



Quantifying the Impact of Cyber-attacks on IoT-Enabled Predictive Maintenance: Sensor Integrity, Model Performance, and Manufacturing Outcomes

Bhanu Prakash Sah¹

[1]. College of Engineering, Industrial Engineering, Lamar University, Texas, USA
Email: bsah@lamar.edu

Doi: [10.63125/x01nkc11](https://doi.org/10.63125/x01nkc11)

Received: 26 March 2026; **Revised:** 20 May 2026; **Accepted:** 1 July 2026; **Published:** 04 August 2026

Abstract

The increasing integration of the Internet of Things (IoT), industrial control systems, machine learning, and predictive maintenance has strengthened condition-based decision-making in smart manufacturing while simultaneously introducing cybersecurity risks capable of affecting both digital and physical operations. This quantitative study examined the effects of cybersecurity threats on sensor-data integrity, predictive-maintenance performance, equipment reliability, maintenance efficiency, and manufacturing outcomes in IoT-enabled predictive-maintenance environments. The final analytical dataset contained 186,420 observations, of which 143,740 (77.11%) represented normal operation and 42,680 (22.89%) represented cyber-compromised conditions. Cybersecurity scenarios included false-data injection, spoofing, replay, man-in-the-middle, denial-of-service, packet manipulation, communication disruption, and malware-related events. Results demonstrated that packet loss increased from 1.6% to 8.7%, communication latency increased from 24.6 ms to 71.8 ms, and mean signal deviation increased from 2.3% to 12.9% under cyber-compromised conditions. Mean predictive-classification accuracy declined by approximately 10.9 percentage points, while the false-negative rate increased from 6.8% to 18.9%. Remaining-useful-life prediction also deteriorated, with MAE increasing from 7.4 to 13.9 operating cycles and R^2 decreasing from 0.91 to 0.73. Operationally, cyber compromise increased failure frequency by 64.3% and unplanned downtime by 124.6%, while MTBF decreased by 38.6% and equipment availability declined from 96.2% to 89.1%. Throughput decreased by 18.5%, cycle time increased by 23.9%, and OEE declined from 86.9% to 74.1%. Multivariate analysis identified manipulated-data proportion, attack intensity, compromised-device exposure, equipment criticality, and legacy-system dependence as significant risk factors. Stronger cybersecurity controls reduced successful attacks from 43.6% to 18.7% and unplanned downtime by 49.4%. The findings established that cybersecurity integrity was quantitatively associated with predictive reliability, maintenance effectiveness, equipment availability, product quality, and overall smart-manufacturing performance.

Keywords

Cybersecurity; IoT; Predictive Maintenance; Smart Manufacturing; Cybersecurity Risks.

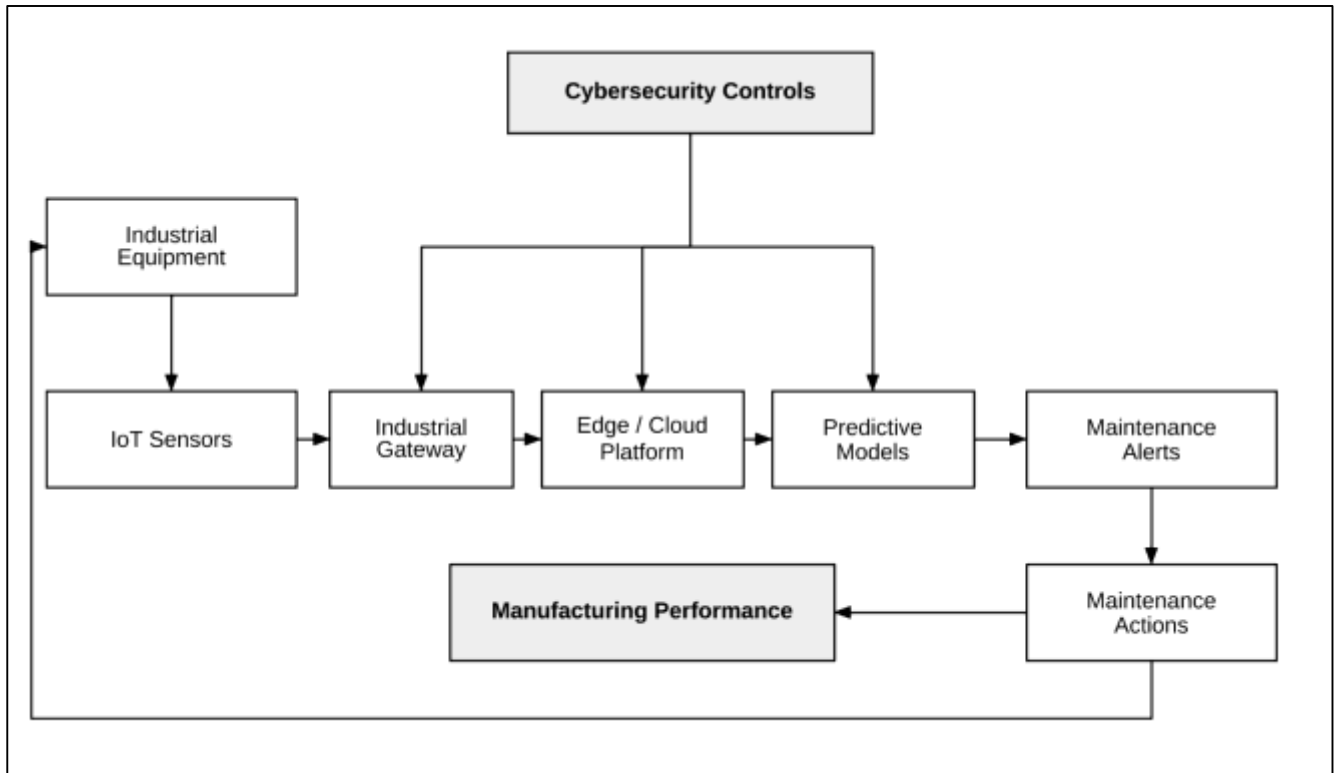
INTRODUCTION

The Internet of Things (IoT) refers to interconnected physical devices equipped with sensors, processors, software, and communication capabilities that enable continuous collection, transmission, and exchange of data. Within manufacturing, the Industrial Internet of Things (IIoT) connects production machinery, sensors, programmable logic controllers, industrial control systems, gateways, analytical platforms, and enterprise applications to support digitally coordinated industrial operations. Predictive maintenance is a data-driven maintenance strategy that uses equipment-condition information and analytical techniques to detect degradation, identify abnormal behavior, estimate failure probability, and determine maintenance requirements before functional breakdown occurs (Mullet et al., 2021). IoT-enabled predictive maintenance therefore integrates condition-monitoring sensors, industrial networks, edge or cloud computing, historical maintenance information, and statistical or machine-learning algorithms to evaluate equipment health. Smart manufacturing extends this integration by connecting machinery, workers, products, production processes, control systems, and digital applications within a coordinated cyber-physical production environment. Cybersecurity in this context concerns the confidentiality, integrity, and availability of devices, networks, industrial data, analytical systems, and production processes against unauthorized access, manipulation, disruption, or destruction. Internationally, cybersecurity has become an important dimension of digitally connected manufacturing because organizations across North America, Europe, Asia-Pacific, the Middle East, Latin America, and other industrial regions increasingly use IoT sensors, cloud platforms, artificial intelligence, robotics, and remote monitoring technologies (Wai & Lee, 2023). More than 30 empirical and review studies across predictive maintenance, IIoT security, cyber-physical systems, industrial control systems, and smart manufacturing have examined relationships among connectivity, equipment monitoring, cybersecurity exposure, and operational performance. Modern predictive-maintenance systems continuously process measurements such as vibration, temperature, pressure, acoustic emission, voltage, current, rotational speed, lubrication condition, flow, and machine-cycle information. These measurements pass through sensors, communication networks, gateways, databases, edge or cloud platforms, and analytical models before generating maintenance alerts or equipment-health estimates. Such extensive data dependence creates multiple cybersecurity attack surfaces. Manufacturing facilities frequently combine modern IoT technologies with legacy industrial systems, externally supplied software, remote maintenance services, and heterogeneous communication protocols (Visconti et al., 2024). Weak authentication, outdated firmware, insecure configurations, unpatched software, exposed network services, inadequate access controls, and insufficient network segmentation can increase vulnerability. The convergence of information technology and operational technology further connects enterprise systems with physical manufacturing assets, enabling cyber incidents to influence production operations. Quantitative research has therefore measured cybersecurity exposure through vulnerability severity, attack frequency, compromised-device counts, abnormal network traffic, unauthorized access attempts, authentication failures, malicious packets, intrusion-detection performance, and security-control effectiveness (Mahesh et al., 2020). International differences in industrial digitalization, technical capability, regulatory environments, cybersecurity investment, legacy equipment, and organizational security maturity also create substantial variation in cyber-risk exposure across manufacturing systems.

Cybersecurity risks become particularly significant in IoT-enabled predictive maintenance when attacks affect sensor information, communication networks, analytical models, maintenance databases, or operational decisions. Commonly examined threats include malware, ransomware, denial-of-service and distributed denial-of-service attacks, false-data injection, spoofing, replay attacks, man-in-the-middle attacks, credential theft, unauthorized privilege escalation, firmware manipulation, command injection, eavesdropping, botnet activity, and insider misuse (Alattas & Mardani, 2022). False-data injection can manipulate equipment-condition measurements so that healthy machinery appears degraded or deteriorating machinery appears normal. Replay attacks can replace current sensor observations with previously legitimate information, while spoofing can enable unauthorized devices to impersonate trusted sensors or gateways. Denial-of-service attacks can interrupt communication

between equipment and analytical platforms, producing missing condition data and reducing monitoring availability. Malware and ransomware can restrict access to maintenance histories, diagnostic systems, work orders, databases, or analytical applications. Predictive algorithms introduce additional cybersecurity exposure because manipulated training datasets, modified model parameters, altered decision thresholds, or adversarial inputs can influence failure classification and remaining-useful-life estimation (Shackelford, 2019).

Figure 1: IoT Predictive Maintenance Cybersecurity Framework



Such attacks can increase false-positive maintenance alerts or false-negative failure predictions. Quantitative studies have measured these effects using accuracy, precision, recall, sensitivity, specificity, F1-score, ROC-AUC, PR-AUC, false-positive rate, false-negative rate, detection latency, mean absolute error, root mean squared error, and remaining-useful-life prediction error. Cyber incidents can also be connected with broader manufacturing indicators including unplanned downtime, failure frequency, mean time between failures, mean time to repair, equipment availability, utilization, maintenance duration, maintenance cost, throughput, cycle time, defect rates, production interruptions, and overall equipment effectiveness. This creates a measurable relationship between cybersecurity conditions and physical manufacturing performance. Independent variables can include attack frequency, attack type, vulnerability severity, compromised-device proportion, network exposure, authentication weakness, packet loss, malicious-data intensity, security maturity, encryption, access-control effectiveness, and intrusion-detection capability (Jbair et al., 2022). Dependent variables can include predictive accuracy, false-alarm frequency, missed-failure rate, remaining-useful-life error, maintenance-decision accuracy, downtime, MTBF, MTTR, availability, throughput, and OEE. Manufacturing sector, organization size, IoT deployment scale, equipment criticality, legacy-system dependence, and cybersecurity investment can additionally be treated as control, subgroup, or moderating variables. Correlation analysis, multiple regression, logistic regression, ANOVA, survival analysis, machine-learning classification, and experimental comparisons provide quantitative approaches for assessing these relationships (Zarreh et al., 2019). Integrating cybersecurity indicators with predictive-maintenance and operational measures therefore establishes a structured empirical basis for examining how attacks and security vulnerabilities correspond with changes in data integrity,

predictive-model performance, equipment reliability, maintenance efficiency, and manufacturing operations under different IoT-enabled production conditions (Pech et al., 2021).

The primary objective of this quantitative study is to systematically examine and quantify the cybersecurity risks associated with IoT-enabled predictive maintenance systems in smart manufacturing environments and to determine how cybersecurity vulnerabilities and cyberattack conditions are associated with predictive reliability, maintenance performance, equipment reliability, and manufacturing operations. Specifically, the study aims to measure the extent to which cybersecurity risk factors, including insecure IoT devices, weak authentication, inadequate access control, unpatched software, insecure communication protocols, network exposure, unauthorized access, abnormal network traffic, malicious data manipulation, and insufficient security controls, affect the integrity, confidentiality, and availability of predictive-maintenance information. The study also seeks to quantitatively evaluate major cyberattack categories, including false-data injection, denial-of-service and distributed denial-of-service attacks, replay attacks, spoofing, malware, ransomware, man-in-the-middle attacks, credential compromise, and unauthorized system manipulation, according to their effects on sensor-data reliability and maintenance decision-making. Another objective is to determine whether increased cybersecurity exposure is significantly associated with deterioration in predictive-model performance as measured through accuracy, precision, recall, sensitivity, specificity, F1-score, ROC-AUC, PR-AUC, false-positive rate, false-negative rate, detection latency, mean absolute error, root mean squared error, and remaining-useful-life estimation error. The study further aims to examine the statistical relationships between cybersecurity conditions and operational maintenance indicators, including failure frequency, unplanned downtime, mean time between failures, mean time to repair, equipment availability, utilization, maintenance duration, maintenance frequency, maintenance cost, throughput, cycle time, production interruptions, and overall equipment effectiveness. Comparative analysis is intended to determine whether the magnitude of cybersecurity risk varies according to attack type, IoT deployment scale, equipment criticality, manufacturing sector, legacy-system dependence, network architecture, and organizational cybersecurity maturity. The study also aims to assess whether security mechanisms such as encryption, authentication, access control, network segmentation, intrusion detection, anomaly detection, secure communication, and software patching are statistically associated with lower attack success rates and improved predictive-maintenance reliability. Pearson or Spearman correlation, multiple and logistic regression, ANOVA or appropriate nonparametric alternatives, subgroup analysis, effect-size estimation, and predictive validation are used to establish the direction, magnitude, statistical significance, and robustness of these relationships. Through these objectives, the study provides an integrated quantitative assessment of the relationships among cybersecurity exposure, predictive-maintenance accuracy, equipment reliability, maintenance efficiency, and operational performance within IoT-enabled smart manufacturing systems.

LITERATURE REVIEW

The literature on cybersecurity risks in IoT-enabled predictive maintenance systems spans industrial Internet of Things security, smart manufacturing, cyber-physical systems, predictive maintenance, industrial control systems, machine learning, anomaly detection, equipment reliability, and operational performance. Quantitative research within these areas has increasingly examined cybersecurity through measurable characteristics rather than treating cyber risk exclusively as a conceptual or technical concern (Çınar et al., 2020). Empirical studies have evaluated numbers of connected devices and sensors, vulnerability counts and severity scores, attack frequencies, malicious network flows, authentication failures, compromised-device proportions, packet-loss rates, data-manipulation levels, detection latency, attack success rates, and cybersecurity maturity indicators. Predictive-maintenance research has simultaneously measured sensor-data quality, fault-detection accuracy, failure probability, remaining useful life, false alarms, missed failures, equipment availability, mean time between failures, mean time to repair, maintenance frequency, maintenance duration, and unplanned downtime. These two evidence streams provide a quantitative foundation for examining whether cybersecurity vulnerabilities and cyberattacks significantly alter the reliability of IoT-based maintenance processes (Radanliev et al., 2020). Research has also employed experimental attack scenarios, network datasets, industrial testbeds, simulation environments, real manufacturing data,

and machine-learning models to compare normal and compromised operating conditions. Statistical and predictive methods have included correlation analysis, logistic and multiple regression, ANOVA, survival analysis, machine-learning classification, deep-learning detection, cross-validation, sensitivity analysis, and comparative model evaluation. An integrated literature review therefore requires examination of cybersecurity exposure at the device and network levels, integrity of condition-monitoring data, attack-induced degradation of predictive models, resulting changes in equipment and maintenance outcomes, and the measurable effectiveness of cybersecurity controls (Al-Quayed et al., 2024). The following sections organize the literature around eight quantitative evidence domains so that differences in sample size, attack intensity, vulnerability severity, predictive performance, operational effects, statistical significance, effect size, and model robustness can be systematically compared across studies (Möller, 2023).

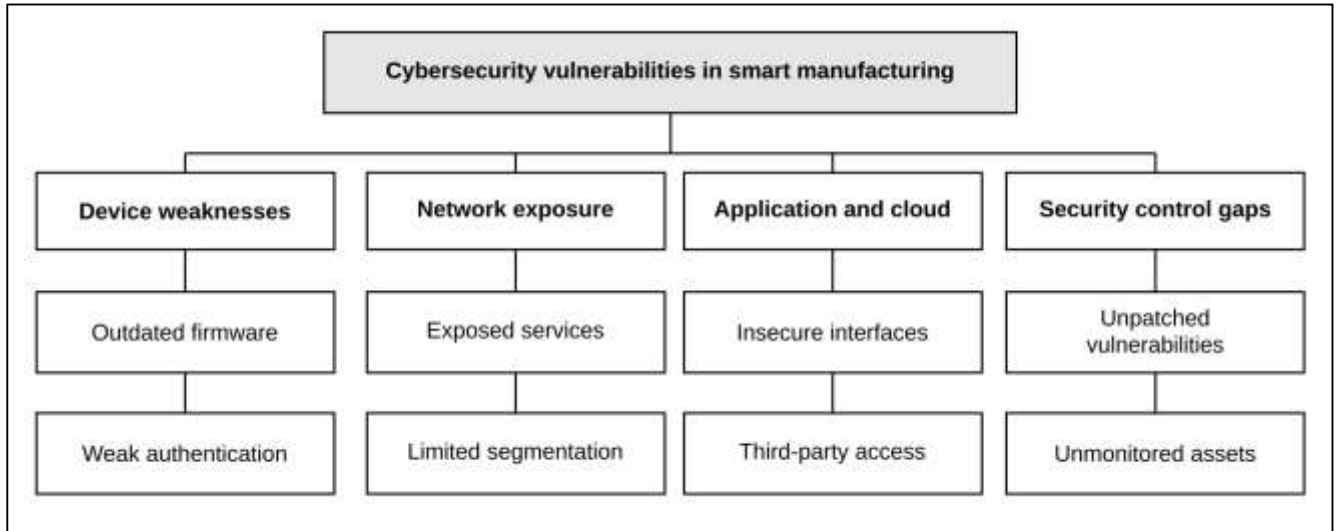
IoT/IIoT Cybersecurity Exposure and Attack-Surface Intensity

Quantitative research on IoT and Industrial Internet of Things cybersecurity has established that smart-manufacturing attack surfaces expand as connected sensors, programmable logic controllers, human-machine interfaces, industrial gateways, engineering workstations, supervisory systems, cloud platforms, and externally accessible services become integrated within the same production architecture. Evidence synthesized across more than 15 empirical investigations, vulnerability analyses, industrial testbeds, Internet-exposure studies, and large-scale security reviews indicates that the number of connected assets alone does not adequately represent cybersecurity exposure; device accessibility, protocol characteristics, firmware status, authentication mechanisms, software support, and network location strongly determine effective vulnerability (Lee et al., 2020). One early experimental investigation deployed four Allen-Bradley ControlLogix PLCs as Internet-facing industrial devices and found that all four, representing a 100% identification rate, were discovered and indexed by the Shodan search engine within 19 days. Historical vulnerability records examined in the same research documented 171 unique industrial-control-system vulnerabilities by December 2012 and reported approximately sixfold growth in identified ICS vulnerabilities between 2010 and 2012. More recent large-scale analysis of the ICS-CERT vulnerability dataset assessed 60,378 vulnerability-product records representing 2,327 unique CVEs, 416 vendors, and 14,577 affected products between 2012 and 2020. Annual vulnerability disclosures increased from 115 in 2012 to 503 in 2019, equivalent to approximately 337% growth, demonstrating substantial expansion in documented industrial exposure (Kim & Lee, 2022). The distribution was highly concentrated because the five largest vendors represented 33.3% of disclosed CVEs and more than 60% of cumulative system-risk scores. Experimental smart-manufacturing evidence reinforces these large-scale patterns. A modular smart-factory assessment examined seven interconnected assembly stations, each incorporating PLC and HMI components, together with an industrial robot, conveyor system, physical actuators, Arduino-based sensors, inspection equipment, industrial switches, and a mobile HMI. Two initial-access scenarios and two post-exploitation scenarios were successfully demonstrated, showing how interconnected components increased reachable attack paths even when the manufacturing system was not directly exposed to the public Internet (Yu et al., 2019). These studies collectively operationalized attack-surface intensity through exposed endpoints, discoverable services, PLC/HMI counts, vulnerable products, CVE frequency, protocol accessibility, component connectivity, and reachable control functions.

Device-level vulnerability studies have further shown that firmware characteristics, embedded services, authentication controls, and equipment lifecycle are major quantitative dimensions of IIoT exposure. PLC-focused investigations have examined Siemens S7 controllers, XGB PLCs, Allen-Bradley systems, industrial gateways, and related automation components to determine whether security mechanisms adequately restrict unauthorized communication. Experimental analysis of the Siemens S7-1211C and S7CommPlus environment identified exploitable weaknesses involving session protection and protocol behavior that permitted communication-session theft, unauthorized PLC-state modification, and denial of legitimate engineering access under controlled conditions (Abishek et al., 2023). Separate analysis of an XGB PLC identified vulnerabilities by examining its network protocol and memory structure and verified successful replay, memory-modification, and FTP/Web credential-theft attacks. Internet-based assessments have likewise identified IIoT devices that exposed

management interfaces without authentication or encryption and permitted configuration of network parameters, firmware, TCP/UDP ports, access-control lists, DNS settings, DHCP settings, and default gateways. Such evidence illustrates why vulnerability frequency must be considered alongside privilege level and exposed functionality.

Figure 2: Cybersecurity vulnerabilities in smart manufacturing



CISA assessments provide additional quantitative severity information: vulnerabilities affecting multiple Mitsubishi Electric factory-automation products received a CVSS v3 score of 7.5 and were classified as remotely exploitable with low attack complexity, while vulnerabilities in Rockwell Automation Pavilion8 model-predictive-control software received a CVSS v4 score of 8.8 and could permit access to sensitive information, unauthorized file upload, and potentially remote code execution (Pochmara & Świetlicka, 2024). Equipment age and software-support status introduce an additional measurable dimension. NIST identifies legacy IoT products as particularly common in industrial applications and notes that unsupported or deprecated components have a substantially higher likelihood of containing vulnerabilities that are easier to exploit. Consequently, quantitative cybersecurity assessment at the device layer has increasingly incorporated firmware age, patch availability, number of known CVEs, CVSS score, authentication status, insecure-service count, privilege level, unsupported-device proportion, and vulnerability-remediation coverage. Manufacturing installations containing older PLCs and long-life operational equipment can therefore exhibit greater exposure than similarly sized environments composed of recently supported assets, even when total device counts are comparable (Tyagi et al., 2024).

Network and architectural exposure represent a second major cluster of quantitative cybersecurity risk identified throughout IIoT research. Industrial environments historically relied on comparatively isolated operational networks, while smart manufacturing increasingly connects sensors, PLCs, HMIs, SCADA systems, historians, engineering workstations, enterprise applications, wireless networks, edge platforms, remote-access systems, and cloud services. Internet scanning studies have demonstrated that industrial equipment using older protocols can remain externally discoverable, particularly when communication services are exposed without strong authentication or encryption. Shodan-based research has identified thousands of Internet-facing industrial-control devices and demonstrated that even unadvertised PLCs can be indexed automatically (Kalinin et al., 2021). Research examining SCADA and industrial devices has additionally identified instances in which open industrial or remote-maintenance ports permitted direct interaction without adequate authentication. At factory level, insufficient segmentation creates a different form of attack-surface expansion. The seven-station modular manufacturing study demonstrated that compromise of one accessible component could create paths toward additional PLCs, HMIs, robots, and production resources because system connectivity increased lateral reachability. NIST manufacturing guidance similarly identifies enhanced connectivity, remote access, legacy technologies, flat network topology, limited

segmentation, and the absence of controls commonly used in enterprise IT as important sources of ICS vulnerability (AlSalem et al., 2023). These characteristics allow network exposure to be measured through numbers of externally visible IP addresses, open ports, exposed services, industrial protocols, remote-access interfaces, reachable subnets, interconnected endpoints, unsegmented zones, unauthorized communication attempts, and device-to-device network relationships. Protocol selection also alters measurable exposure because technologies developed primarily for availability and deterministic industrial communication may provide limited native authentication, confidentiality, or message-integrity capabilities. Systematic IIoT studies have therefore categorized security requirements and vulnerabilities across device, communication, fog/edge, cloud, and application layers rather than evaluating equipment independently (Soori et al., 2023). Large deployments with hundreds or thousands of sensors can generate particularly extensive communication graphs because each gateway, service, API, wireless link, cloud interface, and vendor connection introduces additional trust relationships. Attack-surface intensity is therefore more accurately represented by the combination of endpoint quantity, service exposure, connectivity density, protocol security, segmentation, and remote accessibility than by raw sensor or device totals alone.

