

AI-Driven Fault Diagnosis and System Resilience for Offshore Oil Drilling Platforms

Lezhi Chen *

Shixi High School, Shanghai, China

* Corresponding Author Email: chenlezhi08@gmail.com

Abstract. Offshore oil platforms serve as a critical part of the global energy industry and thus work under high risk and complex environments. Severe accidents in the past have shown that the traditional, reactive methods of fault diagnosis are inadequate in terms of concerning the operational safety. The advent of Artificial Intelligence (AI) is leading to a great change of proactive and predictive models as a more effective way of managing these risks. Nevertheless, a holistic assessment between the diagnosis of fault and system resilience in modern contexts is not present. This article splendidly outlines how the process of diagnosis started with a rudimentary method to a modern and high-tech AI-based approach. Moreover, it presents, and discusses a critical concept of system resilience, specifically regarding solving mutual crises like physical equipment malfunctions and cyber-attacks. These concerns are designed to facilitate a proper picture of how these intelligent technologies in place can improve the safety and efficiency of offshore platforms.

Keywords: Fault diagnosis, system resilience, artificial intelligence, predictive maintenance.

1. Introduction

The offshore oil drilling facilities form a significant part of the energy sector in the world. Resource discovery and exploitation of sea oil and gas has emerged as one of the most influential sources in the growth of energy, especially in China, of which offshore generation has become one of the sectors of energy development [1]. Being one of the leaders in offshore resources extraction, the industry constantly widens its perspective to the entire world due to the advent of technologies and is currently stretching into the deep water and ultra-deep-water zones [2].

Nevertheless, deepwater exploration of oil and gas is a risky, capital intensive and technical intensive industry. The offshore drilling history, which dates back to over 100 years, has been characterized by a lot of platform safety events throughout the world, and these include oil and gas spills, explosions and fires, platform capsizing and sinking. As an illustration case, the Deepwater Horizon oil spill, which caused some devastating casualties and losses in the Gulf of Mexico. Moreover, there is the challenging nature of the operation environment, which includes shallow gas and shallow water flows, low temperature at the deep water and unsafe weather like typhoons. Not only can these dangers and difficulties result in significant accidents that pollute the environment and cost the economy, but they also become a significant danger to the lives of the platform staff [4].

Hence, the development of a powerful fault diagnosis system is a serious technical precaution to guarantee the stable work of platforms, minimize unexpected failures, and lessen the threat of significant accidents [5]. Standard fault diagnosis techniques have mostly been based on either expert experience or single signal analysis. Nevertheless, due to the heavy penetration of information technology in the oil and gas industry, the development of new technologies, including big data, cloud computing, and artificial intelligence, has opened new possibilities in overcoming this challenge.

In such a scenario, intelligent technology paradigms based on artificial intelligence (AI) have proven to have boundless application possibilities, which exist through their robust perception, reasoning, decision-making, and execution abilities [7]. Such technologies are creating a transformation in fault diagnosis towards a proactive prediction model rather than a reactive response, and provide a new technical future in which offshore platforms can operate safely and efficiently.

Although there is a considerable amount of relevant research, no systematic review that elucidates fault diagnosis and system resilience has yet been done. Thus, the purpose of this review is to

systematically summarize the transformation of the traditional methods of fault diagnosis to modern AI-based solutions. It also aims to explain the key idea of System Resilience especially concerning the compound risks, that is dealing with both physical failures and cyber-attacks, on systems such as communication networks.

In the first section of the paper, the author will identify the conventional ways of monitoring and the potential difficulties of the critical subsystems of a system, which are pressure monitoring, power supply, and communication. It will then examine the critical application of artificial intelligence in diagnosis of fault and predictive maintenance. Lastly, the paper shall end up with a conclusion of the results and how AI can be used in the future to improve the overall fault diagnosis potential and system resilience of the drilling platforms.

2. Fault Diagnosis for Offshore Oil Drilling Platforms

2.1. Pressure Monitoring Systems

The downhole pressure during the oil drilling project is also an essential parameter which is directly associated with the stability of the well bore and the safety of drilling. The essence of pressure monitoring systems, in most instances being installed at the terminus of pipes, is the real-time monitoring of variations in pressure in the wellbore to avert and avoid the occurrence of blowouts [8]. Kick is one of the most dangerous accidents in drilling which is caused by the abnormal downhole pressure, basically, the falling of hydrostatic pressure of fluid body in the wellbore and being below the pressure under which the formation pore is opened. This unequal gives fluids, which are invading fluids, an opportunity to be present within the wellbore [9]. Unless early measures are taken, these invading fluids may quickly rise, reaching a devastating blast out that poses a fatal risk to people, equipment, and the environment [10]. Moreover, the leaks of downhole casings, a problem with the management of casing integrity of the wellbores, may also lead the toxic gases to the surface via the annulus, which is also a very serious issue provoked by the pressure anomalies [11]. Continued and precise monitoring and diagnosis of downhole pressure is thus a key ingredient in the endeavor to realize safe and effective drilling.

Based on the literature available, the section will discuss the various developments of downhole pressure monitoring and diagnostic technology in detail with emphasis on the history of development of the sensors which form the early sensors and intelligent modeling and predictive techniques.

In the oil drilling industry and more specifically in as far as the wellbore safety problems related to pressure, fault diagnosis is increasingly moving towards non-traditional basis of diagnosis that is based on experience and manual analysis to automated, and intelligent and data-based models.

