

AI-Enabled Predictive Maintenance for Wavelength-Switched Optical Communication Systems

Bartolomeo Gadda

Department of Computer Science, University of North Texas, Denton, TX, USA.
bartolomeo.gadda@unt.edu

Justyna Skierka

Department of Computer Science, George Mason University, Fairfax, VA, USA.
skierkajustyna@gmu.edu

Thijn Stichter

Department of Electrical Engineering and Computer Science, University of Kansas, Lawrence, KS, USA.
tstichter@ku.edu

Abstract

Wavelength-switched optical communication systems have become central to high-capacity data center interconnection, metro aggregation, and long-haul transport because they allow capacity to be reassigned dynamically across wavelengths, ports, and routes. This flexibility, however, creates a complex failure ecology in which anomalies emerge from interactions among optical amplifiers, wavelength-selective switches, transceivers, fiber plants, synchronization subsystems, and software control planes. Traditional maintenance practices, whether reactive or strictly interval-based, struggle to anticipate such failures without either overprovisioning or exposing services to avoidable outages. This paper examines artificial intelligence enabled predictive maintenance for wavelength-switched optical communication systems from a system-level perspective. It argues that predictive maintenance should not be understood as a narrow anomaly-detection task but as a socio-technical capability that couples optical telemetry, data infrastructure, machine learning, operations governance, and sustainability policy. The paper analyzes architectural requirements for monitoring wavelength-switched fabrics, including the tension between telemetry granularity and network overhead, the role of clock and latency stability, and the need for robust decision support under uncertainty. It further discusses trade-offs involving sensitivity and false alarms, centralized and edge intelligence, vendor autonomy and operator oversight, fairness in maintenance prioritization, and the environmental implications of extending asset lifetimes while increasing computational demand. Drawing on cross-domain comparisons with manufacturing, aviation, and energy infrastructure, the paper identifies deployment, governance, and policy challenges that must be addressed before predictive maintenance can become a trusted layer of optical network operations. The conclusion proposes a research agenda centered on interoperable telemetry, uncertainty-aware models, auditable decision systems, and sustainable lifecycle management.

Keywords

predictive maintenance, wavelength-switched optical networks, artificial intelligence, optical network operations, telemetry, system resilience, governance, sustainability.

1. Introduction

Wavelength-switched optical communication systems form a critical substrate for contemporary digital infrastructure. They support data center interconnects, metropolitan aggregation, backbone transport, and increasingly dynamic service chains that require rapid reconfiguration across wavelengths and routes. Unlike static optical links, wavelength-switched architectures allow operators to reassign spectrum, redirect traffic, and balance load across physical paths in response to demand, failures, or maintenance activities. This agility is enabled by reconfigurable optical add-drop multiplexers, wavelength-selective switches, tunable transceivers, optical amplifiers, and sophisticated control planes. The resulting system offers considerable efficiency, but it also introduces operational complexity that cannot be managed adequately through periodic inspections or reactive troubleshooting alone [1], [2], [3]. As optical networks approach capacity limits and operate closer to nonlinear and noise-related thresholds, the margin for undetected degradation narrows, making predictive capabilities increasingly valuable [2], [4].

Artificial intelligence has been proposed as a means of improving optical network planning, monitoring, and fault management [5], [7]. Machine learning can identify subtle patterns in optical performance monitoring data, infer degraded component behavior, forecast remaining useful life, and support maintenance scheduling. Nevertheless, much of the existing discussion remains component-centric or model-centric, emphasizing classification accuracy or prediction error rather than the operational architecture in which predictions are produced and acted upon. Wavelength-switched systems require a broader perspective because a prediction about a transceiver, amplifier, or switch is inseparable from the topology, traffic load, synchronization state, and service criticality of the surrounding network. A degradation event in one wavelength path may be benign if spare capacity exists, but it may be severe if the path supports latency-sensitive synchronization or high-value financial traffic. This paper therefore treats predictive maintenance as a system-level capability that connects physical-layer telemetry, data pipelines, artificial intelligence models, human decision processes, and governance arrangements.

