Vennila P, 2025, 13:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Techniques to Enhance Production Quality, Safety, and Sustainability through the Use of Machine Learning in IIOT and Smart Production

Research Scholar Vennila P, Associate Professor Maniraj V
Department of Computer Science, A.V.V.M Sri Pushpam College, Poondi, Thanjavur

Abstract- Production has been transformed by Industrial IoT (IIoT), which makes data faster and more granularly available to stakeholders at various levels. The goal of evaluating the data gathered in smart manufacturing is often to increase overall efficiency, which entails raising output while reducing waste and energy consumption. Additionally, the IIoT's connectivity rise necessitates extra consideration for higher safety and security standards. Smart production has been impacted by the recent expansion of machine learning (ML) capabilities in a number of ways. The application of various machine learning approaches for IIoT, smart production, and maintenance is summarized in the current study, with a focus on safety, security, asset localization, quality assurance, and sustainability. Each domain—security and safety, asset localization, quality control, and maintenance—has its own chapter, with a final table on common ML techniques and the relevant references. This is because the paper's approach is to give a thorough overview of ML methods from an application point of view. Lessons learned are outlined in the study along with research gaps and future work areas.

Keywords- machine learning; industry 4.0; industrial IoT; safety; security; asset localization; quality control; proactive maintenance; fault detection; prognostics

I. INTRODUCTION

Boosting efficiency (i.e., by boosting output and decreasing scrap, waste, and energy usage), prolonging system lifetime, and improving safety and security have been the fundamental drivers of industrial data processing for decades. Sustainability has emerged as yet another key issue in contemporary business.

The IIoT (Industrial Internet of Things) research and innovation field started to flourish as individuals realized how important it was to collect data in a dispersed manner and handle large amounts of data in many industrial fields. While the Industry 4.0 program supported its business push, its applications were expanded from the highly overlapping Cyber-Physical Systems (CPS) sector. Domain specialists use a layered approach, but there is no generic, de-facto architecture for IIoT systems. Three, four, or five levels can be recognized since the reasons for dividing them could range from communication kinds owing to infrastructure needs to the viewpoint of ecosystem stakeholders. A tiered architectural picture is shown in Figure 1, demonstrating the distinct technological divisions between the tiers. It also indicates the different security approaches at the different layers [1].

Even while machine learning is utilized in many IIoT application areas, it is only widely applied to a

limited number of target areas (see Figure 2). Processing industrial data serves a variety of purposes, depending on the application area. To just a few, these consist of classification, clustering, anomaly detection, prediction, optimization, and decision support. We require physical resources for data processing, which are now mostly available due to the growth in GPU manufacture, and data, which are often available for industrial participants if IIoT-based data gathering is in place, in order to get the intended results. We may now employ ML (Machine Learning) techniques to get better outcomes than ever before in the aforementioned domains because data and resources are now readily available.

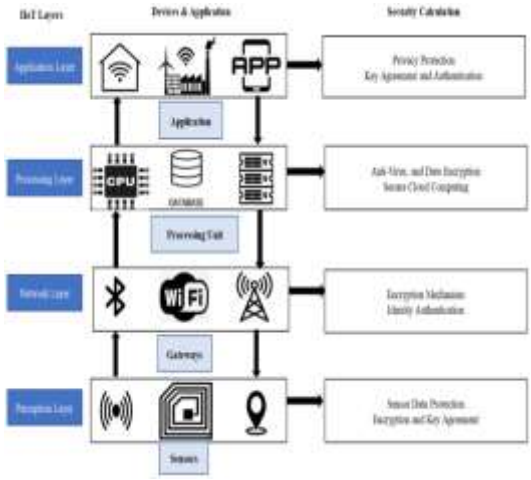

Figure 1. The architectural layers of IIoT systems [1].

Figure 2 shows the stages of production that are normally included in the manufacturing process. Even while machine learning can be used in every aspect of production, only a tiny percentage of them make extensive use of the techniques (bold typeset).

Naturally, textbooks are the first place to look for information on these techniques. Numerous excellent books are available on machine learning in general [2–4] and on contemporary tools for their use [5–8]. Survey studies on the application of machine learning in the sector are also available. An overview of the next phase of machine learning in smart manufacturing is given by the authors of [9]. A survey on the specific subject of using machine learning (ML) to address flaws in the context of industry 4.0 can be found in [10]. The authors of a study on machine learning multi-agent systems [11] only discuss how these systems are used in the oil and gas sector. With reference to various industry 4.0 levels, [12] concentrates on machine learning techniques used in production control and planning. In a similar vein, [13] offers an overview of ML techniques for industrial process optimization.
We can locate other specialized publications that examine ML for production energy efficiency [15] or summarize ML techniques for smart production generally [14] to compare with the subject of our current article. An extensive review of prognostic techniques in the context of Industry 4.0 is given by the authors of [16]. The writers of [17] concentrate on predictive maintenance and sustainability. A focused survey of safety and reliability engineering is given by the authors of [18]. Additionally, a survey of ML support for safety assurance can be found in [19].

This paper's primary contribution is that it offers an organized state-of-the-art perspective of the field, complete with detailed information on the current level of knowledge in this sector and well-structured comparison tables. Despite the fact that industrial innovation is very interested in this field, there isn't yet an organized, application-focused overview of machine learning techniques in the Industrial Internet of Things (IIoT) space. Specifically, there isn't a comprehensive overview of production quality, safety, sustainability, and maintenance available. Therefore, by offering a thorough overview of applicable machine learning techniques within the aforementioned disciplines, the current study aims to close this gap. In order to give readers a better grasp of the methods employed for particular common tasks, the article

also organizes these applications according to their primary goals.

The paper is organized as follows. Every chapter discusses a particular application area and offers a broad synopsis of the problems and potential fixes. The associated machine learning techniques are accompanied by application examples. Each chapter includes summary tables and a section on lessons learned to draw attention to the key ideas. As a result, Section 2 concentrates on security and safety concerns and solutions, Section 3 highlights the key developments in asset localization, Section 4 offers a summary of quality control techniques and application use cases, Section 5 addresses sustainability and maintenance, and Section 6 wraps up the work.

II. SAFETY AND SECURITY

Operational technology (OT) and information technology (IT) combine in the field of industrial IoT, which raises concerns about security and safety. Without a question, one of the most crucial elements of IIoT is security and safety. To emphasize this, the Industry IoT Consortium summarized all of its experience and knowledge in a technical report [20] about security concerns in IIoT systems.

Achieving trustworthiness—defined as "the degree of confidence one has that the system performs as expected in respect to all the key system characteristics in the face of environmental disruptions, human errors, system faults, and attacks"—is the primary objective of IIoT systems. When fending off internal or external dangers, Figure 3 illustrates the essential features of a reliable system. The salient features are [21]:

Protection of the system from unwanted or unauthorized access, alteration, or destruction is guaranteed by security.

Privacy: By determining how information can be shared both inside and outside of an organization, privacy gives businesses authority over the gathering, handling, and archiving of their data.

Reliability: Reliability ensures that the system will function error-free and continuously throughout the allotted period. Reliability and availability are related, but availability also accounts for scheduled operation pauses.

Safety: System safety makes ensuring that there is no intolerable risk to people, property, or the environment while the system is operating.

Resilience—System resilience offers a means of quickly avoiding, absorbing, and recovering from shifting unfavorable circumstances. The capacity to endure and bounce back from intentional assaults and mishaps is a component of resilience or naturally occurring threats or incidents.

Figure 3. Trustworthiness of an IIoT System as specified by the Industrial IoT Consortium [20]. The key characteristics of the trustworthy IoT system are security, privacy, reliability, safety and resilience.

Although proper system design, implementation, and deployment are necessary for a secure and safe industrial IoT system, machine learning-based solutions are frequently utilized to provide extra security and safety layers. While machine learning-based solutions are also offered in [1,22], there are a few survey studies that examine the security concerns of IIoT systems, primarily concentrating on general security issues. A layer-by-layer examination of security problems and fixes, particularly in 5G-based IIoT systems, is presented in [23]. A layer-wise method is also used in ref. [24], which offers a thorough summary of the security features of edge and fog computing in addition to information on common security concerns.

Although all of the essential elements of reliable IIoT systems are significant, the majority of machine learning-based solutions focus on security—the defense against unwanted and illegal access. Intrusion detection is one of its common application areas, where the learning approach looks for unauthorized system access using arbitrary features, such as system logs, monitoring services, etc. The majority of works accomplish this by detecting intrusion from features using supervised learning approaches (i.e., classification), such as k-nearest neighbor (kNN) [25], support vector machines (SVM) [26–28], decision trees [29], Bayes networks [30–32], random forests [33], and neural networks [34–36]. There are fuzzy approaches and association-based methods in addition to standard classification solutions [37].

Hidden Markov models (HMM) have also been proposed in the past [38, 39]. The topic of intrusion detection is so broad that it is the exclusive focus of a few thorough survey publications [40, 41]. Although intrusion detection frequently uses classification, intrusion can be viewed as an anomaly that targets authorized users. The survey in [42] summarizes instances of intrusion detection in the IIoT domain and examines the application areas of outlier detection in IoT systems. In addition to intrusion detection, machine learning in IIoT systems can be used to detect anomalies at a broader level by identifying outliers or anomalous system behavior using supervised or unsupervised techniques [43–45].

Machine learning approaches can support authentication, which is closely related to intrusion detection. Although machine learning algorithms by themselves are rarely employed for authentication, they can offer an extra degree of protection over traditional authentication methods. Using ensemble learning techniques, network traffic analysis-based authentication is carried out in [46]. As demonstrated in [47], WiFi-capable IoT devices can be authenticated by triggering routine tasks. Man-in-the-Middle attacks can be identified during authentication by combining Bregman divergence with the k-nearest neighbor algorithm [48]. Additionally, a high accuracy in identifying WiFi impersonation attacks was attained by the use of stacked autoencoders (SAE) and k-means clustering [49].

Blockchains are used for a variety of applications, such as distributed secure databases, and are crucial to the security of IIoT systems. A deep learning technique taught via transfer learning is frequently combined with user authentication to access blockchain [50,51]. It's interesting to note that authentication can be done just in the physical layer.

Ref [25] suggests a software-defined radio (SDR) approach for RF fingerprinting-based IoT device authentication. The study examines several machine learning techniques, including kNN, SVM, and decision trees, all of which have been shown to be sufficiently accurate to carry out authentication using only RF data.

Although encryption (using cryptography) largely ensures privacy, IIoT systems present some challenges. Although a few machine learning techniques have been used (for example, in authentication and intrusion detection), large datasets are needed for deep neural network training. In addition to publicly available datasets, networks must frequently be trained using distributed real datasets; yet, this may lead to "privacy leaking." Some research and solutions, such as differential privacy and federated learning [53] or privacy-preserving asynchronous deep learning systems (DeepPAR [52]), suggest ways to prevent privacy leakage. A comprehensive evaluation of alternative techniques for protecting IIoT privacy through differential privacy may be found in [54].

An essential component of a reliable IIoT system is data integrity. Data integrity is the state in which information is correct and consistent throughout its lifecycle. False data injection (FDI) is one of the most common attacks against data integrity; nonetheless, data integrity encompasses all potential combinations of data change, data injection, and even data relation disintegrity. Data integrity check algorithms typically learn the

distribution of legitimate data and detect low-probability outlier samples. In [55], where a gas pipeline system remote terminal unit (RTU) was observed, data and the command injection were examined. Six machine learning methods (such as SVM, random forests, etc.) were used to precisely identify the injection attacks.

Ref. [56] suggests a technique for identifying data change in programmable logic controllers (PLC) using k-means clustering. In order to detect data injection threats in smart grids, deep belief networks and limited Boltzmann machines were used in [57]. In order to prevent fake data attacks, autoencoders were trained using smart sensor data from a sophisticated hydraulic IIoT system in [58].

High availability, or the system's readiness to offer services to users, is a prerequisite for a dependable, trustworthy IIoT system. However, a popular attack against IIoT devices is known as a denial-of-service (DoS) attack, which stops the device from providing services and causes it to become momentarily unavailable by imposing a massive workload. Distributed DoS (DDoS) attacks are a typical variant of this assault that can come from multiple sources.
Ref. [59] suggests a hybrid deep learning framework (deep belief networks, auto encoders, etc.) that uses a few network and log features to categorize the kind of attack that is reaching the device, such as DoS attacks, among others. In [60], a reinforcement learning method was put up to detect DDoS attacks using the game-theory approach. Traffic delays and DDoS attacks can also be successfully predicted using Bayesian networks; in [61], for instance, the method was motivated by the economics concept of portfolio theory.

Offload security is a unique security concern for industrial IoT devices. Edge computing, also known as fog computing, is the process of offloading various computations to edge devices in order to use machine learning methods in IIoT systems. Because tasks that are offloaded to the cloud or edge are susceptible to security breaches by hostile devices, this offloading creates new types of security risks. A common solution implements a double-dueling Q-network and avoids the security issues of compute offloading by utilizing blockchains and the reinforcement learning technique [62]. Other solutions, like the one in [63,64], usually make use of reinforcement learning techniques.

Datasets

A few publicly accessible datasets are provided for the purpose of training and validating machine learning algorithms related to IIoT security. By examining these datasets, one can gain a better knowledge of the machine learning algorithms and uncover the potential characteristics and results of each one. These datasets are typically used to train the previously described studies.