Fault diagnosis is based on downhole pressure data. Conventional monitoring has been based on pressure sensors on the end of the pipeline and the wellhead which are pivotal devices to the early warning of kicks [8]. Technology has also seen the use of Measurement While Drilling (MWD) and Logging While Drilling (LWD) technology such that drilling engineers can now access downhole continuous parameters, (annular pressure, temperature and between-cut-off position) in real time.

According to the existing studies, MWD and LWD technologies have already been implemented in practice, and they provide multi-parameter measurements that can substantially increase the safety of deep and ultra-deep wells in their functioning. The high demands of sensor performance are imposed on the downhole conditions during deep well operations, which is a high temperature and pressure environment [12]. According to these approaches of taking measurements during the drilling, engineers may access continuous drilling information, which can be used to support real-time data to make further diagnosis.

There are several factors that cause the down hole pressure changes, among them the nature of the formation and the ability of the drilling oil, the different changes in speed of the pump. The conventional monitoring tools are only capable of detecting the deviation of pressure in its present form but are ineffective in anticipating the outcome of the risk. Researchers have started to adopt

mathematical modeling and intelligent algorithms to forecast pressure behavior to find the solution to the objective of early detection and early control [13].

On the subject of downhole pressure control, MP Vega et al. in their article with the title of the article, Smart Monitoring and decision making in regulating well bottom hole pressure during drilling oil wells, had suggested an intelligent monitoring and decision making system. It is a system that employs real time measurements and algorithms to make sure that down hole pressure is maintained within a safe operation range and to successfully suppress kicks. The technique entails continual examination of the real time information to dynamically reduce downhole annular pressure to address the usual loads [9].

As the artificial intelligence technology evolves, the models of AI-based agents are proving to be highly promising in the fault diagnosis in the oil drilling industry. It has been shown that predictive analytics and generative AI are currently increasingly used to streamline the process of wellbore stability control and detecting hazards. Predictive analytics will allow operators to predict when an issue will occur, thus making failures less likely and increasing safety [14]. Proactive maintenance is possible through the use of AI algorithms to find patterns and anomalies in equipment-related data. In the drilling platforms, this method may be applied in testing the faults in the downhole pressure systems [15].

A kick should be identified early so that well control operations may be conducted successfully. Available literature has shown that logging-while-drilling (LWD) data are able to detect the variation of the formation behavior prior to a kick. Kick data obtained through real time drilling and kick models can be used to enhance kick response measures. This can give a clear source of data to be used when calculating intelligent agents [8].

It is possible to use deep learning and pattern recognition of real-time downhole data, including drilling fluid flow rates, pump pressure, and pit gain with the creation of intelligent agents grounded on big data and machine learning. This allows the detection of the abnormal signals during the start of a kick, which can even be unusual even before the traditional monitoring means reminds the user of an alarm. As we can see, deep learning, such as Recurrent Neural Networks (RNNs) are capable of handling complex and unstructured time-series-based data, and thus, it is a suitable method of detecting anomalies and predicting real-time pressure data [15].

The use of intelligent agent technology has got immense benefits. To begin with, to get early warning, AI models can ascertain normal pressure behavioral patterns from massive quantities of sensor information and recognize the minor and non-linear deviations. This makes it possible to detect and hyperglycemic fluid influx at the initial level [13]. Secondly, the efficiency of decisions made by intelligent agents is great. They are capable of delivering diagnostic results and decision making advice to drilling engineers in real time that can be interpreted and includes an optional adjustment in the speed of pumps or modification in the parameters of drilling. It also assists the drilling team to respond quickly and accurately [9]. Lastly, operational risks are minimized with the use of these agents. By means of active forecasting and avoiding of severe problems, such as wellbore instability and kicks, they may greatly decrease the overall operational risk, allowing to protect both equipment and people with a high level of credibility [8][14].

Nevertheless, the implementation of the approach is accompanied by numerous issues, such as the data quality problem, cybersecurity threats, and the necessity of providing the personnel with training on new technologies [14].

Besides monitoring and intelligent analysis of the surface, research into downhole systems of blowout prevention is also being developed. In their work on Research and application of downhole blow out prevention system during drilling, L. Wei et al. provided the definition of a while-drilling downhole blow out prevention system and their functions. They also pointed at its benefits in guaranteeing safe well control especially when drilling under the platform through sensitive formations. This physical prevention system together with an intelligent monitoring system is a complete wellbore safety assurance system [13].

The increased integration in the future of pressure monitoring systems will be dependent on the amalgamation of multi-source, heterogeneous data, where the integration of details like down hole pressure, temperature, flow rates, mud properties and geological data are all included. No longer will intelligent agents be limited to only one instance of diagnosis of the faults, but rather they will develop to be collaborative in multi-agent systems. Such systems will have a collective control over wellbore stability, optimisation of drilling parameters, and maintenance requirements and eventually give the vision of a smart oil and gas wells, and hence a holistic improvement of the safety and efficacy of the drilling operations [16].

2.2. Pressure Monitoring Systems

Being complex and massive industrial systems, in which the unstable operation is based on the stable existence of offshore oil drilling platforms, the effective power supply system is the key to the stable functioning of offshore oil drilling facilities. Not only does this system supply power to both core drilling equipment, including drilling rigs, mud pumps and the like, but also supplies indefinite electrical power to the life support, communication and safety system of the platform. An autonomous power supply system on an offshore drilling platform is usually an isolated system that supplies power as compared to the onshore power grid. It also works under a severe environment with great variation in loads, and this imposes very high requirements on the reliability of the system.