The importance of timing and wavelength coordination is especially visible in emerging intra-data center interconnects. Recent work on low-latency wavelength-switched clock-synchronized intra-data center interconnects enabled by hollow core fiber illustrates how optical switching, synchronization, and latency constraints can converge in a single architecture [6]. In such environments, maintenance decisions cannot focus only on binary component health; they must also consider clock stability, latency variation, and the consequences of wavelength reconfiguration. Predictive maintenance must therefore reason across layers and across time. This paper contributes a conceptual and architectural analysis of artificial intelligence enabled predictive maintenance for wavelength-switched optical communication systems. It examines failure ecology, telemetry infrastructure, model design, robustness and fairness, deployment governance, sustainability, and cross-domain lessons. The objective is not to propose a single algorithm but to clarify the structural conditions under which predictive maintenance can be technically effective, operationally trustworthy, and socially defensible.

2. System Architecture and Failure Ecology in Wavelength-Switched Optical Networks

Wavelength-switched optical networks are composed of interconnected physical and logical layers. At the physical layer, fiber spans, amplifiers, multiplexers, wavelength-selective switches, and transceivers determine the achievable signal quality. At the logical layer, wavelengths or spectral slots are assigned to paths, and the control plane may reconfigure

these assignments as demand or failures dictate. This architecture produces a distinctive failure ecology. Some failures are local and component-specific, such as laser aging, amplifier gain tilt, filter drift, connector contamination, or photodiode degradation. Others are relational and emerge from interactions among components, such as crosstalk between adjacent channels, transient power excursions after reconfiguration, polarization-dependent effects, or timing instability caused by path-length changes. Predictive maintenance must therefore distinguish between degradation that is intrinsic to an asset and degradation that appears only under particular traffic, wavelength, or topology conditions [1], [4].

The wavelength-switched nature of the system means that maintenance decisions are coupled to routing and spectrum assignment. If a wavelength path is predicted to degrade, the operator may choose to reroute traffic, shift the channel, reduce modulation order, or replace the component. Each response has trade-offs. Rerouting may preserve service but increase latency or consume scarce spectrum. Reducing modulation order may improve signal robustness but lower capacity. Replacing a component may prevent an outage but incur truck rolls, service interruption, and capital expenditure. These decisions are not purely technical. They involve service-level agreements, customer priority, regulatory obligations, and workforce availability. Predictive maintenance thus becomes a decision-support problem in which the model output is only one input among many [8], [9], [10]. The architecture must expose not only predictions but also confidence, likely failure modes, and recommended actions.

The growing use of hollow core fiber and clock-synchronized wavelength switching adds another layer of complexity. In such systems, latency and synchronization may be as important as bit error rate or optical signal-to-noise ratio [6]. A maintenance action that changes path length or switching state can affect clock recovery, jitter, and deterministic latency. Predictive maintenance must therefore incorporate timing telemetry and consider the maintenance window as a synchronization event, not merely a hardware replacement. This is a significant departure from conventional equipment maintenance, where the primary concern is often mechanical wear or electrical degradation. In optical networks, the state of the network itself changes the failure surface. A component may perform acceptably on one wavelength path and poorly on another because of amplifier loading, filter shape, or nonlinear interactions. The predictive system must therefore be context-aware and topology-aware, not merely asset-aware.

The architecture also determines where intelligence can reside. Centralized analytics can correlate data across many network domains and support global optimization, but it requires substantial data movement and may introduce latency in decision cycles. Edge or embedded analytics can process telemetry near the optical device, reducing bandwidth and enabling fast local responses, but it may lack global context. A hybrid architecture is likely: local agents detect anomalies and enforce safety constraints, while centralized systems perform fleet-level learning, maintenance scheduling, and cross-domain correlation. This mirrors the logic of autonomic computing, in which systems self-monitor, self-heal, and self-optimize within policy boundaries [15]. For wavelength-switched optical networks, the policy boundaries must include service continuity, synchronization integrity, security, and fairness in maintenance prioritization. Without such boundaries, predictive maintenance could optimize locally while degrading the network as a whole.