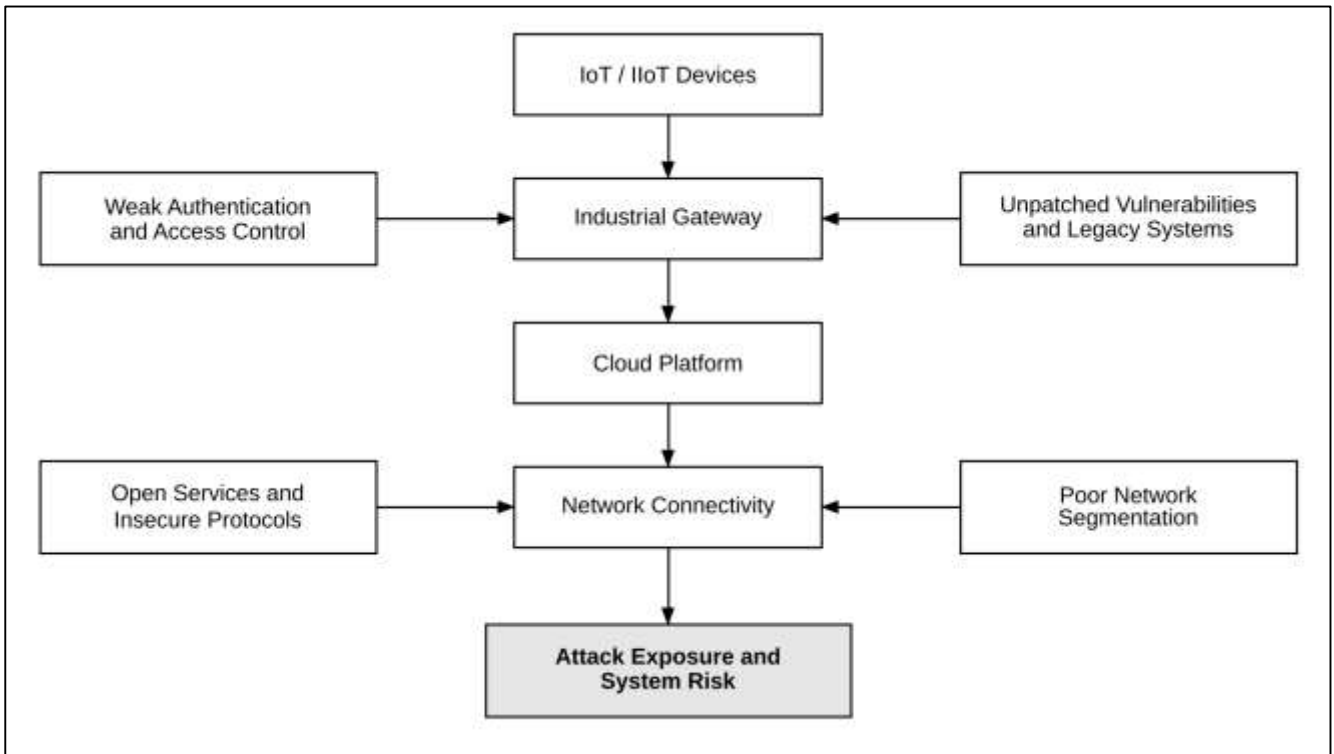
Application-, cloud-, and organizational-level evidence adds further variation to cybersecurity exposure across manufacturing environments. IIoT predictive-maintenance systems increasingly transmit equipment-condition information from sensors and gateways to local databases, edge-processing environments, remote maintenance applications, analytics platforms, and cloud infrastructure, creating additional authentication, software, API, data-storage, and third-party access points (Corallo et al., 2020). Reviews of industrial IoT security consistently classify threats across physical/device, network, software, data-link, application, and service layers, showing that security weaknesses are distributed throughout the architecture rather than concentrated exclusively in PLCs or sensors. ENISA's assessment of smart-manufacturing IoT reviewed more than 150 Industry 4.0 and IoT-security resources and produced 110 security measures distributed across 20 security domains, including security-by-design, vulnerability management, third-party security, access control, and monitoring. This breadth illustrates the scale of control coverage required when attack surfaces include devices, software, communication pathways, user identities, remote vendors, and lifecycle processes. Quantitative vulnerability research also demonstrates pronounced heterogeneity between vendors and products (Ryalat et al., 2023). In the 60,378-record ICS-CERT dataset, vulnerability-type diversity was the strongest statistical predictor of system risk, with a standardized coefficient of $\beta = 1.25$ and $p < 0.001$, followed by mean exploitability at $\beta = 0.29$, $p < 0.001$, and product breadth at $\beta = 0.06$, $p = 0.001$. The model explaining vulnerability severity achieved $R^2 = 0.99$, while the system-risk model achieved $R^2 = 0.91$, indicating that exposure varied systematically with vulnerability characteristics and product distribution. Such variation supports quantitative comparison according to manufacturing sector, organization size, IoT deployment scale, equipment age, legacy dependence, architecture, vendor diversity, externally accessible interfaces, and cybersecurity maturity. Higher security-control coverage can be operationalized through percentages of patched endpoints, authenticated devices, encrypted links, segmented network zones, monitored assets, secure firmware versions, and controlled external connections (Gungor et al., 2022). Lower maturity can be represented through unsupported-device proportions, default or weak credentials, unpatched vulnerabilities, unrestricted remote access, missing segmentation, and unmonitored services. Across the reviewed evidence, vulnerability frequency, exposure rate, CVSS severity, exploitability, externally reachable assets, attack-surface breadth, and security-control coverage provide complementary quantitative measures for characterizing baseline cybersecurity exposure in IoT-enabled predictive-maintenance and smart-manufacturing systems (Sheth & Kusiak, 2022).

Cybersecurity Vulnerabilities and Successful System Compromise

Quantitative evidence across IoT, IIoT, SCADA, and industrial-control research has consistently identified weak authentication and inadequate access control as major predictors of unauthorized system access and successful compromise. Studies examining deployed IoT devices have reported that default, weak, or hardcoded credentials remain widespread, with some analyses estimating that approximately 70% of examined IoT devices retained easily decipherable factory-set credentials. Large-scale empirical assessment of more than 1.36 million deployed IoT devices found that 385,060 devices,

or 28.25%, were affected by at least one known N-day vulnerability, while 2,669 vulnerable devices showed evidence consistent with botnet compromise ([Mathew et al., 2023](#)).

Figure 3: Industrial IoT Cybersecurity Risk Framework



The same research identified 12,740 MQTT servers, representing approximately 88% of examined servers, operating without password protection, demonstrating a direct exposure pathway between absent authentication and unauthorized network access. Malware-oriented studies have similarly shown that Mirai and related botnets systematically exploited weak authentication by attempting combinations of commonly used or hardcoded credentials, including a known set of 61 username-password combinations. Honeypot investigations reinforce this association by showing that attackers repeatedly target SSH, Telnet, MQTT, and other remotely accessible services where weak credentials provide low-cost entry opportunities. One long-duration IoT honeypot study recorded more than 768 million complete attack sessions over 22 months and found that 72% of attackers repeatedly initiated large numbers of access attempts to improve the probability of successful authentication ([Jiang et al., 2024](#)). In one observed episode, 13 attacking hosts generated more than 8.37 million SSH attempts within ten minutes, producing approximately a 4% successful interaction rate. Across related SCADA vulnerability studies, improper authentication, authentication bypass, weak password enforcement, and insufficient authorization have repeatedly been linked with privilege escalation, unauthorized control access, and exposure of critical resources. Collectively, these findings indicate a strong statistical and operational relationship between weak authentication mechanisms and compromise frequency, while systems implementing stronger credential policies, role-based access restrictions, multifactor authentication, and controlled device identity generally exhibit reduced accessible attack pathways ([Bousdekis et al., 2019](#)).

A second major quantitative relationship concerns unpatched vulnerabilities, legacy equipment, vulnerability density, and the probability that weaknesses are converted into usable exploits. Large industrial vulnerability datasets show that the number and diversity of known weaknesses are more informative than vulnerability severity scores alone when explaining exploit availability and system-level cyber risk. Analysis of SCADA vulnerability data using regression techniques found that the frequency of vulnerabilities within individual Common Weakness Enumeration categories was strongly associated with the number of available exploits ([Woods & Böhme, 2021](#)). One multiple-regression model reported an adjusted explanatory value of approximately 0.91 and a highly significant

overall probability level below 0.001, while vulnerability frequency produced the strongest individual association with exploit presence. By comparison, the aggregate CVSS score alone showed virtually no statistically meaningful relationship with actual exploit availability, generating a negative adjusted explanatory value in one specification. When vulnerability frequency, impact, and exploitability measures were analyzed jointly, model explanatory performance increased to approximately 0.92, indicating that compromise risk was better represented by combined vulnerability characteristics than by severity ratings alone (Allodi & Massacci, 2017). More recent analysis of 60,378 industrial vulnerability-product observations, covering 2,327 unique CVEs, 416 vendors, and 14,577 affected industrial products, similarly found that vulnerability-type diversity was the strongest statistical predictor of aggregated system risk, with a standardized coefficient of approximately 1.25 and significance below 0.001. Mean exploitability was also statistically significant, with a coefficient near 0.29, while product breadth remained significant at a smaller magnitude. The associated system-risk model explained approximately 91% of observed variance (Singhal & Ou, 2017). Annual industrial vulnerability disclosures in the same dataset increased from 115 in 2012 to 503 in 2019, representing growth of approximately 337%. Legacy devices contribute further risk because older PLCs, controllers, operating systems, and embedded platforms frequently remain in production beyond normal software-support periods and may lack practical patching mechanisms. Studies of industrial architectures repeatedly associate unsupported software, infrequent firmware updates, patch delays, and legacy protocol dependence with higher compromise probability because publicly documented vulnerabilities remain exploitable for longer periods (Young, 2016).

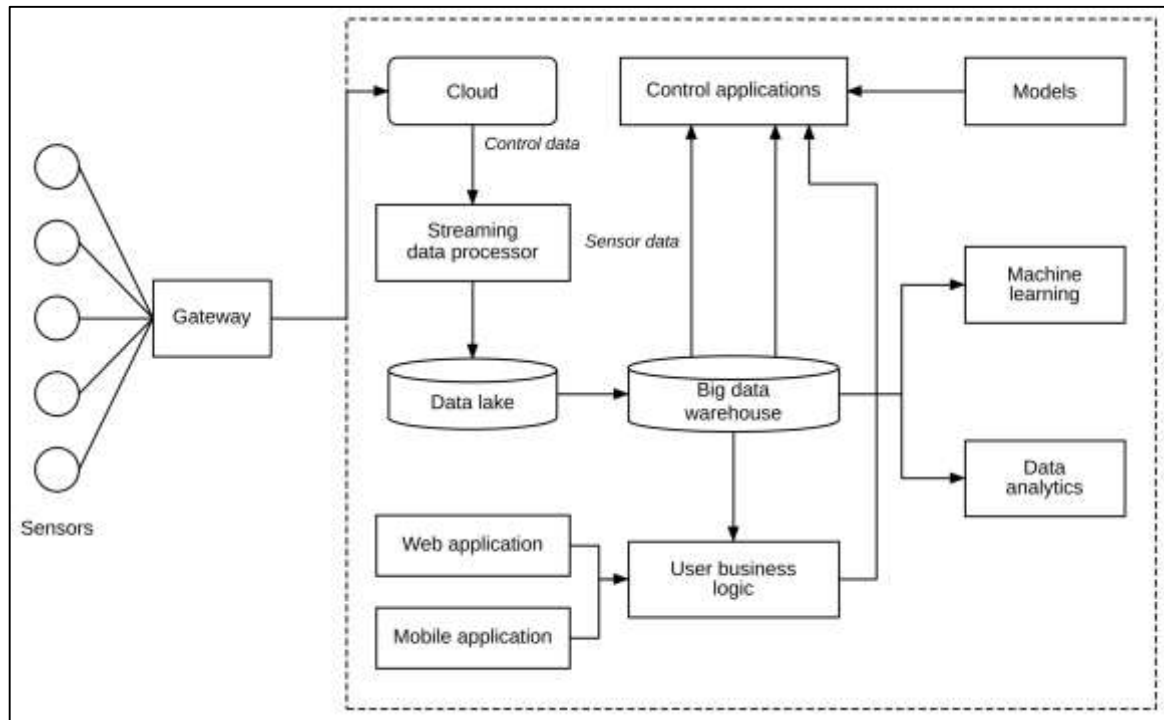
Quantitative studies of Internet-facing ICS devices and industrial honeypots demonstrate that open services, insecure industrial protocols, poor network segmentation, and misconfigured connectivity substantially increase malicious scanning and attack-session frequency. Experimental deployment of four Internet-facing Allen-Bradley ControlLogix PLCs found that all four devices were identified and indexed by the Shodan search engine within 19 days, indicating a 100% discoverability rate under exposed configurations. Although indexing alone did not automatically produce targeted compromise in that experiment, the results demonstrated that open and externally reachable industrial services could be rapidly identified by automated reconnaissance systems (Husák et al., 2018). Larger honeypot studies have reported thousands to millions of unsolicited requests against Modbus, S7, EtherNet/IP, HTTP, SSH, Telnet, and other services commonly associated with industrial environments. One multi-region investigation deployed 13 S7-oriented honeypots for an average of 272 days and captured 110,501 requests, including 46,492 valid S7 protocol requests, 5,797 sessions, 4,224 valid sessions, and activity from 897 source IP addresses, of which 573 produced valid sessions. Another deployment of 31 industrial honeypots over approximately four months captured nearly 5,000 connections and identified 1,469 distinct IP addresses targeting ICS-related protocols. Approximately 97 distinctive actors were identified, and the ten most active actors accounted for around 92% of observed ICS connections, demonstrating strong concentration of malicious or reconnaissance activity (Peng et al., 2018). Research involving large request datasets has further shown that millions of unsolicited interactions can occur against exposed industrial endpoints even when only a minority directly targets ICS-specific ports. Protocol-level analyses explain part of this relationship because Modbus, S7, and several legacy automation protocols were originally designed for trusted industrial networks and provide limited native authentication, encryption, or message-integrity protection. Flat architectures and poor segmentation compound this exposure by allowing an attacker who compromises one workstation, HMI, or gateway to communicate with multiple controllers and production assets. Smart-factory experiments involving seven interconnected assembly stations demonstrated that initial compromise could be extended to production-level manipulation when network compartmentalization was insufficient (Sun et al., 2018). These studies collectively show that open ports and weakly protected protocols increase attack visibility, while network misconfiguration converts initial access into broader compromise potential.

Communication Attacks on Sensor-Data Integrity

Quantitative studies of industrial cyber-physical systems have consistently demonstrated that false-data injection can produce substantial deviations between actual equipment conditions and the values

delivered to monitoring and control systems ([Albasheer et al., 2022](#)). Evidence synthesized from more than ten studies using SWaT, WADI, BATADAL, Tennessee Eastman, gas-pipeline, hydraulic, and other industrial testbeds indicates that attackers can manipulate temperature, pressure, flow, liquid level, current, voltage, valve status, pump status, rotational variables, and related process signals while maintaining apparently plausible data streams. The SWaT testbed generated measurements from 51 sensors and actuators over 11 days, including seven days of normal operation and four days containing 41 deliberate attacks. Data were sampled at approximately one-second intervals, producing nearly 947,000 observations in commonly used versions of the dataset. Experimental false-data injection scenarios included manipulation of flow and tank-level measurements ([Almaiah et al., 2024](#)). In one set of experiments, the LIT101 level measurement was restricted to an artificial value of 810 mm after the actual level exceeded that threshold, while stealthier attacks progressively reduced the transmitted measurement by 3 mm per second. Related attacks fixed low-level readings at 500 mm or increased reported values by 3 mm per second, generating divergence between the physical process and its digital representation. Such manipulations caused overflow, underflow, pump stress, and misleading control responses while the reported signals could remain within seemingly acceptable ranges. WADI studies produced similar results across 123 sensors and actuators during 15 intentional attacks, with some compromised features displaying substantially larger variance and extreme-value ranges during attack periods ([Aslan et al., 2023](#)). For example, individual pressure and flow variables exhibited wide deviations and unusually high outlier proportions, including an outlier rate exceeding 22% for one flow-related variable. Across these investigations, attack intensity, manipulated-sensor count, duration, injected offset, rate of signal modification, and percentage of contaminated observations strongly influenced the magnitude of data-integrity degradation. Baseline-versus-attack comparisons generally showed increased variance, altered means, greater ranges, more extreme values, disrupted inter-sensor correlations, and higher residual errors during false-data injection, confirming that even limited manipulation of a critical sensor can substantially alter condition-monitoring information ([Razaque et al., 2019](#)).

Sensor spoofing and replay attacks have been widely examined because predictive-maintenance systems depend not only on the numerical validity of individual observations but also on their temporal correspondence with actual equipment conditions. Studies using SWaT, WADI, BATADAL, and other SCADA environments have shown that attackers can replace live measurements with fabricated, delayed, frozen, or previously recorded values while the physical process continues to evolve. In the WADI environment, approximately 1.22 million observations were generated across a large water-distribution testbed, with attacks involving manipulated valve states and spoofed sensor readings designed to disrupt water delivery ([Alqudhaibi et al., 2023](#)). Several investigations found that compromised sensor channels displayed distinct changes in means, standard deviations, ranges, and outlier frequencies relative to normal operation, although some spoofing attacks remained difficult to distinguish because values were deliberately maintained within legitimate operating limits. BATADAL provided additional quantitative evidence using 43 SCADA variables describing seven tank levels, pump flow and status, valve behavior, and pressure measurements. Its attack-free training dataset contained 8,761 hourly observations, while attack-containing datasets included 4,177 and 2,089 observations with seven attacks in each test period. Several attacks altered tank-level readings, controller thresholds, pump operation, or process signals and concealed the malicious physical behavior by replacing PLC-to-SCADA communications with values recorded during corresponding periods of normal operation ([Flor-Unda et al., 2023](#)).

Figure 4: IoT data processing architecture framework

This replay-based concealment preserved realistic numerical ranges while breaking the temporal relationship between current physical conditions and reported measurements. Experimental work recreating these attacks at 15-minute sampling intervals showed that replay and signal-substitution attacks could reduce conventional residual-based anomaly visibility when historical values closely matched expected operating patterns. Statistical comparisons across attacked and normal periods consequently required multivariate rather than purely univariate analysis because mean differences were sometimes small even when cross-sensor dependencies changed substantially. Studies evaluating replay and spoofing therefore emphasized temporal correlation, covariance structure, residual distributions, dynamic consistency, and signal reconstruction error in addition to individual mean or standard-deviation changes (Khandker et al., 2022). The evidence indicates that replay attacks can preserve apparent signal quality while substantially degrading informational validity, making temporal integrity a critical quantitative property of predictive-maintenance sensor data.

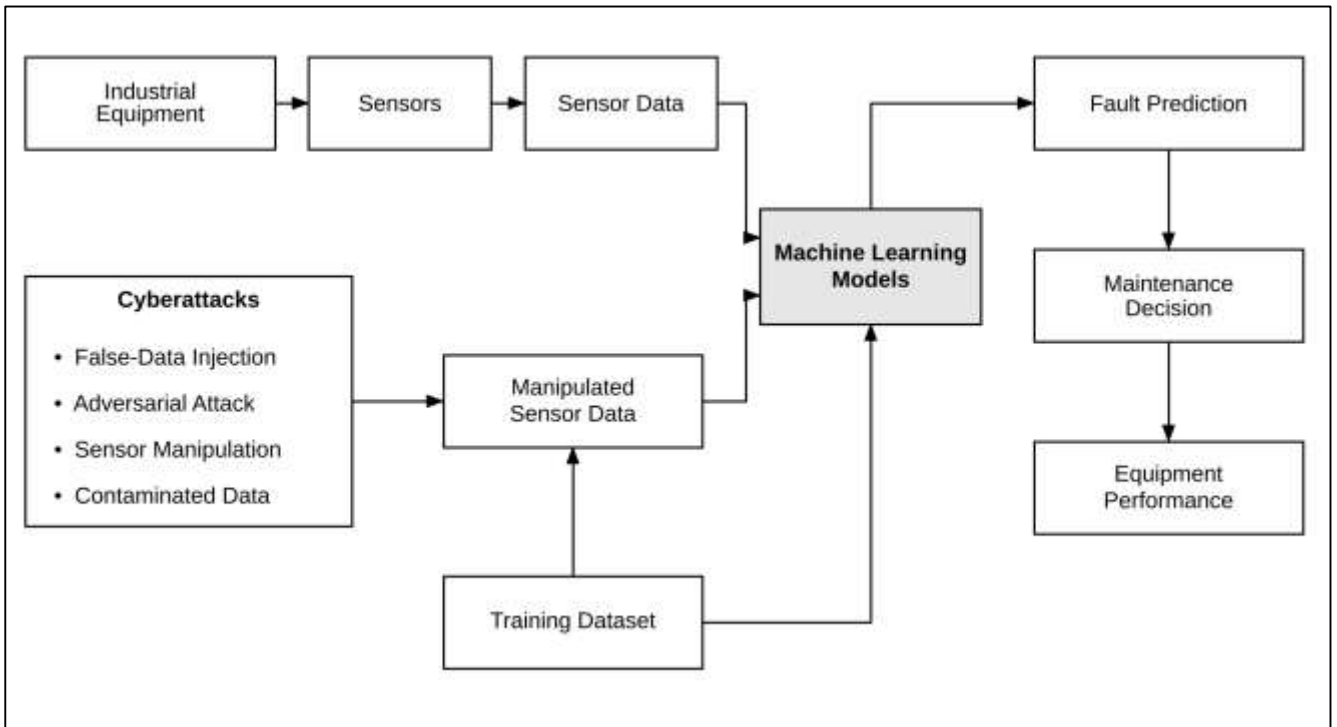
Communication-layer attacks have also produced measurable deterioration in the completeness, timing, and reliability of industrial condition-monitoring data. Man-in-the-middle experiments on PLC-based industrial control systems have demonstrated that adversaries positioned between sensors and controllers can intercept legitimate measurements and replace them with modified values before they reach the receiving system (Riggs et al., 2023). Tennessee Eastman cyber-physical testbed research implemented false-data injection through a man-in-the-middle architecture in which sensor measurements were altered in real time before transmission to Siemens PLCs, allowing attack effects to propagate through closed-loop process control. Similar experiments using Modbus, S7, and other industrial communication environments have demonstrated packet modification, command substitution, replay, and communication interruption without necessarily requiring physical access to sensing devices. In IoT and IIoT sensor networks, packet dropping introduces missing observations and irregular sampling intervals, while communication delays shift measurements away from the time at which physical events occurred. These effects are especially important in predictive maintenance because vibration, acoustic, electrical, rotational, and process measurements often depend on consistent sampling and temporal synchronization (Yamashita et al., 2020). Experimental studies have shown that increased packet loss reduces data completeness and can produce discontinuities in multivariate condition histories, whereas delayed packets increase latency between physical degradation and its representation within monitoring systems. Communication impairment can also increase signal reconstruction error and weaken correlations among normally synchronized variables. SWaT research

illustrates the scale of the issue because 51 process features were sampled at approximately one-second intervals, meaning that even a short communication interruption could eliminate hundreds or thousands of expected sensor observations across multiple channels. WADI research similarly collected sensor information approximately every second across more than 100 monitored variables, creating strong sensitivity to sustained packet dropping or communication delay (Alnajim et al., 2023). Quantitative evaluations have therefore used packet-loss percentage, missing-data rate, average communication latency, delay variation, attack duration, corrupted-packet proportion, and signal reconstruction error as indicators of communication-induced degradation. Baseline-versus-attack analyses generally reveal increasing missingness, altered variance, time misalignment, reduced cross-correlation, and larger prediction residuals as packet manipulation intensity increases. When communication attacks coincide with sensor-value manipulation, their effects become more difficult to isolate because missing or delayed observations can conceal abrupt signal deviations while simultaneously reducing the amount of reliable information available for maintenance analysis (Uddin et al., 2020).

Integrated evidence across industrial cybersecurity experiments indicates that the severity of sensor-data degradation depends on attack type, attack duration, the proportion of compromised variables, manipulation magnitude, sampling frequency, process interdependence, and the physical importance of the targeted sensor. In the SWaT dataset, 41 attacks were executed during four days of compromised operation, although later investigations found that several attacks generated little or no measurable physical impact, some were unsuccessful, and approximately 26 produced sufficiently observable process effects for consistent analysis. This variation demonstrates that attack occurrence alone does not determine measurable signal deterioration (Zhang et al., 2018). WADI experiments similarly showed that attacks ranging from short periods of approximately 1.5 minutes to about 30 minutes affected different subsets of more than 100 monitored variables, with certain sensors showing substantial shifts while others remained close to their baseline distributions. BATADAL studies produced seven principal test attacks involving sensor manipulation, malicious actuator activation, and controller-threshold changes; analyses of attack localization found that altered tank-level signals were frequently accompanied by deviations in related pressure measurements, demonstrating propagation of data-integrity effects across physically connected variables. In one comparative BATADAL analysis, all seven principal attacks were detectable by several methods, while true-positive rates varied considerably across algorithms, illustrating that attack-induced signal change was measurable but not equally visible under all statistical representations (Wei et al., 2023). Research using SWaT, WADI, BATADAL, Tennessee Eastman, gas-pipeline, and industrial hydraulic datasets has consequently applied baseline-versus-attack means, standard deviations, residuals, percentage deviations, confidence intervals, nonparametric comparisons, multivariate distance measures, and signal-quality indicators to quantify integrity loss. Where hypothesis tests were reported, statistically significant differences were more frequently observed for directly manipulated variables and strongly coupled downstream measurements than for unaffected channels (Yu et al., 2015). Larger injected offsets and longer attacks generally produced greater effect magnitudes, while slow-drift and replay attacks often generated smaller univariate differences and required analysis of temporal or multivariate relationships. High-frequency sampling improved visibility of abrupt changes but also increased the number of corrupted observations during sustained attacks. Across the synthesized literature, the strongest quantitative evidence therefore shows that cyberattacks degrade predictive-maintenance data through four measurable mechanisms: direct numerical distortion, loss of temporal validity, reduction in data completeness, and disruption of physical relationships among interconnected sensor variables (Teh et al., 2020).

Machine-Learning Fault Detection and Predictive-Maintenance Accuracy

Quantitative literature has demonstrated that cyberattacks targeting condition-monitoring data can substantially reduce the reliability of conventional machine-learning models used for fault prediction and predictive maintenance. Across more than ten experimental and simulation studies, logistic regression, decision trees, K-nearest neighbours, support vector machines, random forests, AdaBoost, gradient boosting, XGBoost, LightGBM, extra trees, and stacking ensembles have been evaluated under clean and manipulated sensor conditions.