The specifics of the existence of a drilling platform power supply system can be identified in a number of ways. First, it needs to drive a significant amount of high-power actuators, including the primary drilling rig equipment running on a primary DC drive that has massive control precision and power needs. Second, the system is a combination of both an adjustable and non-adjustable actuator which contributes to tougher coordination and management of the system. Conventional systems of power supply are manual and require periodic maintenance in order to be stable, but this method is frequently ineffective in situations involving sudden failures [18].

An offshore drilling platform has a power supply system exposed to various possible faults that have the potential to cause disruption of production, damage equipment, and even safety accidents. These weaknesses are mainly as a result of its dynamic and fast changing operating environment.

To begin with, since the dynamism in the load of the drilling process dramatically swings, especially the frequent starts and stops of high-power processes such as the main drives, the power grid becomes acutely vulnerable to harsh oscillations in the voltage and the unsteadiness. This instability may disrupt electronic devices which are sensitive to the platform and disrupt their usual functioning and lead to other failures of the system. Secondly, the power supply system is too susceptible to overloads and short circuiting. The dynamic and strenuous air of the drilling activities exposes the system to be vulnerable whenever it is subjected to over load operations. An example is that continuous faults on the transformers may occur because of overloading, and one area will experience localized outages. Short circuits represent the most dangerous type of faults, because they may lead to a lot of damage to equipment and uninterrupted downtime. Moreover, with the growth in operating time, the important parts in the power supply system including distribution transformer and power electronic equipment become aged and their performance decays [19]. This degradation in internal performance can however remain unnoticed in the traditional models of maintenance unless there is a total breakdown, which is then rectified in real-time, which is in fact not a viable option in current models of maintenance because of this fact.

To overcome the limitations of the conventional methods of maintenance and increase the reliability of the power supply system, the use of intelligent diagnostic approaches, which are predicated on the data-driven and artificial intelligence methods, has become a common tendency. The fundamental aspect of this strategy is sensors and the Internet of Things (IoT) to monitor the real time operations of the system, alongside the big data analytics and AI algorithms to predict faults and conduct diagnoses [17].

The dense and real-time mode of gathering data in the power supply system is the initial stage in intelligent diagnosis. And these parameters are voltage, current, frequency, temperature, and vibration,

among others. The data is gathered using Internet of Things (IoT) sensor nets, e.g., using long-range LoRa-IoT technology, and fed to a communication architecture, e.g. Software-Defined Networking (SDN), to manage the data through local or cloud-based control. A monitoring system like this in real time also offers the support of critical data that is used in predictive maintenance, thus lessening unexpected downtime.

Data-driven fault diagnosis employs AI algorithms to learn and extract patterns from enormous datasets of operational data, which in turn allows classifying, predicting, and learning how to automatically recover the fault. AI models are more accurate and efficient when compared to the conventional techniques that use fixed thresholds and human judgment to pick up complex patterns in the data that the formal techniques are not effective at detecting.

These traditional methods discussed here are basically of two broad categories: Reactive Maintenance and Preventive Maintenance. Reactive Maintenance, which is basically a run to failure system, is a maintenance approach whereby the repair process is not done until the equipment has failed i.e. Most of the time, it results in unplanned downtime that is very expensive and unsafe. Although Preventive Maintenance is a progressive step, it is based on a fixed frequency, and statistical conditions, i.e. Mean Time Between Failures, MTBF. This method often creates unnecessary maintenance of the equipment that is in good condition or cannot predict any unforeseen breakdown, which consequently results in underutilization of resources [22].

By contrast, Predictive Maintenance AI is the implementation of a paradigm shift, shifting the idea of reaction toward the prediction. To provide a full-fledged depiction of the great benefits of the support offered using the latest method, the given table will compare the traditional and AI-supported maintenance based on various essential aspects, such as maintenance model, timing, cost-effectiveness, downtime, and quality. This comparison (Table 1) is used to bring to the limelight the revolution that artificial intelligence can bring in this field.

Table 1. Comparison: Traditional vs. AI-Driven Maintenance

Comparison Dimension	Traditional Maintenance (Reactive & Preventive)	AI-Driven Predictive Maintenance
Maintenance Model [17]	Passive, Reactive: Action is taken after a failure (reactive) or based on a fixed schedule (preventive)	Uses continuous monitoring and data analysis to predict and act before a failure happens
Maintenance Timing [20]	After a failure or at fixed intervals, ignoring the actual health of the equipment	Performed when a failure is predicted to be imminent, allowing for optimal intervention timing
Basis for Decision [17]	Historical experience, statistical averages (e.g., Mean Time Between Failures), and predefined rules or thresholds	Real-time sensor data, big data analytics, and machine learning/AI models
Data Utilization [21, 22]	Low data utilization, often relying on offline or manual analysis, unable to handle complex, dynamic data	Big Data and IoT-driven: Integrates massive, multi-dimensional real-time data streams for comprehensive analysis
Accuracy [17]	Low: Often leads to false alarms or missed faults, resulting in a high rate of misjudgment	High: Fault prediction accuracy reaches 85%-95%, with specific applications achieving up to 90% or 96.1%
Downtime [20, 21]	Long unplanned downtime, causing significant production interruptions and operational losses (NPT)	Minimized downtime: Unplanned outages are converted to scheduled maintenance; power system restoration time is cut by up to 60%
Cost-Effectiveness [20, 21]	High cost: Includes emergency repairs, production losses, and	Highly cost-effective: Significantly reduces total operational costs by