The "The Third International Knowledge Discovery and Data Mining Tools Competition" KDD-99 dataset is among the most well-known intrusion detection datasets [65]. The DARPA experiment was used to build the dataset, which includes 4 GB of network traffic over seven weeks with attacks falling into four categories (DOS, R2L, U2R, and probing).

A variety of cybersecurity datasets are available from the Canadian Institute for Cybersecurity. The CSE-CIC-IDS2018 dataset [66] includes 30 servers and 420 computers in an infrastructure with seven distinct attack scenarios. The institute also offers a cutting-edge dataset for DDoS attack detection [67].

Additional Intrusion Detection and Privacy Attack Datasets are Available In [68,69].

For a variety of security uses, such as malware and intrusion detection, the University of Arizona offers datasets [70].

Opponents of Security Based on Machine Learning

Some critiques of IIoT security and training datasets were presented in Zolanvari's study [71]. For the training and validation stages, the majority of machine learning-based IIoT security algorithms and solutions (such as intrusion detection and DDoS protection) require some data. For instance, for machine learning algorithms to work well, network traffic datasets need features that have

been carefully chosen. The method won't work if the features don't change in response to the attack. Furthermore, sensor data in IIoT applications is typically collected over a long period of time using varying sample rates, producing large dimensional datasets. Training and detection procedures will be significantly delayed if raw data like this is used. Additionally, confidentiality and privacy regulations make it difficult to obtain actual IIoT data from businesses; as a result, all of the solutions that are offered are usually trained on the same publicly accessible datasets.

Remarkably, the primary issue with the datasets that are now accessible is that there are comparatively few actual attacks in comparison to typical behavior; the extremely unbalanced datasets make it challenging to efficiently train learning algorithms.

Safety and Security Summary

In IIoT security, machine learning is frequently employed as an extra security layer to offer a system that is genuinely reliable. However, there are just a few clearly defined use cases for the often used approaches. The most crucial are the techniques for anomaly detection, or more broadly, intrusion detection. To identify anomalous behavior or, more specifically, intrusion, the majority of works train and use SVM or Bayesian networks. Even when credentials are not used for authentication, such as when only the physical layer is used, a variety of techniques are still used. The detection and prevention of DDoS assaults through the use of unsupervised methods, such as autoencoders, is the other important application of machine learning algorithms in IIoT security.

The security problems that arise from offloading computations in edge computing, or so-called offload security, are a unique area of IIoT security. A few publicly available datasets are available for training machine learning methods, which are necessary for their effective operation. Nevertheless, some researchers oppose the use of these datasets for the training and validation of safe machine learning-based solutions. Table 1 displays the references for the various applications discussed in this section.

Table 1. Summary of applications of machine learning techniques in IIoT security and safety.

Application	Typical Machine Learning Techniques	References
Intrusion detection	Classification on network data (SVM, Bayes networks, decision tree, Random forest, neural network)	[25–42]
Authentication	Classification on network data, Clustering	[25,46–51]
Privacy leaking	Differential privacy and federated learning	[52–54]
Data integrity	Latent space methods (Boltzmann-machine, DBN), Classification (Random Forest, SVM)	[55–58]
Availability	Reinforcement learning and Neural networks (DBN, autoencoders)	[59–61]
Offload security	Reinforcement learning	[62–64]

III. ASSET LOCALIZATION

One of the most crucial and specialized aspects of IIoT systems is asset localization, since tracking the position of potentially semi-finished goods or assets is necessary for site security or the manufacturing process. Figure 4 shows a few common applications for asset monitoring and localization. Although GPS (Global Positioning System) is mostly used for localization outside, interior factories are unable to use it because the building's construction obscures the GPS signal.

To get over this problem, a few radio-based technologies are used to give an asset position that is more or less precise indoors. More specifically, all the radio technologies used in IoT or IIoT systems can provide measurements to acquire asset position; however, some solutions are more suitable for asset localization than others.

Since the characteristics of radio signal propagation can be computed, i.e., the equations for attenuation and propagation delay are well known, localization appears to be a geometric problem at first glance. However, the dense multipath environment indoors, particularly on industrial sites, makes the propagation so stochastic and random that the received signal and its characteristics don't reveal anything about the propagation. For this reason, several works use sophisticated machine learning techniques to address the localization issue rather than the geometrical one. Nonetheless, machine learning techniques are also often applied to raise the geometric solution's correctness.

Figure 4: Common applications for industrial asset location and tracking, both indoors and outside. In addition to the traditional indoor and outdoor use cases, there are a few lesser-known subjects, such as tracking disposable objects or tracing the food chain (icons from Flaticon.com).

UWB

Since Ultra-Wideband (UWB) is specifically designed for localization, it is frequently utilized in IIoT solutions to enable precise localization. UWB's enormous bandwidth (a few hundred megahertz) allows for the application of very brief pulses (e.g., 1-2 ns long) that aid in differentiating the rays in multipath propagation and offer precise timestamps for the received packets, leading to a localization that is centimeter-capable. In UWB systems, the position estimation method often relies on calculating the range (or distance) between anchors and tags; optimization is then used to solve the geometry problem. However, faults in the timestamping process lead to positioning inaccuracies because multipath propagation might distort the received signal.

In order to address this problem, ref. [72] looks into the kNN (knearest neighbour), decision tree, and random forest methods to increase the localization accuracy based just on the computed position data. Using the receiver's indicator to ascertain if the timestamp is part of the actual first path (line-of-sight, or LOS) or not (non line-of-sight, or NLOS) is a more complex method. Using this data, ref. [73] infers the device's better position using a naïve Bayes technique.

In actuality, UWB systems frequently employ machine learning techniques to categorize reception as either LOS or NLOS propagation. The received channel impulse response (CIR) of the packet is provided by the majority of UWB chips, supporting these techniques. The study in [74] uses CIR to train a convolutional neural network to distinguish between LOS and NLOS packet receptions, which aids the localization engine in weighing the measurement when determining position. Although it analyzes three machine learning approaches—support vector machines, random forests, and dense neural networks—Ref [75] also focuses on the classification of reception. Ref. [76] explores various convolutional neural network and recurrent neural network combinations for CIR classification in order to use the temporal behavior of the channel impulse response. It demonstrates that the best accuracy is achieved with a CNN followed by stacked LSTM networks.

In addition to categorization, the CIR can be used to estimate the timestamping error of every packet that is received. Ref [77] improves location accuracy by one order of magnitude on average when compared to the geometric approach by using neural networks to anticipate the timestamping error based on the CIR of received packets. A few further UWB-based solutions are shown in the survey in [78], albeit they are not limited to the IIoT context.

A general approach for estimation of the position from CIR using deep learning techniques can be found in [79].

5G

5G is an advanced mobile technology that facilitates both large-scale infrastructure and on-site installations. The previous LTE standard's location capabilities were greatly enhanced in the 5G standard; with Release 17, IIoT localization has grown in importance within the standard [80]. 5G offers time- and angle-based positioning, and the NR (New Radio) interface's changeable parameters—such as increased bandwidth, variable subcarrier spacing, various antenna layouts, etc.—help to increase the precision of 5G positioning.

Although 5G allows for a variety of localization techniques, these are primarily closed-form or geometrical approaches. Nonetheless, there are a few studies that use machine learning techniques to increase localization accuracy; these studies primarily focus on IIoT environments, or indoor settings. "Fingerprinting" is a common locating technique that relies on easily observable radio channel characteristics, like the receive signal strength (RSSI). Using various machine learning models, ref. [81] attempts to estimate and rectify the location inaccuracy in order to increase the accuracy of such solutions. Vanilla neural networks and the kNN approach were compared to estimate the position.

Referencing the same issue, ref. [82] contrasts the specified DELTA method, which uses a dense neural network to infer the position from RSSI measurements, with kNN- and SVR- (Support Vector Regression)-based approaches.

Angle-based positioning is a more advanced 5G localization technique. The method in [83] uses beamforming to build beamformed fingerprints by sampling the received PDPs (Power Delay Profile). TCN and LSTM networks are trained to use the beamformed fingerprints to infer location. On average, the TCN network can track the location with an accuracy of a few meters. Even in comparison to GPS systems, the solution uses very little energy. Additionally, ref. [84] uses deep neural networks to improve 5G localization based on beamforming, which optimizes the handover process.

A comprehensive study on 5G and positioning can be found in [85], where a couple of methods—including machine learning-aided localization methods—are compared and introduced.

Wi-Fi and Bluetooth Low Energy

Broadband communication technology is made possible by the WiFi standard (IEEE 802.11) and is extensively utilized in commercial and industrial settings. WiFi localization solutions often use fingerprinting techniques without the need for specialized gear. Many trained machine learning models are employed to increase localization accuracy. While [87] included decision trees and naïve Bayes methods in the comparison, [86] compares the baseline kNN solution to the SVM and Random Forest approaches. Dense neural networks are used in the publications [88,89] to learn fingerprint and localization mapping, while denoising autoencoders are used in [90] to enhance the received fingerprints and determine the asset's precise position.

Bluetooth minimal Energy (BLE) is a widely utilized technology in many different fields that uses minimal energy to deliver low-speed, low-range communication. Fingerprinting is the fundamental localization method used in BLE, and the same techniques can be used to increase accuracy as in WiFi. There are, nevertheless, works that are especially about BLE. In order to train and assess random forest, XGBoost, decision tree, and kNN-based algorithms for location inference from the RSSI measurements, Ref. [91] uses a unique data augmentation procedure.

By assisting learners in handling RSSI values with significant fluctuations, the augmentation process produces predictions that are more accurate.

The application of the well-known LDA (Linear Discriminant Analysis) technique in fingerprinting is introduced in Ref. [92], which makes it intriguing.

The study shows that the LDA improves localization accuracy while maintaining a respectable execution time when compared to naive Bayes, kNN, and SVM approaches. There are a few other fingerprinting-based works available [93,94], and the study in [95] describes fingerprinting techniques in BLE instances. Since Bluetooth 5.1 was developed, the BLE standard has enabled direction-of-arrival (DoA) techniques through the use of antenna arrays. In order to substitute the well-known MUSIC (Multiple Signal Classification) algorithm for determining the direction of a signal, [96] uses the BLE DoA capability to apply a tiny neural network suitable for a restricted device.

Other

In addition to these popular technologies, asset localization in IIoT systems offers a few other solutions. In [97], LOS/NLOS classification is demonstrated using SVM, random forests, and neural networks for the less prevalent IEEE 802.15.4 systems. In [98], an IIoT underwater wireless sensor network used acoustic localization technology, and the accuracy of node localization was predicted using linear regression.

There are a growing number of published studies that examine the suitability of so-called device free localization (DFL), which locates users or assets without the need for any gear. These algorithms make use of a few machine learning approaches, such as Bayesian methods [100] and block-sparse coding with the proximal operator [99]. A useful summary of this topic and recent state-of-the-art can be found in [101,102].

Summary of Asset Localization

Although a number of technologies, such as UWB, 5G, WiFi, BLE, and others, can be used to execute asset localization in IIoT systems, UWB is the only one that focuses exclusively on localization. For each technology, machine learning techniques are typically employed for the two reasons listed below:

- To become familiar with the relationship between location and measurements
- To make the location inferred from closed-form, geometrical issues more accurate

The first is primarily utilized in fingerprinting, where machine learning models attempt to discover the relationship between the location and the measurements (usually RSSI). Although a few different regression techniques are employed, perhaps including classification on grids, the kNN learner is frequently the baseline solution. The second one, which blends geometric models with machine learning models, distinguishes between two fundamental techniques: LOS or NLOS propagation prediction and localization error prediction. The techniques typically make use of extra data, such as the channel impulse response. Table 2 displays the references for the various applications discussed in this section.

For further details, an in-depth study on indoor localization using machine learning techniques can be found in [103].

Table 2. Summary of applications of machine learning techniques in IIoT asset localization

Application	Typical Machine Learning Techniques	References
Learning mapping between measurements and location	kNN, SVM, Random Forest, XGBoost, Regression tree, neural networks, etc.	[79,82,83,86–96]
Predicting non-LOS propagation	Neural network (CNN, TCN, etc.), SVM, Random Forests on channel impulse response	[72–76]
Predicting location error	Neural network on channel impulse	[77,81,98]

Quality Assurance

Through the process of quality control, organizations examine the caliber of numerous production-related components. Monitoring, inspection, minimizing product variation, and removing failure cases are the main duties. The two primary steps of quality inspection in industrial manufacturing processes are functional and visual tests, sometimes known as automated visual/surface inspection. These days, both of these inspection types are typically carried out by

machines rather than people, however they still depend on human knowledge. Well-defined quality requirements are necessary for the discovery of defective products. It is quite difficult to comprehend and adjust these parameters for certain automated identification processes in order to automate such quality inspection procedures. Such challenges can be addressed with the aid of machine learning techniques.

Inspection of Visual Quality

In many industry fields, the presence of surface imperfections impacts the product's quality and appearance. Consequently, visual inspection of certain product features is one of the most popular quality inspection techniques used in production. There are numerous options for both exterior and surface flaw inspection in a variety of industry sectors, such as the fiber, metal, and semi-conductor sectors. The primary directions of machine learning-supported visual quality inspection techniques are presented in this section. The overall concept for vision-based product quality inspection, as per [104], is shown in Figure 5.