3. Predictive Maintenance Data Infrastructure and Telemetry

Predictive maintenance depends on data infrastructure as much as on models. Optical networks already generate a wide range of telemetry, including optical power, channel power, amplifier gain, temperature, bias current, bit error rate, pre-forward-error-correction error counts, optical signal-to-noise ratio, polarization state, latency, and clock synchronization metrics. However, the availability, granularity, and reliability of these measurements vary considerably across vendors and generations of equipment. Some devices expose rich streaming telemetry, while others provide only periodic management information base counters. Wavelength-switched systems require telemetry that is correlated with wavelength assignment, path topology, and control-plane events. A power anomaly at an amplifier is difficult to interpret without knowing which wavelengths were active, how they were routed, and whether a reconfiguration occurred at the same time [5], [7].

The data pipeline must therefore support time alignment, event correlation, and contextual enrichment. Maintenance events, software upgrades, traffic shifts, and protection switches must be recorded alongside physical-layer measurements. Without such contextual data, machine learning models may learn spurious associations. For example, a model might attribute increased error rates to a transceiver when the actual cause was a control-plane action that changed the modulation format or path. Data quality is also a major concern. Missing values, clock drift, inconsistent naming, and changing telemetry schemas can undermine model performance. The literature on machine learning systems emphasizes that hidden technical debt often arises from data dependencies, configuration issues, and feedback loops rather than from model architecture alone [14]. Predictive maintenance in optical networks is especially vulnerable to this debt because the physical infrastructure evolves slowly while software and traffic patterns change rapidly.

The foundation of predictive maintenance in other domains offers useful lessons. Condition-based maintenance and prognostics have long emphasized the integration of sensor data, degradation models, and decision policies [8], [9], [10]. Work on machinery diagnostics and prognostics has shown that prediction without an understanding of failure mechanisms can produce brittle results [11]. Similarly, multiple classifier and data-driven approaches in manufacturing demonstrate the value of combining domain knowledge with statistical learning [12], [13]. Optical networks can adapt these lessons by using physical models of amplifier noise, fiber nonlinearity, and laser aging as priors or constraints for machine learning. A purely data-driven model may detect anomalies, but it may not explain whether the anomaly is caused by a failing pump laser, a dirty connector, or an unusual traffic pattern. Explanation is essential for maintenance crews, vendors, and regulators.

Data governance is another structural requirement. Telemetry may cross organizational boundaries when network operators lease fiber, share spectrum, or interconnect with third parties. Predictive maintenance models may require data from multiple operators, but sharing raw telemetry can raise commercial, security, and privacy concerns. Federated learning and privacy-preserving analytics offer possible pathways, but they introduce complexity in model validation and accountability. The governance framework must define who owns the data, who can train on it, how long it is retained, and how predictions are audited. In critical infrastructure, the integrity of telemetry is also a security concern. A malicious actor could inject false measurements to trigger unnecessary maintenance or mask a real degradation. Predictive maintenance systems must therefore include authentication, anomaly detection on the telemetry stream, and fallback procedures when data trust is uncertain [22].

4. AI Models and Decision Support at System Level

Artificial intelligence models for predictive maintenance can be grouped conceptually into anomaly detection, fault classification, degradation modeling, and remaining useful life estimation. In wavelength-switched optical networks, anomaly detection may identify unusual power, error, or latency patterns. Fault classification may distinguish between transceiver degradation, amplifier failure, filter drift, and fiber damage. Degradation modeling may estimate how a component or path will evolve under different traffic and configuration conditions. Remaining useful life estimation may inform replacement scheduling and spare-parts logistics. These tasks are related but not identical, and they require different data, labels, and validation strategies. Supervised learning can be effective when historical failure labels are available, but optical networks often have few labeled failures and many unlabeled normal operating hours. Unsupervised and semi-supervised methods may therefore play a larger role, though they must be carefully calibrated to avoid excessive false alarms [5], [13].