	unnecessary expenses from preventive work	optimizing resources and cutting failures by 40%
Resource Optimization [21, 22]	Inefficient: Wastes manpower and spare parts due to over-maintenance or emergency repairs	Highly optimized: Allocates maintenance resources on an as-needed basis, maximizing asset utilization and output
Advantages [17]	Reactive: Very low initial cost. Preventative: Minimizes certain unforeseen failures in contrast to reactive; intuitive reasoning.	Provides tremendous enhancement of reliability and safety. Reduces the operation cost and downtime. Maximizes the value of assets and increases life. Transitioning from the act of passive reaction to proactive value creation.
Disadvantages [20]	Reactive: Extremely high downtime costs and safety risks. Preventive: Impossible to eliminate failures and is very inefficient in terms of over-maintenance.	Higher initial investment. Needs data and infrastructure that is of high quality. Models may be black boxes and they demand expert knowledge.

The lifeline of such an offshore drilling platform is the power supply system that can guarantee its efficient functioning. The conventional reactive or preventive maintenance systems cannot be relied upon to satisfy the increased complexity and reliable nature of such systems. The change toward active prediction and not reactive response can be conducted by implementing such intelligent diagnostic systems of the Internet of Things (IoT), big data, and artificial intelligence. The most sophisticated technologies like artificial neural networks, digital twins, and self-healing grids have the potential to contribute to a higher accuracy of fault detection, less downtime, and minimized maintenance costs [20].

Despite the fact that there is still room to improve such issues as model interpretability, data integration, and cybersecurity, the perspectives of AI implementation to the power supply systems of the drilling platforms are conscious. This is one of the directions of the future digital and intelligent future of the drilling industry. Besides enhancing the resilience and efficiency of the platform, the transition keeps the exploration and production of energy in the harsh conditions uninterrupted and consistent.

2.3. Communication Systems

Offshore oil drilling stations represent a highly sophisticated and hazardous critical infrastructure requiring safe and efficient functioning in harsh conditions, thus becoming more dependent on the usage of advanced technologies. A stable, efficient, and secure communication system is absolutely essential to the implementation of such advanced functions as predictive fault diagnosis and automated collaborative operations, as well as remote control and onshore expert help. These so-called critical communication systems as some have been outlined in a study by A.M. Ammar et al. in their paper, *Optimizing Critical Communication Systems for Offshore Oil and Gas Operations through Computational Methods*, are not only meant to keep the personnel safe and ensure coordination of the production processes, but in fact they are the basis through which smart platform operations can be provided [23].

The success of a predictive maintenance system is supported by the processes of constant gathering and real-time processing of the large streams of sensor data, which are exchanged by widely-spread Industrial Internet of Things (IIoT) devices. At the same time, the organized functioning of different units of the industrial control system is based on specialized communication sources that guarantee the effectiveness of transferring control waves and the timely feedback regarding the equipment state.

Basically, the communication system is the connector between the physical drilling platform and the network. Any type of disruption, be it caused by a technical failure or a cyber-attack, can cause

data silos, loss of control and even disastrous outcomes. Ransomware attacks, in particular, are very troubling, since the recovery process in question is further reliant on the presence of the communication channels. This reliance underscores the pivotal position of the communication system in emergency response and post disaster recovery [24]. Thus, the integrity, availability and confidentiality of communication links have become one of the main requirements to provide the safe, intelligent and efficient functioning of the current offshore oil drilling platforms.

The disruptions and latency due to non-malicious factors must be thoroughly analyzed first before a comprehensive vulnerability assessment of the communication system of a drilling platform can be conducted. These problems, rooted in the very harsh conditions of the physical environment around the platform, the very nature of the appliances, and the pressure of the data flow, are the totality of the underlying problems of communication reliability.

To begin with, the severe marine environment is the major threat to the stability of communication connections. Natural signal attenuation is simply caused by the long geographical distance between a mainland and an offshore platform. On top of this, the very platform, being a massive and thick metallic structure, introduces extreme multipath effects, reflection and shadowing. The result is regions of inconsistent signal strength and even dead zones during the process of communication all over the platform. The unfavourable weather conditions like humid weather, salt spray and heavy rain, which additionally absorb and scatter radio waves further deteriorate the signal quality.

Also, according to the research conducted by A.M. Ammar in the article entitled *Optimizing Critical Communication Systems for Offshore Oil and Gas Operations via Computational Methods*, the presence of strong electromagnetic interference (EMI) due to on-platform devices, such as radar systems and high-power motors, can disrupt communication signals, which leads to a significant increase in the rate of errors in the transmission of data [23]. Thus, even in perfect circumstances, the communication system on the platform will have to constantly struggle against the severe electromagnetic environment full of noise and interference.

Secondly, the hardware systems that comprise the periphery of the sensing network of the platform, especially Wireless Sensor Networks (WSNs) have physical and resource-based vulnerabilities. According to the academic paper by D.R. Raymond et al., *Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses*, the limitations of resources allocated to WSN nodes are explained. These small contrivances are common buy with limited energy sources and are usually operated using batteries. Constant transmission, reception and data processing of signals contribute to faster energy depletion resulting in node silent failure and consequently introducing permanent or intermittent gaps in data collection.