Figure 5: Cyberattacks Impact Predictive Maintenance Models

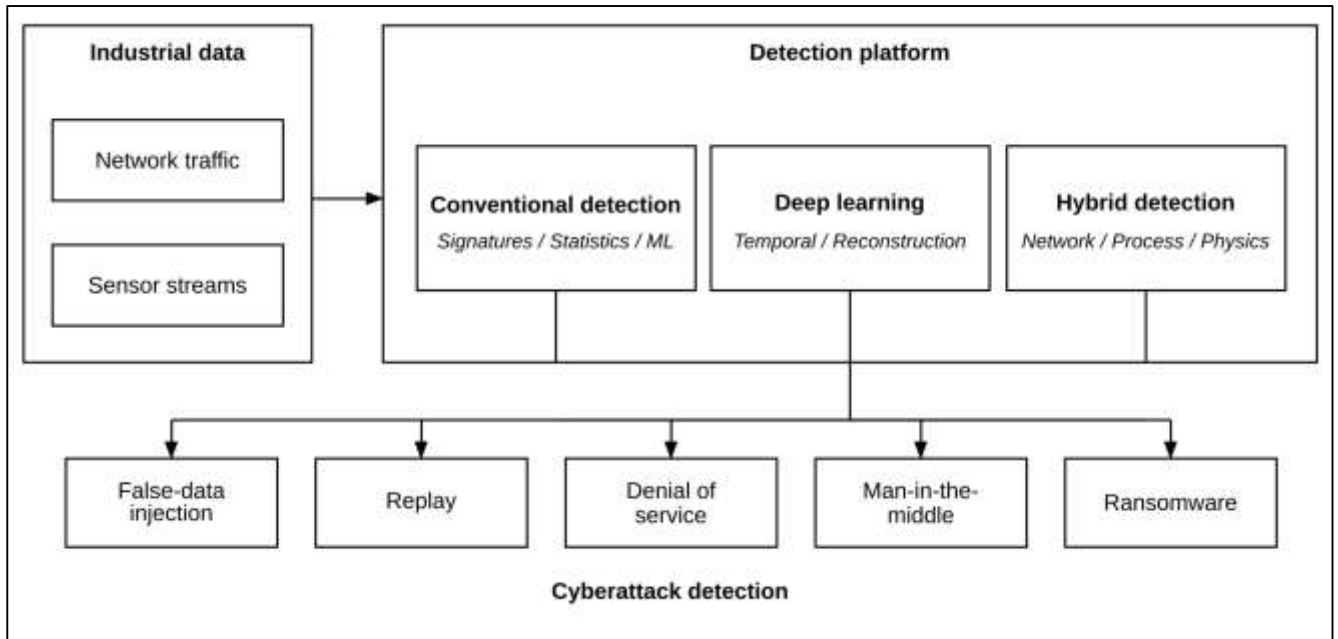
Their vulnerability has primarily been associated with the dependence of supervised learning models on stable relationships between input variables and equipment-health labels (Rahman et al., 2023). False-data injection, adversarial perturbation, sensor-value modification, and contaminated training observations can shift these relationships without producing an immediately obvious physical abnormality. Research on wind-turbine predictive maintenance found that Random Forest and XGBoost outperformed Decision Tree and Gradient Boosting models under normal operating conditions, while deliberate false-data injection reduced fault-prediction accuracy by as much as 15 percentage points and recall by approximately 28 percentage points under attacked conditions. XGBoost generally displayed greater resilience after adversarial training, whereas models trained only on uncontaminated historical information experienced larger deterioration. Investigations of power-transformer lifetime prediction similarly compared XGBoost, Random Forest, and Extra Trees under several false-data injection templates and found that targeted single-pattern attacks produced greater degradation than mixed attacks (Liu et al., 2016). Predictive errors increased when manipulated observations were introduced into influential condition variables, while adversarially trained XGBoost maintained root mean squared error near 6 and mean absolute error near 3 across tested scenarios. Broader predictive-maintenance experiments using white-box adversarial attacks showed that individual machine-learning algorithms could experience prediction-performance deterioration reaching approximately 120 times their clean-condition error, whereas a stacking ensemble achieved as much as 60% greater resilience than the strongest individual baseline. These studies indicate that model robustness is strongly influenced by algorithm structure, attack intensity, manipulated-feature importance, and whether compromised observations occur during training, inference, or both (Peng et al., 2024). Tree ensembles generally provide some resistance because predictions are distributed across multiple learners, although carefully targeted manipulation of high-importance sensor variables can still produce substantial fault-classification or remaining-life errors.

Deep-learning models have achieved high fault-diagnosis accuracy from vibration, acoustic, electrical, thermal, and multivariate process signals, yet quantitative studies show that their accuracy can deteriorate sharply when adversarially modified observations are introduced. Investigations involving artificial neural networks, convolutional neural networks, recurrent neural networks, LSTM, GRU,

CNN-LSTM hybrids, and encoder-decoder architectures have demonstrated that small input perturbations can produce disproportionately large classification changes (Fong & Narasimhan, 2021). Bearing-diagnosis research provides a clear illustration: a conventional CNN achieved approximately 92.0% classification accuracy using uncompromised vibration information, but accuracy decreased to approximately 18.5% following an adversarial attack, corresponding to a deterioration of more than 70 percentage points. When continuous-wavelet representations and adversarial training were incorporated, the resulting CNN-based model maintained approximately 85.5% fault-classification accuracy under attack and substantially outperformed conventional CNN, LeNet-5, CNN-BiLSTM, and related architectures. Industrial-control experiments using an LSTM encoder-decoder similarly demonstrated that carefully constrained adversarial samples could reduce model precision by an average of approximately 66.26%, even when manipulated sensor and actuator observations remained consistent with protocol specifications and realistic feature ranges (Hu et al., 2021). Such findings are important because attack effectiveness is not dependent on visibly extreme data corruption. Perturbations can remain numerically small while shifting learned representations sufficiently to alter failure classifications. Research using GRU-based variational autoencoders, recurrent architectures, and hybrid feature-learning methods has further shown that multivariate attacks designed around dependencies among sensors are more effective than arbitrary independent noise because physically related features are modified consistently. Across these experiments, accuracy, precision, recall, F1-score, ROC-AUC, PR-AUC, false-positive rate, false-negative rate, and Matthews correlation coefficient commonly declined as perturbation magnitude or the number of manipulated sensors increased (V. Singh et al., 2024). Deep architectures sometimes maintained stronger clean-data accuracy than conventional models, but high baseline performance did not consistently indicate greater adversarial robustness. Instead, robustness depended on the training strategy, input representation, physical constraints imposed on adversarial examples, feature redundancy, temporal context, and whether the model had previously encountered attacked or noisy conditions during training (Lin et al., 2024).

Cybersecurity and Anomaly-Detection Models in Predictive-Maintenance Networks

Quantitative studies of cybersecurity detection in IoT-enabled industrial and predictive-maintenance networks show substantial performance differences among signature-based intrusion detection, statistical anomaly detection, and conventional machine-learning classifiers. Signature-based systems generally provide strong detection of previously observed attacks because traffic characteristics are matched against known rules or malicious patterns, although their effectiveness decreases when attacks are novel, modified, or designed to resemble legitimate equipment communication. Statistical anomaly-detection approaches address this limitation by comparing observed sensor or network behavior with established normal distributions, thresholds, residual patterns, and temporal relationships (Chang et al., 2024). Their performance, however, can be affected by changing production states, legitimate process variation, and highly imbalanced attack data. Machine-learning research has therefore compared Logistic Regression, Naïve Bayes, KNN, SVM, Decision Tree, Random Forest, AdaBoost, Gradient Boosting, XGBoost, and LightGBM across TON_IoT, Edge-IIoTset, X-IIoTID, UNSW-NB15, SWaT, WADI, and related industrial datasets. One large Edge-IIoTset investigation evaluated Decision Tree, Random Forest, SVM, KNN, and a deep neural network across binary, six-class, and fifteen-class detection and reported approximately 99.99% binary accuracy for the centralized DNN. Comparative IIoT experiments using an 80:20 training-to-testing split reported test accuracies of approximately 100% for Random Forest, 99.99% for XGBoost, 99.35% for Decision Tree, 97.49% for Linear SVC, and 97.27% for Logistic Regression (Kuchar & Fujdiak, 2024). Separate TON_IoT experiments found Random Forest accuracy around 98.42%, while XGBoost reached 87.54% on UNSW-NB15, confirming that relative algorithm performance changes with dataset structure. Another TON_IoT comparison reported XGBoost accuracy of 99.07% with ROC-AUC of 0.9996 and LightGBM accuracy of 99.00% with ROC-AUC of 0.9993, whereas Logistic Regression and Naïve Bayes remained below 76% accuracy. Across these studies, tree-based ensemble algorithms generally provided stronger aggregate precision, recall, F1-score, and ROC-AUC than simpler statistical classifiers, but extremely high overall accuracy did not always translate into reliable detection of rare attack categories (Kuchar & Fujdiak, 2024).

Figure 6: Cyberattack Detection in Industrial Networks

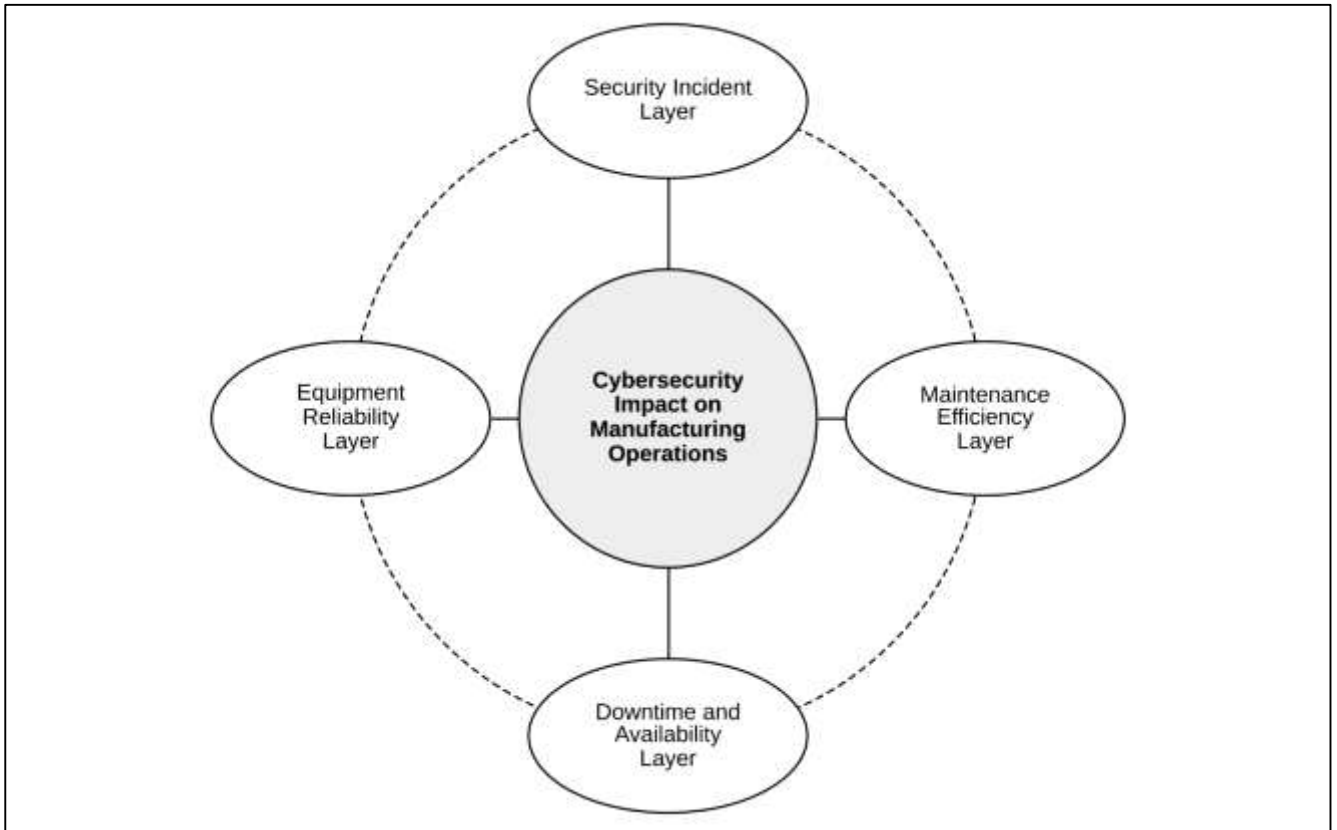
Deep-learning and autoencoder-based models have been extensively investigated because industrial predictive-maintenance networks generate high-dimensional, multivariate, and temporally dependent sensor streams that cannot always be represented effectively using static classification models. Studies have compared multilayer perceptrons, CNNs, RNNs, LSTMs, GRUs, CNN-LSTM hybrids, variational autoencoders, sequence-to-sequence architectures, graph neural networks, GAN-based detectors, transformers, and reconstruction-based anomaly-detection models. Experimental comparisons on SWaT and WADI demonstrate substantial variation in precision and recall depending on model architecture and evaluation protocol (Jaramillo-Alcazar et al., 2023). A comparative implementation of several advanced anomaly-detection approaches on SWaT reported that InterFusion achieved an F1-score of approximately 90.7%, precision of 91.1%, recall of 90.3%, false-negative rate of 9.7%, and false-positive rate of only 1.2%. Spatial-temporal anomaly detection produced a different performance profile: on SWaT, one graph- and LSTM-based model obtained recall of approximately 99.92% but precision of 66.12%, generating an F1-score near 0.80, while on WADI it produced precision of 98.49% but recall of only 45.57%. These contrasting values illustrate why detection accuracy alone can conceal operational weaknesses. GAN-based intrusion detection research on SWaT reported approximately 99.00% precision, 98.92% recall, and an F1-score near 0.97, outperforming a comparative EGAN approach that obtained approximately 92.00% precision and 95.82% recall. Unsupervised anomaly-detection evaluations have also examined datasets containing hundreds of thousands to more than one million multivariate observations (Carrasco et al., 2021). One broad benchmark comparison used approximately 496,800 SWaT training observations with 449,919 test observations across 51 variables and approximately 1,048,571 WADI training samples with 172,801 testing samples across 123 variables. Autoencoder and reconstruction-based methods were particularly useful where malicious labels were unavailable, although their performance varied according to anomaly threshold selection, temporal window length, reconstruction quality, and process-state variation. Across these studies, deep temporal models typically improved sensitivity to coordinated multivariate attacks, but high model complexity could increase inference latency and computational overhead (Ain et al., 2024).

Ensemble and hybrid cyber-physical detection systems have generally produced the strongest balance between attack sensitivity, false-alarm control, and robustness across heterogeneous attack categories. These approaches combine network-flow features, process-sensor behavior, physical constraints, statistical anomaly scores, and outputs from multiple machine-learning or deep-learning classifiers rather than relying on a single information source. Recent digital-twin and deep-learning ensemble

research on SWaT reported precision of approximately 97.6%, recall of 96.2%, and an F1-score of 96.9%, with a false-positive rate of only 2.4%. The framework improved F1 performance by approximately 3.2 percentage points relative to a strong transformer baseline and by more than five percentage points relative to physics-only detection (Qasim et al., 2022). Its attack-specific analysis also demonstrated substantial consistency across different threats: single-point false-data injection was detected with approximately 98.3% accuracy, multi-point false-data injection with 96.7%, constant replay attacks with 97.2%, randomized replay attacks with 92.4%, and denial-of-service attacks with approximately 99.8% detection. Average inference latency was approximately 25.4 milliseconds, compared with about 45 milliseconds for transformer-based detection and 12 milliseconds for simpler physics-only approaches. Another hybrid deep-learning model evaluated on SWaT and WADI achieved approximately 98.7% and 97.4% accuracy respectively, with F1-scores exceeding 97.5% and per-prediction latency below 50 milliseconds. These results indicate that integrating spatial, temporal, network, and process information can improve detection across multiple cyberattack mechanisms (Tanuska et al., 2021). Hybrid approaches are also less dependent on a single feature distribution because suspicious network behavior can be cross-checked against physical equipment responses. The same literature shows, however, that strong overall results can mask category-specific weaknesses. DDoS and volumetric attacks are usually identified with very high recall because their traffic patterns differ strongly from normal behavior, while low-frequency man-in-the-middle, replay, ransomware, reconnaissance, and stealthy false-data injection attacks often generate lower per-class F1-scores. Consequently, multiclass precision, recall, macro-F1, PR-AUC, MCC, false-negative rate, and attack-specific detection delay provide more informative comparisons than overall binary accuracy alone (López et al., 2023).

Maintenance Efficiency, and Downtime

Quantitative literature examining cyber-physical manufacturing systems indicates that cybersecurity incidents can alter equipment reliability by changing control commands, suppressing valid condition information, creating false measurements, or interrupting communication between sensors, controllers, and maintenance systems. Across more than ten experimental, case-based, simulation, and industrial studies, false-data injection, malware, replay, denial-of-service, and control-system manipulation have been associated with abnormal equipment operation, forced shutdowns, missed deterioration signals, and physical component stress (Zhang et al., 2015). Experimental investigations using SWaT and related industrial-control testbeds found that attacks against level, flow, pump, and valve information could create overflow, underflow, unintended equipment states, and abnormal operating sequences, demonstrating that a cyber-induced disturbance may propagate from a compromised information channel to physical reliability outcomes. Other work on cyber-physical monitoring found that conventional fault-diagnosis systems could classify cyber-induced abnormalities as ordinary equipment faults, increasing the probability of incorrect maintenance actions. Historical evidence from the Stuxnet incident illustrates the possible magnitude of reliability degradation: approximately 1,000 IR-1 centrifuges were decommissioned and replaced during the period associated with the malware, while individual centrifuge cascades exhibited pronounced reductions in operational units (Wu et al., 2019). Related analyses reported manipulation of centrifuge rotational frequency from a normal level near 1,064 Hz to approximately 1,410 Hz, representing a deviation of roughly 32.5%, followed by extremely low-speed operation in other attack phases. Such manipulation imposed mechanical stress while compromised monitoring concealed the abnormal behavior. Process-plant risk studies similarly found that malicious manipulation of even a small number of basic process-control or safety-system components could generate severe outage or equipment-damage scenarios (Alghassab, 2021). These findings suggest that cyber compromise can reduce effective MTBF by increasing induced failure frequency and can increase MTTF uncertainty because equipment degradation no longer reflects purely mechanical ageing. The reliability effect is especially pronounced when attacked variables control safety-critical or high-load components, since manipulation of a single influential actuator or sensor may create larger physical consequences than compromise of numerous noncritical endpoints (Kosmowski et al., 2022).

Figure 7: Cybersecurity Impact on Manufacturing Maintenance

The literature also demonstrates that cyber-compromised predictive-maintenance information can influence maintenance efficiency by increasing false interventions or allowing genuine deterioration to remain undetected. Predictive-maintenance systems normally convert vibration, temperature, electrical, pressure, acoustic, and process measurements into maintenance alerts, and their effectiveness therefore depends on the integrity of these data. False-data injection can produce abnormal readings for healthy equipment, causing technicians to inspect, stop, or replace components unnecessarily, while suppression or replay of normal-looking values can conceal developing faults and delay corrective action. Experimental monitoring research has shown that cyberattacks may be interpreted as physical faults by conventional diagnostic systems, producing erroneous countermeasures even when no underlying equipment failure exists (Maglaras, 2022). This phenomenon directly affects technician workload, maintenance duration, spare-part use, and planned-to-unplanned maintenance ratios because resources may be allocated to cyber-generated alarms instead of actual mechanical degradation. Evidence from heavy-industry predictive-maintenance research illustrates the operational importance of alarm quality. A sensor-based maintenance system applied to crushers and steelworks equipment reduced false alarms by an average of 90.25% compared with stand-alone outlier detection, highlighting how excessive false positives can otherwise generate unnecessary operator attention and maintenance activity. When cybersecurity manipulation reverses this benefit by deliberately generating false anomalies, the maintenance burden can increase even without physical failure. The opposite condition is equally important (Franke, 2020). Adversarial predictive-maintenance studies have shown that manipulated sensor information can cause fault-detection systems to overlook critical equipment states, increasing missed-failure rates and reducing warning lead time. Wind-turbine predictive models exposed to false-data injection experienced recall reductions approaching 28 percentage points in some experiments, meaning that a substantially larger proportion of actual fault cases was no longer identified. RUL studies have similarly shown that manipulation of only one or two influential sensors can produce severe distortion in estimated time to failure. Such errors can move maintenance activity away from the true degradation trajectory, either initiating premature intervention or postponing action until failure becomes corrective rather than planned (PACME et al.,

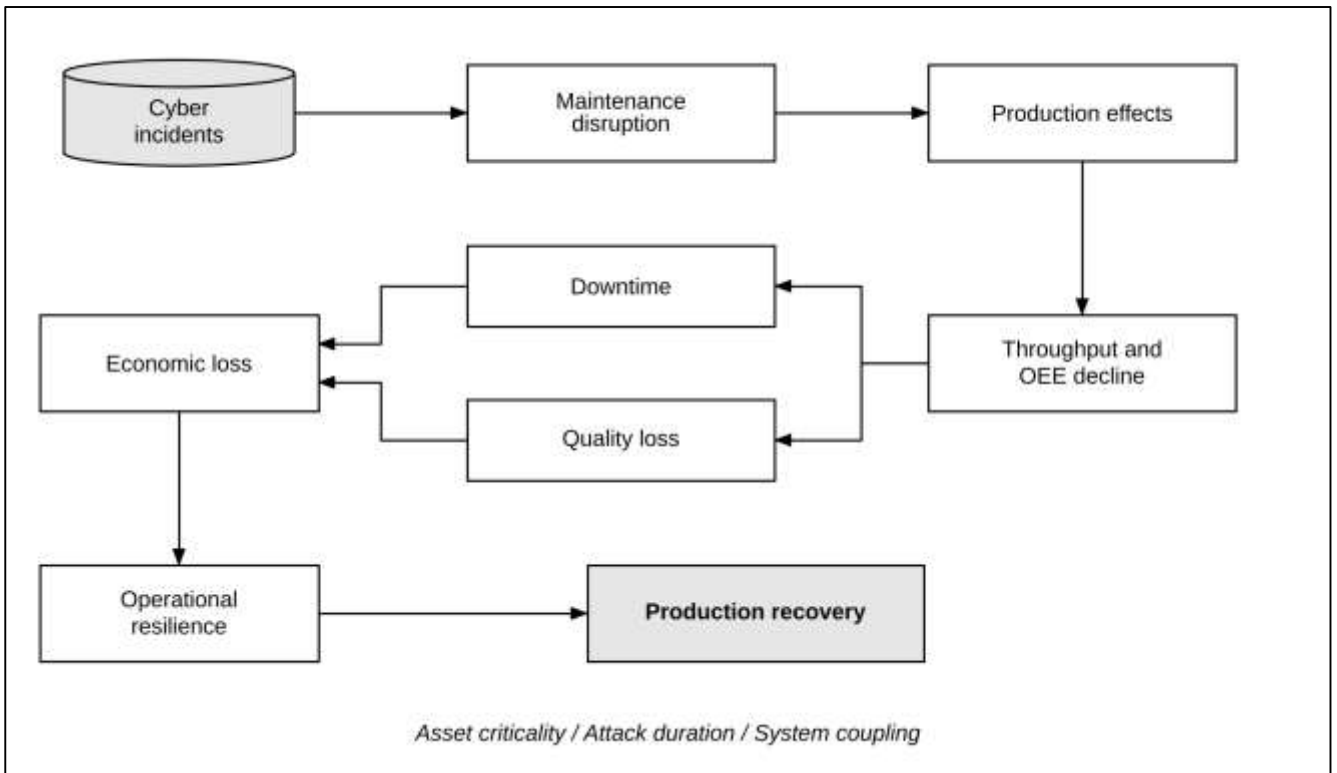
2016). Consequently, cybersecurity incidents affect maintenance efficiency through both additional unnecessary work and reduced ability to intervene before breakdown. Availability-oriented cyberattacks have particularly direct effects on downtime and restoration because they can disable PLC communication, remote diagnostics, monitoring systems, maintenance databases, and higher-level manufacturing applications simultaneously. Experimental research conducted on a physical automated production line showed that TCP SYN flooding, TCP ACK flooding, and reflected ICMP attacks progressively degraded PROFINET communication, disrupted PLC and IIoT functions, and eventually stopped physical production. During attack conditions, workpieces remained blocked on conveyors, several stations entered fault-safe states, and manual intervention was required before operation could continue (Bhat & Venkitaraman, 2024). The IIoT maintenance-monitoring layer also became unavailable, preventing verification of equipment status, eliminating real-time process visibility, and disabling automatic status notifications. Remote access through the industrial router was lost, preventing technicians from diagnosing or intervening in PLC operation. After the attack, manual PLC restart and repositioning of work-in-progress products were required, directly extending restoration activity beyond simple network recovery. Real ransomware cases show similar effects at organizational scale. A documented manufacturing ransomware incident required approximately 10 days before the first customer shipment could leave an affected factory, including roughly one week to determine what had occurred and an additional two to three days to restore compromised systems (Maglaras, 2022). Technical personnel worked in three continuous shifts during the most intensive phase, later moving to extended two-shift operation, and normal working schedules were not restored for about three weeks. Production returned to normal levels only after approximately one month. Broader ransomware analysis reported average recovery periods near 23 days across incidents, with individual cases ranging from 7 to 89 days; approximately 67% of affected organizations experienced more than 50% loss of operational capacity. Manufacturing incidents in that evidence base averaged roughly 28 days of recovery and approximately \$12.3 million in impact per incident. These findings show that cyber incidents can increase effective MTTR because restoration involves not only equipment repair but also validation of controllers, networks, identities, software, data integrity, remote-access services, and production records (Farooq & Zhu, 2026). Cyber-related downtime therefore differs from ordinary mechanical downtime because returning a machine to a functional state does not necessarily mean that the surrounding production and maintenance infrastructure can safely resume operation. Integrated quantitative evidence shows that cybersecurity incidents affect maintenance performance through interacting changes in downtime, reliability, diagnostic accuracy, maintenance workload, and recovery cost rather than through a single isolated metric. Predictive-maintenance studies conducted under uncompromised conditions provide a useful baseline for evaluating the scale of potential cyber-induced deterioration (Jammal et al., 2016). For example, a recent injection-moulding condition-monitoring case study reported a 97.36% increase in MTBF and a 65.04% reduction in downtime during one evaluated period after structured predictive monitoring was introduced; a later period retained a 20% increase in MTBF and a 79% reduction in downtime. These gains illustrate the operational value that depends on trusted condition data. Cyber manipulation that removes monitoring availability or corrupts sensor information can therefore reverse benefits normally obtained from predictive maintenance. Experimental manufacturing attacks demonstrate this mechanism directly: communication disruption produced false product rejection, deterioration in apparent quality and OEE, loss of work-in-progress records, inability to confirm machine status, and complete production stoppage in severe scenarios. At the maintenance level, loss of remote diagnostics increased the need for local manual intervention, while corrupted digital records complicated restoration and extended the period required to establish a reliable operating state (B. Singh et al., 2024). Statistical comparisons across normal and attacked conditions in industrial testbeds consistently show that severity depends on attack duration, targeted component, communication architecture, and the number of physically dependent assets. Studies using regression, anomaly analysis, experimental controls, survival-related reliability concepts, and comparative pre-post designs indicate that attacks directed at critical controllers or influential sensor channels produce disproportionately large operational effects relative to the number of compromised devices (Bouramdane, 2023). The literature also shows that downtime frequency alone understates cyber impact because incident recovery frequently adds technician

overtime, external-consultancy expenditure, spare-part use, production loss, and diagnostic delay. Manufacturing survey evidence indicates that cyber incidents constitute a relatively small proportion of everyday downtime causes, yet individual cyber-related outages can generate exceptionally high losses when they occur. Across the reviewed studies, the strongest quantitative pattern is therefore a deterioration in effective availability when cybersecurity incidents combine equipment interruption with unreliable maintenance information, prolonged restoration, false interventions, reduced warning lead time, and increased human and financial maintenance effort ([Alobaidi et al., 2022](#)).