System-level decision support requires more than a prediction. It requires an action policy that accounts for service impact, cost, risk, and uncertainty. A model might predict that an amplifier will fail within two weeks with moderate confidence. The operator must decide whether to replace it immediately, schedule maintenance during a low-traffic window, reroute traffic, or continue monitoring. This decision depends on the criticality of the affected wavelengths, the availability of spare capacity, the cost of a truck roll, and the probability of a catastrophic failure. Reinforcement learning and optimization methods can support such decisions, but they must operate within safety constraints and human oversight. The concept of society-in-the-loop is relevant here: automated systems should not merely optimize a technical objective but should reflect the values and priorities of the affected community [20]. In optical networks, that community includes operators, customers, maintenance workers, and regulators.

Digital twins and simulation environments can improve decision support by allowing operators to test maintenance scenarios without disrupting live traffic. A digital twin of a wavelength-switched network can model how a wavelength reassignment affects amplifier loading, latency, and synchronization. It can also help validate predictive models by replaying historical telemetry and comparing predicted versus actual outcomes. However, digital twins require accurate physical models and continuous calibration. If the twin diverges from the real network, it may produce misleading recommendations. The same concern applies to machine learning models trained in simulation and deployed in production. Domain adaptation and continual learning are therefore necessary, but they introduce risks of catastrophic forgetting and uncontrolled model drift. The operational architecture must include model monitoring, versioning, rollback, and human review [14], [16].

Deep learning has achieved remarkable success in pattern recognition, but it is not automatically suited to all predictive maintenance tasks [17]. Optical telemetry is often multivariate, time-dependent, and subject to nonstationary conditions. Deep sequence models can capture complex temporal dependencies, but they may require large amounts of data and computational resources. Simpler models may be more interpretable and easier to validate. The choice of model should be driven by the decision context, not by novelty. For safety-critical maintenance, an interpretable model with slightly lower accuracy may be preferable to a black-box model that cannot explain its predictions. The governance framework should require documentation of model assumptions, training data, performance across network segments, and known failure modes. This aligns with broader efforts to define trustworthy artificial intelligence in critical infrastructures [21], [22].

5. Trade-offs, Robustness, and Fairness in Predictive Maintenance

Predictive maintenance involves unavoidable trade-offs. A sensitive model may detect early degradation but generate many false alarms, leading to unnecessary maintenance and reduced trust. A conservative model may avoid false alarms but miss subtle failures that later cause outages. The optimal balance depends on the cost of downtime, the cost of maintenance, the availability of spare parts, and the tolerance of customers. In wavelength-switched optical networks, the cost of a false positive may include not only truck rolls but also unnecessary wavelength reconfiguration, which can affect synchronization and latency. The cost of a false negative may include service outages, regulatory penalties, and reputational damage. These costs are not uniform across the network. A failure on a high-priority financial route may be far more consequential than a failure on a best-effort access link. The decision policy must therefore be risk-weighted and context-dependent [8], [10].

Robustness is another central concern. Predictive models trained on historical data may fail when the network changes. New transceiver models, new fiber types, new modulation formats, and new traffic patterns can shift the data distribution. Extreme events such as fiber cuts, power outages, or cyberattacks may be underrepresented in training data. A robust system must detect when it is operating outside its training domain and fall back to conservative rules. It must also be resilient to adversarial manipulation. If maintenance decisions can be influenced by false telemetry, attackers may cause economic damage or service disruption. Security and maintenance analytics must therefore be co-designed. The system should authenticate telemetry, detect anomalies in the data stream, and require human confirmation for high-impact actions. Robustness also includes graceful degradation: if the predictive system fails, the network should still be operable through conventional monitoring and manual procedures [14], [22].