Moreover, sensors used in critical equipment are very vulnerable to intensive vibrations, high temperatures, and corrosion, hence physical damage is a normal phenomenon. The characteristics of these single-point devices failures include communication cavities that are random and unpredictable; this creates a serious difficulty in the fault diagnosis model based on complete data chain. Besides sensors, any core network infrastructure such as switches, routers, antennas, cables, etc. may fail because of corrosion, vibration, or aging. Network segmentation, which occurs due to the failure of any one critical node, leaves vast spaces of equipment inoperable [25].

Meanwhile, the growing amount of data traffic is a new challenge as the degree of automation and intelligence on platforms constantly increases. This problem of network congestion, described by I. Yaqoob et al. in their article titled *The rise of ransomware and emerging security challenges on the Internet of Things*, is specifically topical on drilling platforms. The combination of information provided by high-frequency vibration sensors, high-definition video surveillance and control commands (in real-time) and a huge number of equipment status parameters form a huge data flood. When the volume of these streams of data flowing simultaneously over the network rises beyond the switching capacity or bandwidth constraints of the network, a congestion ensues. This results in lost packets, a significant rise in the transmission latency and timing disturbances.

All these factors do not work in opposition but create a complex network of issues, resulting in signal degradation, loss of packets, and latency in communication. In the case of a fault diagnosis

system, it implies the incoming stream of data are incomplete, lagging and possibly distorted. This not merely grossly impairs the prediction of faults in the system before they start, effectively reducing it to a managing mode, rather than a predicting one, but more importantly, it can result in the loss of the best intervention window at the time of an emergency since the control commands cannot be relayed in a timely manner. This circumstance can enable the possible equipment breakdown to turn into a disastrous safety event.

These design flaws of their operations are not merely serious challenges that need to be surmounted in the day to day running but offer vulnerabilities that can be exploited by cyber-attackers thus increasing the devastating effects of the offending attacks.

Nevertheless, the communication interruptions, latency, and security issues brought by electronic assaults are increasingly more devastating and hidden as compared to the non-malicious factors. The contemporary cyber threat environment is becoming more dynamic, with highly organized and fully funded attackers, constantly changing their Tactics, Techniques, and Procedures (TTPs).

The attackers can no longer be confined to one point of entry; they are now using multi-vector attack strategies and exploiting vulnerabilities in the physical, network, and application layers at the same time. Some of the most important threats include so-called zero-day attacks that use the unknown weaknesses that have been discovered in the software or hardware but there is no patch. This makes conventional defense strategies virtually useless.

With ransomware in combination with a zero-day vulnerability, the destructive capabilities are multiplied several times. Attackers are capable of bypassing all known defenses to issue direct encrypted data on critical control systems, and communication nodes that can paralyze the operations of platforms. This type of attack not only leads to communication breaches but also a total loss of control over the major functions of the platform, which is a direct threat to the safety of production and human life [24].

Denial-of-Service (DoS) attacks represent one of the first attacker approaches that attack the communication availability directly.

Signal jamming is the most direct kind of attack at the physical layer. Through the production of high-power noise, an attacker can easily subdue or distort valid communication signals resulting in massive packet corruption and communication outages.

However, the techniques of attack are more diverse at the link and network levels. The denial-of-sleep attack, specific to Wireless Sensor Networks (WSNs), is based on forged control message (i.e., spoofed RTS (Request to send)) messages being sent by the attacker to force low-power nodes to spend all their power in a high-energy receiving state. This quickly exhausts their battery capacity leading to the permanent failure of the node and blind spots in data collection [25].

On the other hand, routing disruption attacks defeat the paths of packets by introducing counterfeit routing data with the intent of generating black holes or wormholes. This leads to either fragmentation or full circle data loss of packet and very high latency [26]. Moreover, flooding attacks are characterized by transmitting a huge amount of junk packets to either saturate the network bandwidth or manage to saturate the processing resources of important devices such as switches and routers to the extent that legitimate communication could not occur. When combined, these multi-layered DoS attacks can directly result in the total or crippling of the communication links, subsequently interrupting the data stream needed by the fault diagnosis system and incapacitating it to successfully and promptly respond to the operational status of the platform.

At the same time, Industrial Control Systems (ICS) and adjacent communication protocols, as well as the ever more common Industrial Internet of Things (IIoT) edge devices, make them essential points of entry for cyber-attack. Such systems are usually poorly designed with security weaknesses, which give a rich pool of opportunities to attackers. Kaspersky has released a report on its statistics of vulnerabilities in the industrial control system components, which puts the prevalence of critical vulnerabilities at 97 percent in terms of buffer overflows, hard-coded credentials, and cross-site scripting.

A study of the vulnerability to cyber attack of control communication protocols in industrial operations by Y. Xu et al. in Review on Cyber Vulnerabilities of Communication Protocols further systematically exposes the fact that most widely used and popular control protocols, including DNP3, Modbus, and IEC 61850, do not protect themselves with authentication, authorization, and encryption. This means that often plaintext transmissions are made of sensitive control commands and device data, enabling an attacker to easily eavesdrop on, compromise or replay communications. This allows them to implement Man-in-the-Middle (MITM) attacks, and compromise data integrity and confidentiality.

The recent introduction of the IIoT poses a new target point as edge gateways at intersections between Operational Technology (OT) and Information Technology (IT) networks are becoming a new point of focus. M. Al-Hawawreh et al. in Targeted Ransomware: A New Cyber Threat to Edge System of Brownfield Industrial Internet of Things and I. Yaqoob et al. in The rise of ransomware and emerging security challenges in the Internet of Things have both focused on the threat of ransomware against these edge devices.