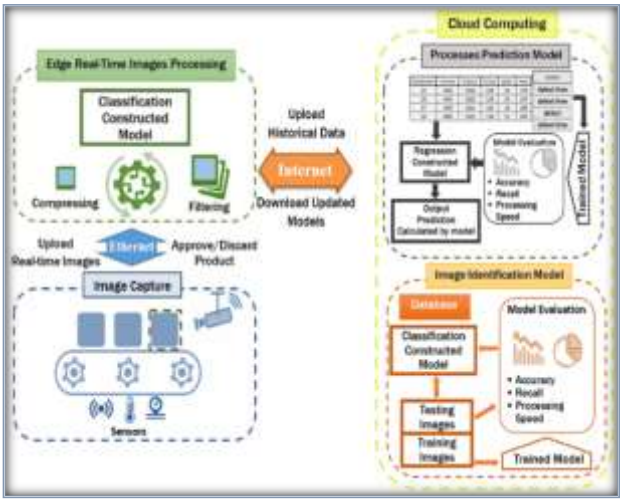

Figure 5. General architecture model for vision-based product quality inspection [104].

Generally speaking, feature extraction and defect detection are the two clearly defined procedures needed to identify a problematic product. Features of the product may be in the transform domain or the spatial domain. Furthermore, the state-of-the-art employs a number of feature extraction techniques, such as clustering (K-means, PCA), regression (linear regression, logistic regression), and classification (KNN, Naive Bayes classifier, SVM, Decision trees). Unlike previous methods, deep-learning algorithms eliminate the requirement to build a set of features, such as statistical or spectral features. The state-of-the-art surface inspection for supervised (CNN, LSTM) and unsupervised (Autoencoder) learning solutions includes a number of instances.

A machine learning-based computer vision system for examining the outside and interior of aircraft components is shown in Ref. [105]. CNN and LSTM are combined to categorize problems in the internal sections of the product, while SVM is utilized to classify defects in the external parts. On the other hand, a quality-level estimate method for steel microstructure inspection utilizing the VGG network model is presented in ref. [106]. Convolutional Neural Networks (CNN) and Convolutional Autoencoders (CAE) are used in Ref. [107] to evaluate the casting surface. A supervised learning-based method for inspecting press-casting goods utilizing CNN, Random Forest, PCA, and XGBoost is presented in Ref. [108].

The use of supervised machine learning (random forest, gradient boosting) in defect identification, quality control, and throughput enhancement for optical transceiver production is also examined in ref. [109]. By using a CNN model for optical inspection of assembling machines, Ref. [110] suggests an approach for error detection.

In order to categorize Pin-in-Paste solder connections using a YOLOv4 architecture, [111] uses a CNN-based method. The framework includes near real-time solder joint localization based on a YOLO single-stage detector and highly automated picture data labeling functionality utilizing a Convolutional Autoencoder. For metal workpieces, surface flaw detection is introduced in Ref. [112]. The study presents the outcomes of the DenseNet40 and ResNet50 architectures.

Ref. [104] offers a machine vision model to detect faulty products and classifies defects using CNN and SVM. Semi-supervised deep learning-based

surface inspection methods for labeled data are presented in Ref. [113] for automated surface fault detection. An unsupervised clustering technique for spatial patterns using wafer map measurement data is presented in Ref. [114]. After pre-processing the measured test values using computer vision techniques, high-dimensional wafer maps are broken down into a low-dimensional latent representation using feature extraction based on variational autoencoders.

Finding Anomalies

Anomaly detection is the other important area of quality inspection. Finding all instances that are different from the rest or the necessary instances is the aim of anomaly detection, also known as outlier detection. According to Ref. [115], an outlier is an observation that differs from other observations in such a way that it raises the possibility that it was produced by a separate mechanism. A machine learning method that can identify faulty bearings and continuously adjust the parameters of the quality testing procedure is presented in Ref. [116]. In particular, a vote classifier fed statistical metrics derived from the gathered experiments is used to identify faulty bearings. k-neighbors, SVC, Decision Tree, Random Forest, Multi-Layer Perceptron, AdaBoost, Naive Bayes, Gradient Boost, and Voting Classifier methods are among the machine learning techniques evaluated in this work.

Ref. [117] suggests a method wherein (1) the Support Vector Machine (SVM) algorithm is used to classify manufacturing processes, (2) the Horse Optimization Algorithm (HOA) is used to optimize the regularization parameter value and the gamma coefficient value of the SVM algorithm, and (3) the results of the HOA-based SVM algorithm are compared to those of Particle Swarm Optimization (PSO) and Chicken Swarm Optimization (CSO)-based SVM algorithms. Additionally, PSO and DNN are used for a similar problem in ref. [118].

The SEMCOM dataset is used to validate both approaches [119]. For industry product quality inspection, ref. [120] presents an anomaly detection technique based on the Gaussian Restricted Boltzmann Machine without application dependability or a case study. The key problems with machine learning-based condition monitoring systems are covered in Ref. [121]. Using six industrial test datasets, Ref. [122] examines a number of unsupervised learning approaches, including the Gaussian model, SVM, isolation forest, and autoencoder. A specific usage of telemetry—anomaly detection on time-series data—is the subject of Ref. [123]. It offers an enhanced iteration of the cutting-edge machine learning algorithm ReRe, which is based on long short-term memory.

[124] presents a malfunction diagnosis method for rotating machinery using vibration signals that is based on fuzzy neural networks. A long short-term memory (LSTM)-Gauss-NBayes approach for IIoT outlier detection is presented in Ref. [125].

By using the Gaussian Naive Bayes model's predictive error, LSTM-NN creates a model based on a normal time series and finds outliers. An on-device federated learning-based deep anomaly detection system for IIoT timeseries data sensing is proposed in Ref. [126]. To precisely identify abnormalities, the framework employed a convolutional neural network-long short-term memory (AMCNN-LSTM) model based on an attention mechanism. In a similar vein, ref. [127] suggests a federated learning-based anomaly detection method for IIoT. Specifically, it applies the federated learning technique to build a universal anomaly detection model with each local model trained by the deep reinforcement learning algorithm.

On the other hand, a useful study on graph neural networks (GNNs) for anomaly detection in IIoT-enabled smart factories, smart energy, and smart transportation is presented in ref. [128]. To evaluate the plant's operating conditions, Ref. [127] creates an anomaly detection program that makes use of deep learning techniques. K-means clustering carries out the actual anomaly detection, PCA handles a subsequent reduction, while AE and deepAE handle the initial dimensionality reduction. Using a PCA-based approach, Ref. [129] creates a framework for identifying anomalous behavior in the context of aging IIoT.

Anomaly Detection Datasets

Machine learning techniques for IIoT quality inspection and outlier detection can be trained and validated using a few publicly available datasets. By examining these datasets, one can gain a better knowledge of the machine learning algorithms and uncover the potential characteristics and results of each one. The machine learning community uses the databases, domain theories, and data generators listed in Ref. [119] to empirically analyze machine learning algorithms. The semi-conductor domain is one of several datasets from the manufacturing domain that are used to validate algorithms. A sizable collection of outlier detection datasets including ground truth (if available) can be found in Ref. [130].

The focus of the repository is to provide datasets from different domains and present them under a single platform for the research community, including several manufacturing domains (wafer map).

Summary of Quality Control Using Machine Learning

The most widely used quality inspection techniques are visual quality inspection and surface detection, which are applied in practically every sector of the economy and in manufacturing (see Table 3). While autoencoders are utilized for feature extraction, pretrained CNN networks (ResNet, DenseNet, and VGG) can be employed for object recognition.

Accurate and even real-time anomaly detection is becoming more and more crucial in the Industrial Internet of Things (IIoT) since device failures have a significant impact on the manufacturing of industrial products. Federated learning systems are utilized in numerous industrial areas due to the nature of the IIoT. Since time series data is one of the most prevalent data sources in anomaly detection situations, LSTM networks have drawn a lot of interest for their ability to classify, process, and predict data.

Table 3. Summary of applications of machine learning techniques in IIoT quality control.

Application	Typical Machine Learning Techniques	References
Visual quality inspection	CNN (Yolo, VGG, ResNet, DenseNet), Autoencoders	[104,106,107,110–112,114]
Anomaly detection	LSTM and PSO, kNN, SVM, PCA, XGBoost, Regressions, etc.	[117,122,125–127,127,129]

IV. MAINTENANCE

Because it involves essential duties that have a direct impact on productivity, maintenance has long been a significant part of industrial manufacturing. The cost of replacing or repairing equipment and the expense of stopping production lines when necessary tools or equipment are not available are the two main components of maintenance as they have historically been defined. As a result, maintenance changes in tandem with new methods and industrial technology.

Reactive and proactive maintenance are two distinct strategies. The intuitive approach to maintenance, known as reactive maintenance, is carrying out the activity when an item breaks or wears out. In order to prevent failure to save costs by guaranteeing shorter-term and scheduled maintenance and longer operational capabilities, proactive maintenance uses a variety of approaches to actively monitor the equipment, develop strategies, and estimate the conditions.

Predictive and preventive maintenance are the approaches that are most frequently used. The goal of the second is to create a regular, periodic maintenance procedure for preventing failures and keeping machinery operational for as long as possible by extending its life-time [131–133], as illustrated in Figure 6, whereas the first focuses on estimating the time of failure to enable scheduled maintenance—and thus production line down-times.

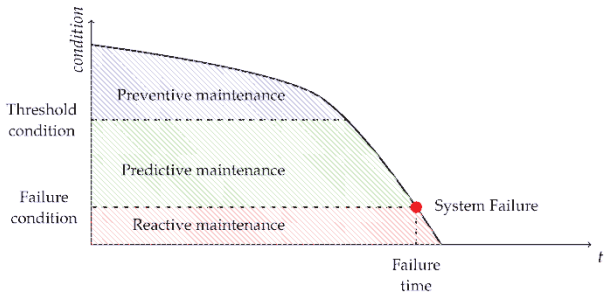

Figure 6. Difference between maintenance approaches in terms of condition and time

Usually, proactive maintenance refers to the application of predictive with preventive approaches in the same maintenance ecosystem to overcome the disadvantages of wasting working hours and costs by performing unnecessary, periodic maintenance.

Proactive Maintenance Tasks

Proactive maintenance is not only made possible by Industry 4.0 applications, which typically also incorporate IoT systems, but they also gain from its implementation. This brings us to the idea of cyber-physical systems, which are made up of many interconnected subsystems on both a digital and physical level. In order to optimize specific system parameters and establish a feedback loop, such a CPS gathers information about the state and condition of the subsystems or pieces of equipment. In order to develop a proactive maintenance system that is enabled by CPS and IoT, this scheme can also be used for maintenance duties. Several key components of such a system fall under the following categories [134–136]:

Fault Detection—Identifying malfunctions is a difficult operation that requires information from multiple sources, including telemetry data, environment monitoring sensors, equipment monitoring sensors, etc. Vibration monitoring, sound or acoustic monitoring, and oil-analysis or lubricant monitoring are the most often collected data by sensors [137,138].

Diagnostics—Prognostics and strategy planning are based on diagnostic processes, which analyze failures and hazards and allow for the development of models. Root cause analysis, a methodology for examining risks and methodically identifying potential root causes, is one of the primary tasks of diagnostics [139–141].

Prognostics—Predicting the future state of equipment by modeling it using diagnostic data is the goal of prognostics. Calculating the Mean Time to Failure (MTTF) and Remaining Useful Life (RUL) is typically the last objective of prognostics. These elements aid in the timely scheduling of necessary maintenance chores and are crucial in anticipating and averting potential future faults and breakdowns [142].

As previously said, these maintenance activities include data analysis, pattern recognition, creating intricate models of objects or processes, and predicting occurrences (failures and dangers), all of which are areas where machine learning techniques have historically performed better than alternative approaches and solutions. State-of-the-art solutions can be developed based on requirements and expectations because the maintenance, repair, and overhaul (MRO) fields are not subject to strict regulations. They can also adopt previously implemented solutions that are available in the literature or as an open-source project.

Fault Detection

A vast amount of data is needed for every aspect of maintenance, including fault detection (FD) and anomaly identification. Because of their similarities, this task's solutions are similar to those of the previously mentioned anomaly detection approach in quality control. Classification, clustering, regression, and anomaly detection techniques are most appropriate for this use-case since the primary objective is to watch and identify problems [143]. A clustering-based approach for a Power Distribution Network fault detection is covered in [144], where the decision tree algorithm performed better in terms of accuracy than KNN and SVM. A clustering method for identifying multi-component deterioration in airplane fuel systems was put forth by the authors in [145]. While keeping their computational complexity low, decision tree-based systems, like the one described in [146,147], can also offer an accurate detection rate.

However, employing neural networks for this function is also a popular approach, as seen in [148], where a finished maintenance framework is constructed using them. As demonstrated in [149,150], artificial neural network-based methods can be employed successfully for feature extraction and time-series data analysis. Furthermore, one of the primary predictive maintenance activities that heavily depends on real-time processing is defect detection. A Convolutional Neural Network (CNN)-based method for motor defect detection that can deliver precise estimations in real time is presented in Ref. [151].

Diagnostics

Classification or clustering-based solutions are frequently needed because diagnostic procedures, most notably root cause analysis, examine dangers by methodically generating problem subsets.