Fairness in predictive maintenance is less discussed but increasingly important. Maintenance resources are finite, and predictive models may allocate attention to the most profitable or most instrumented parts of the network. This can create a feedback loop in which well-monitored segments receive more data, better models, and more maintenance, while underserved or rural segments remain under-monitored and more prone to failure. In shared infrastructure, smaller tenants may have less influence over maintenance scheduling than large tenants. Fairness concerns also arise in workforce management. If predictive maintenance changes the timing and location of work, it may affect working conditions, skill requirements, and job security. A fair system should make maintenance prioritization transparent and should include criteria beyond short-term profit, such as regulatory obligations, public safety, and digital inclusion [18], [19]. The ethics of algorithms literature emphasizes that fairness is not a purely technical property; it depends on institutional context and affected stakeholders [19], [21].

The governance of trade-offs requires participation from multiple actors. Vendors, operators, customers, workers, and regulators may have different definitions of acceptable risk. A vendor may prioritize equipment longevity, an operator may prioritize service availability, and a customer may prioritize latency predictability. Predictive maintenance systems should therefore support negotiation and auditability. They should record why a maintenance action was taken, what alternatives were considered, and what uncertainties were present. This record is essential for accountability after an outage or an unnecessary intervention. It also supports continuous improvement: operators can compare predicted outcomes with actual

outcomes and adjust models and policies. In this sense, predictive maintenance is not a one-time deployment but an ongoing socio-technical process [20].

6. Deployment, Governance, and Policy Implications

Deployment models for artificial intelligence enabled predictive maintenance vary according to ownership, trust, and technical capability. In a vendor-managed model, the equipment vendor collects telemetry and provides maintenance predictions as a service. This can accelerate adoption and leverage vendor expertise, but it may reduce operator visibility and create lock-in. In an operator-managed model, the network operator builds its own analytics platform and retains control of data and decisions. This requires significant expertise and may be difficult for smaller operators. A hybrid model may combine vendor-provided device-level analytics with operator-level orchestration. Each model has implications for liability, security, and interoperability. If a vendor predicts a failure that does not occur, who bears the cost of unnecessary maintenance? If an operator ignores a vendor warning and an outage follows, how is responsibility allocated? These questions must be addressed in contracts, service-level agreements, and regulatory frameworks [22].

Interoperability is a major barrier. Optical networks are multi-vendor environments, and telemetry formats, data models, and management interfaces often differ. Standards bodies and industry consortia have made progress in defining streaming telemetry and open configuration models, but predictive maintenance requires semantic interoperability, not just syntactic compatibility. A power measurement from one vendor must be interpretable alongside a power measurement from another, with consistent units, timestamps, and context. Without such interoperability, predictive models will be siloed by vendor or domain, limiting their ability to detect cross-domain failures. Policy can encourage openness by requiring public operators to adopt standardized telemetry and by funding research on open data models for optical networks. However, standards must balance openness with security and commercial confidentiality [5], [7].

Governance also involves the regulatory status of optical networks as critical infrastructure. Many jurisdictions impose availability, security, and reporting requirements on telecommunications providers. Predictive maintenance can help meet these requirements, but it can also create new risks. If maintenance decisions are automated, regulators may ask whether the system is auditable, whether it discriminates unfairly, and whether it can be overridden in an emergency. Trustworthy artificial intelligence guidelines emphasize human oversight, technical robustness, privacy, transparency, and accountability [21], [22]. These principles must be translated into operational practices for optical networks. For example, a predictive maintenance system should log model versions, input data, confidence scores, and human decisions. It should provide explanations that maintenance crews can understand. It should have a clear escalation path when predictions conflict with physical inspections. It should also be tested under stress conditions before being trusted with high-impact decisions.

Policy implications extend beyond individual operators. Governments may need to support workforce retraining as maintenance shifts from reactive repair to data-informed intervention. They may need to fund shared testing facilities where vendors and operators can validate predictive models on neutral ground. They may need to clarify liability when artificial intelligence contributes to an outage. They may also need to address cross-border data flows if telemetry is processed in different jurisdictions. These issues are not unique to optical networks. Aviation, energy, and manufacturing have faced similar challenges in adopting

predictive maintenance. Cross-domain comparisons can help identify best practices and avoid known pitfalls [9], [11], [13].