Firmware vulnerabilities, weak authentication or open service ports can be used by attackers to remotely implant malware. This gives them not just data to be encrypted with the intent of a ransom, but it is also able to alter the functionality of the devices by means of so-called "Logic Locking," such as horribly shutting a cooling pump off to prevent the device from functioning or such as physically changing the safety thresholds, directly converting a cyber-attack into a physical hardship. These particular weaknesses make communication channels in remote operations extremely prone to hijacking, which may result in data alteration, forging of commands, or failure of the entire communication operation, which are crippling to the security of operations of the platform.

Ransomware is the most important threat to the communication systems availability and data integrity of all cyber-attacks. It does not just aim to impair services but has a sort of ability to hold the digital assets and operational capability in totality of the platform as a hostage. According to research papers by M. Humayun et al., e.g., Internet of Things and Ransomware: Evolution, Mitigation and Prevention and The Rise of Ransomware and Emerging Security Challenges in the Internet of Things, ransomware directly denies operators control over the system, as well as access to data, by encrypting important data and system files or locking user interfaces.

Communication networks have a dual purpose in the ransomware attack as they can be both a victim and a propagation medium. Attackers often select key nodes, which are of OT and IT networks, like IIoT edge gateways as the initial entry point. Upon success, the ransomware will be able to use the communication connections to spread laterally within the platform, infecting more critical systems.

These are devastating effects. On drilling platforms, which are very dependent on real-time feeds of data, in their article Targeted Ransomware: A New Cyber Threat to Edge System of Brownfield Industrial Internet of Things, M. Al-Hawawreh et al. observe that a lag of a couple of seconds can be devastating. As soon as the servers handling control commands or transferring high alert sensor data are ransomwareed, the whole mechanism of monitoring and response is shocked on the spot. It is not just a communication glitch or a glitch in communication, it is the paralysis of the whole operation.

It may cause enormous financial loss, reputation destruction, and organizational debacle causing massive service disruption. Thus, an attack of ransom worsens the security of the system of communications not only a technical problem but a serious operational challenge endangering the existence of the platform [24].

In summary, the communication system in an offshore oil drilling platform is exposed to a three-fold set of threats that is a result of physical condition, equipment constraints, and mischievous cyber-attacks. These problems include signal loss and interruption by adverse weather conditions and hardware wear, network intrusion such as DoS and Man-in-the-Middle directly impairing availability and integrity of communication, and the final problem, ransomware, is planned to take down the whole system of operation.

All these aspects make up a dynamic and intricate risk environment. Communication breakdowns at any level may result in data discontinuity, control instructions being slow or twisted, therefore weakening fault-diagnostic facilities and making a disaster unavoidable.

Thus, the safety and stability of the communication system must be a key to the safe and intelligent platform operation.

The research below presents high-level solutions to both the performance degradation and high-tech cyber-attacks in this field. In the case of Performance Faults, such as reduction of Link Quality Estimation, network congestion, and hardware aging, the main issues are the difficult marine environment and resource limitation of edge equipment. The basic diagnosis technique is moving out of the balance line monitoring to the LQE predictive diagnosis. Single physical metrics are an important tool used in traditional LQE, limiting its use. Current approaches are using Machine Learning models, specifically Deep Learning models (such as MLP or LSTM) to combine multi-dimensional features such as RSSI, SNR, LQI, PRR, and predict non-linear link degradation before it fails entirely [27]. As an example of this, Fiber Optic Sensing Networks test the new approach to data structure analysis to substitute expensive components such as the Optical Time Domain Reflectometer in order to detect fault points in real-time and improve the diagnostic efficiency and cost. In case performance degradation is observed, the mitigation methods emphasize on the use of redundancy and reconstruction of a path to reestablish the absorbing and recovery potential of the system [28]. This is achieved in FOSN by smart algorithms, including greedy paths, that steer the optical switches to quickly repath traffic to the best redundant path, and complete self-healing in milliseconds [29]. In wireless systems, it would be equated to the Self-Healing capability of SON, where compensation is attained by optimizing the coverage-area or SINR by automatically reconfiguring the neighboring cell parameters [30].

In the case of Security Attacks, such as DDoS, Man-in-the-Middle (MITM), malware, such as ransomware, and zero-day attacks, hybrid and multi-layered strategies should be the gateway to diagnosis. Entropy and Connection rate based statistical techniques are effective in detecting DDoS or DoS attacks, and are low cost and can be applied to real time traffic monitoring of flooding traffic. Zekri et al. have shown the banality of integrating information theory-based classification algorithms and signature identification to produce high-accuracy flood attack diagnosis in their study on DDoS attack detection on the basis of machine learning classification in cloud computing systems [31]. Diagnosis in order to overcome MITM attacks, which are usually covert, has moved beyond network packets to adopt the MIDS, Measurement Intrusion Detection System, paradigm. This method identifies network-based deception through observation and detection of abnormal behavior in physical sensor measurements by SCADA systems [32]. In the case of Zero-day and Unknown Attacks, Anomaly-based IDS are preferred when signature-based systems cannot deal with them. These are systems, which are based on models such as AutoEncoder or One-Class SVM, which are trained only on normal traffic and will tag any significant changes as an unknown anomaly [33]. Moreover, in the study Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning, Ferrag et al. proved the effectiveness of federated learning on a distributed IIoT setting to overcome the problem of data privacy and resource availability without compromising the high diagnostic accuracy of federated learning with complex attacks. Mitigation of attack is based on Automated Incident Response after diagnosis. In the case of DDoS/DoS, Centrally managed control over SDN architecture ensures fast response systems, e.g. by deploying malicious packet dropping rules, port paneling, or flow diversion. In case of MITM and malware, The system needs to do fault localization to estimate and isolate infected nodes in a limited time frame to avoid the spread in lateral direction and to start a structural adaptation measure such as redundant component replacement to enable timely service restoration.