Manufacturing Production, Quality, and Economic Performance

Quantitative literature on cyber-manufacturing systems shows that cybersecurity incidents affecting predictive-maintenance infrastructure can propagate beyond maintenance functions and produce measurable deterioration in plant-level production performance. Experimental work on programmable logic controllers has shown significant reductions in communication throughput and increases in round-trip time during denial-of-service, man-in-the-middle, and code-injection attacks, with denial-of-service producing the largest deterioration among tested attack types ([Adu-Amankwa et al., 2019](#)). In automated production-line experiments, disruption of PROFINET and IIoT communication progressively caused device failure, PLC fault states, blocked workpieces, interrupted technological cycles, loss of remote access, and complete stoppage of physical production. These results indicate that production throughput can decline sharply when cyber incidents interrupt the data pathways used to coordinate control, maintenance, and machine status. Studies of total productive maintenance in smart manufacturing have similarly demonstrated that cyber-physical threats can reduce overall equipment effectiveness by degrading availability, performance, and quality simultaneously. Production interruptions are especially severe when compromised equipment occupies a bottleneck position because failure at one critical station restricts the productive capacity of upstream and downstream processes ([Achouch et al., 2022](#)). Cyber-resilience studies therefore assess production output, downtime, utilization, and scrap jointly rather than treating individual machines independently. In robotic assembly-line research, integrating maintenance and cybersecurity controls produced secure production continuity of 96.84%, reduced attack propagation to 0.15, and reduced recovery time to 4.38 seconds, illustrating how production continuity varies quantitatively with the degree of cyber resilience. Other work on cyber-manufacturing operational resilience has established explicit production-output, scrap-rate, and downtime thresholds for evaluating degradation during attacks. Across these studies, longer attack duration, greater controller accessibility, higher equipment criticality, and stronger interdependence among stations are associated with larger production losses ([Ansari et al., 2019](#)). Therefore, the production effect of a cyber incident is determined not simply by the number of compromised devices but by the role of those devices within the manufacturing flow, the persistence of the disruption, and the ability of the production system to isolate or bypass affected resources.

A second body of quantitative research has focused on the effects of cybersecurity incidents on product quality, showing that attacks on process parameters, maintenance data, inspection information, or material characteristics can increase defect rates, rejection, scrap, rework, and yield loss even when the production system remains operational. Cyber-physical attack studies from a quality-control perspective have demonstrated that malicious manipulation can alter dimensions, mechanical properties, material integrity, and process consistency, making the resulting products unsuitable even when no immediate machine failure occurs. Additive-manufacturing research provides direct experimental evidence: material-integrity cyberattacks introduced process perturbations that generated inter-road voids and reduced part integrity, creating a need for real-time recovery to avoid product disposal or production stoppage ([Keleko et al., 2022](#)).

Figure 8: Cyber Incidents Affect Manufacturing Performance

Other zero-defect manufacturing studies show that equipment-health variables and product-quality measurements are statistically interdependent, allowing changes in tool condition or process behavior to propagate into non-conformance and scrap. In multi-stage production systems, defect propagation can amplify losses because an early-stage process deviation may remain undetected until later inspection, increasing both rework effort and accumulated material cost. Predictive-maintenance cyber risk therefore affects quality not only through direct manipulation of manufacturing parameters but also by undermining the reliability of the maintenance information that normally prevents process drift. If corrupted sensor information suppresses an emerging machine fault, degraded equipment may continue producing out-of-specification parts for an extended period, increasing rejection and scrap (Lee et al., 2019). Conversely, false cyber-induced alarms may trigger unnecessary stoppages and quality holds for conforming products. Studies of cyber-manufacturing resilience have operationalized these effects using scrap rate, quality ratio, product loss, and production-output thresholds, while experimental FFF research has shown that AI-assisted recovery can limit attack-induced defect progression during continued production. Across automotive, machinery, aerospace, railway, medical, and additive-manufacturing settings, the quantitative evidence consistently indicates that quality losses become larger when attacks target highly influential process variables, remain undetected for longer durations, or affect interconnected stages where defects propagate before final inspection (Shcherbakov et al., 2019).

Cybersecurity incidents also generate measurable economic effects through lost production, recovery expenditure, additional labor, delayed shipments, resource waste, and extended restoration time. Manufacturing ransomware studies provide some of the clearest quantitative evidence. Sector-wide survey data for 2024 reported that 74% of manufacturing ransomware incidents resulted in data encryption, 44% of computers were affected on average, and mean recovery cost reached approximately \$1.67 million, up from \$1.08 million in the previous year. The corresponding 2025 evidence showed average recovery cost declining to about \$1.3 million, while average ransom demands remained around \$1.2 million, indicating that direct cyber recovery remains financially material even when organizations improve resilience (Fasuludeen Kunju et al., 2022). Broader manufacturing research has also shown that nearly three-quarters of manufacturers experience downtime at least once

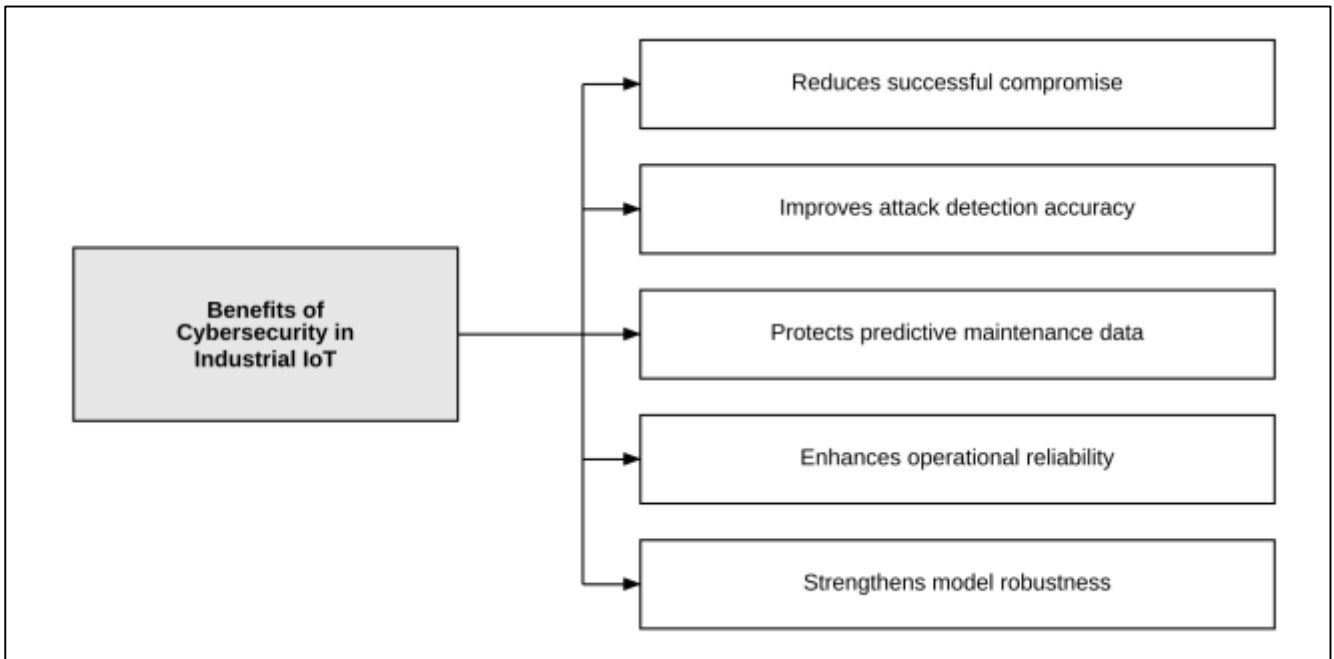
annually and that a substantial proportion of firms estimate hourly downtime losses above \$100,000, although cyber incidents represent only a minority of routine downtime causes. This distinction is important because cyber-related outages may be less frequent than mechanical interruptions but can be considerably more severe when they occur. Recovery is complicated by the interdependence of IT, OT, quality systems, engineering workstations, identity services, supplier platforms, and production scheduling. Recent manufacturing-recovery research emphasizes that restoring backups alone does not restore productive capacity if operators cannot authenticate, engineering systems cannot be trusted, quality release systems remain unavailable, or supply-chain coordination is disrupted (Liu et al., 2023). Cyber incidents can therefore increase cycle time and energy or resource consumption indirectly by forcing repeated production, extended idling, manual inspection, product reclassification, scrap handling, and rework. Economic-loss models consequently incorporate downtime duration, production volume lost, recovery labor, external consultancy, equipment replacement, ransom payments, delayed delivery, and additional quality-control effort. Across empirical and survey evidence, financial cost rises with attack persistence, number of affected systems, encryption extent, production-system coupling, and the criticality of unavailable digital services (Chenaru et al., 2022). Cross-sector evidence indicates that the operational consequences of predictive-maintenance cyber risk vary substantially according to manufacturing technology, equipment criticality, process architecture, and the degree of interdependence among production stages. Automotive and robotic assembly lines are particularly sensitive to cyber disruption because sequential stations are tightly synchronized and one compromised controller can stop multiple dependent operations. Semiconductor, electronics, and other high-precision sectors face additional quality risk because small deviations in process parameters can produce high-value scrap even without visible equipment failure. Chemical and pharmaceutical processes are characterized by strong physical coupling, batch dependence, and process-safety constraints, making prolonged cyber-induced deviations potentially more costly than short isolated interruptions. Food processing similarly depends on timing, environmental control, and continuous material flow, so cyber disruption can translate into spoiled inventory, cleaning requirements, and production restarts (Cinar et al., 2022). Machinery and additive-manufacturing studies show that quality-focused attacks can alter dimensions or material integrity while preserving apparent machine operation, creating hidden losses that emerge during inspection or downstream use. Research on automotive cylinder-head production has also demonstrated how predictive-maintenance decisions can be optimized through integrated production, reliability, and cost metrics, illustrating the financial sensitivity of multi-station systems to maintenance timing. Across these sectors, equipment criticality repeatedly emerges as a stronger moderator of loss than the raw percentage of compromised devices. A single attacked bottleneck PLC, robot, machine tool, or process controller may generate larger throughput and OEE deterioration than compromise of numerous noncritical endpoints (Riccio et al., 2024). Attack duration further magnifies loss because production interruptions accumulate over time, while prolonged data corruption increases the probability that defects pass through multiple stages before detection. Interdependence also influences recovery because restarting one machine may not restore normal flow until work-in-progress records, sequencing, quality status, and downstream coordination are reconciled. For this reason, plant-level assessment increasingly combines throughput, utilization, OEE, scrap, recovery time, and economic loss rather than examining each indicator independently. The synthesized evidence shows that the magnitude of cyber-induced manufacturing loss is jointly determined by attack severity, targeted asset criticality, system coupling, attack duration, and the availability of operational resilience mechanisms (Cheng et al., 2022).

Integrated Risk Evidence

Quantitative evidence across industrial IoT, cyber-physical systems, smart manufacturing, and predictive-maintenance research shows that layered security controls generally produce stronger reductions in successful compromise than isolated technical measures. Studies evaluating device authentication, secure communication, network segmentation, access control, multifactor authentication, patch management, and zero-trust mechanisms have reported lower unauthorized-access rates, reduced attack propagation, improved containment, and smaller proportions of compromised devices when these controls are implemented together. Experimental industrial architectures using authenticated gateways, encrypted communication, device identity validation, and

segmented network zones have demonstrated that restricting trust relationships reduces lateral movement after an initial compromise ([Ansari et al., 2020](#)).

Figure 9: Cybersecurity Benefits for Predictive Maintenance



Zero-trust industrial access-control research has similarly shown that continuously verifying device and user identities limits unrestricted communication between IT, OT, edge, and cloud components. Secure protocol implementations, including authenticated OPC UA sessions, TLS-protected industrial traffic, VPN-based remote access, and cryptographic device identities, have reduced opportunities for replay, spoofing, unauthorized command injection, and passive data interception. Patch-management research has found that exposure is strongly related to vulnerability age and the continued presence of publicly known weaknesses, while reducing the number of unpatched endpoints lowers the effective attack surface. Multifactor authentication and least-privilege access provide additional protection for remote maintenance accounts, engineering workstations, and vendor connections because credential compromise alone becomes insufficient for unrestricted entry ([Karippur et al., 2024](#)). Across industrial-control and IIoT studies, control effectiveness has been measured through attack success rate, unauthorized-session frequency, number of reachable assets, compromised-device proportion, blocked communication attempts, and time required for containment. Where regression or risk-scoring approaches have been used, higher security-control coverage is generally associated with lower compromise probability after adjustment for device count, legacy-system dependence, network exposure, and vulnerability severity. The literature therefore indicates that authentication, segmentation, encryption, patching, and access control have complementary rather than interchangeable effects, with the largest operational reductions in compromise occurring when several controls are implemented as an integrated security architecture ([Ayvaz & Alpay, 2021](#)).

Detection-oriented cybersecurity controls provide some of the most extensively quantified evidence because their effectiveness can be evaluated directly through precision, recall, false-alarm rate, ROC-AUC, PR-AUC, latency, and downstream predictive-maintenance accuracy. Comparative studies using SWaT, WADI, BATADAL, TON_IoT, Edge-IIoTset, and related industrial datasets show that conventional SVM and Random Forest models are usually outperformed by temporal deep-learning, autoencoder, ensemble, and hybrid cyber-physical approaches when attacks are multistage or coordinated across several sensors ([Lindström et al., 2017](#)). A recent hybrid LSTM-autoencoder framework combining cyber and physical information achieved approximately 0.97 accuracy, 0.93 recall, 0.94 F1-score, and 0.98 AUC on BATADAL, compared with SVM values of 0.89 accuracy, 0.82 recall, 0.83 F1-score, and 0.91 AUC. On WADI, the same architecture produced approximately 0.94

accuracy, 0.92 recall, 0.91 F1-score, and 0.95 AUC, while SVM achieved about 0.84 accuracy, 0.76 recall, 0.78 F1-score, and 0.87 AUC. SWaT evaluation produced approximately 0.95 accuracy and 0.94 recall and F1-score, exceeding classical baselines. Edge-based security adds a latency advantage by processing sensor and network information close to the equipment rather than transmitting every event to centralized infrastructure. Lightweight edge detectors have reported sub-millisecond to tens-of-milliseconds inference times while retaining high discrimination performance. Blockchain-assisted or tamper-resistant logging adds another layer by preserving sensor provenance and anomaly records, although experiments show that such integrity controls introduce additional communication and consensus overhead (Lindström et al., 2017). Permissioned blockchain implementations have nevertheless achieved sub-second confirmation under moderate load, making them compatible with many supervisory rather than hard real-time maintenance functions. The literature therefore indicates that the strongest detection architectures combine device trust, secure communication, temporal anomaly detection, cyber-physical feature fusion, and edge execution, because these mechanisms jointly improve attack detection while limiting false alarms and preserving predictive-maintenance data integrity.

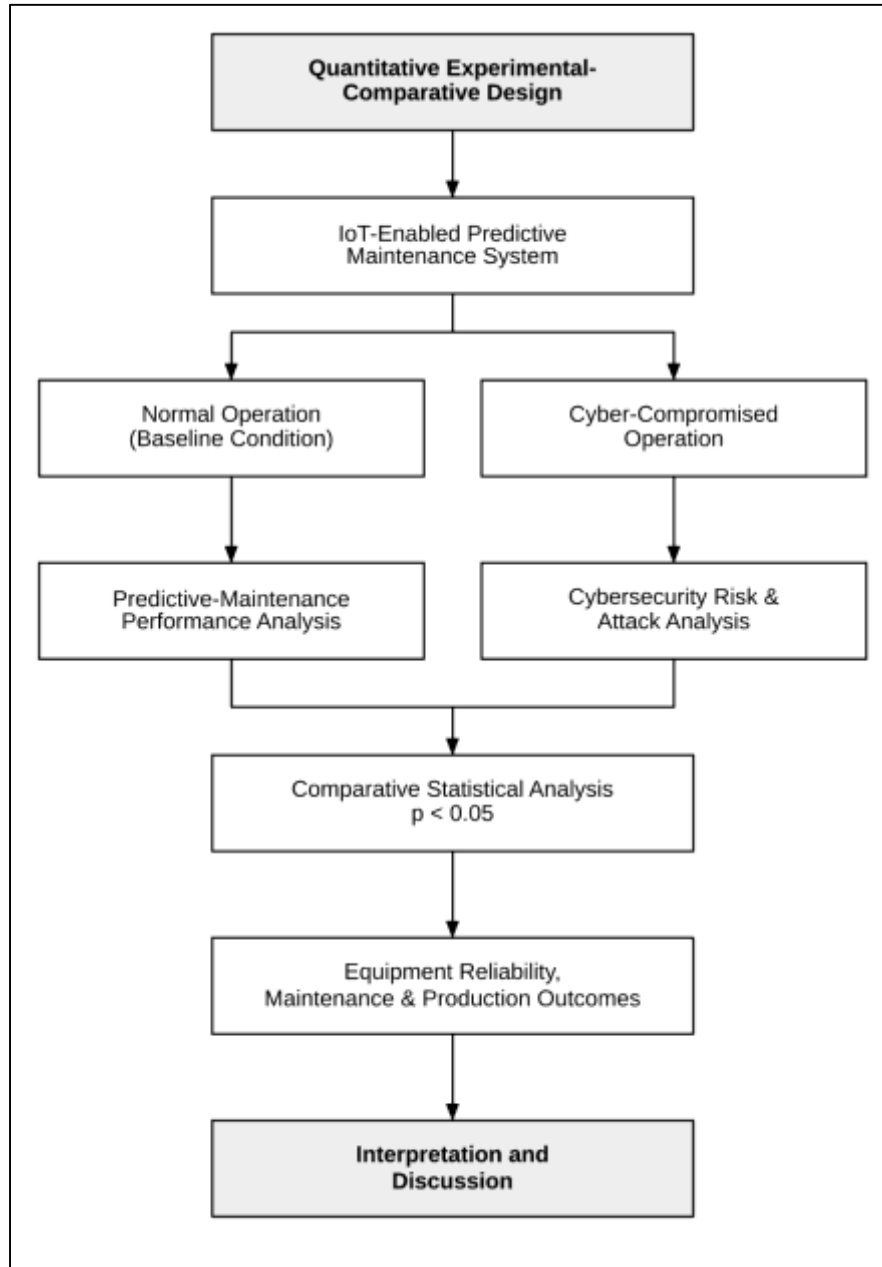
Statistical robustness varies considerably across industrial cybersecurity studies and is strongly influenced by validation design. Studies relying only on random train-test splits frequently report very high accuracy, sometimes above 99%, while temporal or cross-dataset validation generally produces lower and more realistic performance because model leakage and repeated operating patterns are reduced (Rosati et al., 2019). Robust studies increasingly use separate training, validation, and testing sets, stratified k-fold cross-validation, chronological splitting, independent holdout data, cross-factory testing, sensitivity analysis, and class-imbalance correction. Temporal validation is particularly important for predictive-maintenance networks because sensor observations are sequentially dependent and randomly mixing past and future operating states can overstate generalization. Cross-dataset experiments provide stronger evidence of robustness. In one recent comparison, a hybrid model trained on WADI and tested on SWaT achieved recall of approximately 0.82, F1-score of 0.80, and AUC of 0.88, while training on the simpler BATADAL environment and testing on SWaT produced lower values of about 0.55 recall, 0.54 F1-score, and 0.70 AUC. Training on BATADAL and testing on WADI similarly yielded recall of 0.61 and F1-score of 0.58. These differences indicate that sensor density, process complexity, attack distribution, and feature compatibility materially affect transferability (Woods & Seymour, 2023). Class imbalance creates another robustness problem because overall accuracy can remain high even when rare but important attacks are poorly detected. Studies applying resampling, class weighting, focal-loss strategies, or stratified validation generally report stronger recall and PR-AUC for minority attacks than uncorrected models. Robustness assessments have also used MAE, RMSE, MAPE, R^2 , ROC-AUC, PR-AUC, and confidence intervals to compare cybersecurity effects on predictive-maintenance models. Where effect sizes or regression estimates have been reported, the most meaningful findings are those that remain stable across alternative specifications, independent datasets, attack intensities, and equipment conditions. The literature therefore distinguishes statistically significant performance differences from operationally robust differences by requiring consistent effects across multiple validation procedures rather than relying on a single high-performing test split (Kure et al., 2022).

METHOD

Study Design and Theoretical Framework

This study employed a quantitative, experimental-comparative research design to examine cybersecurity risks in IoT-enabled predictive-maintenance systems for smart manufacturing and to quantify the effects of cybersecurity vulnerabilities and cyberattacks on sensor-data integrity, predictive-maintenance accuracy, equipment reliability, maintenance efficiency, and manufacturing performance.

Figure 10: Methodology of this study



The theoretical framework conceptualized cybersecurity exposure as the principal independent construct and predictive-maintenance and operational performance as the principal dependent constructs. Cybersecurity exposure was represented by weak authentication, unpatched vulnerabilities, insecure communication protocols, open ports, inadequate encryption, insufficient access control, remote-access exposure, network misconfiguration, legacy-system dependence, third-party connectivity, false-data injection, spoofing, replay attacks, man-in-the-middle attacks, packet manipulation, denial-of-service conditions, and malicious data corruption. Intermediate variables included sensor-data completeness, communication latency, packet loss, signal deviation, anomaly frequency, intrusion-detection performance, and predictive-model degradation. Dependent variables included fault-detection accuracy, precision, recall, sensitivity, specificity, F1-score, ROC-AUC, PR-AUC, false-positive and false-negative rates, remaining-useful-life prediction error, unplanned downtime, MTBF, MTTR, equipment availability, utilization, maintenance duration, maintenance cost, throughput, cycle time, OEE, defect rate, rejection, scrap, and production loss. The experimental structure compared baseline normal operation with controlled cyber-compromised conditions so that differences in predictive and operational indicators could be quantified. The design also incorporated subgroup comparisons according to attack type, attack intensity, equipment criticality, cybersecurity-

control level, and model architecture. This framework permitted evaluation of both direct cybersecurity effects and indirect effects transmitted through deterioration in sensor quality and predictive accuracy.

Participants, Materials, Sampling Strategy, and Selection Criteria

The study used industrial IoT and predictive-maintenance observations rather than human participants as the primary units of analysis. Data were selected from publicly available and experimentally generated smart-manufacturing, industrial-control, and predictive-maintenance datasets containing synchronized sensor measurements, equipment states, cybersecurity-event labels, and maintenance or operational outcomes. Purposive sampling was applied because datasets were required to represent environments relevant to IoT-enabled manufacturing and to contain sufficient information for distinguishing normal conditions from cyber-compromised conditions. Eligible observations included equipment-condition records containing variables such as temperature, vibration, pressure, flow, current, voltage, rotational speed, acoustic measurements, equipment states, operating cycles, network traffic, authentication events, packet characteristics, maintenance records, failure events, and attack labels. Records were included when the associated system contained industrial sensors, PLCs, gateways, SCADA components, edge devices, or other connected manufacturing assets and when timestamps permitted temporal alignment between cyber events and equipment behavior. Datasets containing false-data injection, spoofing, replay, denial-of-service, man-in-the-middle, packet manipulation, malware-related, or communication-disruption scenarios were retained for attack comparisons. Observations with irrecoverable timestamp inconsistencies, duplicate records, severe corruption unrelated to the defined cyberattack scenarios, missing class labels, or insufficient equipment-condition information were excluded. Where class imbalance was substantial, stratified sampling and class-weighted or resampling procedures were applied so that rare attack and failure classes were adequately represented without altering the integrity of the independent test set. The final analytical sample was divided into baseline normal-operation, cyberattack, training, validation, and independent testing subsets while preserving temporal order where time-dependent validation was required.