7. Sustainability and Economic Lifecycle Considerations

Predictive maintenance has significant sustainability potential. By detecting degradation early, operators can repair or replace components before catastrophic failure, extend asset lifetimes, reduce emergency truck rolls, and avoid energy-intensive downtime. In optical networks, downtime can have cascading effects across data centers, cloud services, and communication platforms. Avoiding unnecessary outages can reduce the need for backup capacity and overprovisioning, which in turn lowers energy consumption and material use. Predictive maintenance can also support circular economy practices by enabling component reuse, refurbishment, and better spare-parts management. If a transceiver is predicted to fail, it may be replaced during a scheduled window and refurbished for less critical use. This contrasts with reactive maintenance, where failed components may be discarded or replaced under time pressure with less attention to lifecycle impact [10], [13].

However, artificial intelligence itself has an environmental footprint. Training and running machine learning models consume energy and water, especially if large models are used for telemetry analytics. The sustainability case for predictive maintenance must therefore include the computational overhead of the analytics platform. A system that saves one truck roll but consumes disproportionate data center energy may not be environmentally beneficial. The net benefit depends on the scale of the network, the efficiency of the models, and the carbon intensity of the energy sources. Operators should measure the lifecycle impacts of both the physical maintenance activities and the digital infrastructure that supports prediction. Edge computing may reduce data movement and energy use, while centralized training may be more efficient for large models. The optimal architecture is likely a balance between local inference and centralized learning [14], [16].

Economically, predictive maintenance affects both capital and operating expenditure. It can reduce unplanned outages, improve service-level agreement compliance, and defer capital upgrades by extending the useful life of existing equipment. It can also reduce spare-parts inventory by enabling just-in-time maintenance. However, it requires investment in sensors, telemetry, data platforms, models, and skilled personnel. The return on investment depends on the criticality of the network, the cost of downtime, and the maturity of maintenance operations. Smaller operators may struggle to justify the upfront costs, raising concerns about a digital divide in network reliability. Policy interventions such as shared analytics platforms, subsidies for telemetry upgrades, or open-source models could help smaller operators participate. Without such interventions, predictive maintenance may concentrate reliability benefits in wealthy, high-density markets while leaving rural and underserved networks behind [18], [21].

8. Case Illustrations and Cross-Domain Comparisons

A useful case illustration is a wavelength-switched intra-data center interconnect using hollow core fiber and clock synchronization. In this environment, latency and timing are tightly coupled to wavelength assignment and switching state [6]. Predictive maintenance must monitor not only optical power and error rates but also synchronization quality and latency stability. A gradual increase in latency variance might indicate a failing switch, a fiber connector issue, or a clock recovery problem. If the system automatically reroutes traffic to a longer path, latency may improve or worsen depending on the topology and synchronization

protocol. A predictive system could recommend a maintenance window during low traffic, but it must also account for the fact that switching itself may introduce transient errors. The case shows that predictive maintenance in wavelength-switched optical networks is a control problem as much as a diagnostic problem. It requires models that understand the consequences of actions, not just the likelihood of failure.

A second case is a long-haul or submarine optical network with high-value traffic and limited repair access. In such networks, a component failure can take days or weeks to repair, and the cost of downtime is enormous. Predictive maintenance can prioritize early warning for critical amplifiers, power feeds, and repeaters. However, the data may be sparse because failures are rare. Models must therefore rely on physics-based simulation, expert knowledge, and transfer learning from similar assets. The governance challenge is also acute: maintenance decisions may involve multiple operators, cable owners, and regulators. Transparency and liability allocation are essential. This resembles aviation, where predictive maintenance for engines and avionics must meet strict safety and certification standards. Aviation has developed extensive reliability programs, but it also faces challenges in certifying machine learning for safety-critical decisions [11], [22].