3. Conclusion

This paper has critically reviewed and discussed the technological development of the topics of fault detection and system maintenance of offshore oil drilling platforms. According to the research, with the continually growing complexity of platform structures, more extreme operational environments, and the constant growth of threats to cybersecurity, the traditional operational and maintenance models, which are based on absolute norms and human experience, have proven their own inadequacies. Such traditional techniques are reactive and can hardly handle multi-factor and complex faults whose latencies are long and in particular those caused by stealth malicious cyber-attacks.

The main thesis of this paper lies in the fact that the key way of getting over these issues and ensuring safe and efficient operation of platforms is to make a smart change fueled by artificial intelligence, the Internet of Things, and big data analytics. Not only is it a technological upgrade but it is also a paradigm revolution in maintenance as it shifts off the post-failure repair and towards pre-emptive warning, even offensive onslaught. Having critically examined three key systems, namely, the pressure monitoring system, the power supply stability system and the communication security system, the paper has demonstrated the huge potential and usefulness of AI in precisely predicting the occurrence of risks in kicking, maximizing the energy savings and reliability of power systems, and creating dual cyber-physical resilience in communication systems.

Going forward, the ability to have an innovative generation of offshore drilling platforms that are intelligent, autonomous and very resilient will be guided by a few significant directions. To begin with, the Digital Twin technology will be used to run integrated analysis and simulation. Through the development of a virtual model, which works in line with the physical platform, it is possible to combine and study various data that is sourced by different sources, which include equipment, processes, and the power grid. This model of the virtual world will give a secure response of testing different failure scenarios or cyber-attack cases to make better appraisals of risks and streamline emergency response plans to a greater extent. Second, the explainable AI (XAI) should be developed to mitigate the black box challenge of AI models. This technology aims to transparently structure the decision-making process of the AI to make its results of the diagnostic process traceable. Indicatively, where the system raises a warning, it is able to clearly state the data anomalies which raised the alert. This is necessary in improving operator trust and helping them do root cause analysis. Thirdly, system design will stop focusing on a single area, which is establishing high reliability of avoiding failures, but focus on establishing high resilience of facilitating quick recovery. This includes putting in place an active defense mechanism whereby AI identifies various threats automatically, i.e. aging equipment and cyber attacks, and in a short time carry out a counter attack, i.e. isolating equipment, switching and adjusting them. This will put the ability of the system to heal itself thus reducing down-time. Lastly, to maintain the overall complexity of the platform, intelligent agents that are distributed where various agents interact will be created. Rather than using one, huge centralized AI, special agents will be used on the various subsystems, like drilling and power supply. Such agents get an opportunity to cooperate and exchange data, and the resources of the platform are managed more efficiently and enhance the efficiency and stability of the decision-making process.

Conclusively, the system of artificial intelligence is radically transforming the system of some operational, maintenance, and safety assurance of the offshore oil drilling systems. The further research will be dedicated to the state-of-the-art areas including digital twins, reliable AI, autonomous protection, and collaborative intelligence. The final vision will be to build intelligent oil and gas wells with the functioning of deep perception, intelligent decision-making, and autonomous recovery, which will guarantee the safe, efficient, and sustainable exploration and production of national energy amidst the constantly evolving challenges.