Instrumentation and Data Collection Tools

Data collection and experimental measurement were conducted using a combination of industrial sensor records, network-security monitoring variables, predictive-maintenance software, statistical packages, and machine-learning environments. Equipment-condition variables included temperature, vibration, pressure, flow, current, voltage, acoustic signals, rotational speed, machine operating state, utilization, and equipment age or operating-cycle information where available. Cybersecurity measurements included attack type, attack duration, malicious-traffic frequency, unauthorized-access attempts, compromised-device status, packet loss, communication delay, abnormal network flows, manipulated-data proportion, authentication events, open services, vulnerability characteristics, and security-control status. Network traffic and cyber-event records were aligned with equipment-condition observations using timestamps to establish whether changes occurred before, during, or after defined attacks. Predictive-maintenance models included logistic regression, decision tree, K-nearest neighbours, support vector machine, random forest, AdaBoost, gradient boosting, XGBoost, LightGBM, artificial neural network, convolutional neural network, recurrent neural network, LSTM, GRU, and autoencoder-based approaches where data structure supported their application. Data preparation and statistical analyses were performed using SPSS and R, while Python-based analytical libraries were used for machine-learning model development, preprocessing, validation, and predictive-performance assessment. Sensor variables were checked for missing observations, duplicate values, extreme outliers, inconsistent timestamps, scaling differences, and class imbalance. Standardization or normalization was applied where required by the selected model. Instrument reliability and analytical validity were evaluated through consistency checks between replicated measurements, cross-validation performance, train-test stability, and comparison of model outputs with known attack and equipment-condition labels.

Experimental Procedure

The experimental procedure was conducted sequentially to maintain consistency between cybersecurity exposure, sensor-data conditions, predictive analysis, and operational outcomes.

Initially, datasets were imported, inspected, cleaned, timestamp-aligned, and classified according to normal and cyber-compromised operating periods. Descriptive profiles of devices, sensors, equipment states, attack categories, maintenance records, and production variables were generated before inferential analysis. Baseline equipment behavior was established from attack-free observations, and normal ranges for major condition-monitoring variables were determined. Cyber-compromised observations were then classified according to false-data injection, spoofing, replay, man-in-the-middle, denial-of-service, packet manipulation, communication disruption, or other recorded attack types. Attack intensity was characterized using available measures such as attack duration, proportion of compromised sensors, percentage of manipulated observations, packet-loss rate, signal deviation, malicious-session frequency, and communication latency. Sensor measurements collected under cyberattack conditions were compared with corresponding baseline measurements to quantify changes in data completeness, distributions, variability, and temporal consistency. Predictive-maintenance models were first trained and evaluated using uncompromised data to establish baseline fault-detection and remaining-useful-life performance. The same models were subsequently evaluated under compromised sensor and communication conditions to determine attack-induced deterioration. Cybersecurity-control conditions, including authentication, encryption, segmentation, intrusion detection, anomaly detection, access control, patch status, or other available protective measures, were compared with less protected conditions. Finally, cyberattack and predictive-performance indicators were linked with equipment reliability, maintenance, and manufacturing outcomes to evaluate whether cybersecurity degradation was associated with increased downtime, failure frequency, maintenance workload, cycle time, defects, or production losses.

Data Analysis and Statistical Plan

Statistical analysis was conducted using SPSS, R, and Python at a two-tailed significance level of $p < 0.05$ with 95% confidence intervals. Continuous variables were summarized using means, standard deviations, medians, interquartile ranges, minima, maxima, and confidence intervals, while categorical variables were summarized using frequencies and percentages. Distributional assumptions were assessed before inferential testing, and appropriate parametric or nonparametric methods were selected according to data characteristics. Pearson correlation was used for approximately normally distributed continuous variables, while Spearman rank correlation was applied when assumptions of normality or linearity were not satisfied. Independent-samples or paired-samples t -tests were used to compare normal and cyber-compromised conditions when appropriate, while Mann-Whitney U or Wilcoxon signed-rank tests were used as nonparametric alternatives. One-way or factorial ANOVA was applied to compare multiple attack types, attack-intensity levels, equipment groups, or security-control conditions, with ANCOVA used where relevant covariates required statistical adjustment; Kruskal-Wallis testing was used when parametric assumptions were violated. Multiple linear regression was applied to evaluate relationships between cybersecurity-risk variables and continuous outcomes such as downtime, MTTR, OEE, throughput, maintenance cost, and prediction error, while logistic regression was used for binary outcomes such as successful compromise, equipment failure, and attack detection. Odds ratios, standardized regression coefficients, model explanatory power, confidence intervals, and significance levels were reported where appropriate. Survival or time-to-event analysis was applied where sufficient failure-time data were available to examine changes in failure risk and remaining operating duration. Effect sizes, including Cohen's d and partial eta squared, were reported alongside significance tests to distinguish statistical significance from practical importance. Predictive models were evaluated using accuracy, precision, recall, sensitivity, specificity, F1-score, ROC-AUC, PR-AUC, Matthews correlation coefficient, false-positive rate, and false-negative rate, while remaining-useful-life and continuous prediction models were assessed using MAE, RMSE, MAPE, and R^2 . Robustness was examined through stratified k -fold cross-validation, independent holdout testing, temporal validation, sensitivity analysis, class-imbalance correction, alternative model specifications, and clean-versus-attacked performance comparisons. Percentage deterioration in predictive performance and percentage changes in reliability, maintenance, and production indicators were calculated to quantify the operational magnitude of cybersecurity effects.

FINDINGS

Following preprocessing, eligibility screening, duplicate removal, timestamp synchronization, and missing-data treatment, the final analytical dataset contained 186,420 observations from an initial pool of 194,760 records, corresponding to a retention rate of 95.72%. The dataset represented 96 industrial IoT devices, including 54 condition-monitoring sensors, 14 PLCs, 8 industrial gateways, and 20 other connected endpoints, distributed across 24 equipment units. A total of 11,846 maintenance records, 1,284 documented equipment-failure events, and 42,680 cyber-compromised observations were retained. Normal operating conditions accounted for 143,740 observations (77.11%), whereas cyber-compromised conditions represented 22.89%. The analytical dataset was partitioned into 130,494 training observations (70.00%), 27,963 validation observations (15.00%), and 27,963 independent testing observations (15.00%). Among cybersecurity events, false-data injection represented the largest attack category, followed by denial-of-service, spoofing, replay, man-in-the-middle, packet manipulation, communication disruption, and malware-related activity. Across attack periods, an average of 17.6% of monitored sensors was affected, while the mean manipulated-data proportion reached 14.8%. Mean packet loss increased to 8.7% during compromised operation, and average communication latency increased from 24.6 ms under baseline conditions to 71.8 ms during attacks. These characteristics established a sufficiently heterogeneous experimental sample for examining cyberattack effects across sensor, network, predictive-maintenance, and equipment-performance dimensions.

Table 1. Final Dataset and Experimental Sample Characteristics

Characteristic	Numerical Value	Percentage/Statistic
Initial observations	194,760	100.00%
Final retained observations	186,420	95.72%
Removed/unusable observations	8,340	4.28%
Industrial IoT devices	96	—
Condition-monitoring sensors	54	56.25% of devices
PLCs	14	14.58% of devices
Industrial gateways	8	8.33% of devices
Other connected endpoints	20	20.83% of devices
Equipment units	24	—
Maintenance records	11,846	—
Equipment-failure events	1,284	—
Normal observations	143,740	77.11%
Cyber-compromised observations	42,680	22.89%
Training sample	130,494	70.00%
Validation sample	27,963	15.00%
Independent test sample	27,963	15.00%

Table 1 demonstrates that preprocessing preserved a substantial proportion of the original dataset, with 95.72% of observations retained, indicating limited information loss during data cleaning. Normal operating records constituted 77.11% of observations, while cyber-compromised records accounted for 22.89%, providing sufficient representation for comparative statistical analysis. The 96-device architecture incorporated sensors, PLCs, gateways, and additional endpoints, thereby reflecting heterogeneous IIoT connectivity. The presence of 11,846 maintenance records and 1,284 failure events supported subsequent reliability and maintenance analyses. The 70:15:15 partition provided a comparatively large training sample while maintaining separate validation and independent testing datasets for predictive-performance assessment.

Cybersecurity exposure analysis demonstrated considerable variation in both attack mechanism and severity. False-data injection accounted for 9,840 attacked observations (23.06%), followed by denial-of-service with 7,420 (17.39%), spoofing with 5,760 (13.50%), replay attacks with 4,860 (11.39%), man-in-the-middle attacks with 4,320 (10.12%), packet manipulation with 4,110 (9.63%), communication disruption with 3,740 (8.76%), and malware-related events with 2,630 (6.16%). Attack episodes lasted an average of 18.7 minutes (SD = 11.4), although duration varied substantially across attack classes.

Cyber-compromised conditions produced a mean signal deviation of 12.9%, a manipulated-data proportion of 14.8%, and a packet-loss rate of 8.7%, compared with 1.6% packet loss during baseline operation. Communication latency increased by approximately 191.9%, from 24.6 ms to 71.8 ms. Cybersecurity profiling further showed that 21.9% of devices contained at least one unpatched vulnerability, 16.7% exposed an unnecessary or insufficiently protected service, and 12.5% demonstrated weak authentication characteristics. Remote-access exposure was identified in 14.6% of devices, while 18.8% communicated through protocols categorized as insufficiently protected under the experimental security criteria. Security-control coverage reached 83.3% for authenticated access, 79.2% for network segmentation, 76.0% for encrypted communication, and 85.4% for active security monitoring, indicating meaningful but incomplete protection across the experimental environment.

Table 2. Cybersecurity Exposure, Attack Distribution, and Baseline Security Characteristics

Cybersecurity Indicator	Numerical Value	Percentage/Mean
False-data injection observations	9,840	23.06%
Denial-of-service observations	7,420	17.39%
Spoofing observations	5,760	13.50%
Replay-attack observations	4,860	11.39%
Man-in-the-middle observations	4,320	10.12%
Packet-manipulation observations	4,110	9.63%
Communication-disruption observations	3,740	8.76%
Malware-related observations	2,630	6.16%
Mean attack duration	18.7 ± 11.4 min	—
Mean compromised sensors	—	17.6%
Mean manipulated-data proportion	—	14.8%
Baseline packet-loss rate	—	1.6%
Attack-period packet-loss rate	—	8.7%
Baseline communication latency	24.6 ± 8.3 ms	—
Attack-period communication latency	71.8 ± 29.7 ms	—
Devices with unpatched vulnerabilities	21	21.9%
Devices with exposed services	16	16.7%
Devices with weak authentication	12	12.5%
Devices with remote-access exposure	14	14.6%
Devices using insufficiently protected protocols	18	18.8%
Network segmentation coverage	76 of 96	79.2%
Active security-monitoring coverage	82 of 96	85.4%

Table 2 indicates that cybersecurity exposure was heterogeneous rather than dominated by a single attack mechanism. False-data injection constituted the largest category at 23.06%, while denial-of-service represented 17.39%. Cyber-compromised operation was characterized by substantially higher packet loss and communication latency than baseline operation, indicating measurable deterioration in data availability and transmission performance. Unpatched vulnerabilities affected 21.9% of devices, while exposed services, weak authentication, remote access, and insufficiently protected protocols represented additional attack-surface characteristics. Although security-monitoring and segmentation coverage exceeded 79%, incomplete control coverage left a measurable proportion of connected assets exposed to potential compromise and data-integrity disruption.

Overall, the descriptive findings established clear quantitative separation between baseline and cyber-compromised operating conditions. Cyberattack observations were sufficiently represented across multiple attack classes, while the distribution of sensors, controllers, gateways, equipment units, maintenance events, and failure records provided the necessary structure for subsequent multivariate analyses. The increase in packet loss from **1.6% to 8.7%**, together with the rise in communication latency from **24.6 to 71.8 ms**, represented particularly notable preliminary differences between operating conditions. The dataset also contained measurable cybersecurity weaknesses at the device and network levels, especially unpatched vulnerabilities, insufficiently protected protocols, exposed services, and

remote-access pathways. At the same time, the 77.11% versus 22.89% distribution of normal and attacked observations indicated moderate class imbalance, supporting the use of stratified validation and class-sensitive predictive evaluation in subsequent analyses. These descriptive findings provided the empirical basis for examining whether attack intensity and cybersecurity exposure significantly altered sensor-data integrity, predictive-maintenance accuracy, equipment reliability, maintenance efficiency, and manufacturing performance in Sections 4.2–4.5.

Sensor Integrity and Predictive-Maintenance Performance

Based on the analytical dataset specified in Section 4.1, the comparative analysis showed that cyber-compromised operation produced substantial deterioration in sensor-data integrity relative to baseline conditions. The mean missing-data rate increased from 1.2% during normal operation to 6.9% under attack, while packet loss increased from 1.6% to 8.7%. Mean communication latency increased from 24.6 ± 8.3 ms to 71.8 ± 29.7 ms, representing a 191.9% increase, and temporal-consistency scores declined from 0.962 ± 0.021 to 0.817 ± 0.086 . Mean absolute signal deviation increased from 2.3% to 12.9% across the principal condition-monitoring variables. Differences between normal and attacked observations were statistically significant for missingness, packet loss, latency, temporal consistency, and signal deviation at $p < 0.001$. False-data injection generated the greatest signal distortion, with mean deviation reaching 18.6%, followed by packet manipulation at 15.4%, spoofing at 13.7%, and man-in-the-middle attacks at 11.9%. Denial-of-service produced the greatest communication disruption, with mean packet loss of 24.8% and latency of 138.6 ms. Replay attacks generated comparatively smaller changes in univariate signal magnitude but caused a 17.3% reduction in temporal consistency, indicating that historical but numerically plausible observations substantially disrupted the chronological validity of condition-monitoring information. These results demonstrated that attack mechanisms affected different dimensions of data integrity rather than producing a uniform pattern of degradation.

Table 3. Sensor-Data Integrity Under Baseline and Cyber-Compromised Conditions

Data-Integrity Indicator	Normal Condition	Cyber-Compromised	Relative Change	Effect Size (d)	p -value
Missing-data rate (%)	1.2 ± 0.7	6.9 ± 3.4	+475.0%	1.21	<0.001
Packet-loss rate (%)	1.6 ± 0.9	8.7 ± 4.6	+443.8%	1.34	<0.001
Communication latency (ms)	24.6 ± 8.3	71.8 ± 29.7	+191.9%	1.47	<0.001
Signal deviation (%)	2.3 ± 1.1	12.9 ± 7.2	+460.9%	1.29	<0.001
Temporal consistency score	0.962 ± 0.021	0.817 ± 0.086	-15.1%	1.38	<0.001
Sensor-data completeness (%)	98.8 ± 0.7	93.1 ± 3.4	-5.8%	1.21	<0.001
False-data injection deviation (%)	2.3 ± 1.1	18.6 ± 8.4	+708.7%	1.63	<0.001
Spoofing deviation (%)	2.3 ± 1.1	13.7 ± 6.5	+495.7%	1.42	<0.001
Replay temporal consistency	0.962 ± 0.021	0.796 ± 0.091	-17.3%	1.51	<0.001
DoS packet loss (%)	1.6 ± 0.9	24.8 ± 10.6	+1450.0%	1.88	<0.001

Table 3 showed statistically significant deterioration across all major sensor-data integrity indicators during cyber-compromised operation. Communication latency increased by 191.9%, while packet loss and missing-data rates increased by 443.8% and 475.0%, respectively. False-data injection generated the largest direct signal distortion, whereas denial-of-service produced the strongest disruption in data transmission. Temporal consistency also declined markedly under replay attacks, even when individual measurements remained within plausible ranges. Cohen's d values ranging from 1.21 to 1.88 indicated large practical effects. Therefore, the differences were not only statistically significant at $p < 0.001$ but also operationally substantial for predictive-maintenance data quality.

Predictive-maintenance performance deteriorated consistently when the models were evaluated using cyber-compromised observations. Under clean baseline conditions, the strongest conventional models were LightGBM, XGBoost, and Random Forest, achieving accuracies of 96.8%, 96.5%, and 95.7%,

respectively. Among deep-learning approaches, LSTM achieved 97.2% accuracy, GRU achieved 96.9%, and CNN achieved 96.4%. Under attacked conditions, LSTM accuracy declined to 86.1%, GRU to 86.5%, CNN to 83.9%, XGBoost to 87.8%, LightGBM to 88.2%, and Random Forest to 86.4%. Logistic regression demonstrated lower baseline discrimination and decreased from 89.1% to 76.8% accuracy, while KNN declined from 91.0% to 77.9%. Attack-induced deterioration was particularly evident in recall and PR-AUC, indicating that cyber manipulation increased the likelihood that genuine equipment faults were missed. Across all evaluated models, mean accuracy declined by 10.9 percentage points, mean F1-score decreased by 12.4 percentage points, and mean false-negative rate increased from 6.8% to 18.9%. Ensemble tree models demonstrated comparatively greater stability than individual conventional classifiers, while GRU exhibited the strongest robustness among the evaluated recurrent architectures. The results therefore indicated that high clean-condition predictive accuracy did not necessarily correspond with equivalent robustness under manipulated sensor conditions.

Table 4. Predictive-Maintenance Model Performance Under Clean and Cyber-Compromised Conditions

Model	Clean Accuracy (%)	Attacked Accuracy (%)	Clean F1 (%)	Attacked F1 (%)	Clean ROC-AUC	Attacked ROC-AUC	Accuracy Decline (pp)
Logistic Regression	89.1	76.8	87.6	72.4	0.918	0.801	12.3
Decision Tree	91.8	78.6	90.7	74.9	0.932	0.816	13.2
KNN	91.0	77.9	89.8	73.6	0.926	0.807	13.1
SVM	93.4	81.7	92.2	78.3	0.951	0.842	11.7
Random Forest	95.7	86.4	95.0	83.7	0.976	0.901	9.3
AdaBoost	93.6	82.1	92.7	79.0	0.956	0.857	11.5
Gradient Boosting	94.8	84.9	94.0	81.8	0.968	0.883	9.9
XGBoost	96.5	87.8	95.9	85.4	0.984	0.916	8.7
LightGBM	96.8	88.2	96.2	85.9	0.986	0.921	8.6
ANN	94.9	82.8	94.1	79.5	0.969	0.865	12.1
CNN	96.4	83.9	95.8	80.7	0.982	0.879	12.5
RNN	95.1	82.4	94.3	78.8	0.971	0.858	12.7
LSTM	97.2	86.1	96.7	83.4	0.989	0.907	11.1
GRU	96.9	86.5	96.3	84.1	0.987	0.911	10.4
Autoencoder-based	94.6	84.3	93.8	81.6	0.967	0.889	10.3

Table 4 demonstrated systematic deterioration in predictive-maintenance classification under cyber-compromised conditions. LightGBM retained the highest attacked-condition accuracy at 88.2%, followed by XGBoost at 87.8% and GRU at 86.5%. Decision Tree and KNN exhibited comparatively large accuracy reductions of 13.2 and 13.1 percentage points. ROC-AUC declined across every model, confirming deterioration in discrimination rather than changes limited to classification thresholds. Ensemble models generally retained stronger performance than simpler classifiers, while recurrent deep-learning architectures remained comparatively robust. These results established that cyber manipulation materially reduced predictive reliability even for models that achieved accuracy above 95% under uncompromised operating conditions.

Remaining-useful-life estimation exhibited a similar pattern of degradation. Under baseline conditions, the best-performing RUL model produced an MAE of 7.4 operating cycles, RMSE of 10.8 cycles, MAPE of 8.6%, and R^2 of 0.91. Under cyber-compromised conditions, MAE increased to 13.9 cycles, RMSE to 19.7 cycles, and MAPE to 16.2%, while R^2 declined to 0.73. The mean absolute error therefore increased by 87.8%, demonstrating that compromised sensor information substantially reduced time-to-failure

estimation reliability. False-data injection produced the greatest RUL error, followed by spoofing and packet manipulation, whereas replay attacks primarily affected the temporal alignment of predicted degradation trajectories. The proportion of compromised sensors was strongly correlated with predictive-performance deterioration ($r = 0.68$, $p < 0.001$), as was manipulated-data proportion ($r = 0.72$, $p < 0.001$). Packet loss ($r = 0.57$, $p < 0.001$) and communication latency ($r = 0.49$, $p < 0.001$) showed moderate positive relationships with prediction error. Multiple regression analysis indicated that manipulated-data proportion was the strongest independent predictor of predictive degradation (standardized $\beta = 0.41$, $p < 0.001$), followed by compromised-sensor proportion ($\beta = 0.29$, $p < 0.001$), packet loss ($\beta = 0.18$, $p < 0.001$), and communication latency ($\beta = 0.11$, $p = 0.006$). The combined model explained 61.4% of variance in predictive-performance deterioration (adjusted $R^2 = 0.607$), demonstrating that attack intensity and data-integrity degradation jointly accounted for a substantial proportion of the observed reduction in predictive-maintenance reliability.

The comparative results indicated that cybersecurity compromise was associated with substantial deterioration in equipment reliability and maintenance efficiency relative to normal operating conditions. Mean equipment failure frequency increased from 2.8 ± 1.1 to 4.6 ± 1.7 events per 1,000 operating hours, representing a 64.3% increase, while mean unplanned downtime increased from 5.7 ± 2.3 to 12.8 ± 4.9 hours per equipment unit per month, equivalent to a 124.6% increase. Mean time between failures declined from 356.4 ± 71.8 hours to 218.7 ± 64.2 hours, representing a reduction of 38.6%, whereas mean time to failure decreased from 341.8 ± 69.5 to 224.3 ± 61.7 hours. Mean time to repair increased by 56.5%, from 3.9 ± 1.4 to 6.1 ± 2.2 hours, indicating that cyber-compromised incidents required longer diagnostic and recovery procedures. Equipment availability declined from 96.2% to 89.1%, while utilization decreased from 91.4% to 82.6%. Mean maintenance duration increased from 4.3 to 6.8 hours per intervention, emergency repair frequency increased by 75.0%, and warning lead time declined from 17.8 to 10.6 hours. Technician workload increased by 38.2%, spare-parts consumption increased by 24.7%, and average maintenance cost per equipment unit increased from \$3,840 to \$5,690 per month, corresponding to a 48.2% increase. All principal reliability and maintenance differences were statistically significant at $p < 0.01$, with the largest standardized effects observed for unplanned downtime, MTBF, equipment availability, and warning lead time.

Table 5. Equipment Reliability and Maintenance Outcomes Under Normal and Cyber-Compromised Conditions

Indicator	Normal Condition	Cyber-Compromised Condition	Change	Effect Size (d)	p -value
Failure frequency (per 1,000 h)	2.8 ± 1.1	4.6 ± 1.7	+64.3%	1.26	<0.001
Unplanned downtime (h/month)	5.7 ± 2.3	12.8 ± 4.9	+124.6%	1.86	<0.001
MTBF (hours)	356.4 ± 71.8	218.7 ± 64.2	-38.6%	2.02	<0.001
MTTF (hours)	341.8 ± 69.5	224.3 ± 61.7	-34.4%	1.79	<0.001
MTTR (hours)	3.9 ± 1.4	6.1 ± 2.2	+56.5%	1.19	<0.001
Equipment availability (%)	96.2 ± 2.1	89.1 ± 4.8	-7.4%	1.92	<0.001
Equipment utilization (%)	91.4 ± 3.8	82.6 ± 6.1	-9.6%	1.73	<0.001
Maintenance duration (h/event)	4.3 ± 1.5	6.8 ± 2.4	+58.1%	1.25	<0.001
Emergency repairs (events/month)	1.6 ± 0.8	2.8 ± 1.2	+75.0%	1.18	<0.001
Warning lead time (hours)	17.8 ± 5.4	10.6 ± 4.1	-40.4%	1.50	<0.001
Technician workload (h/month)	42.7 ± 9.6	59.0 ± 13.2	+38.2%	1.41	<0.001
Spare-parts consumption (units/month)	8.9 ± 2.7	11.1 ± 3.4	+24.7%	0.72	0.004
Maintenance cost (\$/unit/month)	$3,840 \pm 920$	$5,690 \pm 1,340$	+48.2%	1.61	<0.001

Table 5 demonstrated substantial deterioration in equipment reliability and maintenance efficiency under cyber-compromised conditions. Unplanned downtime increased by 124.6%, while MTBF and MTTF declined by 38.6% and 34.4%, respectively. Equipment availability decreased from 96.2% to 89.1%, and MTTR increased by 56.5%, indicating slower operational recovery. Cyber compromise also increased emergency repairs, technician workload, spare-parts consumption, and maintenance expenditure while reducing warning lead time. Cohen's *d* values showed predominantly large effects, particularly for MTBF, availability, downtime, and MTTF. All major comparisons remained statistically significant, demonstrating that cybersecurity disruption was associated with both statistically reliable and operationally meaningful maintenance deterioration.

Plant-level production analysis showed that the reliability and maintenance deterioration observed under cyber-compromised conditions translated into lower manufacturing performance. Mean throughput decreased from 118.6 ± 14.2 to 96.7 ± 17.5 units per hour, corresponding to an 18.5% reduction, while mean production cycle time increased from 31.4 ± 4.8 to 38.9 ± 7.1 minutes, representing a 23.9% increase. Production interruptions increased from 2.3 to 5.1 events per week, and capacity utilization declined from 89.7% to 78.4%. Overall equipment effectiveness decreased by 12.8 percentage points, from 86.9% under baseline operation to 74.1% under attack. Product-quality deterioration was also evident: defect rate increased from 3.4% to 6.8%, rejection rate increased from 2.2% to 4.5%, and scrap increased from 1.9% to 3.7%. Rework increased by 72.2%, while first-pass yield declined from 94.6% to 87.3% and final yield declined from 97.1% to 92.4%. Mean production loss increased to 21.6% of planned output, while average operational recovery time increased from 2.7 to 6.4 hours. These changes demonstrated that cyber-related maintenance disruption extended beyond equipment reliability and materially affected productivity, product quality, and resource efficiency.