Manufacturing provides a third comparison. Factories have adopted predictive maintenance for motors, pumps, and production lines using vibration, temperature, and acoustic data [12], [13]. Manufacturing environments are often more controlled than optical networks, with stable operating conditions and clear failure labels. Optical networks are more dynamic, multi-vendor, and geographically distributed. Nevertheless, manufacturing offers lessons about data quality, model maintenance, and workforce integration. Successful predictive maintenance programs in manufacturing often depend on collaboration between data scientists, maintenance technicians, and process engineers. In optical networks, the equivalent collaboration is between network engineers, optical physicists, software developers, and field technicians. Without this collaboration, models may be technically accurate but operationally irrelevant. The cross-domain lesson is that predictive maintenance succeeds when it is embedded in maintenance workflows and supported by organizational culture, not when it is treated as a standalone software tool [8], [15].

9. Open Challenges and Research Agenda

Several open challenges remain. First, standardized telemetry for wavelength-switched optical networks is still incomplete. Research should focus on open data models that capture wavelength assignment, topology, synchronization state, and maintenance events in a vendor-neutral way. Second, uncertainty quantification is essential. Predictive models should provide calibrated confidence estimates and identify when they are operating outside their training domain. Third, explainability must be practical. Maintenance crews need to understand why a prediction was made and what action is recommended. Fourth, fairness metrics for maintenance prioritization must be developed. These metrics should account for regional equity, tenant diversity, and public interest, not only commercial value. Fifth, sustainability assessment must include both the benefits of avoided outages and the costs of computational infrastructure. Sixth, governance mechanisms must be designed for multi-stakeholder environments. This includes audit trails, liability rules, and processes for contesting automated decisions [18], [19], [20], [22].

Another challenge is the integration of predictive maintenance with network control. If predictions influence routing and spectrum assignment, then the maintenance system becomes part of the control loop. This creates opportunities for optimization but also risks of instability.

A predictive model that frequently recommends rerouting could cause oscillations in the network. Therefore, control-theoretic analysis and safety constraints are needed. The system should distinguish between slow maintenance actions, such as scheduling a replacement, and fast control actions, such as rerouting a wavelength. These timescales require different governance and validation. Fast actions may be automated with strict safeguards, while slow actions may require human approval. Research should also explore federated learning and privacy-preserving analytics to enable cross-operator collaboration without sharing raw telemetry. Finally, longitudinal studies are needed to evaluate predictive maintenance in real networks over years, not just in simulations or short trials. Such studies should measure not only technical performance but also organizational, economic, and environmental outcomes [14], [16], [21].

10. Conclusion

Artificial intelligence enabled predictive maintenance for wavelength-switched optical communication systems is a promising but structurally demanding capability. It requires more than accurate models. It requires telemetry infrastructure that captures physical-layer, logical-layer, and synchronization data; data governance that ensures quality, security, and interoperability; decision support that accounts for uncertainty, risk, and service impact; and governance arrangements that ensure accountability, fairness, and trust. Wavelength-switched networks are dynamic and multi-vendor, and their failure modes emerge from interactions among components, traffic, and control actions. Predictive maintenance must therefore be context-aware, topology-aware, and policy-aware. It must also be sustainable, considering both the environmental benefits of extended asset lifetimes and the computational costs of artificial intelligence. Cross-domain comparisons with manufacturing, aviation, and energy show that successful predictive maintenance depends on organizational integration and clear accountability. The research agenda should prioritize interoperable telemetry, uncertainty-aware models, explainable decision support, fairness auditing, and lifecycle sustainability. If these challenges are addressed, predictive maintenance can become a foundational capability for reliable, efficient, and equitable optical communication infrastructure.

References

1. Agrawal, G. P. (2021). *Fiber-optic communication systems* (5th ed.). Wiley.
2. Essiambre, R.-J., Kramer, G., Winzer, P. J., Foschini, G. J., & Goebel, B. (2010). Capacity limits of optical fiber networks. *Journal of Lightwave Technology*, 28(4), 662–701. <https://doi.org/10.1109/JLT.2009.2039464>
3. Winzer, P. J., & Essiambre, R.-J. (2006). Advanced optical modulation formats. *Proceedings of the IEEE*, 94(5), 952–985. <https://doi.org/10.1109/JPROC.2006.873438>
4. Kachris, C., Kanonakis, K., & Tomkos, I. (2013). Optical interconnection networks in data centers: Recent trends and future challenges. *IEEE Communications Magazine*, 51(9), 39–45. <https://doi.org/10.1109/MCOM.2013.6588648>
5. Musumeci, F., Rottondi, C., Nag, A., Macaluso, I., Zibar, D., Ruffini, M., & Tornatore, M. (2019). An overview on application of machine learning techniques in optical networks. *IEEE Communications Surveys & Tutorials*, 21(2), 1383–1408. <https://doi.org/10.1109/COMST.2018.2880039>