References

- [1] YANG Jin, LI Lei, SONG Yu, TONG Gang, ZHANG Minghe, ZHANG Hui. Current status and prospects of offshore oil and gas drilling technology development in China[J]. *Acta Petrolei Sinica*, 2023, 44(12): 2308-2318.
- [2] Pinder D. Offshore oil and gas: global resource knowledge and technological change[J]. *Ocean & Coastal Management*, 2001, 44(9-10): 579-600.
- [3] WANG Youhua, WANG Wenhai, JIANG Xingxun. Challenges and Countermeasures for Deepwater Drilling Operations in the South China Sea [J]. *Petroleum Drilling Techniques*, 2011, 39(2): 50-55.
- [4] BAO Mutai, PI Yongrui, SUN Peiyan, et al. Research Progress on the Response to the "Deepwater Horizon" Oil Spill in the Gulf of Mexico [J]. *Journal of Ocean University of China (Natural Science Edition)*, 2015 (1): 55-62.
- [5] LIU Kan, ZHOU Shasha. Analysis of Safety Design for Online Fault Monitoring of Key Equipment on Offshore Oil Drilling Platforms [J]. *Chemical Safety and Environment*, 2022, 35(18): 21-24.
- [6] Ribeiro L, Barata J. Re-thinking diagnosis for future automation systems: An analysis of current diagnostic practices and their applicability in emerging IT based production paradigms[J]. *Computers in Industry*, 2011, 62(7): 639-659.
- [7] Mendel E, Rauber T W, Varejão F M, et al. Rolling element bearing fault diagnosis in rotating machines of oil extraction rigs[C]//2009 17th European Signal Processing Conference. IEEE, 2009: 1602-1606.
- [8] Huque M M, Imtiaz S, Rahman A, et al. Kick detection and remedial action in managed pressure drilling: a review[J]. *SN Applied Sciences*, 2020, 2(7): 1178.
- [9] Vega M P, Vieira F B, Fernandes L D, et al. Smart monitoring and decision making for regulating annulus bottom hole pressure while drilling oil wells[J]. *Brazilian Journal of Chemical Engineering*, 2016, 33: 969-983.
- [10] Abdali M R, Mohamadian N, Ghorbani H, et al. Petroleum well blowouts as a threat to drilling operation and wellbore sustainability: causes, prevention, safety and emergency response[J]. *Journal of Construction Materials| Special Issue on Sustainable Petroleum Engineering ISSN*, 2021, 2652: 3752.
- [11] Al-Shehri D A. Oil and gas wells: Enhanced wellbore casing integrity management through corrosion rate prediction using an augmented intelligent approach[J]. *Sustainability*, 2019, 11(3): 818.
- [12] Wang H, Huang H, Bi W, et al. Deep and ultra-deep oil and gas well drilling technologies: Progress and prospect[J]. *Natural Gas Industry B*, 2022, 9(2): 141-157.
- [13] Wei L, Yang X, Xi C, et al. Research and application of downhole blowout prevention system while drilling: A review[J]. *Journal of Petroleum Science and Engineering*, 2020, 188: 106882.
- [14] Kakolu S, Faheem M A. Predictive Analytics and Generative AI in Oil & Gas: Transforming Wellbore Stability and Hazard Detection[J]. *Iconic Research And Engineering Journals*, 2024, 8(1): 635-649.
- [15] Mohamed Almazrouei S, Dweiri F, Aydin R, et al. A review on the advancements and challenges of artificial intelligence based models for predictive maintenance of water injection pumps in the oil and gas industry[J]. *SN Applied Sciences*, 2023, 5(12): 391.
- [16] Taha A, Amani M. Introduction to Smart Oil and Gas Wells: Drilling, Completion and Monitoring Solutions[J]. *Int. J. Petrochem. Res*, 2019, 3: 249-254.
- [17] Al Mhdawi A K, Al-Raweshidy H S. A smart optimization of fault diagnosis in electrical grid using distributed software-defined IoT system[J]. *IEEE Systems Journal*, 2019, 14(2): 2780-2790.
- [18] Chernyi S G, Bordug A S, Kozachenko L N, et al. The reliability assessment of functioning of autonomous power system of drilling rigs[C]//2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). IEEE, 2020: 259-263.
- [19] Zhao S, Wang H. Enabling data-driven condition monitoring of power electronic systems with artificial intelligence: Concepts, tools, and developments[J]. *IEEE Power Electronics Magazine*, 2021, 8(1): 18-27.
- [20] Rana S. AI-driven fault detection and predictive maintenance in electrical power systems: A systematic review of data-driven approaches, digital twins, and self-healing grids[J]. *American Journal of Advanced Technology and Engineering Solutions*, 2025, 1(01): 258-289.

- [21] Anderson R N. 'Petroleum Analytics Learning Machine'for optimizing the Internet of Things of today's digital oil field-to-refinery petroleum system[C]//2017 IEEE International Conference on Big Data (Big Data). IEEE, 2017: 4542-4545.
- [22] Kirschbaum L, Roman D, Singh G, et al. AI-driven maintenance support for downhole tools and electronics operated in dynamic drilling environments[J]. Ieee Access, 2020, 8: 78683-78701.
- [23] Ammar A M, Ellafi A Y. Optimizing Critical Communication Systems for Offshore Oil and Gas Operations via Computational Methods[C]//2024 IEEE 4th International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA). IEEE, 2024: 531-537.
- [24] Fagioli A. Zero-day recovery: the key to mitigating the ransomware threat[J]. Computer Fraud & Security, 2019, 2019(1): 6-9.
- [25] Raymond D R, Midkiff S F. Denial-of-service in wireless sensor networks: Attacks and defenses[J]. IEEE pervasive computing, 2008, 7(1): 74-81.
- [26] Huseinović A, Mrdović S, Bicakci K, et al. A survey of denial-of-service attacks and solutions in the smart grid[J]. Ieee Access, 2020, 8: 177447-177470.
- [27] Cerar G, Yetgin H, Mohorčič M, et al. Machine learning for wireless link quality estimation: A survey[J]. IEEE Communications Surveys & Tutorials, 2021, 23(2): 696-728.
- [28] Arghandeh R, Von Meier A, Mehrmanesh L, et al. On the definition of cyber-physical resilience in power systems[J]. Renewable and Sustainable Energy Reviews, 2016, 58: 1060-1069.
- [29] Zhang R, Fan L, Lu D. Research on Self-Diagnosis and Self-Healing Technologies for Intelligent Fiber Optic Sensing Networks[J]. Sensors, 2025, 25(6): 1641.
- [30] Asghar A, Farooq H, Imran A. Self-healing in emerging cellular networks: Review, challenges, and research directions[J]. IEEE Communications Surveys & Tutorials, 2018, 20(3): 1682-1709.
- [31] Zekri M, El Kafhali S, Aboutabit N, et al. DDoS attack detection using machine learning techniques in cloud computing environments[C]//2017 3rd international conference of cloud computing technologies and applications (CloudTech). IEEE, 2017: 1-7.
- [32] Mokhtari S, Abbaspour A, Yen K K, et al. A machine learning approach for anomaly detection in industrial control systems based on measurement data[J]. Electronics, 2021, 10(4): 407.
- [33] Ahmad R, Alsmadi I, Alhamdani W, et al. Zero-day attack detection: a systematic literature review[J]. Artificial Intelligence Review, 2023, 56(10): 10733-10811.