 1389–1405, 2018.