6. Zhou, Zichuan, et al. "Low-latency wavelength-switched clock-synchronized intra-data center interconnects enabled by hollow core fiber." *Optics Express* 31.15 (2023): 24739-24748.
7. Mata, J., de Miguel, I., Durán, R. J., Merayo, N., Singh, S. K., Jukan, A., & Chamanian, M. (2018). Artificial intelligence (AI) methods in optical networks: A comprehensive survey. *Optical Switching and Networking*, 28, 43–57. <https://doi.org/10.1016/j.osn.2017.12.006>
8. Vachtsevanos, G., Lewis, F. L., Roemer, M., Hess, A., & Wu, B. (2006). *Intelligent fault diagnosis and prognosis for engineering systems*. Wiley.
9. Jardine, A. K. S., Lin, D., & Banjevic, D. (2006). A review on machinery diagnostics and prognostics implementing condition-based maintenance. *Mechanical Systems and Signal Processing*, 20(7), 1483–1510. <https://doi.org/10.1016/j.ymssp.2005.09.012>
10. Mobley, R. K. (2002). *An introduction to predictive maintenance* (2nd ed.). Butterworth-Heinemann.
11. Lee, J., Wu, F., Zhao, W., Ghaffari, M., Liao, L., & Siegel, D. (2014). Prognostics and health management design for rotary machinery systems—Reviews, methodology and applications. *Mechanical Systems and Signal Processing*, 42(1–2), 314–334. <https://doi.org/10.1016/j.ymssp.2013.06.004>
12. Susto, G. A., Schirru, A., Pampuri, S., McLoone, S., & Beghi, A. (2015). Machine learning for predictive maintenance: A multiple classifier approach. *IEEE Transactions on Industrial Informatics*, 11(3), 812–820. <https://doi.org/10.1109/TII.2014.2349359>
13. Carvalho, T. P., Soares, F. A. A. M. N., Vita, R., Francisco, R. P., Basto, J. P., & Alcalá, S. G. S. (2019). A systematic literature review of machine learning methods applied to predictive maintenance. *Computers & Industrial Engineering*, 137, 106024. <https://doi.org/10.1016/j.cie.2019.106024>
14. Sculley, D., Holt, G., Golovin, D., Davydov, E., Phillips, T., Ebner, D., Chaudhary, V., Young, M., Crespo, J.-F., & Dennison, D. (2015). Hidden technical debt in machine learning systems. *Advances in Neural Information Processing Systems*, 28, 2503–2511.
15. Kephart, J. O., & Chess, D. M. (2003). The vision of autonomic computing. *Computer*, 36(1), 41–50. <https://doi.org/10.1109/MC.2003.1160055>
16. Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245), 255–260. <https://doi.org/10.1126/science.aaa8415>
17. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436–444. <https://doi.org/10.1038/nature14539>
18. Barocas, S., Hardt, M., & Narayanan, A. (2019). *Fairness and machine learning*. fairmlbook.org.
19. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1–21. <https://doi.org/10.1177/2053951716679679>
20. Rahwan, I. (2018). Society-in-the-loop: Programming the algorithmic social contract. *Ethics and Information Technology*, 20(1), 5–14. <https://doi.org/10.1007/s10676-017-9430-8>

21. Floridi, L., Cows, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28(4), 689–707.
<https://doi.org/10.1007/s11023-018-9482-5>
22. High-Level Expert Group on AI. (2019). Ethics guidelines for trustworthy AI. European Commission.