The authors of [152] suggested an RCA solution for rotating machinery based on Decision Trees and Principal Component Analysis (PCA), where Decision Trees can accurately categorize data and PCA can remove duplicate features. Additionally, it was demonstrated in Ref. [153] that ensemble and decision tree algorithms work well with huge data sets and uncertain issues. In their suggested methodological framework, [154] employed Random Forest and KNN as classifiers for timeseries data in the particular rotating equipment use-case, and [155] likewise employed Random Forest for time-domain classification.

RCA is not the only crucial diagnostic activity; modeling, which forms the foundation of prognostics, is also part of diagnostics. In order to create models for such tasks, feature extraction is typically required. The authors of [156] suggested a method for diagnosing rotating machinery faults that relies on a fish swarm algorithm to optimize its critical parameters and an auto-encoder to extract features. A comparable technique for rolling bearings is also suggested in Ref. [157], but it makes use of an improved Deep Wavelet Auto-encoder and Extreme Learning Machine. In [158,159], various CNN-based techniques for processing time and frequency series data from sensors were introduced for bearings. In [157], a further approach utilizing RNN and GRU for strong performance and high accuracy is provided.

Prognostics

Prognostics typically entails designing or creating models that may explain the behavior of the equipment or component under investigation, in addition to estimating RUL and MTTF. Physical model-based, knowledge-based, data-driven, and other approaches are among the many that can be used in this sector; however, because of the vast quantity of data that is already available and the burgeoning machine learning applications, data-driven approaches are currently the most common. However, some learning strategies, like fuzzy logic, can also be used to make knowledge-based predictions [160].

A method based on Support Vector Machines (SVM) and Restricted Boltzmann Machines (RBM) is suggested for predicting RUL with reference to the data-driven approach in [161].

In this work, RBM was utilized to enable learning without aberrant data, and SVM was employed to classify a dataset measured using a vibration sensor. In this field, a functional combination like this is common, with one technique being used for classification and the other for overcoming uneven data. SVM is one of the most widely used classification algorithms, according to [162]. Nevertheless, statistical algorithms like Bayesian Networks are still useful, primarily in situations with little data or in unpredictable contexts [163,164].

A common issue with modeling large systems is the enormous state space, which makes it challenging to build a model that accounts for every attribute. Therefore, in this industry, where auto-encoder-based [165] solutions can be heavily used, lowering complexity is a regular task. Before determining RUL, the authors of [166] suggested using an Auto-Encoder Gated Recurrent Unit (GRU) for dimension reduction; in [167], the same method was used, but in a framework.

It is typically advantageous to put in place systems that can handle time-series data because these forecasts are mostly dependent on it. Because of its strong time-series prediction capabilities, Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) were used for high-speed railway power equipment in Ref. [168]. A combined LTSM-RNN approach was used in the same way in [169], although the study noted that because of its complexity, it is only appropriate for essential systems, whereas vanilla-RNN is better suited for large amounts of data.

Optimization of Manufacturing

The main ideas and machine learning techniques for manufacturing optimization are presented in this section. It exclusively addresses procedures that are directly related to manufacturing and production lines. The production optimization process's goal variables include the product's quality, cost, time, power usage, and other aspects unique to the product. There are relationships among these optimization elements, of course, but these are the most prominent ones. The foundation of factory optimization processes, pattern recognition, greatly benefits from the application of machine learning techniques. Correlations between various data types or manufacturing domains can be found and used to optimize the manufacturing process with the aid of machine learning techniques.

Q-learning in an automated system is used in ref. [170] for electricity optimization in order to lower electricity consumption. A Deep Q-network algorithm based on mixed online bipartite matching is suggested in ref. [171] for smart manufacturing that maximizes profits. The paper tackles the crucial problem of efficiency and latency in the blockchain-based live manufacturing process by formulating a joint optimization of the block size, task scheduling, and supply-demand configuration to maximize customers' net profit with the probabilistic delay requirements. On the other hand, the study in [172] troubleshoots production data using a support vector regression technique with an RBF kernel to find the parameters causing fluctuations in high energy conversion efficiency.

In order to transfer the input mask patterns straight to the output resist patterns, Ref. [173] suggests LithoGAN, an end-to-end lithography modeling system built on a generative adversarial network (GAN). The findings demonstrate that LithoGAN can accurately anticipate resist designs at a speed orders of magnitude faster than traditional lithography simulation and earlier machine learning-based methods. Ultrasound imaging applications include CNN and RNN in addition to GAN and Q-learning. In an IIoT setting, Ref. [174] suggests an automatic fetal ultrasound standard plane recognition model that uses multi-task learning to understand the temporal and spatial characteristics of the ultrasound video stream. While the RNN component gathers the temporal information between neighboring frames, the CNN component recognizes important anatomical features of the fetus and it realizes the precise localization and tracking of fetal organs across frames.

Particle Swarm Optimization has been used to solve a number of optimization problems. For example, in [175], a PSO-based method is proposed to optimize the LSTM's hyperparameter settings in a FL environment, and in [176], combined multi-Objective particle swarm optimization (CMOPSO) is suggested for an energy system used in green manufacturing. Additionally, regression difficulties are rather common in the production optimization industry. Ref. [177] suggests using machine learning (ML) based on a regression technique to optimize semiconductor production operations. The effectiveness of several supervised machine learning techniques, such as Linear Regression and Artificial Neural Network solutions, for the field calibration of inexpensive IoT sensors is compared in Ref. [178]. Furthermore, a solution for solving the inverse problem in electrical impedance tomography using logistic regression is presented in ref. [179].

Nonetheless, the industrial sector typically offers fully integrated NN systems. A NN model and Finite

Element Analysis are suggested in Ref. [180] for chip package design optimization. An optimization technique for Bipolar-CMOS-DMOS process development based on NN and an Automatic Multi-objective Optimization solution is presented in Ref. [181].

In the area of production optimization, there are a few survey works. The majority of pertinent literature from 2008 to 2018 that deals with machine learning and optimization techniques for process or product quality improvement in the manufacturing sector is covered in the study in [13]. According to the review, there is very little relationship between the use of data, data volume, machine learning techniques, optimizers, and the corresponding production issue. Furthermore, there are publications that provide an overview of some of the most current developments in machine learning, emphasizing how they are used in process industries like additive manufacturing [182,183]. Additionally, ref. [185] analyzes the applicability of RL for various scheduling problems, summarizes state and action designs, and offers RL-based scheduling methods.

Smart Maintenance Datasets

Machine learning algorithms for smart maintenance chores can be trained and validated using a few publicly available datasets. By examining these datasets, one can gain a better knowledge of the machine learning algorithms and uncover the potential characteristics and results of each one. The majority of these datasets are synthetic due to the dearth of actual, industrial data. Ref. [119] is also a helpful source for smart maintenance applications because defect identification is a part of both quality control and maintenance.

The benchmark dataset for predictive maintenance, MetroPT, which was gathered in 2022 regarding an urban metro public transportation service in Porto, is used in Ref. [186]. For the objectives of anomaly detection and failure prediction, the data includes samples from digital signals (control signals, discrete signals), analog sensor signals (pressure, temperature, current consumption), and GPS data (latitude, longitude, and speed). A dataset of alarms recorded by packaging machinery in an industrial setting is provided in Ref. [187] for categorization, forecasting, and anomaly detection applications. The collection comprises data from 20 equipment that were deployed at various sites worldwide between February 21, 2019, and June 17, 2020. The distribution is extremely lopsided for the 154 different alarm codes.

The Platform for Proactive Maintenance by MANTIS

In 2015, 47 partners from 12 different countries in Europe began working on the Electronic Components and Systems for European Leadership (MANTIS) project.

The primary goal, according to the authors in [188], was to create a proactive maintenance service platform architecture based on CPS that would facilitate collaborative maintenance ecosystems. In order to maximize maintenance, the requirements were defined to align with expectations.

CPS mechanisms [189]. The Remaining Useful Life (RUL) of components, Fault Prediction (FP), Root Cause Analysis (RCA), and Maintenance Strategy Optimization (MSO) are the four primary proactive maintenance focus areas that they suggested.

As seen in Figure 7, the architecture model adheres to the Industrial Internet of Things Reference Architecture of the Industrial Internet Consortium and comprises the edge, platform, and enterprise tiers. It also facilitates multi-stakeholder interactions and has undergone various evaluations for validation. In addition to using the Open Standards for the Physical Asset Management of Machinery Information Management Open System Alliance (MIMOSA) for data ontology, databus, and shared understanding across partners and applications, MANTIS processes data using the Lambda architecture pattern.

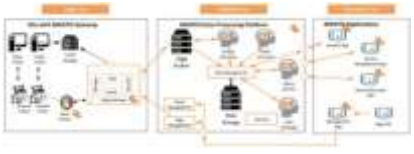

Figure 7. Overview of the MANTIS reference architecture [188].

The authors of [190] offer an expansion of MANTIS that incorporates Big Data technologies and an implementation, including Apache Spark and the Hadoop Distributed File System.

They employed two methods: Remaining Useful Life, which was based on time series forecasting, and Root Cause Analysis, which was fueled by Attribute Oriented Induction (AOI) Clustering.

The four primary building blocks of the platform's technology implementation are described as follows: Data ingestion and access via batch processors, data storage systems, edge brokers, and human-machine interfaces.

The authors of [191] described CPS-populated systems that employ MANTIS for proactive maintenance. In addition to summarizing the three primary research challenges—system performance, quality, and acceptance; applied development and deployment; and science and engineering foundations—they presented the key features of a CPS. Additionally, they discussed MANTIS's interoperability viewpoint, covering its technical, conceptual, application, and specification integrations.

The authors of [192,193] provide intricate case studies on proactive maintenance and ongoing track and switch monitoring. They made use of the MANTIS platform and principles during the entire process. They described the procedures involved in data processing, implementation strategies, and visualization options, emphasizing the benefits of using MANTIS at each stage.

Summary of Maintenance and Manufacturing Optimization Using Machine Learning

Fault detection, diagnostics, and prognostics—the three primary facets of proactive maintenance—share certain prerequisites and goals, and as a result, the tasks that must be completed. Classification, clustering, regression, complexity reduction, system modeling, and data series analysis are typically among these crucial activities. Though the latter are more concerned with prognostics, the former are more closely tied to fault identification and diagnostics; the applied machine-learning techniques also overlap to some extent. Nevertheless, both domains have unique goals. Table 4 provides an overview of the maintenance techniques. KNN and SVM are commonly used for clustering, whereas decision trees, random forests, and principal component analysis are utilized for classification and regression. The most popular techniques for modelling, complexity reduction, and data series analysis are neural network-based applications including CNN, auto-encoder, RNN, GRU and LSTM.

It goes without saying that the manufacturing sector has a wide range of application-specific optimization challenges, with variations in their regularities depending on the machine learning approaches employed. In most situations, supervised machine learning techniques (SVM, regression) are employed for classification and prediction, as well as as an analytical tool throughout the optimization process. In many manufacturing processes, reinforcement learning—particularly Q-learning—is used to solve decision-making issues like single- and multi-objective scheduling difficulties. Nonetheless, it may be said that quality inspection and manufacturing optimization are just slightly different. The two processes are frequently inseparable; these machine learning-supported manufacturing processes depend on one another in a number of ways.

Table 4. Summary of applications of machine learning techniques in IIoT proactive maintenance

Application	Typical Machine Learning Techniques	References
Fault Detection	KNN, SVM, Decision Tree, CNN	[143–151]
Diagnostics	Decision Tree, Random Forest, KNN, SVM, CNN, RNN	[152–157,157–159]
Prognostics	SVM, Bayesian Networks, RNN, CNN, Auto-Encoder, LSTM, Gated Recurrent	[160–169]

	Unit (GRM)	
Manufacturing optimization	Unsupervised learning (Regressions, SVM, GAN), Reinforcement learning (Q-learning, LSTM)	[170,171,173–175,177,178,181]

V. CONCLUSION

This study included a thorough analysis of machine learning methods used in IIoT and smart production for a variety of applications. Proactive maintenance, asset localization, quality assurance, and safety and security are among the topics discussed.

Since IIoT security and safety are crucial to the Industry 4.0 technological shift, ML approaches have a wide range of application sectors.

Intrusion detection, authentication support, privacy leak detection, data integrity checks, availability support, and security service offloading are a few of these. One highly specialized area of smart manufacturing where machine learning has been widely used is asset localization. forecasting non-LOS propagation, learning the mapping between measurements and location, and forecasting location inaccuracy are some of the application areas for asset localization. In terms of quality control, it was discovered that machine learning techniques were particularly needed for applications involving visual quality inspection and anomaly detection. The primary application areas for maintenance include prognostics, diagnostics, fault detection, and some factory optimization applications that were also examined.

This work made it simpler for researchers and practitioners to identify ML-application trends for their respective fields by summarizing the relevant references found for application domains in addition to offering a broad overview of the used approaches for the listed application areas. The most crucial public dataset references for creating domain-specific algorithms and applications are also included in the study (see Table 5). To support the key conclusions regarding the state-of-the-art and the research needs in the application area under discussion, each major chapter contains a special lessons-learned section.