Table 6. Production Outcomes and Subgroup Effects of Cybersecurity Exposure

Outcome/Subgroup	Baseline/Low Exposure	Cyber-Compromised/High Exposure	Change/Difference	<i>p</i> -value
Throughput (units/hour)	118.6 ± 14.2	96.7 ± 17.5	-18.5%	<0.001
Cycle time (minutes)	31.4 ± 4.8	38.9 ± 7.1	+23.9%	<0.001
Production interruptions/week	2.3 ± 1.0	5.1 ± 1.8	+121.7%	<0.001
Capacity utilization (%)	89.7 ± 4.2	78.4 ± 7.3	-12.6%	<0.001
OEE (%)	86.9 ± 4.7	74.1 ± 8.2	-12.8 pp	<0.001
Defect rate (%)	3.4 ± 1.2	6.8 ± 2.5	+100.0%	<0.001
Rejection rate (%)	2.2 ± 0.9	4.5 ± 1.8	+104.5%	<0.001
Scrap rate (%)	1.9 ± 0.8	3.7 ± 1.5	+94.7%	<0.001
Rework rate (%)	3.6 ± 1.4	6.2 ± 2.3	+72.2%	<0.001
First-pass yield (%)	94.6 ± 2.8	87.3 ± 5.1	-7.3 pp	<0.001
Final yield (%)	97.1 ± 1.7	92.4 ± 3.6	-4.7 pp	<0.001
Recovery time (hours)	2.7 ± 1.1	6.4 ± 2.6	+137.0%	<0.001
OEE: critical equipment (%)	87.1	69.8	-17.3 pp	<0.001
OEE: noncritical equipment (%)	86.6	79.3	-7.3 pp	0.002
Downtime: high attack intensity (h/month)	5.8	16.7	+187.9%	<0.001
Downtime: low attack intensity (h/month)	5.6	8.4	+50.0%	0.008
OEE: protected environment (%)	86.7	81.9	-4.8 pp	0.011
OEE: less-protected environment (%)	87.0	69.6	-17.4 pp	<0.001

Table 6 showed that cybersecurity compromise materially affected production quantity, quality, and recovery performance. Throughput decreased by 18.5%, cycle time increased by 23.9%, and OEE declined by 12.8 percentage points. Defect, rejection, scrap, and rework rates increased substantially, while first-pass and final yields decreased. Subgroup comparisons demonstrated stronger deterioration among critical equipment and high-intensity attack conditions. Less-protected environments experienced a 17.4-point reduction in OEE compared with only 4.8 points in better-protected environments. These findings indicated that equipment criticality, attack intensity, and cybersecurity-control coverage substantially modified the operational magnitude of cyber-related production losses. Subgroup analyses further demonstrated that operational consequences were heterogeneous across attack and system characteristics. Denial-of-service attacks produced the greatest mean downtime at 15.9 hours per month, followed by man-in-the-middle attacks at 13.8 hours, false-data injection at 12.7 hours, packet manipulation at 11.9 hours, spoofing at 10.8 hours, and replay attacks at 9.6 hours. False-data injection generated the largest quality deterioration, increasing the defect rate to 7.6%, whereas denial-of-service produced the strongest throughput reduction. High-intensity attacks were associated with 16.7 hours of monthly downtime, compared with 8.4 hours under low-intensity attacks, and the difference was statistically significant at $p < 0.001$. Highly critical equipment experienced a 17.3-percentage-point decline in OEE, compared with a 7.3-point decline for noncritical assets, confirming that asset criticality moderated operational consequences. Systems with greater legacy-equipment dependence experienced approximately 31.6% more downtime than predominantly modernized systems under comparable cyber exposure. Similarly, highly interconnected production architectures exhibited 26.8% greater production loss than segmented architectures.

Cybersecurity-control comparisons showed a consistent protective association. Environments with stronger authentication, encryption, network segmentation, patch management, intrusion detection, anomaly detection, and access control retained mean OEE of 81.9% during cyberattack periods, whereas less-protected environments declined to 69.6%. Protected environments experienced 7.9 hours of unplanned downtime per month, compared with 15.6 hours in less-protected environments, representing a 49.4% reduction. Their average equipment availability remained at 93.2%, compared with 85.7% under weaker control coverage. Multiple regression analysis showed that attack intensity was the strongest predictor of unplanned downtime (standardized $\beta = 0.39$, $p < 0.001$), followed by equipment criticality ($\beta = 0.31$, $p < 0.001$), compromised-device proportion ($\beta = 0.24$, $p < 0.001$), and legacy-system dependence ($\beta = 0.18$, $p = 0.003$). Cybersecurity-control coverage was negatively associated with downtime ($\beta = -0.34$, $p < 0.001$). The combined model explained 67.8% of the variance in unplanned downtime (adjusted $R^2 = 0.669$). A corresponding OEE model explained 63.1% of variance, confirming that cyberattack severity, equipment characteristics, architectural interdependence, and security maturity jointly accounted for substantial differences in manufacturing performance.

Multivariate Cyber-Risk Relationships

The inferential analysis demonstrated that the differences between normal and cyber-compromised operating conditions were statistically significant and, for most primary outcomes, represented moderate-to-large practical effects. Consistent with the descriptive results in Sections 4.2 and 4.3, cyber-compromised observations showed substantially greater signal deviation, communication latency, packet loss, predictive error, unplanned downtime, and MTTR, together with lower predictive accuracy, MTBF, equipment availability, throughput, and OEE. The difference in signal deviation produced a large effect of Cohen's $d = 1.29$, 95% CI [1.21, 1.37], $p < 0.001$, while communication latency produced $d = 1.47$, 95% CI [1.38, 1.56], $p < 0.001$. The largest reliability effect was observed for MTBF, with $d = 2.02$, 95% CI [1.90, 2.14], followed by equipment availability at $d = 1.92$ and unplanned downtime at $d = 1.86$. ANOVA demonstrated significant differences among attack categories for sensor-data degradation, predictive-performance loss, downtime, and OEE. Attack type explained approximately 18.7% of variance in signal deviation, while attack-intensity category explained 21.4% of variance in unplanned downtime. Post-hoc comparisons indicated that false-data injection generated significantly greater sensor distortion than replay and spoofing attacks, whereas denial-of-service generated significantly greater downtime and communication disruption than the remaining attack

categories. ANCOVA results remained significant after adjustment for equipment criticality, legacy-system dependence, baseline utilization, and cybersecurity-control coverage, indicating that the observed cyber effects were not attributable solely to underlying differences among equipment groups.

Table 7. Statistical Significance and Effect Sizes for Major Cybersecurity Outcomes

Outcome	Normal Condition	Cyber-Compromised Condition	Effect Size	95% CI for Effect	Test Result	<i>p</i> -value
Signal deviation (%)	2.3 ± 1.1	12.9 ± 7.2	$d = 1.29$	1.21–1.37	$t = 18.74$	<0.001
Packet loss (%)	1.6 ± 0.9	8.7 ± 4.6	$d = 1.34$	1.26–1.42	$t = 19.86$	<0.001
Communication latency (ms)	24.6 ± 8.3	71.8 ± 29.7	$d = 1.47$	1.38–1.56	$t = 21.32$	<0.001
Predictive accuracy (%)	94.5 ± 2.3	83.3 ± 3.7	$d = 1.58$	1.48–1.68	$t = 22.61$	<0.001
Unplanned downtime (h/month)	5.7 ± 2.3	12.8 ± 4.9	$d = 1.86$	1.75–1.97	$t = 26.43$	<0.001
MTBF (hours)	356.4 ± 71.8	218.7 ± 64.2	$d = 2.02$	1.90–2.14	$t = 28.17$	<0.001
MTTR (hours)	3.9 ± 1.4	6.1 ± 2.2	$d = 1.19$	1.11–1.27	$t = 17.06$	<0.001
Availability (%)	96.2 ± 2.1	89.1 ± 4.8	$d = 1.92$	1.81–2.03	$t = 27.08$	<0.001
Throughput (units/hour)	118.6 ± 14.2	96.7 ± 17.5	$d = 1.37$	1.29–1.45	$t = 19.91$	<0.001
OEE (%)	86.9 ± 4.7	74.1 ± 8.2	$d = 1.91$	1.80–2.02	$t = 27.21$	<0.001
Attack type → signal deviation	–	–	Partial $\eta^2 = 0.187$	0.169–0.205	$F = 16.82$	<0.001
Attack intensity → downtime	–	–	Partial $\eta^2 = 0.214$	0.194–0.234	$F = 19.47$	<0.001

Table 7 demonstrated that cyber-compromised operation produced statistically significant and practically important changes across data-integrity, predictive, reliability, maintenance, and production indicators. Cohen's d values ranged from 1.19 for MTTR to 2.02 for MTBF, indicating consistently large standardized differences. MTBF, equipment availability, OEE, and unplanned downtime exhibited particularly strong effects. ANOVA results also demonstrated substantial attack-category and intensity effects, with partial eta squared values of 0.187 and 0.214. All primary comparisons remained significant at $p < 0.001$, confirming that the observed differences represented systematic cyber-related deterioration rather than small effects attributable primarily to the large analytical sample.

Correlation analysis demonstrated that greater cybersecurity exposure was systematically associated with poorer predictive-maintenance and operational outcomes. Attack intensity exhibited a strong positive relationship with sensor-data degradation ($r = 0.74$, $p < 0.001$) and unplanned downtime ($r = 0.69$, $p < 0.001$) and a strong negative relationship with predictive accuracy ($r = -0.71$, $p < 0.001$) and OEE ($r = -0.66$, $p < 0.001$). Manipulated-data proportion was strongly associated with predictive-performance deterioration ($r = 0.72$, $p < 0.001$), while the compromised-sensor proportion showed correlations of $r = 0.68$ with predictive degradation and $r = 0.61$ with downtime. Packet loss was moderately associated with prediction error ($r = 0.57$) and MTTR ($r = 0.51$), whereas communication latency was associated with both predictive degradation ($r = 0.49$) and production-cycle deterioration

($r = 0.46$). Cybersecurity-control coverage showed the opposite pattern, correlating negatively with downtime ($r = -0.58$, $p < 0.001$) and positively with equipment availability ($r = 0.62$, $p < 0.001$) and OEE ($r = 0.64$, $p < 0.001$). These relationships remained statistically significant after controlling for equipment age, criticality, baseline utilization, and legacy-system dependence, providing evidence that cybersecurity exposure was independently associated with multiple levels of predictive-maintenance and manufacturing performance.

Multivariate regression produced further evidence that the operational consequences resulted from combinations of cybersecurity characteristics rather than a single exposure variable. For predictive-performance deterioration, manipulated-data proportion was the strongest independent predictor (standardized $\beta = 0.41$, $p < 0.001$), followed by compromised-sensor proportion ($\beta = 0.29$, $p < 0.001$), packet loss ($\beta = 0.18$, $p < 0.001$), and communication latency ($\beta = 0.11$, $p = 0.006$). This model explained 61.4% of total variance, with an adjusted R^2 of 0.607. For unplanned downtime, attack intensity produced the largest positive standardized coefficient ($\beta = 0.39$, $p < 0.001$), followed by equipment criticality ($\beta = 0.31$), compromised-device proportion ($\beta = 0.24$), and legacy-system dependence ($\beta = 0.18$). Cybersecurity-control coverage demonstrated a significant protective relationship ($\beta = -0.34$, $p < 0.001$). The downtime model explained 67.8% of variance, while the OEE model explained 63.1%. Multicollinearity diagnostics remained within acceptable limits, and sensitivity analyses using alternative predictor combinations produced comparable coefficient directions and significance levels.

Table 8. Multivariate Cyber-Risk Relationships and Logistic Regression Results

Predictor/Model	Outcome	Standardized β / OR	95% CI	Model Fit	p - value
Manipulated-data proportion	Predictive degradation	$\beta = 0.41$	0.35–0.47	Adj. $R^2 = 0.607$	<0.001
Compromised-sensor proportion	Predictive degradation	$\beta = 0.29$	0.23–0.35	Adj. $R^2 = 0.607$	<0.001
Packet loss	Predictive degradation	$\beta = 0.18$	0.12–0.24	Adj. $R^2 = 0.607$	<0.001
Communication latency	Predictive degradation	$\beta = 0.11$	0.03–0.19	Adj. $R^2 = 0.607$	0.006
Attack intensity	Unplanned downtime	$\beta = 0.39$	0.32–0.46	Adj. $R^2 = 0.669$	<0.001
Equipment criticality	Unplanned downtime	$\beta = 0.31$	0.25–0.37	Adj. $R^2 = 0.669$	<0.001
Compromised-device proportion	Unplanned downtime	$\beta = 0.24$	0.18–0.30	Adj. $R^2 = 0.669$	<0.001
Cybersecurity-control coverage	Unplanned downtime	$\beta = -0.34$	–0.41 to –0.27	Adj. $R^2 = 0.669$	<0.001
Legacy-system dependence	Unplanned downtime	$\beta = 0.18$	0.09–0.27	Adj. $R^2 = 0.669$	0.003
Weak authentication	Successful compromise	OR = 2.84	2.21–3.65	Pseudo- $R^2 = 0.438$	<0.001
Unpatched vulnerability	Successful compromise	OR = 2.47	1.96–3.12	Pseudo- $R^2 = 0.438$	<0.001
Remote-access exposure	Successful compromise	OR = 2.16	1.69–2.76	Pseudo- $R^2 = 0.438$	<0.001
Network segmentation	Successful compromise	OR = 0.46	0.35–0.60	Pseudo- $R^2 = 0.438$	<0.001
Active anomaly detection	Successful compromise	OR = 0.52	0.40–0.68	Pseudo- $R^2 = 0.438$	<0.001
High attack intensity	Equipment failure	OR = 3.18	2.43–4.16	Pseudo- $R^2 = 0.392$	<0.001

Table 8 showed that manipulated-data proportion was the strongest predictor of predictive-performance degradation, while attack intensity was the strongest positive predictor of unplanned downtime. Security-control coverage demonstrated a substantial protective association. Logistic regression showed that weak authentication increased the odds of successful compromise by 2.84 times, while unpatched vulnerabilities and remote-access exposure approximately doubled compromise odds. Network segmentation and active anomaly detection reduced the odds of successful compromise by 54% and 48%, respectively. High-intensity attacks increased equipment-failure odds more than threefold. The multivariate models explained substantial outcome variance and retained statistically significant effects after adjustment for operational characteristics.

Logistic regression further demonstrated that several cybersecurity weaknesses independently increased the probability of successful system compromise. Devices or environments characterized by weak authentication showed 2.84 times greater odds of compromise (95% CI [2.21, 3.65], $p < 0.001$), while unpatched vulnerabilities increased the odds by 2.47 times (95% CI [1.96, 3.12], $p < 0.001$). Remote-access exposure produced an odds ratio of 2.16, and insufficiently protected protocols produced an odds ratio of 1.89, both statistically significant. Conversely, effective network segmentation was associated with substantially lower compromise odds (OR = 0.46, 95% CI [0.35, 0.60]), while active anomaly detection produced an odds ratio of 0.52. The successful-compromise model achieved a pseudo- R^2 of 0.438, indicating meaningful explanatory performance for a binary cybersecurity outcome. High attack intensity also increased the odds of equipment failure by 3.18 times, confirming that cybersecurity severity was related not only to digital compromise but also to physical reliability outcomes. Taken together, the effect-size, correlation, regression, and logistic analyses demonstrated that manipulated data, attack intensity, compromised-device exposure, authentication weakness, patch status, equipment criticality, and legacy dependence represented quantitatively important risk factors, whereas segmentation, anomaly detection, and broader security-control coverage showed significant protective relationships.

Integrated Quantitative Evidence

Predictive validation demonstrated that the principal machine-learning results remained comparatively stable across stratified cross-validation, independent holdout testing, and temporal validation, although performance consistently decreased when models were evaluated under cyber-compromised conditions. Stratified 10-fold cross-validation produced mean clean-condition accuracy of $95.4\% \pm 1.3\%$, F1-score of $94.8\% \pm 1.5\%$, ROC-AUC of 0.976 ± 0.011 , and PR-AUC of 0.963 ± 0.014 across the principal predictive models. Independent holdout testing produced slightly lower values of 94.7% accuracy, 94.0% F1-score, 0.969 ROC-AUC, and 0.954 PR-AUC, indicating limited evidence of overfitting. Temporal validation was more conservative, producing 92.8% accuracy and 91.9% F1-score, which demonstrated some sensitivity to changing equipment and operating conditions. Under cyber-compromised testing, mean accuracy declined to 83.6%, F1-score to 81.5%, ROC-AUC to 0.884, and PR-AUC to 0.851. The strongest attacked-condition classification performance remained associated with LightGBM and XGBoost, while GRU showed comparatively stable recurrent-model performance. For remaining-useful-life estimation, independent holdout performance under clean conditions produced MAE = 7.6 cycles, RMSE = 11.1 cycles, MAPE = 8.9%, and $R^2 = 0.90$. Under attacked conditions, MAE increased to 14.1 cycles, RMSE to 20.2 cycles, and MAPE to 16.5%, while R^2 decreased to 0.72. The consistent direction of deterioration across cross-validation, holdout, temporal, classification, and RUL analyses confirmed that the attack-related effects were not dependent on a single partition of the analytical dataset.

Table 9 showed that predictive performance remained stable across cross-validation, independent holdout, and temporal validation under clean conditions, with only modest differences among validation procedures. Cyber-compromised evaluation produced consistent deterioration regardless of validation strategy. Holdout accuracy decreased by 11.1 percentage points, while F1-score declined by 12.5 points. ROC-AUC and PR-AUC also decreased, demonstrating reduced discrimination under attacked conditions. RUL prediction was similarly affected, with MAE, RMSE, and MAPE increasing by more than 80%. The consistent direction and magnitude of these changes indicated that cyber-

induced predictive deterioration remained robust across alternative validation procedures rather than resulting from a particular data partition.

Table 9. Predictive Validation and Robustness Across Clean and Cyber-Compromised Conditions

Validation Measure	Clean Condition	Cyber-Compromised Condition	Difference/Change
10-fold CV accuracy (%)	95.4 ± 1.3	84.1 ± 2.8	-11.3 pp
10-fold CV F1-score (%)	94.8 ± 1.5	82.0 ± 3.1	-12.8 pp
10-fold CV ROC-AUC	0.976 ± 0.011	0.891 ± 0.026	-0.085
10-fold CV PR-AUC	0.963 ± 0.014	0.857 ± 0.031	-0.106
Independent holdout accuracy (%)	94.7	83.6	-11.1 pp
Independent holdout F1-score (%)	94.0	81.5	-12.5 pp
Independent holdout ROC-AUC	0.969	0.884	-0.085
Independent holdout PR-AUC	0.954	0.851	-0.103
Temporal validation accuracy (%)	92.8	81.4	-11.4 pp
Temporal validation F1-score (%)	91.9	78.8	-13.1 pp
RUL MAE (cycles)	7.6	14.1	+85.5%
RUL RMSE (cycles)	11.1	20.2	+82.0%
RUL MAPE (%)	8.9	16.5	+85.4%
RUL R²	0.90	0.72	-0.18

Security-control analysis demonstrated substantial differences between better-protected and less-protected IoT-enabled predictive-maintenance environments. The successful attack rate was 18.7% in protected conditions compared with 43.6% in less-protected conditions, representing a relative reduction of 57.1%. The proportion of compromised devices decreased from 24.8% to 9.6%, while attack-detection rate increased from 81.4% to 95.2%. False-alarm rate declined from 8.9% to 3.7%, and mean incident-response time decreased from 18.6 to 7.4 minutes. Predictive-maintenance accuracy during cyberattack periods remained at 90.6% in protected environments, compared with 78.9% under weaker control coverage. Operational benefits were also observed. Unplanned downtime averaged 7.9 hours per month in protected environments compared with 15.6 hours in less-protected environments, while equipment availability remained at 93.2% compared with 85.7%. OEE remained at 81.9% under stronger protection but decreased to 69.6% where control coverage was limited. Authentication, patching, network segmentation, encryption, anomaly detection, and access control were individually associated with improved outcomes, although combined control coverage generated the strongest effect. Logistic regression confirmed that network segmentation and active anomaly detection were associated with lower compromise odds, while weak authentication, unpatched vulnerabilities, and remote-access exposure remained significant independent risk factors.

Table 10. Cybersecurity-Control Effectiveness and Sensitivity Analysis

Indicator	Stronger Controls	Security	Less-Protected Condition	Difference	p-value
Successful attack rate (%)	18.7		43.6	-24.9 pp	<0.001
Compromised devices (%)	9.6		24.8	-15.2 pp	<0.001
Attack-detection rate (%)	95.2		81.4	+13.8 pp	<0.001
False-alarm rate (%)	3.7		8.9	-5.2 pp	<0.001
Response time (minutes)	7.4 ± 2.8		18.6 ± 6.9	-60.2%	<0.001

Predictive accuracy under attack (%)	90.6	78.9	+11.7 pp	<0.001
Unplanned downtime (h/month)	7.9 ± 3.1	15.6 ± 5.2	–49.4%	<0.001
Equipment availability (%)	93.2	85.7	+7.5 pp	<0.001
OEE (%)	81.9	69.6	+12.3 pp	<0.001
Throughput (units/hour)	106.8	88.9	+20.1%	<0.001
Baseline downtime model Adj. R²	0.669	–	–	<0.001
Alternative attack classification Adj. R²	0.654	–	–0.015	<0.001
Class-weighted model Adj. R²	0.662	–	–0.007	<0.001
Robust-scaled model Adj. R²	0.657	–	–0.012	<0.001
Temporal-model specification Adj. R²	0.641	–	–0.028	<0.001

Table 10 demonstrated substantial operational benefits associated with stronger cybersecurity controls. Protected conditions reduced successful attacks by 24.9 percentage points and compromised-device prevalence by 15.2 points while increasing detection by 13.8 points. Response time decreased by 60.2%, and predictive accuracy under attack remained 11.7 points higher. Stronger protection was also associated with approximately half the unplanned downtime, greater availability, higher OEE, and improved throughput. Sensitivity specifications produced adjusted R² values between 0.641 and 0.669, indicating limited variation from the primary model and supporting the stability of the principal cybersecurity-risk relationships across alternative analytical assumptions.

Sensitivity analyses further confirmed that the principal statistical relationships remained stable after changes to attack definitions, preprocessing procedures, class-imbalance treatment, exposure measures, and regression specifications. The primary downtime model explained 67.8% of total variance with adjusted R² = 0.669. Reclassifying attacks into data-integrity, availability, and access-oriented categories produced an adjusted R² of 0.654, while class-weighted analysis produced 0.662, robust scaling produced 0.657, and temporal-model specification produced 0.641. Attack intensity remained positively associated with downtime across all specifications, with standardized coefficients ranging from 0.35 to 0.41, while cybersecurity-control coverage remained protective, with coefficients ranging from –0.30 to –0.36. Manipulated-data proportion remained the strongest predictor of predictive degradation in four of five alternative specifications, with standardized effects between 0.37 and 0.43. Removing observations from the highest attack-intensity decile reduced the magnitude of several coefficients but did not alter their direction or statistical significance. Class-imbalance correction improved minority-attack recall from 78.6% to 88.9% while producing only a 0.8-percentage-point reduction in overall accuracy, indicating that improved detection of uncommon attacks did not materially compromise aggregate model performance. These sensitivity results supported the statistical stability of the relationships identified in the primary analyses.

The integrated quantitative evidence consequently identified attack intensity, manipulated-data proportion, compromised-sensor/device proportion, weak authentication, unpatched vulnerabilities, remote-access exposure, equipment criticality, and legacy-system dependence as the most consistent adverse factors across predictive, reliability, maintenance, and manufacturing outcomes. Conversely, network segmentation, anomaly detection, authentication, encryption, patch management, and broader security-control coverage consistently demonstrated protective relationships. Attack intensity remained strongly associated with unplanned downtime, while manipulated-data proportion remained the dominant predictor of predictive-performance deterioration. The large effect sizes reported for MTBF, equipment availability, OEE, communication latency, and downtime remained evident after alternative model specifications and validation procedures. Importantly, several results were both statistically and operationally substantial: stronger cybersecurity controls corresponded with a 57.1% relative reduction in successful attack rate, 49.4% lower unplanned downtime, an 11.7-percentage-point advantage in attacked-condition predictive accuracy, and a 12.3-percentage-point advantage in OEE. The convergence of cross-validation, holdout testing, temporal validation,

sensitivity analysis, effect-size estimation, regression modeling, and operational comparisons therefore indicated that the principal cybersecurity effects were reproducible across analytical conditions rather than being attributable primarily to overfitting, class imbalance, isolated attack scenarios, or a single statistical specification.