Table 5. Summary of major and typical datasets for IIoT machine learning applications

Topic	Name of Dataset	Description
Smart maintenance	MetroPT [186]	Consists of samples of analog sensor signals (pressure, temperature, current consumption), digital signals (control signals, discrete signals), and GPS information (latitude, longitude, and speed).
	Alarm Logs in Packaging Industry (ALPI) [187]	Contains a sequence of alarms logged by packaging equipment in an industrial environment. The collection includes data logged by 20 machines, deployed in different plants around the world, from 21 February 2019 to 17 June 2020.
Quality inspection	UCI Machine Learning Repository [119]	A UCI collection of databases, domain theories, and data generators. There are several datasets from the manufacturing domain that are used for algorithm validation, including the semi-conductor domain.
	Outlier Detection DataSets [130]	ODDS provide access to a large collection of outlier detection datasets with ground truth (if available). The focus of the repository is to provide datasets

		from different domains including several manufacturing domains (wafer map).
Safety and security	KDD-99 dataset [65]	The dataset used for The Third International Knowledge Discovery and Data Mining Tools Competition, the competition task was to build a network intrusion detector algorithm.
	CSE-CIC-IDS2018 dataset [66]	The dataset includes seven different attack scenarios, namely Brute-force, Heartbleed, Botnet, DoS, DDoS, Web attacks, and infiltration of the network from inside. The attacking infrastructure includes 50 machines and the victim organization has 5 departments including 420 PCs and 30 servers.
	CIC DDoS attack dataset [67]	The dataset contains different modern reflective DDoS attacks such as PortMap, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, SYN, NTP, DNS and SNMP
	Intrusion detection and privacy attack dataset [68,69]	Dataset for developing and evaluating different IEEE 802.11 Wi-Fi algorithms.
	The University of Arizona datasets [70]	Different malware and network traffic datasets for developing and evaluating network security algorithms.
Localization	UTIL: An Ultra-wideband Time-difference-of-arrival Indoor Localization Dataset [194]	An Ultra-wideband Time-difference-of-arrival Indoor Localization Dataset. Raw sensor data including UWB TDOA, inertial measurement unit (IMU), optical flow, time-of-flight (ToF) laser, and millimeter-accurate ground truth data were collected during the flights of drones.
	CSI Dataset towards 5G NR High-Precision Positioning [195]	This dataset can be used for indoor positioning, indoor-outdoor-integrated positioning, NLoS, 5G channel estimation and other types of research, providing researchers with CSI-level position-related feature data.

REFERENCES

1. Varga, P.; Plosz, S.; Soos, G.; Hegedus, C. Security threats and issues in automation IoT. In Proceedings of the 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), Trondheim, Norway, 31 May–2 June 2017; pp. 1–6. [CrossRef]
2. Mitchell, T.M. Machine Learning; McGraw-Hill Education: New York, NY, USA, 1997.
3. Goodfellow, I.; Bengio, Y.; Courville, A. Deep Learning; MIT Press: Cambridge, MA, USA, 2016. Available online: http: //www.deeplearningbook.org (accessed on 1 November 2022).
4. Shalev-Shwartz, S.; Ben-David, S. Understanding Machine Learning: From Theory to Algorithms; Cambridge University Press: Cambridge, UK, 2014.
5. Géron, A. Hands-on Machine Learning with Scikit-Learn, Keras, and TensorFlow; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2022.
6. Müller, A.C.; Guido, S. Introduction to Machine Learning with Python: A Guide for Data

Scientists; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2016.
7. Lantz, B. Machine Learning with R: Expert Techniques for Predictive Modeling; Packt Publishing Ltd.: Birmingham, UK, 2019.
8. Lakshmanan, V.; Robinson, S.; Munn, M. Machine Learning Design Patterns; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2020.
9. Sharp, M.; Ak, R.; Hedberg, T., Jr. A survey of the advancing use and development of machine learning in smart manufacturing. J. Manuf. Syst. 2018, 48, 170–179. [CrossRef] [PubMed]
10. Angelopoulos, A.; Michailidis, E.T.; Nomikos, N.; Trakadas, P.; Hatziefremidis, A.; Voliotis, S.; Zahariadis, T. Tackling faults in the industry 4.0 era—A survey of machine-learning solutions and key aspects. Sensors 2019, 20, 109. [CrossRef] [PubMed]
11. Hanga, K.M.; Kovalchuk, Y. Machine learning and multi-agent systems in oil and gas industry applications: A survey. Comput. Sci. Rev. 2019, 34, 100191. [CrossRef]
12. Usuga Cadavid, J.P.; Lamouri, S.; Grabot, B.; Pellerin, R.; Fortin, A. Machine learning applied in production planning and control: A state-of-the-art in the era of industry 4.0. J. Intell. Manuf. 2020, 31, 1531–1558. [CrossRef]
13. Weichert, D.; Link, P.; Stoll, A.; Rüping, S.; Ihlenfeldt, S.; Wrobel, S. A review of machine learning for the optimization of production processes. Int. J. Adv. Manuf. Technol. 2019, 104, 1889–1902. [CrossRef]
14. Cioffi, R.; Travaglioni, M.; Piscitelli, G.; Petrillo, A.; De Felice, F. Artificial intelligence and machine learning applications in smart production: Progress, trends, and directions. Sustainability 2020, 12, 492. [CrossRef]
15. Narciso, D.A.; Martins, F. Application of machine learning tools for energy efficiency in industry: A review. Energy Rep. 2020, 6, 1181–1199. [CrossRef]
16. Diez-Olivan, A.; Del Ser, J.; Galar, D.; Sierra, B. Data fusion and machine learning for industrial prognosis: Trends and perspectives towards Industry 4.0. Inf. Fusion 2019, 50, 92–111. [CrossRef]
17. Çınar, Z.M.; Abdussalam Nuhu, A.; Zeeshan, Q.; Korhan, O.; Asmael, M.; Safaei, B. Machine learning in predictive maintenance towards sustainable smart manufacturing in industry 4.0. Sustainability 2020, 12, 8211. [CrossRef]
18. Xu, Z.; Saleh, J.H. Machine learning for reliability engineering and safety applications: Review of current status and future opportunities. Reliab. Eng. Syst. Saf. 2021, 211, 107530. [CrossRef]
19. Schwalbe, G.; Schels, M. A survey on methods for the safety assurance of machine learning based systems. In Proceedings of the 10th European Congress on Embedded Real Time Software and Systems (ERTS 2020), Toulouse, France, 29–31 January 2020.
20. Martin, R.; Schrecker, S.; Soroush, H.; Molina, J.; LeBlanc, J.; Hirsch, F.; Buchheit, M.; Ginter, A.; Banavara, H.; Eswarahally, S.; et al. Industrial Internet Security Framework Technical Report; Technical Report; CreateSpace Independent Publishing Platform: Scotts Valley, CA, USA, 2016. [CrossRef]
21. Fraile, F.; Tagawa, T.; Poler, R.; Ortiz, A. Trustworthy Industrial IoT Gateways for Interoperability Platforms and Ecosystems. IEEE Internet Things J. 2018, 5, 4506–4514. [CrossRef]
22. Abomhara, M.; Køien, G.M. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. J. Cyber Secur. Mobil. 2015, 4, 65–88.
23. Sharma, P.; Jain, S.; Gupta, S.; Chamola, V. Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. Ad Hoc Netw. 2021, 123, 102685. [CrossRef]
24. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access 2019, 7, 82721–82743. [CrossRef]
25. Baldini, G.; Giuliani, R.; Steri, G.; Neisse, R. Physical layer authentication of Internet of Things wireless devices through permutation and dispersion entropy. In Proceedings of the 2017 Global Internet of Things Summit (GIoTS), Geneva, Switzerland, 6–9 June 2017; pp. 1–6. [CrossRef]
26. Hosseini Bamakan, S.M.; Wang, H.; Yingjie, T.; Shi, Y. An effective intrusion detection framework based on MCLP/SVM optimized by

time-varying chaos particle swarm optimization. Neurocomputing 2016, 199, 90–102. . [CrossRef]
27. Kabir, E.; Hu, J.; Wang, H.; Zhuo, G. A novel statistical technique for intrusion detection systems. Future Gener. Comput. Syst. 2018, 79, 303–318. [CrossRef]
28. Bagaa, M.; Taleb, T.; Bernabe, J.B.; Skarmeta, A. A Machine Learning Security Framework for Iot Systems. IEEE Access 2020, 8, 114066–114077. [CrossRef]
29. Zissis, D. Intelligent security on the edge of the cloud. In Proceedings of the 2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC), Madeira Island, Portugal, 27–29 June 2017; pp. 1066–1070. [CrossRef]
30. Goeschel, K. Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive Bayes for off-line analysis. In Proceedings of the SoutheastCon 2016, Norfolk, VA, USA, 30 March–3 April 2016; pp. 1–6. [CrossRef]
31. Mehmood, T.; Md Rais, H.B. Machine learning algorithms in context of intrusion detection. In Proceedings of the 2016 3rd International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, Malaysia, 15–17 August 2016; pp. 369–373. [CrossRef]
32. Jincy, V.J.; Sundararajan, S. Classification Mechanism for IoT Devices towards Creating a Security Framework. In Intelligent Distributed Computing; Buyya, R., Thampi, S.M., Eds.; Springer International Publishing: Cham, Switzerland, 2015; pp. 265–277.
33. Hassan, M.M.; Gumaei, A.; Huda, S.; Almogren, A. Increasing the Trustworthiness in the Industrial IoT Networks through a Reliable Cyberattack Detection Model. IEEE Trans. Ind. Inform. 2020, 16, 6154–6162. [CrossRef]
34. Shenfield, A.; Day, D.; Ayesh, A. Intelligent intrusion detection systems using artificial neural networks. ICT Express 2018, 4, 95–99.
35. Yin, C.; Zhu, Y.; Fei, J.; He, X. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access 2017, 5, 21954–21961. [CrossRef]
36. Vinayakumar, R.; Soman, K.P.; Poornachandran, P. Applying convolutional neural network for network intrusion detection. In Proceedings of the 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Manipal, India, 13–16 September 2017; pp. 1222–1228. [CrossRef]
37. Tajbakhsh, A.; Rahmati, M.; Mirzaei, A. Intrusion detection using fuzzy association rules. Appl. Soft Comput. 2009, 9, 462–469. [CrossRef]
38. Hoang, X.D.; Hu, J.; Bertok, P. A program-based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference. J. Netw. Comput. Appl. 2009, 32, 1219–1228. [CrossRef]
39. Warrender, C.; Forrest, S.; Pearlmutter, B. Detecting intrusions using system calls: Alternative data models. In Proceedings of the 1999 IEEE Symposium on Security and Privacy (Cat. No. 99CB36344), Oakland, CA, USA, 9–12 May 1999; pp. 133–145. [CrossRef]
40. Zarpelão, B.B.; Miani, R.S.; Kawakani, C.T.; de Alvarenga, S.C. A survey of intrusion detection in Internet of Things. J. Netw. Comput. Appl. 2017, 84, 25–37. [CrossRef]
41. Branch, J.W.; Giannella, C.; Szymanski, B.; Wolff, R.; Kargupta, H. In-network outlier detection in wireless sensor networks. Knowl. Inf. Syst. 2013, 34, 23–54.
42. Al Samara, M.; Bennis, I.; Abouaissa, A.; Lorenz, P. A Survey of Outlier Detection Techniques in IoT: Review and Classification. J. Sens. Actuator Netw. 2022, 11, 4.
43. Lee, S.Y.; Wi, S.R.; Seo, E.; Jung, J.K.; Chung, T.M. ProFiOt: Abnormal Behavior Profiling (ABP) of IoT devices based on a machine learning approach. In Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, Australia, 22–24 November 2017; pp. 1–6. [CrossRef]
44. Miettinen, M.; Marchal, S.; Hafeez, I.; Asokan, N.; Sadeghi, A.R.; Tarkoma, S. IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS),

Atlanta, GA, USA, 5–8 June 2017; pp. 2177–2184. [CrossRef]
45. Siddavatam, I.A.; Satish, S.; Mahesh, W.; Kazi, F. An ensemble learning for anomaly identification in SCADA system. In Proceedings of the 2017 7th International Conference on Power Systems (ICPS), Pune, India, 21–23 December 2017; pp. 457–462. [CrossRef]
46. Meidan, Y.; Bohadana, M.; Shabtai, A.; Guarnizo, J.D.; Ochoa, M.; Tippenhauer, N.O.; Elovici, Y. ProfilIoT: A Machine Learning Approach for IoT Device Identification Based on Network Traffic Analysis. In Proceedings of the Symposium on Applied Computing, Marrakech, Morocco, 3–7 April 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 506–509. [CrossRef]
47. Shi, C.; Liu, J.; Liu, H.; Chen, Y. Smart User Authentication through Actuation of Daily Activities Leveraging WiFi-Enabled IoT. In Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Chennai, India, 10–14 July 2017; Association for Computing Machinery: New York, NY, USA, 2017. [CrossRef]
48. Eigner, O.; Kreimel, P.; Tavolato, P. Detection of Man-in-the-Middle Attacks on Industrial Control Networks. In Proceedings of the 2016 International Conference on Software Security and Assurance (ICSSA), St. Pölten, Austria, 24–25 August 2016; pp. 64–69. [CrossRef]
49. Aminanto, M.E.; Kim, K. Improving Detection of Wi-Fi Impersonation by Fully Unsupervised Deep Learning. In Information Security Applications; Kang, B.B., Kim, T., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 212–223.
50. Wang, X.; Garg, S.; Lin, H.; Piran, M.J.; Hu, J.; Hossain, M.S. Enabling Secure Authentication in Industrial IoT With Transfer Learning Empowered Blockchain. IEEE Trans. Ind. Inform. 2021, 17, 7725–7733. [CrossRef]
51. Anjomshoaa, A.; Curry, E. Blockchain as an Enabler for Transfer Learning in Smart Environments. arXiv 2022, arXiv:2204.03959.
52. Zhang, X.; Chen, X.; Liu, J.K.; Xiang, Y. DeepPAR and DeepDPA: Privacy Preserving and Asynchronous Deep Learning for Industrial IoT. IEEE Trans. Ind. Inform. 2020, 16, 2081–2090. [CrossRef]
53. Arachchige, P.C.M.; Bertok, P.; Khalil, I.; Liu, D.; Camtepe, S.; Atiquzzaman, M. A Trustworthy Privacy Preserving Framework for Machine Learning in Industrial IoT Systems. IEEE Trans. Ind. Inform. 2020, 16, 6092–6102. [CrossRef]
54. Jiang, B.; Li, J.; Yue, G.; Song, H. Differential Privacy for Industrial Internet of Things: Opportunities, Applications, and Challenges. IEEE Internet Things J. 2021, 8, 10430–10451. [CrossRef]
55. Beaver, J.M.; Borges-Hink, R.C.; Buckner, M.A. An Evaluation of Machine Learning Methods to Detect Malicious SCADA Communications. In Proceedings of the 2013 12th International Conference on Machine Learning and Applications, Miami, FL, USA, 4–7 December 2013; Volume 2, pp. 54–59. [CrossRef]
56. Alves, T.; Das, R.; Morris, T. Embedding Encryption and Machine Learning Intrusion Prevention Systems on Programmable Logic Controllers. IEEE Embed. Syst. Lett. 2018, 10, 99–102. [CrossRef]
57. He, Y.; Mendis, G.J.; Wei, J. Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism. IEEE Trans. Smart Grid 2017, 8, 2505–2516. [CrossRef]
58. Aboelwafa, M.M.N.; Seddik, K.G.; Eldefrawy, M.H.; Gadallah, Y.; Gidlund, M. A Machine-Learning-Based Technique for False Data Injection Attacks Detection in Industrial IoT. IEEE Internet Things J. 2020, 7, 8462–8471. . [CrossRef]
59. Potluri, S.; Henry, N.F.; Diedrich, C. Evaluation of hybrid deep learning techniques for ensuring security in networked control systems. In Proceedings of the 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Limassol, Cyprus, 12–15 September 2017; pp. 1–8. [CrossRef]
60. Li, Y.; Quevedo, D.E.; Dey, S.; Shi, L. SINR-Based DoS Attack on Remote State Estimation: A Game-Theoretic Approach. IEEE Trans. Control Netw. Syst. 2017, 4, 632–642. [CrossRef]

61. Hogan, M.; Esposito, F. Stochastic delay forecasts for edge traffic engineering via Bayesian Networks. In Proceedings of the 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 30 October–1 November 2017; pp. 1–4. [CrossRef]
62. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Secure Computation Offloading in Blockchain based IoT Networks with Deep Reinforcement Learning. arXiv 2019, arXiv:1908.07466. https://doi.org/10.48550/ARXIV.1908.07466.
63. Xiao, L.; Xie, C.; Chen, T.; Dai, H.; Poor, H.V. A Mobile Offloading Game Against Smart Attacks. IEEE Access 2016, 4, 2281–2291. [CrossRef]
64. Liu, X.; Yu, W.; Liang, F.; Griffith, D.; Golmie, N. On deep reinforcement learning security for Industrial Internet of Things. Comput. Commun. 2021, 168, 20–32. [CrossRef]
65. Stolfo, S.; Fan, W.; Lee, W.; Prodromidis, A.; Chan, P. Cost-Based Modeling and Evaluation for Data Mining with Application to Fraud and Intrusion Detection: Results from the JAM Project; IEEE: Piscataway, NJ, USA, 1999.
66. Canadian Institute for Cybersecurity. CSE-CIC-IDS2018 Dataset. Available online: https://registry.opendata.aws/cse-cic-ids2018 (accessed on 1 November 2022).
67. Canadian Institute for Cybersecurity. CIC-DDoS2019 Dataset. Available online: https://www.unb.ca/cic/datasets/ddos-2019 .html (accessed on 1 November 2022).
68. Kolias, C.; Kambourakis, G.; Stavrou, A.; Gritzalis, S. Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset. IEEE Commun. Surv. Tutor. 2016, 18, 184–208. [CrossRef]
69. Chatzoglou, E.; Kambourakis, G.; Kolias, C. Empirical evaluation of attacks against IEEE 802.11 enterprise networks: The AWID3 dataset. IEEE Access 2021, 9, 34188–34205. [CrossRef]
70. University of Arizona, AZSecure-data.org. Intelligence and Security Informatics Data Sets. Available online: https://www. azsecure-data.org/other-data.html (accessed on 1 November 2022).
71. Zolanvari, M.; Teixeira, M.A.; Jain, R. Effect of Imbalanced Datasets on Security of Industrial IoT Using Machine Learning. In Proceedings of the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, USA, 9–11 November 2018; pp. 112–117. [CrossRef]
72. Yin, A.; Lin, Z. Machine Learning aided Precise Indoor Positioning. arXiv 2022, arXiv:2204.03990.
73. Che, F.; Ahmed, A.; Ahmed, Q.Z.; Zaidi, S.A.R.; Shakir, M.Z. Machine Learning Based Approach for Indoor Localization Using Ultra-Wide Bandwidth (UWB) System for Industrial Internet of Things (IIoT). In Proceedings of the 2020 International Conference on UK-China Emerging Technologies (UCET), Glasgow, UK, 20–21 August 2020; pp. 1–4. [CrossRef]
74. Stahlke, M.; Kram, S.; Mutschler, C.; Mahr, T. NLOS Detection using UWB Channel Impulse Responses and Convolutional Neural Networks. In Proceedings of the 2020 International Conference on Localization and GNSS (ICL-GNSS), Tampere, Finland, 2–4 June 2020; pp. 1–6. [CrossRef]
75. Lian Sang, C.; Steinhagen, B.; Homburg, J.; Adams, M.; Hesse, M. Identification of NLOS and Multi-Path Conditions in UWB Localization Using Machine Learning Methods. Appl. Sci. 2020, 10, 3980. [CrossRef]
76. Jiang, C.; Shen, J.; Chen, S.; Chen, Y.; Liu, D.; Bo, Y. UWB NLOS/LOS Classification Using Deep Learning Method. IEEE Commun. Lett. 2020, 24, 2226–2230. [CrossRef]
77. Ridolfi, M.; Fontaine, J.; Van Herbruggen, B.; Joseph, W.; Hoebeke, J.; De Poorter, E. UWB anchor nodes self-calibration in NLOS conditions: A machine learning and adaptive PHY error correction approach. Wirel. Netw. 2021, 27, 3007–3023. [CrossRef]
78. Xianjia, Y.; Qingqing, L.; Queralta, J.P.; Heikkonen, J.; Westerlund, T. Applications of UWB Networks and Positioning to Autonomous Robots and Industrial Systems. In Proceedings of the 2021 10th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 7–10 June 2021; pp. 1–6. [CrossRef]

79. Niitsoo, A.; Edelhäußer, T.; Eberlein, E.; Hadaschik, N.; Mutschler, C. A Deep Learning Approach to Position Estimation from Channel Impulse Responses. Sensors 2019, 19, 1064. [CrossRef]
80. 3GPP. Study on NR Positioning Enhancements. Technical Specification (TS) 38.857, 3rd Generation Partnership Project (3GPP). 2021. Version 17.0.0. Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3732 (accessed on 1 November 2022).
81. Al-Habashna, A.; Wainer, G.; Aloqaily, M. Machine learning-based indoor localization and occupancy estimation using 5G ultra-dense networks. Simul. Model. Pract. Theory 2022, 118, 102543. [CrossRef]
82. El Boudani, B.; Kanaris, L.; Kokkinis, A.; Kyriacou, M.; Chrysoulas, C.; Stavrou, S.; Dagiuklas, T. Implementing Deep Learning Techniques in 5G IoT Networks for 3D Indoor Positioning: DELTA (DeEp Learning-Based Co-operaTive Architecture). Sensors 2020, 20, 5495. [CrossRef]
83. Gante, J.; Sousa, L.; Falcao, G. Dethroning GPS: Low-Power Accurate 5G Positioning Systems Using Machine Learning. IEEE J. Emerg. Sel. Top. Circuits Syst. 2020, 10, 240–252. [CrossRef]
84. Klus, R.; Klus, L.; Solomitckii, D.; Valkama, M.; Talvitie, J. Deep Learning Based Localization and HO Optimization in 5G NR Networks. In Proceedings of the 2020 International Conference on Localization and GNSS (ICL-GNSS), Tampere, Finland, 2–4 June 2020; pp. 1–6. [CrossRef]
85. Mogyorósi, F.; Revisnyei, P.; Paši´c, A.; Papp, Z.; Törös, I.; Varga, P.; Paši´c, A. Positioning in 5G and 6G Networks: A Survey. Sensors 2022, 22, 4757. [CrossRef]
86. Salamah, A.H.; Tamazin, M.; Sharkas, M.A.; Khedr, M. An enhanced WiFi indoor localization system based on machine learning. In Proceedings of the 2016 International Conference on Indoor Positioning and Indoor Navigation (IPIN), Madrid, Spain, 4–7 October 2016; pp. 1–8. [CrossRef]
87. Sabanci, K.; Yigit, E.; Ustun, D.; Toktas, A.; Aslan, M.F. WiFi Based Indoor Localization: Application and Comparison of Machine Learning Algorithms. In Proceedings of the 2018 XXIIIrd International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (DIPED), Tbilisi, Georgia, 24–27 September 2018; pp. 246–251. [CrossRef]
88. Xue, J.; Liu, J.; Sheng, M.; Shi, Y.; Li, J. A WiFi fingerprint based high-adaptability indoor localization via machine learning. China Commun. 2020, 17, 247–259. [CrossRef]
89. Njima, W.; Ahriz, I.; Zayani, R.; Terre, M.; Bouallegue, R. Deep CNN for Indoor Localization in IoT-Sensor Systems. Sensors 2019, 19, 3127. [CrossRef]
90. Abbas, M.; Elhamshary, M.; Rizk, H.; Torki, M.; Youssef, M. WiDeep: WiFi-based Accurate and Robust Indoor Localization System using Deep Learning. In Proceedings of the 2019 IEEE International Conference on Pervasive Computing and Communications (PerCom), Kyoto, Japan, 11–15 March 2019; pp. 1–10. [CrossRef]
91. Jain, C.; Sashank, G.V.S.; N, V.; Markkandan, S. Low-cost BLE based Indoor Localization using RSSI Fingerprinting and Machine Learning. In Proceedings of the 2021 Sixth International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 25–27 March 2021; pp. 363–367. [CrossRef]
92. Subhan, F.; Saleem, S.; Bari, H.; Khan, W.Z.; Hakak, S.; Ahmad, S.; El-Sherbeeny, A.M. Linear Discriminant Analysis-Based Dynamic Indoor Localization Using Bluetooth Low Energy (BLE). Sustainability 2020, 12, 10627. . [CrossRef]
93. Cannizzaro, D.; Zafiri, M.; Jahier Pagliari, D.; Patti, E.; Macii, E.; Poncino, M.; Acquaviva, A. A Comparison Analysis of BLE-Based Algorithms for Localization in Industrial Environments. Electronics 2020, 9, 44. [CrossRef]
94. Hu, Q.; Wu, F.; Wong, R.; Millham, R.; Fiaidhi, J. A novel indoor localization system using machine learning based on bluetooth low energy with cloud computing. Computing 2021 . [CrossRef]
95. Ji, T.; Li, W.; Zhu, X.; Liu, M. Survey on indoor fingerprint localization for BLE. In Proceedings of the 2022 IEEE 6th Information Technology and Mechatronics Engineering Conference