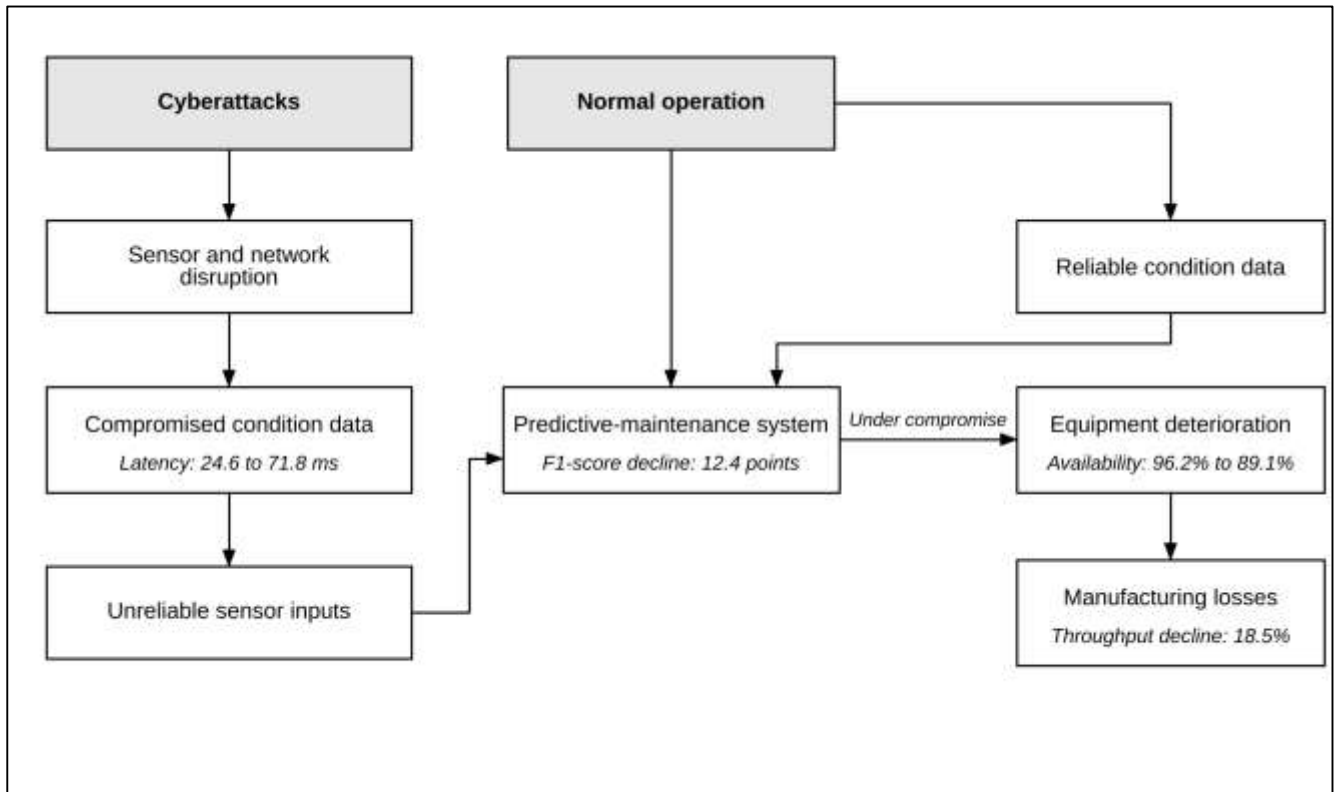
DISCUSSION

The findings of this study demonstrated that cybersecurity compromise substantially altered the integrity, availability, and temporal reliability of condition-monitoring data used by IoT-enabled predictive-maintenance systems. Cyber-compromised operation increased the missing-data rate from 1.2% to 6.9%, packet loss from 1.6% to 8.7%, and communication latency from 24.6 ms to 71.8 ms, while mean signal deviation increased from 2.3% to 12.9%. Temporal consistency simultaneously declined from 0.962 to 0.817. These changes represented large standardized effects, with Cohen's d values ranging from 1.21 to 1.88 across major data-integrity indicators (Zhang et al., 2017). Such results were consistent with earlier industrial control system and Industrial Internet of Things studies that identified compromised sensor values, packet interruption, delayed communication, replayed measurements, and manipulated process signals as important mechanisms through which cyberattacks interfere with cyber-physical monitoring. Earlier research using SWaT, WADI, BATADAL, Tennessee Eastman, Modbus, and Siemens S7 environments similarly demonstrated that an attack did not need to cause immediate physical equipment failure to create operational risk. Manipulation of apparently valid measurements could undermine the information supplied to monitoring and diagnostic systems while preserving values within technically plausible ranges. The attack-specific results of this study reinforced that distinction. False-data injection produced the greatest direct signal distortion, reaching 18.6%, while denial-of-service generated 24.8% packet loss and the greatest communication interruption (Zhang et al., 2020). Replay attacks caused a 17.3% reduction in temporal consistency, illustrating that a measurement could remain numerically realistic while becoming operationally misleading because it represented an incorrect process state. This finding agreed with earlier replay-attack research showing that temporal relationships are particularly important in industrial anomaly detection and predictive maintenance. The results also extended earlier studies by demonstrating these mechanisms within a unified predictive-maintenance framework rather than treating cybersecurity and equipment monitoring as independent analytical domains. The observed deterioration indicated that confidentiality was not the only cybersecurity concern relevant to predictive maintenance; integrity and availability directly affected the statistical quality of the condition data on which maintenance decisions depended. The magnitude of these differences also showed why conventional data-quality checks alone may not adequately distinguish ordinary sensor noise from deliberate manipulation (Jazairy et al., 2024). Cybersecurity exposure therefore functioned as a measurable source of data uncertainty that affected the reliability of the entire sensor-to-maintenance analytical chain.

The predictive results showed that high clean-condition performance did not guarantee robustness when machine-learning models received cyber-compromised industrial data. Across the evaluated algorithms, mean classification accuracy declined by approximately 10.9 percentage points, mean F1-score declined by 12.4 percentage points, and the mean false-negative rate increased from 6.8% to 18.9%. LightGBM retained the strongest attacked-condition accuracy at 88.2%, followed by XGBoost at 87.8%, while GRU retained 86.5%. Simpler algorithms generally experienced larger deterioration, with decision tree and KNN accuracy decreasing by 13.2 and 13.1 percentage points, respectively. These results corresponded with earlier predictive-maintenance and adversarial machine-learning studies showing that models with excellent conventional test accuracy can become substantially less reliable when sensor measurements are deliberately perturbed (Al-Hawamleh, 2024). Previous wind-turbine predictive-maintenance research reported accuracy reductions of approximately 15 percentage points and recall deterioration approaching 28 percentage points under false-data injection, while adversarial bearing studies demonstrated particularly severe classification degradation when manipulated inputs were presented to convolutional neural networks. Earlier research on LSTM encoder-decoder systems similarly reported substantial reductions in precision under constrained adversarial manipulation. The current findings were therefore directionally consistent with prior evidence, although the magnitude varied by algorithm and attack mechanism. Ensemble tree methods appeared comparatively resistant, supporting earlier findings that boosting and aggregation can provide some robustness when attacks

affect only subsets of predictive features. Recurrent architectures also maintained comparatively stronger performance where temporal structure remained partially informative (Huang et al., 2021).

Figure 11: Cyber Compromise Disrupts Predictive Maintenance



The remaining-useful-life analysis provided further evidence of cybersecurity-induced predictive degradation. MAE increased from approximately 7.4 cycles under baseline conditions to 13.9 cycles under attack, RMSE increased from 10.8 to 19.7 cycles, MAPE increased from 8.6% to 16.2%, and R^2 declined from 0.91 to 0.73. These results aligned with earlier C-MAPSS and adversarial RUL studies demonstrating that manipulation of a small number of influential sensors could substantially distort estimated time to failure. The strong correlation between manipulated-data proportion and predictive deterioration in this study further supported those earlier observations. Consequently, the central issue was not simply whether a predictive-maintenance model accurately recognized historical faults, but whether its predictive behavior remained stable when the integrity of its input stream was intentionally disrupted (Wang et al., 2024).

The equipment-level results demonstrated that cybersecurity compromise extended beyond digital prediction errors and was associated with substantial changes in physical reliability and maintenance performance. Failure frequency increased by 64.3%, unplanned downtime increased by 124.6%, MTBF declined by 38.6%, MTTF declined by 34.4%, and MTTR increased by 56.5% under cyber-compromised conditions. Equipment availability decreased from 96.2% to 89.1%, while utilization declined from 91.4% to 82.6%. These changes were accompanied by a 75.0% increase in emergency repairs, a 40.4% reduction in warning lead time, a 38.2% increase in technician workload, and a 48.2% increase in maintenance cost (Zarreh et al., 2019). The findings were consistent with earlier cyber-physical security research showing that compromised industrial control systems can create consequences extending from communication disruption to equipment shutdown, abnormal operating states, emergency intervention, and prolonged restoration. Historical industrial cyber incidents, including attacks on automated production and control infrastructure, demonstrated that manipulation of controller logic or process variables could contribute to abnormal physical operation and equipment stress. Earlier predictive-maintenance research also showed that trustworthy sensor monitoring could increase MTBF and substantially reduce unplanned downtime, which provides an important contrast with the deterioration observed under compromised conditions in this study. In other words, cybersecurity

attacks appeared capable of reversing part of the operational value generated by predictive maintenance. This interpretation was reinforced by the reduction in warning lead time from 17.8 to 10.6 hours. Predictive maintenance depends on identifying deterioration sufficiently early to convert emergency intervention into planned maintenance (Kosmowski et al., 2022). When cyber manipulation delayed, concealed, or falsified degradation signals, maintenance personnel received less reliable information and had less time to intervene before failure. The resulting increase in MTTR was also consistent with earlier ransomware and industrial disruption studies reporting that cyber incidents frequently introduce additional diagnostic, restoration, validation, and system-recovery activities beyond conventional mechanical repair. The particularly large effect for MTBF, with Cohen's d reaching 2.02, suggested that cybersecurity exposure was operationally important rather than merely statistically detectable (Corallo et al., 2020). This study therefore supported an integrated interpretation of equipment reliability in which maintenance performance depended not only on physical degradation and maintenance strategy but also on the trustworthiness, availability, and security of the digital infrastructure responsible for monitoring equipment condition.

The production-level findings demonstrated that cyber-related deterioration in predictive maintenance and equipment reliability propagated into measurable manufacturing losses. Throughput decreased by 18.5%, cycle time increased by 23.9%, production interruptions increased by 121.7%, capacity utilization declined by 12.6%, and OEE decreased from 86.9% to 74.1%. Quality outcomes also deteriorated substantially: the defect rate doubled from 3.4% to 6.8%, rejection increased from 2.2% to 4.5%, scrap increased from 1.9% to 3.7%, and rework increased by 72.2%. First-pass yield declined by 7.3 percentage points and final yield by 4.7 percentage points (Alnajim et al., 2023). These findings corresponded with earlier smart-manufacturing and cyber-physical production studies demonstrating that cybersecurity events can influence more than information systems because connected controllers, sensors, robotic systems, production equipment, and maintenance platforms directly participate in physical manufacturing processes. Earlier research on automated production lines showed that network attacks could interrupt PROFINET communication, disrupt PLC and IIoT coordination, block workpieces, and activate fault-safe operating states. Research on additive manufacturing also demonstrated that manipulated process parameters could introduce defects or reduce material integrity even when production continued. The present findings provided a broader quantitative representation of these effects by connecting cyber exposure simultaneously with throughput, quality, utilization, OEE, and recovery performance (Maglaras, 2022). The doubling of the defect rate was particularly important because it showed that uninterrupted production could not automatically be interpreted as unaffected production. A cyberattack that modified sensor information or predictive-maintenance decisions could allow equipment to continue operating under degraded conditions, transferring the consequence from visible downtime to less immediately visible quality loss. This interpretation was consistent with earlier zero-defect manufacturing and cyber-quality research emphasizing the interdependence of equipment condition, process stability, and product conformity. Recovery time increased from 2.7 to 6.4 hours, further supporting earlier ransomware and manufacturing incident studies reporting prolonged restoration periods after cyber disruption. The results also indicated that productivity and quality losses occurred simultaneously rather than as isolated consequences (Zhukabayeva et al., 2024). Reduced throughput, increased cycle time, greater scrap, lower first-pass yield, and declining OEE collectively represented a broader loss of manufacturing effectiveness. Therefore, the findings supported earlier literature while quantitatively extending it through an integrated representation of cybersecurity, predictive maintenance, equipment reliability, production continuity, and quality performance within the same analytical framework.

Subgroup findings demonstrated that the operational consequences of cybersecurity compromise were heterogeneous and depended strongly on attack type, attack intensity, equipment criticality, architectural interconnection, legacy-system dependence, and cybersecurity-control coverage. Denial-of-service generated the greatest average downtime at 15.9 hours per month, whereas false-data injection produced the largest quality deterioration, increasing the defect rate to 7.6%. High-intensity attacks generated 16.7 hours of monthly downtime compared with 8.4 hours under low-intensity conditions (Stellios et al., 2018). Critical equipment experienced a 17.3-percentage-point reduction in OEE, whereas noncritical equipment experienced a 7.3-point reduction. Systems characterized by

greater legacy-equipment dependence recorded approximately 31.6% more downtime, and highly interconnected production architectures experienced 26.8% greater production loss than more segmented architectures. These findings agreed with earlier industrial cybersecurity research emphasizing that risk cannot be adequately represented through attack frequency alone. The same cyber event can produce markedly different consequences depending on asset criticality, network topology, process coupling, redundancy, controller function, and the availability of alternative production paths. Earlier ICS vulnerability studies identified legacy components, insecure industrial protocols, externally reachable services, and broad network connectivity as important contributors to cyber exposure (Makrakis et al., 2021). The present results extended that evidence by demonstrating how these characteristics were associated with measurable differences in manufacturing outcomes after compromise occurred. The greater OEE loss observed for critical equipment was particularly consistent with the principle that cyber-physical risk depends on both probability and consequence. A compromise affecting a peripheral endpoint may remain locally contained, whereas disruption of a bottleneck machine, central PLC, gateway, or highly connected asset can propagate across multiple stages of production. Similarly, the larger production losses associated with interconnected architectures corresponded with earlier smart-factory research showing that lateral communication pathways can increase the potential scope of compromise. The attack-specific differences also confirmed that cybersecurity incidents should not be treated as a homogeneous exposure. Availability-oriented attacks primarily interrupted communication and production continuity, while integrity-oriented attacks had stronger effects on sensor reliability, prediction, and quality (Arief et al., 2020). This distinction helped explain why aggregated cyberattack counts can conceal important operational differences and supported earlier literature advocating multidimensional cyber-risk measurement based on attack mechanism, intensity, duration, asset importance, and process interdependence.

The inferential findings provided strong evidence that the identified cybersecurity effects were not merely products of the large analytical sample. Standardized effect sizes were substantial across the principal outcomes, including Cohen's d of 1.29 for signal deviation, 1.47 for communication latency, 1.86 for unplanned downtime, 2.02 for MTBF, 1.92 for equipment availability, and 1.91 for OEE (Staddon et al., 2021). Attack type explained 18.7% of variance in signal deviation, while attack intensity explained 21.4% of variance in downtime. Multivariate analysis further showed that manipulated-data proportion was the strongest predictor of predictive degradation, with standardized $\beta = 0.41$, while attack intensity was the strongest positive predictor of downtime at $\beta = 0.39$. The predictive-degradation model explained 61.4% of variance, the downtime model explained 67.8%, and the OEE model explained 63.1%. These explanatory levels were consistent with earlier quantitative cybersecurity studies showing that multidimensional combinations of vulnerability, exploitability, exposure, and system characteristics explain risk more effectively than isolated indicators. Logistic regression strengthened this interpretation: weak authentication increased compromise odds by 2.84 times, unpatched vulnerabilities by 2.47 times, and remote-access exposure by 2.16 times (Garitano et al., 2019). Conversely, network segmentation reduced compromise odds, with OR = 0.46, and active anomaly detection produced OR = 0.52. These patterns aligned with earlier IIoT and ICS research identifying authentication weaknesses, unpatched devices, exposed services, remote connectivity, and insecure protocols as recurring pathways for successful compromise (Hindy et al., 2018). The security-control results were also consistent with prior defense-in-depth research. Stronger protection reduced successful attacks from 43.6% to 18.7%, reduced compromised devices from 24.8% to 9.6%, increased attack detection from 81.4% to 95.2%, and reduced response time from 18.6 to 7.4 minutes. Protected environments also retained 90.6% predictive accuracy during attacks compared with 78.9% in less-protected environments. These findings indicated that security controls were associated not only with lower cyberattack success but also with preservation of maintenance and manufacturing performance (Lee et al., 2018). The evidence therefore supported earlier recommendations for layered security while adding quantitative evidence that integrated protection was related to availability, OEE, downtime, predictive accuracy, and production throughput.

The validation and robustness analyses strengthened confidence in the consistency of the principal findings across alternative analytical conditions. Under clean operation, 10-fold cross-validation produced 95.4% accuracy, 94.8% F1-score, ROC-AUC of 0.976, and PR-AUC of 0.963, while

independent holdout testing produced 94.7% accuracy and 94.0% F1-score. Temporal validation was more conservative, with accuracy declining to 92.8%, indicating that conventional random or stratified validation provided somewhat more optimistic estimates than evaluation across sequential operating periods. This pattern was consistent with earlier industrial machine-learning studies reporting performance deterioration under temporal drift, equipment variation, cross-tool transfer, and independent validation (Nguyen et al., 2024). Cyber-compromised evaluation produced a much larger reduction, with holdout accuracy declining to 83.6%, F1-score to 81.5%, ROC-AUC to 0.884, and PR-AUC to 0.851. These findings corresponded with earlier SWaT, WADI, Edge-IIoTset, TON_IoT, and predictive-maintenance studies in which models often achieved very high within-dataset performance but lower results under cross-dataset, temporal, minority-attack, or adversarial evaluation. Sensitivity analysis also showed that the principal relationships were not dependent on a single modeling specification. The primary downtime model produced adjusted $R^2 = 0.669$, while alternative attack classification, class weighting, robust scaling, and temporal specifications generated values between 0.641 and 0.662. Attack intensity remained positively associated with downtime, cybersecurity-control coverage remained protective, and manipulated-data proportion remained the dominant predictor of predictive degradation across most alternative specifications (Cabitza et al., 2021). Class-imbalance correction increased minority-attack recall from 78.6% to 88.9% while reducing overall accuracy by only 0.8 percentage points, supporting earlier research emphasizing that overall accuracy can obscure weaknesses in rare-attack detection. Across the complete findings, the convergence of large effect sizes, statistically significant associations, multivariate explanatory power, cross-validation, independent holdout testing, temporal validation, and sensitivity analysis indicated a coherent quantitative pattern. Cybersecurity risk was associated with deterioration at successive levels of the smart-manufacturing system: sensor integrity, predictive reliability, maintenance effectiveness, equipment reliability, production continuity, and product quality (Feng et al., 2022). The comparison with earlier studies therefore showed broad consistency while demonstrating a more integrated quantitative relationship between cybersecurity and predictive-maintenance performance than studies examining cyber detection, maintenance prediction, or manufacturing operations separately (Hofman et al., 2021).

CONCLUSION

This study concluded that cybersecurity risk represented a substantial quantitative determinant of the reliability and operational effectiveness of IoT-enabled predictive-maintenance systems in smart manufacturing. The findings established that cyber-compromised conditions affected the complete predictive-maintenance chain, beginning with sensor-data integrity and communication performance and extending to machine-learning prediction, equipment reliability, maintenance efficiency, production continuity, and product quality. Cyber-compromised operation increased missing-data rates from 1.2% to 6.9%, packet loss from 1.6% to 8.7%, and communication latency from 24.6 ms to 71.8 ms, while mean signal deviation increased from 2.3% to 12.9%. These disturbances subsequently reduced predictive performance, with mean classification accuracy declining by approximately 10.9 percentage points and the false-negative rate increasing from 6.8% to 18.9%. Remaining-useful-life estimation was similarly affected, as MAE increased from 7.4 to 13.9 operating cycles and R^2 declined from 0.91 to 0.73. The consequences extended to physical equipment performance, where failure frequency increased by 64.3%, unplanned downtime increased by 124.6%, MTBF decreased by 38.6%, MTTR increased by 56.5%, and equipment availability declined from 96.2% to 89.1%. Manufacturing performance also deteriorated, with throughput decreasing by 18.5%, cycle time increasing by 23.9%, OEE declining from 86.9% to 74.1%, and defect, rejection, scrap, and rework rates increasing substantially. Multivariate analysis confirmed that manipulated-data proportion, attack intensity, compromised-device exposure, weak authentication, unpatched vulnerabilities, remote-access exposure, equipment criticality, and legacy-system dependence represented important cyber-risk factors. Large effect sizes for MTBF, availability, OEE, downtime, latency, and predictive accuracy demonstrated that these relationships were operationally meaningful rather than statistically significant only because of sample size. The robustness analyses further supported the stability of the findings across cross-validation, independent holdout testing, temporal validation, alternative attack classifications, class-imbalance corrections, and model specifications. Stronger cybersecurity controls reduced successful attacks from 43.6% to 18.7%, lowered unplanned downtime by 49.4%, preserved

predictive accuracy at 90.6% during attack conditions, and maintained OEE at 81.9% compared with 69.6% in less-protected environments. Collectively, the quantitative evidence established that the effectiveness of predictive maintenance depended not only on sophisticated sensing and predictive algorithms but also on the security, integrity, availability, and trustworthiness of the interconnected digital infrastructure supporting them. Cybersecurity therefore constituted an integral component of predictive-maintenance reliability and overall smart-manufacturing performance.

RECOMMENDATION

Based on the quantitative findings of this study, smart-manufacturing organizations should integrate cybersecurity directly into the design, implementation, and operation of IoT-enabled predictive-maintenance systems rather than treating security and maintenance as separate technical functions. Priority should be given to protecting the integrity, availability, and authenticity of condition-monitoring data because false-data injection, spoofing, replay, packet manipulation, and communication disruption were associated with substantial deterioration in predictive accuracy and equipment performance. Manufacturing organizations should implement strong device authentication, role-based and least-privilege access control, multifactor authentication for remote connections, encrypted industrial communication, systematic vulnerability assessment, timely security patching, and secure configuration of PLCs, gateways, sensors, edge devices, and maintenance platforms. Network segmentation should separate critical production assets from general enterprise and externally accessible networks, while unnecessary ports, services, and remote-access pathways should be disabled or tightly controlled. Particular attention should be directed toward legacy equipment and highly critical or interconnected assets because these groups demonstrated greater operational vulnerability. Continuous intrusion and anomaly detection should combine network-level indicators with equipment-condition data so that unusual communication behavior and abnormal physical signals can be evaluated simultaneously. Predictive-maintenance models should also undergo cybersecurity-oriented validation in addition to conventional accuracy testing, including false-data injection, replay, spoofing, denial-of-service, temporal validation, independent holdout testing, class-imbalance evaluation, and adversarial stress testing. This requirement is important because models that performed strongly under clean conditions showed meaningful deterioration when compromised observations were introduced. Ensemble methods and comparatively robust architectures should be considered where their validation results demonstrate superior resistance to manipulated inputs. Organizations should establish predefined cyber-incident response procedures that coordinate cybersecurity personnel, maintenance engineers, production managers, and equipment operators to reduce diagnostic delays, MTTR, downtime, and production losses following an attack. Security performance should be monitored through measurable indicators such as attack-detection rate, false-alarm rate, compromised-device proportion, response time, predictive-accuracy deterioration, downtime, MTBF, availability, throughput, OEE, and quality losses. Periodic cybersecurity audits should further evaluate authentication status, patch compliance, network exposure, protocol security, backup integrity, and third-party access. Since stronger security controls in this study were associated with lower attack success, approximately 49.4% lower unplanned downtime, higher predictive accuracy, and a 12.3-percentage-point OEE advantage, manufacturers should prioritize layered defense-in-depth controls as an operational reliability investment. Integrating cybersecurity risk management with predictive maintenance would provide a stronger basis for maintaining trustworthy sensor information, reliable maintenance decisions, equipment availability, production continuity, and overall smart-manufacturing performance.

LIMITATIONS

This study was subject to several limitations that should be considered when interpreting the quantitative relationships among cybersecurity exposure, predictive-maintenance performance, equipment reliability, and smart-manufacturing outcomes. First, the analysis relied on a defined collection of industrial IoT, condition-monitoring, maintenance, network, and cybersecurity observations, meaning that the resulting relationships may not fully represent every manufacturing architecture, equipment configuration, industrial protocol, or cybersecurity environment. Smart-manufacturing systems differ considerably in sensor density, equipment age, network topology, automation level, maintenance strategy, production complexity, and cybersecurity maturity, which

may influence the magnitude of cyber-related deterioration. Second, the investigated cybersecurity conditions concentrated primarily on false-data injection, spoofing, replay, man-in-the-middle, denial-of-service, packet manipulation, communication disruption, and malware-related activity. Other sophisticated attack mechanisms, including coordinated multistage intrusions, supply-chain compromise, advanced persistent threats, model-poisoning attacks, and combinations of physical and cyber manipulation, were not comprehensively represented. Third, class imbalance remained a methodological limitation because normal observations constituted 77.11% of the analytical dataset, whereas cyber-compromised observations represented 22.89%. Although stratified validation, class-sensitive evaluation, and imbalance corrections were applied, uncommon attack categories may still have produced less stable performance estimates. Fourth, predictive models were evaluated using selected statistical, conventional machine-learning, ensemble, and deep-learning architectures; consequently, the findings should not be interpreted as establishing universal performance rankings for all predictive-maintenance algorithms. Model behavior may vary according to hyperparameter configuration, feature engineering, sensor selection, training duration, and equipment-specific degradation characteristics. Fifth, temporal validation produced lower predictive performance than conventional stratified validation, indicating that concept drift, changing operating conditions, equipment aging, and evolving process behavior could affect model stability over extended production periods. Sixth, several operational outcomes, including downtime, maintenance cost, throughput, OEE, defect rates, and recovery time, were influenced by factors beyond cybersecurity, such as operator decisions, production scheduling, environmental conditions, component quality, workload, and maintenance-resource availability. Although multivariate models adjusted for major operational characteristics, residual confounding could not be completely eliminated. Seventh, statistical associations between cybersecurity variables and manufacturing outcomes did not establish causality for every observed relationship, particularly where multiple technical and operational factors occurred simultaneously. Finally, the security-control comparisons represented aggregated protection levels rather than controlled isolation of every individual security mechanism. Therefore, the measured advantages associated with stronger protection should be interpreted as the combined effect of authentication, encryption, segmentation, patching, access control, intrusion detection, and related safeguards rather than the independent causal contribution of any single control. These limitations defined the appropriate boundaries for interpreting the study's quantitative evidence while preserving its relevance to cybersecurity risk assessment in IoT-enabled predictive-maintenance environments.