(ITOEC), Chongqing, China, 4–6 March 2022; Volume 6, pp. 129–134. [CrossRef]
96. Perrone, M.; Pau, D.P.; Piazzese, N.I. Constrained Neural Estimation of Bluetooth Direction of Arrival with Non-Uniform Arrays. In Proceedings of the 2022 IEEE International Conference on Consumer Electronics (ICCE), Virtual, 7–9 January 2022; pp. 1–6. [CrossRef]
97. Bombino, A.; Grimaldi, S.; Mahmood, A.; Gidlund, M. Machine Learning-Aided Classification Of LoS/NLoS Radio Links In Industrial IoT. In Proceedings of the 2020 16th IEEE International Conference on Factory Communication Systems (WFCS), Porto, Portugal, 27–29 April 2020; pp. 1–8. [CrossRef]
98. Gang, Q.; Muhammad, A.; Khan, Z.U.; Khan, M.S.; Ahmed, F.; Ahmad, J. Machine Learning-Based Prediction of Node Localization Accuracy in IIoT-Based MI-UWSNs and Design of a TD Coil for Omnidirectional Communication. Sustainability 2022, 14, 9683. [CrossRef]
99. Zhao, L.; Huang, H.; Su, C.; Ding, S.; Huang, H.; Tan, Z.; Li, Z. Block-Sparse Coding-Based Machine Learning Approach for Dependable Device-Free Localization in IoT Environment. IEEE Internet Things J. 2021, 8, 3211–3223. [CrossRef]
100. Savazzi, S.; Nicoli, M.; Carminati, F.; Riva, M. A Bayesian Approach to Device-Free Localization: Modeling and Experimental Assessment. IEEE J. Sel. Top. Signal Process. 2014, 8, 16–29. [CrossRef]
101. Shit, R.C.; Sharma, S.; Puthal, D.; James, P.; Pradhan, B.; Moorsel, A.v.; Zomaya, A.Y.; Ranjan, R. Ubiquitous Localization (UbiLoc): A Survey and Taxonomy on Device Free Localization for Smart World. IEEE Commun. Surv. Tutor. 2019, 21, 3532–3564. [CrossRef]
102. Patwari, N.; Wilson, J. RF Sensor Networks for Device-Free Localization: Measurements, Models, and Algorithms. Proc. IEEE 2010, 98, 1961–1973. [CrossRef]
103. Nessa, A.; Adhikari, B.; Hussain, F.; Fernando, X. A Survey of Machine Learning for Indoor Positioning. IEEE Access 2020, 8, 214945–214965. [CrossRef]
104. Benbarrad, T.; Kenitar, S.B.; Arioua, M. Intelligent machine vision model for defective product inspection based on machine learning. In Proceedings of the 2020 International Symposium on Advanced Electrical and Communication Technologies (ISAECT), Kenitra, Morocco, 25–27 November 2020; pp. 1–6. [CrossRef]
105. Beltrán-González, C.; Bustreo, M.; Del Bue, A. External and internal quality inspection of aerospace components. In Proceedings of the 2020 IEEE 7th International Workshop on Metrology for AeroSpace (MetroAeroSpace), Pisa, Italy, 22–24 June 2020; pp. 351–355. [CrossRef]
106. Nishiura, H.; Miyamoto, A.; Ito, A.; Suzuki, S.; Fujii, K.; Morifuji, H.; Takatsuka, H. Machine-learning-based Quality-levelestimation System for Inspecting Steel Microstructures. In Proceedings of the 2021 17th International Conference on Machine Vision and Applications (MVA), Virtual, 25–27 July 2021; pp. 1–4. [CrossRef]
107. Oh, S.; Cha, J.; Kim, D.; Jeong, J. Quality Inspection of Casting Product Using CAE and CNN. In Proceedings of the 2020 4th International Conference on Imaging, Signal Processing and Communications (ICISPC), Kumamoto, Japan, 23–25 October 2020; pp. 34–38. [CrossRef]
108. Lin, C.H.; Hu, G.H.; Ho, C.W.; Hu, C.Y.; Kuo, P.C. Press Casting Quality Detection and Analysis Based on Machine Learning. In Proceedings of the 2021 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), Hualien, Taiwan, 16–19 November 2021; pp. 1–2. [CrossRef]
109. Choong, L.M.; Cheng, W.K. Machine Learning in Failure Analysis of Optical Transceiver Manufacturing Process. In Proceedings of the 2021 International Conference on Computer & Information Sciences (ICCOINS), Online, 13–15 July 2021; pp. 160–162. [CrossRef]
110. Kim, J. Development of Visual Inspection System for Assembly Machine. In Proceedings of the 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN),

Prague, Czech Republic, 3–6 July 2018; pp. 859–861. [CrossRef]
111. Schmidt, K.; Rauchensteiner, D.; Voigt, C.; Thielen, N.; Bönig, J.; Beitinger, G.; Franke, J. An Automated Optical Inspection System for PIP Solder Joint Classification Using Convolutional Neural Networks. In Proceedings of the 2021 IEEE 71st Electronic Components and Technology Conference (ECTC), Virtual, 1 June–4 July 2021; pp. 2205–2210. [CrossRef]
112. He, H.; Yuan, M.; Liu, X. Research on Surface Defect Detection Method of Metal Workpiece Based on Machine Learning. In Proceedings of the 2021 6th International Conference on Intelligent Computing and Signal Processing (ICSP), Xi'an, China, 9–11 April 2021; pp. 881–884. [CrossRef]
113. Zheng, X.; Wang, H.; Chen, J.; Kong, Y.; Zheng, S. A Generic Semi-Supervised Deep Learning-Based Approach for Automated Surface Inspection. IEEE Access 2020, 8, 114088–114099. [CrossRef]
114. Tulala, P.; Mahyar, H.; Ghalebi, E.; Grosu, R. Unsupervised Wafermap Patterns Clustering via Variational Autoencoders. In Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, 8–13 July 2018; pp. 1–8. [CrossRef]
115. Hawkins, D.M. Identification of Outliers; Springer: Berlin/Heidelberg, Germany, 1980; Volume 11.
116. Bonomi, N.; Cardoso, F.; Confalonieri, M.; Daniele, F.; Ferrario, A.; Foletti, M.; Giordano, S.; Luceri, L.; Pedrazzoli, P. Smart quality control powered by machine learning algorithms. In Proceedings of the 2021 IEEE 17th International Conference on Automation Science and Engineering (CASE), Lyon, France, 23–27 August 2021; pp. 764–770. [CrossRef]
117. Moldovan, D.; Anghel, I.; Cioara, T.; Salomie, I. Machine Learning in Manufacturing: Processes Classification Using Support Vector Machine and Horse Optimization Algorithm. In Proceedings of the 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet), Bucharest, Romania, 10–11 December 2020; pp. 1–6. [CrossRef]
118. Moldovan, D.; Anghel, I.; Cioara, T.; Salomie, I. Particle Swarm Optimization Based Deep Learning Ensemble for Manufacturing Processes. In Proceedings of the 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, 3–5 September 2020; pp. 563–570. [CrossRef]
119. Dua, D.; Graff, C. UCI Machine Learning Repository; UCI: Aigle, Switzerland, 2017.
120. Zhang, Y.; Peng, P.; Liu, C.; Zhang, H. Anomaly Detection for Industry Product Quality Inspection based on Gaussian Restricted Boltzmann Machine. In Proceedings of the 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), Bari, Italy, 6–9 October 2019; pp. 1–6. [CrossRef]
121. Yuan, F.Q. Critical issues of applying machine learning to condition monitoring for failure diagnosis. In Proceedings of the 2016 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bali, Indonesia, 4–7 December 2016; pp. 1903–1907. [CrossRef]
122. Hu, H.; Nguyen, N.; He, C.; Li, P. Advanced Outlier Detection Using Unsupervised Learning for Screening Potential Customer Returns. In Proceedings of the 2020 IEEE International Test Conference (ITC), Washington, DC, USA, 1–6 November 2020; pp. 1–10. [CrossRef]
123. Vajda, D.; Pekar, A.; Farkas, K. Towards Machine Learning-based Anomaly Detection on Time-Series Data. Infocommunications J. 2021, XIII, 36–44. [CrossRef]
124. Wang, C.C.; Lee, C.W.; Ouyang, C.S. A machine-learning-based fault diagnosis approach for intelligent condition monitoring. In Proceedings of the 2010 International Conference on Machine Learning and Cybernetics, Qingdao, China, 11–14 July 2010; Volume 6, pp. 2921–2926. [CrossRef]
125. Wu, D.; Jiang, Z.; Xie, X.; Wei, X.; Yu, W.; Li, R. LSTM Learning With Bayesian and Gaussian Processing for Anomaly Detection in Industrial IoT. IEEE Trans. Ind. Inform. 2020, 16, 5244–5253. [CrossRef]
126. Liu, Y.; Garg, S.; Nie, J.; Zhang, Y.; Xiong, Z.; Kang, J.; Hossain, M.S. Deep Anomaly Detection

for Time-Series Data in Industrial IoT: A Communication-Efficient On-Device Federated Learning Approach. IEEE Internet Things J. 2021, 8, 6348–6358. [CrossRef]
127. Wang, X.; Garg, S.; Lin, H.; Hu, J.; Kaddoum, G.; Jalil Piran, M.; Hossain, M.S. Toward Accurate Anomaly Detection in Industrial Internet of Things Using Hierarchical Federated Learning. IEEE Internet Things J. 2022, 9, 7110–7119. [CrossRef]
128. Wu, Y.; Dai, H.N.; Tang, H. Graph Neural Networks for Anomaly Detection in Industrial Internet of Things. IEEE Internet Things J. 2022, 9, 9214–9231. [CrossRef]
129. Genge, B.; Haller, P.; En ˘achescu, C. Anomaly Detection in Aging Industrial Internet of Things. IEEE Access 2019, 7, 74217–74230. [CrossRef]
130. Rayana, S. ODDS Library; ODDS: Hong Kong, China, 2016.
131. EN 13306:2017; Maintenance. Maintenance Terminology. iTeh, Inc.: Newark, DE, USA, 2017; ISBN 978-0-580-90370-0.
132. Krupitzer, C.; Wagenhals, T.; Züfle, M.; Lesch, V.; Schäfer, D.; Mozaffarin, A.; Edinger, J.; Becker, C.; Kounev, S. A Survey on Predictive Maintenance for Industry 4.0. arXiv 2020, arXiv:2002.08224.
133. Frankó, A.E.; Varga, P. A Survey on Machine Learning based Smart Maintenance and Quality Control Solutions. Infocommunications J. 2021, XIII, 28–35. [CrossRef]
134. Merkt, O. On the Use of Predictive Models for Improving the Quality of Industrial Maintenance: An Analytical Literature Review of Maintenance Strategies. In Proceedings of the 2019 Federated Conference on Computer Science and Information Systems (FedCSIS), Leipzig, Germany, 1–4 September 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 693–704.
135. Ruschel, E.; Santos, E.A.P.; Loures, E.d.F.R. Industrial maintenance decision-making: A systematic literature review. J. Manuf. Syst. 2017, 45, 180–194. [CrossRef]
136. Lee, J.; Wang, H. New technologies for maintenance. In Complex System Maintenance Handbook; Springer: Berlin/Heidelberg, Germany, 2008; pp. 49–78.
137. Ahmad, R.; Kamaruddin, S. An overview of time-based and condition-based maintenance in industrial application. Comput. Ind. Eng. 2012, 63, 135–149. [CrossRef]
138. Albano, M.; Ferreira, L.L.; Di Orio, G.; Maló, P.; Webers, G.; Jantunen, E.; Gabilondo, I.; Viguera, M.; Papa, G.; Novak, F. Sensors: The Enablers for Proactive Maintenance in the Real World. In Proceedings of the 2018 5th International Conference on Control, Decision and Information Technologies (CoDIT), Thessaloniki, Greece, 10–13 April 2018; pp. 569–574. [CrossRef]
139. Mann, L.; Saxena, A.; Knapp, G.M. Statistical-based or condition-based preventive maintenance? J. Qual. Maint. Eng. 1995, 1, 46–59. [CrossRef]
140. Chemweno, P.; Morag, I.; Sheikhalishahi, M.; Pintelon, L.; Muchiri, P.; Wakiru, J. Development of a novel methodology for root cause analysis and selection of maintenance strategy for a thermal power plant: A data exploration approach. Eng. Fail. Anal. 2016, 66, 19–34. . [CrossRef]
141. Maurer, M.; Festl, A.; Bricelj, B.; Schneider, G.; Schmeja, M. Automl for log file analysis (alfa) in a production line system of systems pointed towards predictive maintenance. Infocommunications J. 2021, 3, 13. [CrossRef]
142. de Jonge, B.; Teunter, R.; Tinga, T. The influence of practical factors on the benefits of condition-based maintenance over time-based maintenance. Reliab. Eng. Syst. Saf. 2017, 158, 21–30. [CrossRef]
143. Theissler, A.; Pérez-Velázquez, J.; Kettelgerdes, M.; Elger, G. Predictive maintenance enabled by machine learning: Use cases and challenges in the automotive industry. Reliab. Eng. Syst. Saf. 2021, 215, 107864. [CrossRef]
144. Sowah, R.A.; Dzabeng, N.A.; Ofoli, A.R.; Acakpovi, A.; Koumadi, K.M.; Ocrah, J.; Martin, D. Design of Power Distribution Network Fault Data Collector for Fault Detection, Location and Classification using Machine Learning. In Proceedings of the 2018 IEEE 7th International Conference on Adaptive Science & Technology

(ICAST), Accra, Ghana, 22–24 August 2018; pp. 1–8. [CrossRef]