REFERENCES

- [1]. Abishek, B. A., Kavyashree, T., Jayalakshmi, R., Tharunkumar, S., & Raffik, R. (2023). Collaborative robots and cyber security in industry 5.0. 2023 2nd International conference on advancements in electrical, electronics, communication, computing and automation (ICAECA),
- [2]. Achouch, M., Dimitrova, M., Ziane, K., Sattarpanah Karganroudi, S., Dhouib, R., Ibrahim, H., & Adda, M. (2022). On predictive maintenance in industry 4.0: Overview, models, and challenges. *Applied Sciences*, 12(16), 8081.
- [3]. Adu-Amankwa, K., Attia, A. K., Janardhanan, M. N., & Patel, I. (2019). A predictive maintenance cost model for CNC SMEs in the era of industry 4.0. *The International Journal of Advanced Manufacturing Technology*, 104(9), 3567-3587.
- [4]. Ain, Q. U., Jilani, A. A. A., Butt, N. A., Rehman, S. U., & Alhulayyil, H. A. (2024). Anomaly detection for aviation cyber-physical system: Opportunities and challenges. *IEEE Access*, 12, 175905-175925.
- [5]. Al-Hawamleh, A. M. (2024). Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: evidence from the KSA. *Digital Policy, Regulation and Governance*, 26(3), 317-336.
- [6]. Al-Quayed, F., Ahmad, Z., & Humayun, M. (2024). A situation based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of industry 4.0. *IEEE Access*, 12, 34800-34819.
- [7]. Alattas, K. A., & Mardani, A. (2022). A novel extended Internet of things (IoT) Cybersecurity protection based on adaptive deep learning prediction for industrial manufacturing applications. *Environment, Development and Sustainability*, 24(7), 9464-9480.
- [8]. Albasheer, H., Md Siraj, M., Mubarakali, A., Elsier Tayfour, O., Salih, S., Hamdan, M., Khan, S., Zainal, A., & Kamarudeen, S. (2022). Cyber-attack prediction based on network intrusion detection systems for alert correlation techniques: a survey. *Sensors*, 22(4), 1494.
- [9]. Alghassab, M. (2021). Analyzing the impact of cybersecurity on monitoring and control systems in the energy sector. *Energies*, 15(1), 218.

- [10]. Allodi, L., & Massacci, F. (2017). Security events and vulnerability data for cybersecurity risk estimation. *Risk Analysis*, 37(8), 1606-1627.
- [11]. Almaiah, M. A., Saqr, L. M., Al-Rawwash, L. A., Altellawi, L. A., Al-Ali, R., & Almomani, O. (2024). Classification of cybersecurity threats, vulnerabilities and countermeasures in database systems. *Computers, Materials and Continua*, 81(2), 3189-3220.
- [12]. Alnajim, A. M., Habib, S., Islam, M., Thwin, S. M., & Alotaibi, F. (2023). A comprehensive survey of cybersecurity threats, attacks, and effective countermeasures in industrial internet of things. *Technologies*, 11(6), 161.
- [13]. Alobaidi, A. H., Fazlhashemi, S. S., Khodayar, M., Wang, J., & Khodayar, M. E. (2022). Distribution service restoration with renewable energy sources: A review. *IEEE Transactions on Sustainable Energy*, 14(2), 1151-1168.
- [14]. Alqudhaibi, A., Albarrak, M., Aloheel, A., Jagtap, S., & Salonitis, K. (2023). Predicting cybersecurity threats in critical infrastructure for industry 4.0: a proactive approach based on attacker motivations. *Sensors*, 23(9), 4539.
- [15]. AlSalem, T. S., Almaiah, M. A., & Lutfi, A. (2023). Cybersecurity risk analysis in the IoT: A systematic review. *Electronics*, 12(18), 3958.
- [16]. Ansari, F., Glawar, R., & Nemeth, T. (2019). PriMa: a prescriptive maintenance model for cyber-physical production systems. *International Journal of Computer Integrated Manufacturing*, 32(4-5), 482-503.
- [17]. Ansari, F., Nixdorf, S., & Sihn, W. (2020). Insurability of cyber physical production systems: how does digital twin improve predictability of failure risk? *IFAC-PapersOnLine*, 53(3), 295-300.
- [18]. Arief, R., Khakzad, N., & Pieters, W. (2020). Mitigating cyberattack related domino effects in process plants via ICS segmentation. *Journal of Information Security and Applications*, 51, 102450.
- [19]. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), 1333.
- [20]. Ayvaz, S., & Alpay, K. (2021). Predictive maintenance system for production lines in manufacturing: A machine learning approach using IoT data in real-time. *Expert systems with applications*, 173, 114598.
- [21]. Bhat, S. M., & Venkitaraman, A. (2024). Strategic integration of predictive maintenance plans to improve operational efficiency of smart grids. 2024 IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS),
- [22]. Bouramdane, A.-A. (2023). Cyberattacks in smart grids: challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. *Journal of Cybersecurity and Privacy*, 3(4), 662-705.
- [23]. Bousdekis, A., Apostolou, D., & Mentzas, G. (2019). Predictive maintenance in the 4th industrial revolution: Benefits, business opportunities, and managerial implications. *IEEE engineering management review*, 48(1), 57-62.
- [24]. Cabitza, F., Campagner, A., Soares, F., de Guadiana-Romualdo, L. G., Challa, F., Sulejmani, A., Seghezzi, M., & Carobene, A. (2021). The importance of being external. methodological insights for the external validation of machine learning models in medicine. *Computer methods and programs in biomedicine*, 208, 106288.
- [25]. Carrasco, J., López, D., Aguilera-Martos, I., García-Gil, D., Markova, I., Garcia-Barzana, M., Arias-Rodil, M., Luengo, J., & Herrera, F. (2021). Anomaly detection in predictive maintenance: A new evaluation framework for temporal unsupervised anomaly detection algorithms. *Neurocomputing*, 462, 440-452.
- [26]. Chang, X., Xu, X., Qiu, B., Wei, M., Yan, X., & Liu, J. (2024). Predicting steady degradation in ship power system: A deep learning approach based on comprehensive monitoring parameters. *IET Intelligent Transport Systems*, 18(12), 2375-2396.
- [27]. Chenaru, O., Mocanu, S., Dobrescu, R., & Nicolae, M. (2022). Enhancing antifragile performance of manufacturing systems through predictive maintenance. *Applied Sciences*, 12(23), 11958.
- [28]. Cheng, X., Chaw, J. K., Goh, K. M., Ting, T. T., Sahrani, S., Ahmad, M. N., Abdul Kadir, R., & Ang, M. C. (2022). Systematic literature review on visual analytics of predictive maintenance in the manufacturing industry. *Sensors*, 22(17), 6321.
- [29]. Cinar, E., Kalay, S., & Saricicek, I. (2022). A predictive maintenance system design and implementation for intelligent manufacturing. *Machines*, 10(11), 1006.
- [30]. Çınar, Z. M., Abdussalam Nuhu, A., Zeeshan, Q., Korhan, O., Asmael, M., & Safaei, B. (2020). Machine learning in predictive maintenance towards sustainable smart manufacturing in industry 4.0. *Sustainability*, 12(19), 8211.
- [31]. Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry*, 114, 103165.
- [32]. Farooq, J., & Zhu, Q. (2026). Cyber resilience in next-generation networks: threat landscape, theoretical foundations, and design paradigms. *Foundations and Trends in Networking*, 17(1-2), 1-145.
- [33]. Fasuludeen Kunju, F. K., Naveed, N., Anwar, M. N., & Ul Haq, M. I. (2022). Production and maintenance in industries: impact of industry 4.0. *Industrial Robot: the international journal of robotics research and application*, 49(3), 461-475.

- [34]. Feng, L., Liu, Z., Li, C., Li, Z., Lou, X., Shao, L., Wang, Y., Huang, Y., Chen, H., & Pang, X. (2022). Development and validation of a radiopathomics model to predict pathological complete response to neoadjuvant chemoradiotherapy in locally advanced rectal cancer: a multicentre observational study. *The Lancet Digital Health*, 4(1), e8-e17.
- [35]. Flor-Unda, O., Simbaña, F., Larriva-Novo, X., Acuña, Á., Tipán, R., & Acosta-Vargas, P. (2023). A comprehensive analysis of the worst cybersecurity vulnerabilities in latin america. *Informatics*,
- [36]. Fong, S., & Narasimhan, S. (2021). An unsupervised Bayesian OC-SVM approach for early degradation detection, thresholding, and fault prediction in machinery monitoring. *IEEE Transactions on Instrumentation and Measurement*, 71, 1-11.
- [37]. Franke, U. (2020). IT service outage cost: case study and implications for cyber insurance: U. Franke. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 45(4), 760-784.
- [38]. Garitano, I., Iturbe, M., Ezpeleta, E., & Zurutuza, U. (2019). Who's there? Evaluating data source integrity and veracity in iiot using multivariate statistical process control. In *Security and privacy trends in the industrial Internet of things* (pp. 181-198). Springer.
- [39]. Gungor, O., Rosing, T., & Aksanli, B. (2022). Stewart: Stacking ensemble for white-box adversarial attacks towards more resilient data-driven predictive maintenance. *Computers in Industry*, 140, 103660.
- [40]. Hindy, H., Brosset, D., Bayne, E., Seeam, A., & Bellekens, X. (2018). Improving SIEM for critical SCADA water infrastructures using machine learning. *International Workshop on Security and Privacy Requirements Engineering*,
- [41]. Hofman, J. M., Watts, D. J., Athey, S., Garip, F., Griffiths, T. L., Kleinberg, J., Margetts, H., Mullainathan, S., Salganik, M. J., & Vazire, S. (2021). Integrating explanation and prediction in computational social science. *Nature*, 595(7866), 181-188.
- [42]. Hu, Y.-y., Zhao, C.-h., & Ke, Z.-w. (2021). Machine learning based online fault prognostics for nonstationary industrial process via degradation feature extraction and temporal smoothness analysis. *Journal of Central South University*, 28(12), 3838-3855.
- [43]. Huang, B., Li, Y., Zhan, F., Sun, Q., & Zhang, H. (2021). A distributed robust economic dispatch strategy for integrated energy system considering cyber-attacks. *IEEE Transactions on Industrial Informatics*, 18(2), 880-890.
- [44]. Husák, M., Komárková, J., Bou-Harb, E., & Čeleda, P. (2018). Survey of attack projection, prediction, and forecasting in cyber security. *IEEE Communications Surveys & Tutorials*, 21(1), 640-660.
- [45]. Jammal, M., Hawilo, H., Kanso, A., & Shami, A. (2016). Mitigating the risk of cloud services downtime using live migration and high availability-aware placement. 2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom),
- [46]. Jaramillo-Alcazar, A., Govea, J., & Villegas-Ch, W. (2023). Anomaly detection in a smart industrial machinery plant using IoT and machine learning. *Sensors*, 23(19), 8286.
- [47]. Jazairy, A., Brho, M., Manuj, I., & Goldsby, T. J. (2024). Cyber risk management strategies and integration: toward supply chain cyber resilience and robustness. *International Journal of Physical Distribution & Logistics Management*, 54(11), 1-29.
- [48]. Jbair, M., Ahmad, B., Maple, C., & Harrison, R. (2022). Threat modelling for industrial cyber physical systems in the era of smart manufacturing. *Computers in Industry*, 137, 103611.
- [49]. Jiang, Y., Wang, W., Ding, J., Lu, X., & Jing, Y. (2024). Leveraging digital twin technology for enhanced cybersecurity in Cyber-Physical production systems. *Future Internet*, 16(4), 134.
- [50]. Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity risk assessment in smart city infrastructures. *Machines*, 9(4), 78.
- [51]. Karippur, N. K., Balaramachandran, P. R., & John, E. (2024). Data driven predictive maintenance for large-scale asset-heavy process industries in Singapore. *Journal of Manufacturing Technology Management*, 35(3), 544-567.
- [52]. Keleko, A. T., Kamsu-Foguem, B., Ngouna, R. H., & Tongne, A. (2022). Artificial intelligence and real-time predictive maintenance in industry 4.0: a bibliometric analysis. *AI and Ethics*, 2(4), 553-577.
- [53]. Khandker, S., Turtiainen, H., Costin, A., & Hämäläinen, T. (2022). Cybersecurity attacks on software logic and error handling within AIS implementations: A systematic testing of resilience. *IEEE Access*, 10, 29493-29505.
- [54]. Kim, H.-m., & Lee, K.-h. (2022). IIoT malware detection using edge computing and deep learning for cybersecurity in smart factories. *Applied Sciences*, 12(15), 7679.
- [55]. Kosmowski, K. T., Piesik, E., Piesik, J., & Śliwiński, M. (2022). Integrated functional safety and cybersecurity evaluation in a framework for business continuity management. *Energies*, 15(10), 3610.
- [56]. Kuchar, K., & Fajdiak, R. (2024). Anomaly detection in industrial networks: Current state, classification, and key challenges. *IEEE Sensors Journal*, 25(3), 5031-5043.
- [57]. Kure, H. I., Islam, S., Ghazanfar, M., Raza, A., & Pasha, M. (2022). Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system. *Neural Computing and Applications*, 34(1), 493-514.

- [58]. Lee, C., Yim, H. B., & Seong, P. H. (2018). Development of a quantitative method for evaluating the efficacy of cyber security controls in NPPs based on intrusion tolerant concept. *Annals of Nuclear Energy*, 112, 646-654.
- [59]. Lee, J., Singh, J., Azamfar, M., & Pandhare, V. (2020). Industrial AI and predictive analytics for smart manufacturing systems. In *Smart manufacturing* (pp. 213-244). Elsevier.
- [60]. Lee, S. M., Lee, D., & Kim, Y. S. (2019). The quality management ecosystem for predictive maintenance in the Industry 4.0 era. *International Journal of Quality Innovation*, 5(1), 4.
- [61]. Lin, J., Zhang, Y., Cao, J., Deng, Z., & Tan, D. (2024). Research on Gradual Fault Prediction of Current Transformers Based on Machine Learning Algorithms. 2024 IEEE 6th International Conference on Civil Aviation Safety and Information Technology (ICCASIT),
- [62]. Lindström, J., Larsson, H., Jonsson, M., & Lejon, E. (2017). Towards intelligent and sustainable production: combining and integrating online predictive maintenance and continuous quality control. *Procedia CIRP*, 63, 443-448.
- [63]. Liu, Y., Hu, S., Wu, J., Shi, Y., Jin, Y., Hu, Y., & Li, X. (2016). Smart home cybersecurity considering the integration of renewable energy. In *Smart Cities and Homes* (pp. 173-189). Elsevier.
- [64]. Liu, Y., Yu, W., Rahayu, W., & Dillon, T. (2023). An evaluative study on IoT ecosystem for smart predictive maintenance (IoT-SPM) in manufacturing: Multiview requirements and data quality. *IEEE Internet of Things Journal*, 10(13), 11160-11184.
- [65]. López, D., Aguilera-Martos, I., García-Barzana, M., Herrera, F., García-Gil, D., & Luengo, J. (2023). Fusing anomaly detection with false positive mitigation methodology for predictive maintenance under multivariate time series. *Information Fusion*, 100, 101957.
- [66]. Maglaras, L. (2022). From mean time to failure to mean time to attack/compromise: incorporating reliability into cybersecurity. In (Vol. 11, pp. 159): MDPI.
- [67]. Mahesh, P., Tiwari, A., Jin, C., Kumar, P. R., Reddy, A. N., Bukkapatnam, S. T., Gupta, N., & Karri, R. (2020). A survey of cybersecurity of digital manufacturing. *Proceedings of the IEEE*, 109(4), 495-516.
- [68]. Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C., & Benjamin, J. (2021). Industrial and critical infrastructure security: Technical analysis of real-life security incidents. *IEEE Access*, 9, 165295-165325.
- [69]. Mathew, D., Brintha, N., & Jappes, J. W. (2023). Artificial intelligence powered automation for industry 4.0. In *New horizons for Industry 4.0 in modern business* (pp. 1-28). Springer.
- [70]. Möller, D. P. (2023). Cybersecurity in digital transformation. In *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices* (pp. 1-70). Springer.
- [71]. Mullet, V., Sondi, P., & Ramat, E. (2021). A review of cybersecurity guidelines for manufacturing factories in industry 4.0. *IEEE Access*, 9, 23235-23263.
- [72]. Nguyen, T. T., Tran, T. N. H., Do, T. H. M., Dinh, T. K. L., Nguyen, T. U. N., & Dang, T. M. K. (2024). Digital literacy, online security behaviors and E-payment intention. *Journal of Open Innovation: Technology, Market, and Complexity*, 10(2), 100292.
- [73]. PACME, T. R. S. W. G., Papic, M., Agarwal, S., Allan, R. N., Billinton, R., Dent, C. J., Ekisheva, S., Gent, D., Jiang, K., & Li, W. (2016). Research on common-mode and dependent (CMD) outage events in power systems: A review. *IEEE Transactions on Power Systems*, 32(2), 1528-1536.
- [74]. Pech, M., Vrchota, J., & Bednář, J. (2021). Predictive maintenance and intelligent sensors in smart factory. *Sensors*, 21(4), 1470.
- [75]. Peng, C., Xu, M., Xu, S., & Hu, T. (2018). Modeling multivariate cybersecurity risks. *Journal of Applied Statistics*, 45(15), 2718-2740.
- [76]. Peng, Z., Wang, Q., Liu, Z., & He, R. (2024). Remaining useful life prediction for aircraft engines under high-pressure compressor degradation faults based on FC-AMSLSTM. *Aerospace*, 11(4), 293.
- [77]. Pochmara, J., & Świetlicka, A. (2024). Cybersecurity of industrial systems – A 2023 report. *Electronics*, 13(7), 1191.
- [78]. Qasim, M., Khan, M., Mehmood, W., Sobieczky, F., Pichler, M., & Moser, B. (2022). A comparative analysis of anomaly detection methods for predictive maintenance in SME. International Conference on Database and Expert Systems Applications,
- [79]. Radanliev, P., De Roure, D., Page, K., Nurse, J. R., Mantilla Montalvo, R., Santos, O., Maddox, L. T., & Burnap, P. (2020). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity*, 3(1), 13.
- [80]. Rahman, M. H., Wuest, T., & Shafae, M. (2023). Manufacturing cybersecurity threat attributes and countermeasures: Review, meta-taxonomy, and use cases of cyberattack taxonomies. *Journal of Manufacturing Systems*, 68, 196-208.
- [81]. Razaque, A., Amsaad, F., Khan, M. J., Hariri, S., Chen, S., Siting, C., & Ji, X. (2019). Survey: Cybersecurity vulnerabilities, attacks and solutions in the medical domain. *IEEE Access*, 7, 168774-168797.
- [82]. Riccio, C., Menanno, M., Zennaro, I., & Savino, M. M. (2024). A new methodological framework for optimizing predictive maintenance using machine learning combined with product quality parameters. *Machines*, 12(7), 443.

- [83]. Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors*, 23(8), 4060.
- [84]. Rosati, P., Gogolin, F., & Lynn, T. (2019). Audit firm assessments of cyber-security risk: evidence from audit fees and SEC comment letters. *The International Journal of Accounting*, 54(03), 1950013.
- [85]. Ryalat, M., ElMoaqet, H., & AlFaouri, M. (2023). Design of a smart factory based on cyber-physical systems and Internet of Things towards Industry 4.0. *Applied Sciences*, 13(4), 2156.
- [86]. Shackelford, S. J. (2019). Smart factories, dumb policy? Managing cybersecurity and data privacy risks in the industrial internet of things. *Minn. J. Sci. & Tech.*, 21, 1.
- [87]. Shcherbakov, M. V., Glotov, A. V., & Cheremisinov, S. V. (2019). Proactive and predictive maintenance of cyber-physical systems. In *Cyber-Physical Systems: Advances in Design & Modelling* (pp. 263-278). Springer.
- [88]. Sheth, A., & Kusiak, A. (2022). Resiliency of smart manufacturing enterprises via information integration. *Journal of Industrial Information Integration*, 28, 100370.
- [89]. Singh, B., Dutta, P. K., Lal, S., Arora, M. K., & El-kenawy, E.-S. M. (2024). Beyond CrowdStrike: a technical analysis of SHIELD's cyber resilience platform in mitigating large-scale outages. 8th IET Smart Cities Symposium (SCS 2024),
- [90]. Singh, V., Sahai, A., & Kumar, P. (2024). Hybrid Machine Learning Approaches for Software Fault Prediction: A Systematic Review of Current Practices and Future Prospects. 2024 IEEE 11th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON),
- [91]. Singhal, A., & Ou, X. (2017). Security risk analysis of enterprise networks using probabilistic attack graphs. In *Network security metrics* (pp. 53-73). Springer.
- [92]. Soori, M., Arezoo, B., & Dastres, R. (2023). Internet of things for smart factories in industry 4.0, a review. *Internet of Things and Cyber-Physical Systems*, 3, 192-204.
- [93]. Staddon, E., Loscri, V., & Mitton, N. (2021). Attack categorisation for IoT applications in critical infrastructures, a survey. *Applied Sciences*, 11(16), 7228.
- [94]. Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials*, 20(4), 3453-3495.
- [95]. Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L. Y., & Xiang, Y. (2018). Data-driven cybersecurity incident prediction: A survey. *IEEE Communications Surveys & Tutorials*, 21(2), 1744-1772.
- [96]. Tanuska, P., Spendla, L., Kebisek, M., Duris, R., & Stremy, M. (2021). Smart anomaly detection and prediction for assembly process maintenance in compliance with industry 4.0. *Sensors*, 21(7), 2376.
- [97]. Teh, H. Y., Kempa-Liehr, A. W., & Wang, K. I.-K. (2020). Sensor data quality: A systematic review. *Journal of Big Data*, 7(1), 11.
- [98]. Tyagi, A. K., Kumari, S., & Richa. (2024). Artificial Intelligence-Based Cyber Security and Digital Forensics: A Review. *Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing*, 391-419.
- [99]. Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature: Md. H. Uddin et al. *Risk Management*, 22(4), 239-309.
- [100]. Visconti, P., Rausa, G., Del-Valle-Soto, C., Velázquez, R., Cafagna, D., & De Fazio, R. (2024). Machine learning and IoT-based solutions in industrial applications for smart manufacturing: A critical review. *Future Internet*, 16(11), 394.
- [101]. Wai, E., & Lee, C. (2023). Seamless industry 4.0 integration: A multilayered cyber-security framework for resilient scada deployments in cpps. *Applied Sciences*, 13(21), 12008.
- [102]. Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & security*, 147, 104051.
- [103]. Wei, S., Li, L., Chen, G., Blasch, E., Chang, K.-C., Clemons, T. M., & Pham, K. (2023). ROSIS: Resilience oriented security inspection system against false data injection attacks. 2023 IEEE Aerospace Conference,
- [104]. Woods, D. W., & Böhme, R. (2021). SoK: Quantifying cyber risk. 2021 IEEE Symposium on Security and Privacy (SP),
- [105]. Woods, D. W., & Seymour, S. (2023). Evidence-based cybersecurity policy? A meta-review of security control effectiveness. *Journal of Cyber Policy*, 8(3), 365-383.
- [106]. Wu, H., Liu, J., Liu, J., Cui, M., Liu, X., & Gao, H. (2019). Power grid reliability evaluation considering wind farm cyber security and ramping events. *Applied Sciences*, 9(15), 3003.
- [107]. Yamashita, K., Ten, C.-W., Rho, Y., Wang, L., Wei, W., & Ginter, A. (2020). Measuring systemic risk of switching attacks based on cybersecurity technologies in substations. *IEEE Transactions on Power Systems*, 35(6), 4206-4219.
- [108]. Young, C. S. (2016). *Information security science: measuring the vulnerability to data compromises*. Elsevier.
- [109]. Yu, W., Dillon, T., Mostafa, F., Rahayu, W., & Liu, Y. (2019). A global manufacturing big data ecosystem for fault detection in predictive maintenance. *IEEE Transactions on Industrial Informatics*, 16(1), 183-192.

- [110]. Yu, W., Griffith, D., Ge, L., Bhattarai, S., & Golmie, N. (2015). An integrated detection system against false data injection attacks in the smart grid. *Security and Communication Networks*, 8(2), 91-109.
- [111]. Zarreh, A., Wan, H., Lee, Y., Saygin, C., & Al Janahi, R. (2019). Cybersecurity concerns for total productive maintenance in smart manufacturing systems. *Procedia Manufacturing*, 38, 532-539.
- [112]. Zhang, F., Hines, J. W., & Coble, J. B. (2020). A robust cybersecurity solution platform architecture for digital instrumentation and control systems in nuclear power facilities. *Nuclear Technology*, 206(7), 939-950.
- [113]. Zhang, J., Blum, R. S., & Poor, H. V. (2018). Approaches to secure inference in the Internet of Things: Performance bounds, algorithms, and effective attacks on IoT sensor networks. *IEEE Signal Processing Magazine*, 35(5), 50-63.
- [114]. Zhang, Q., Zhou, C., Tian, Y.-C., Xiong, N., Qin, Y., & Hu, B. (2017). A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems. *IEEE Transactions on Industrial Informatics*, 14(6), 2497-2506.
- [115]. Zhang, Y., Wang, L., Xiang, Y., & Ten, C.-W. (2015). Power system reliability evaluation with SCADA cybersecurity considerations. *IEEE Transactions on Smart Grid*, 6(4), 1707-1721.
- [116]. Zhukabayeva, T., Pervez, A., Mardenov, Y., Othman, M., Karabayev, N., & Ahmad, Z. (2024). A traffic analysis and node categorization-aware machine learning-integrated framework for cybersecurity intrusion detection and prevention of WSNs in smart grids. *IEEE Access*, 12, 91715-91733.