145. Zaporowska, A.; Liu, H.; Skaf, Z.; Zhao, Y. A clustering approach to detect faults with multi-component degradations in aircraft fuel systems. IFAC-PapersOnLine 2020, 53, 113–118.
146. Amihai, I.; Gitzel, R.; Kotriwala, A.M.; Pareschi, D.; Subbiah, S.; Sosale, G. An Industrial Case Study Using Vibration Data and Machine Learning to Predict Asset Health. In Proceedings of the 2018 IEEE 20th Conference on Business Informatics (CBI), Vienna, Austria, 11–13 July 2018; Volume 1, pp. 178–185. [CrossRef]
147. Kolokas, N.; Vafeiadis, T.; Ioannidis, D.; Tzovaras, D. A generic fault prognostics algorithm for manufacturing industries using unsupervised machine learning classifiers. Simul. Model. Pract. Theory 2020, 103, 102109. . [CrossRef]
148. Kim, D.; Lee, S.; Kim, D. An Applicable Predictive Maintenance Framework for the Absence of Run-to-Failure Data. Appl. Sci. 2021, 11, 5180. [CrossRef]
149. Zabihi-Hesari, A.; Ansari-Rad, S.; Shirazi, F.A.; Ayati, M. Fault detection and diagnosis of a 12-cylinder trainset diesel engine based on vibration signature analysis and neural network. Proc. Inst. Mech. Eng. Part C J. Mech. Eng. Sci. 2019, 233, 1910–1923. [CrossRef]
150. Lei, Y.; Yang, B.; Jiang, X.; Jia, F.; Li, N.; Nandi, A.K. Applications of machine learning to machine fault diagnosis: A review and roadmap. Mech. Syst. Signal Process. 2020, 138, 106587. [CrossRef]
151. Ince, T.; Kiranyaz, S.; Eren, L.; Askar, M.; Gabbouj, M. Real-Time Motor Fault Detection by 1-D Convolutional Neural Networks. IEEE Trans. Ind. Electron. 2016, 63, 7067–7075. [CrossRef]
152. Sun, W.; Chen, J.; Li, J. Decision tree and PCA-based fault diagnosis of rotating machinery. Mech. Syst. Signal Process. 2007, 21, 1300–1317. [CrossRef]
153. Kimotho, J.K.; Sondermann-Woelke, C.; Meyer, T.; Sextro, W. Application of event based decision tree and ensemble of data driven methods for maintenance action recommendation. Int. J. Progn. Health Manag. 2013, 4, 1–6. [CrossRef]
154. Sánchez, R.V.; Lucero, P.; Vásquez, R.E.; Cerrada, M.; Macancela, J.C.; Cabrera, D. Feature ranking for multi-fault diagnosis of rotating machinery by using random forest and KNN. J. Intell. Fuzzy Syst. 2018, 34, 3463–3473. [CrossRef]
155. Vamsi, I.V.; Abhinav, N.; Verma, A.K.; Radhika, S. Random forest based real time fault monitoring system for industries. In Proceedings of the 2018 4th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 14–15 December 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.
156. Shao, H.; Jiang, H.; Zhao, H.; Wang, F. A novel deep autoencoder feature learning method for rotating machinery fault diagnosis. Mech. Syst. Signal Process. 2017, 95, 187–204. [CrossRef]
157. Haidong, S.; Hongkai, J.; Xingqiu, L.; Shuaipeng, W. Intelligent fault diagnosis of rolling bearing using deep wavelet auto-encoder with extreme learning machine. Knowl. Based Syst. 2018, 140, 1–14. [CrossRef]
158. Li, G.; Deng, C.; Wu, J.; Xu, X.; Shao, X.; Wang, Y. Sensor Data-Driven Bearing Fault Diagnosis Based on Deep Convolutional Neural Networks and S-Transform. Sensors 2019, 19, 2750. [CrossRef] [PubMed]
159. Wang, J.; Mo, Z.; Zhang, H.; Miao, Q. A Deep Learning Method for Bearing Fault Diagnosis Based on Time-Frequency Image. IEEE Access 2019, 7, 42373–42383. [CrossRef]
160. Zonta, T.; da Costa, C.A.; da Rosa Righi, R.; de Lima, M.J.; da Trindade, E.S.; Li, G.P. Predictive maintenance in the Industry 4.0: A systematic literature review. Comput. Ind. Eng. 2020, 150, 106889. [CrossRef]
161. Hwang, S.; Jeong, J.; Kang, Y. SVM-RBM based Predictive Maintenance Scheme for IoT-enabled Smart Factory. In Proceedings of the 2018 Thirteenth International Conference on Digital Information Management (ICDIM), Berlin, Germany, 24–26 September 2018; pp. 162–167.

162. Huang, H.Z.; Wang, H.K.; Li, Y.F.; Zhang, L.; Liu, Z. Support vector machine based estimation of remaining useful life: Current research status and future trends. J. Mech. Sci. Technol. 2015, 29, 151–163. [CrossRef]
163. Abu-Samah, A.; Shahzad, M.; Zamai, E.; Said, A.B. Failure prediction methodology for improved proactive maintenance using Bayesian approach. IFAC-PapersOnLine 2015, 48, 844–851. [CrossRef]
164. Cai, Z.; Sun, S.; Si, S.; Yannou, B. Maintenance Management System Based on Bayesian Networks. In Proceedings of the 2008 International Seminar on Business and Information Management, Wuhan, China, 19 December 2008; Volume 2, pp. 42–45. [CrossRef]
165. Gopalakrishnan, P.K.; Kar, B.; Bose, S.K.; Roy, M.; Basu, A. Live Demonstration: Autoencoder-Based Predictive Maintenance for IoT. In Proceedings of the 2019 IEEE International Symposium on Circuits and Systems (ISCAS), Sapporo, Japan, 26–29 May 2019; p. 1.
166. Lu, Y.W.; Hsu, C.Y.; Huang, K.C. An Autoencoder Gated Recurrent Unit for Remaining Useful Life Prediction. Processes 2020, 8, 1155. [CrossRef]
167. Zhao, R.; Wang, D.; Yan, R.; Mao, K.; Shen, F.; Wang, J. Machine Health Monitoring Using Local Feature-Based Gated Recurrent Unit Networks. IEEE Trans. Ind. Electron. 2018, 65, 1539–1548. [CrossRef]
168. Wang, Q.; Bu, S.; He, Z. Achieving Predictive and Proactive Maintenance for High-Speed Railway Power Equipment with LSTM-RNN. IEEE Trans. Ind. Inform. 2020, 16, 6509–6517. [CrossRef]
169. Rahhal, J.S.; Abualnadi, D. IOT Based Predictive Maintenance Using LSTM RNN Estimator. In Proceedings of the 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Istanbul, Turkey, 12–13 June 2020; pp. 1–5. [CrossRef]
170. Li, H. An approach to improve flexible manufacturing systems with machine learning algorithms. In Proceedings of the IECON 2016—42nd Annual Conference of the IEEE Industrial Electronics Society, Florence, Italy, 23–26 October 2016; pp. 54–59. [CrossRef]
171. Teng, Y.; Li, L.; Song, L.; Yu, F.R.; Leung, V.C.M. Profit Maximizing Smart Manufacturing Over AI-Enabled Configurable Blockchains. IEEE Internet Things J. 2022, 9, 346–358. [CrossRef]
172. Klöter, B. Application of machine learning for production optimization. In Proceedings of the 2018 IEEE 7th World Conference on Photovoltaic Energy Conversion (WCPEC) (A Joint Conference of 45th IEEE PVSC, 28th PVSEC & 34th EU PVSEC), Waikoloa Village, HI, USA, 10–15 June 2018; pp. 3489–3491. [CrossRef]
173. Ye, W.; Alawieh, M.B.; Lin, Y.; Pan, D.Z. LithoGAN: End-to-End Lithography Modeling with Generative Adversarial Networks. In Proceedings of the 2019 56th ACM/IEEE Design Automation Conference (DAC), Vegas, NV, USA, 2–6 June 2019; pp. 1–6.
174. Pu, B.; Li, K.; Li, S.; Zhu, N. Automatic Fetal Ultrasound Standard Plane Recognition Based on Deep Learning and IIoT. IEEE Trans. Ind. Inform. 2021, 17, 7771–7780. [CrossRef]
175. Qolomany, B.; Ahmad, K.; Al-Fuqaha, A.; Qadir, J. Particle Swarm Optimized Federated Learning For Industrial IoT and Smart City Services. In Proceedings of the GLOBECOM 2020—2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6. [CrossRef]
176. Tian, X.; Ma, B.; Meng, C. Research on CMOPSO Particle Swarm Optimization Algorithm for Green Manufacturing Energy System in Ecological Park. In Proceedings of the 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 12–14 March 2021; Volume 5, pp. 2155–2159. [CrossRef]
177. Moriya, T. Machine Learning Approaches Optimizing Semiconductor Manufacturing Processes. In Proceedings of the 2021 5th IEEE Electron Devices Technology & Manufacturing Conference (EDTM), Chengdu, China, 8–11 April 2021; pp. 1–3. [CrossRef]
178. Okafor, N.U.; Delaney, D.T. Application of Machine Learning Techniques for the Calibration of Low-cost IoT Sensors in

Environmental Monitoring Networks. In Proceedings of the 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2–16 June 2020; pp. 1–3. [CrossRef]
179. Rymarczyk, T.; Klosowski, G.; Kozlowski, E. Innovative Methods of Tomographic Image Reconstruction Based on Machine Learning to Improve Monitoring and optimization in Industrial Processes. In Proceedings of the 2019 19th International Symposium on Electromagnetic Fields in Mechatronics, Electrical and Electronic Engineering (ISEF), Nancy, France, 29–31 August 2019; pp. 1–2. [CrossRef]
180. Jiahe, L. Machine Learning Aided Design Optimization for Micro-chip Reliability Improvement. In Proceedings of the 2020 3rd World Conference on Mechanical Engineering and Intelligent Manufacturing (WCMEIM), Shanghai, China, 4–6 December 2020; pp. 131–135. [CrossRef]
181. Kim, J.; Yoo, J.H.; Jung, J.; Kim, K.; Bae, J.; Kim, Y.s.; Kwon, O.; Kwon, U.; Kim, D. Novel Optimization Method using Machinelearning for Device and Process Competitiveness of BCD Process. In Proceedings of the 2020 International Conference on Simulation of Semiconductor Processes and Devices (SISPAD), Virtual, 23 September–6 October 2020; pp. 343–346. [CrossRef]
182. Dogan, A.; Birant, D. Machine learning and data mining in manufacturing. Expert Syst. Appl. 2021, 166, 114060. [CrossRef]
183. Gopaluni, R.B.; Tulsyan, A.; Chachuat, B.; Huang, B.; Lee, J.M.; Amjad, F.; Damarla, S.K.; Kim, J.W.; Lawrence, N.P. Modern Machine Learning Tools for Monitoring and Control of Industrial Processes: A Survey. IFAC-PapersOnLine 2020, 53, 218–229.
184. Wang, C.; Tan, X.; Tor, S.; Lim, C. Machine learning in additive manufacturing: State-of-the-art and perspectives. Addit. Manuf. 2020, 36, 101538. [CrossRef]
185. Wang, L.; Pan, Z.; Wang, J. A Review of Reinforcement Learning Based Intelligent Optimization for Manufacturing Scheduling. Complex Syst. Model. Simul. 2021, 1, 257–270. [CrossRef]
186. Veloso, B.; Gama, J.; Ribeiro, R.P.; Pereira, P.M. A Benchmark dataset for predictive maintenance. arXiv 2022, arXiv:2207.05466.
187. Tosato, D.; Dalle Pezze, D.; Masiero, C.; Susto, G.A.; Beghi, A. Alarm Logs in Packaging Industry (ALPI); Università Studi Padova Tech. Rep. ; Università Studi Padova: Padova, Italy, 2020. [CrossRef]
188. Heged ˝us, C.; Varga, P.; Moldován, I. The MANTIS Architecture for Proactive Maintenance. In Proceedings of the 2018 5th International Conference on Control, Decision and Information Technologies (CoDIT), Thessaloniki, Greece, 10–13 April 2018; pp. 719–724.
189. Jantunen, E.; Zurutuza, U.; Ferreira, L.L.; Varga, P. Optimising maintenance: What are the expectations for Cyber Physical Systems. In Proceedings of the 2016 3rd International Workshop on Emerging Ideas and Trends in Engineering of Cyber-Physical Systems (EITEC), Vienna, Austria, 11 April 2016; pp. 53–58. [CrossRef]
190. Larrinaga Barrenechea, F.; Zugasti Uriguen, E.; Garitano Garitano, I.; Zurutuza Ortega, U. A Big Data implementation of the MANTIS Reference Architecture for Predictive Maintenance. Proc. Inst. Mech. Eng. Part I J. Syst. Control Eng. 2019, 233, 1361–1375. [CrossRef]
191. Di Orio, G.; Maló, P.; Barata, J.; Albano, M.; Ferreira, L.L. Towards a Framework for Interoperable and Interconnected CPSpopulated Systems for Proactive Maintenance. In Proceedings of the 2018 IEEE 16th International Conference on Industrial Informatics (INDIN), Porto, Portugal, 18–20 July 2018; pp. 146–151. [CrossRef]
192. Heged ˝us, C.; Ciancarini, P.; Frankó, A.; Kancilija, A.; Moldován, I.; Papa, G.; Poklukar, Š.; Riccardi, M.; Sillitti, A.; Varga, P. Proactive maintenance of railway switches. In Proceedings of the 2018 5th international conference on control, decision and information technologies (CoDIT), Thessaloniki, Greece, 10–13 April 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 725–730.

193. Papa, G.; Poklukar, Š.; Frankó, A.; Sillitti, A.; Kancilija, A.; Šterk, M.; Heged ˝us, C.; Moldován, I.; Varga, P.; Riccardi, M.; et al. Improving the Maintenance of Railway Switches through Proactive Approach. Electronics 2020, 9, 1260. [CrossRef]
194. Zhao, W.; Goudar, A.; Qiao, X.; Schoellig, A.P. UTIL: An Ultra-wideband Time-difference-of-arrival Indoor Localization Dataset. arXiv 2022, arXiv:2203.14471. https://doi.org/10.48550/ARXIV.2203.14471.
195. Gao, K.; Wang, H.; Lv, H. CSI Dataset towards 5G NR High-Precision Positioning; IEEE DataPort: Piscataway, NJ, USA, 2021. [CrossRef]