



Digital Twin-Based Network Reliability Modeling for LAN And WAN Infrastructure Resilience

Md Shahid Nazir¹;

[1]. Assistant Maintenance Engineer (Network). Dhaka Water Supply and Sewerage Authority (government utility). Dhaka, Bangladesh;
MA in Procurement & Supply Management; BRAC University, Dhaka, Bangladesh
Email: nazir.dwasa@gmail.com

Doi: [10.63125/ahjvxi14](https://doi.org/10.63125/ahjvxi14)

Received: 15 September 2023; **Revised:** 25 October 2023; **Accepted:** 11 November 2023; **Published:** 16 December 2023

Abstract

This study quantitatively examined digital twin-based network reliability modeling for Local Area Network (LAN) and Wide Area Network (WAN) infrastructure resilience, with particular emphasis on network failure severity, traffic intensity, redundancy, failover behavior, routing convergence, service restoration, and physical–virtual model fidelity. A quantitative experimental design was employed using a reference LAN/WAN infrastructure and its corresponding digital twin under controlled baseline, single-link failure, multiple-link failure, device-failure, traffic-load, failover, and recovery conditions. A total of 420 experimental trials were conducted, of which 408 valid observations were retained, representing a 97.14% retention rate and 204 matched reference-network and digital-twin measurement pairs. Network reliability was evaluated through availability, latency, throughput, packet loss, jitter, link utilization, routing convergence time, failover time, service interruption, and recovery duration. The findings demonstrated progressive reliability degradation with increasing failure severity. Mean latency increased from 38.72 ms at baseline to 78.93 ms under multiple-link failure, while throughput decreased from 184.73 Mbps to 126.58 Mbps. Packet loss increased from 0.31% to 4.17%, availability declined from 99.82% to 97.86%, and service interruption increased from 3.61 to 11.84 seconds. All major failure-related differences were statistically significant at $p < .001$, with large effect sizes ranging from partial $\eta^2 = .48$ to $.66$. High traffic further increased latency to 82.47 ms and packet loss to 4.36%, whereas redundancy increased availability from 97.81% to 99.16% and reduced service interruption from 10.36 to 5.81 seconds. Multiple-link failures required 9.27 seconds for service restoration compared with 4.96 seconds for single-link failures. Digital twin validation produced strong physical–virtual correlations ranging from $r = .941$ to $.988$, with relatively low prediction errors across the principal reliability indicators. Regression models explained 72%–81% of the variance in major network outcomes. Overall, the results demonstrated that failure severity and traffic intensity significantly reduced infrastructure reliability, while redundancy improved service continuity and recovery performance, and the calibrated digital twin accurately represented LAN/WAN behavior across stable, disrupted, and recovery states.

Keywords

Digital Twin, Network Reliability, LAN, WAN, Resilience.

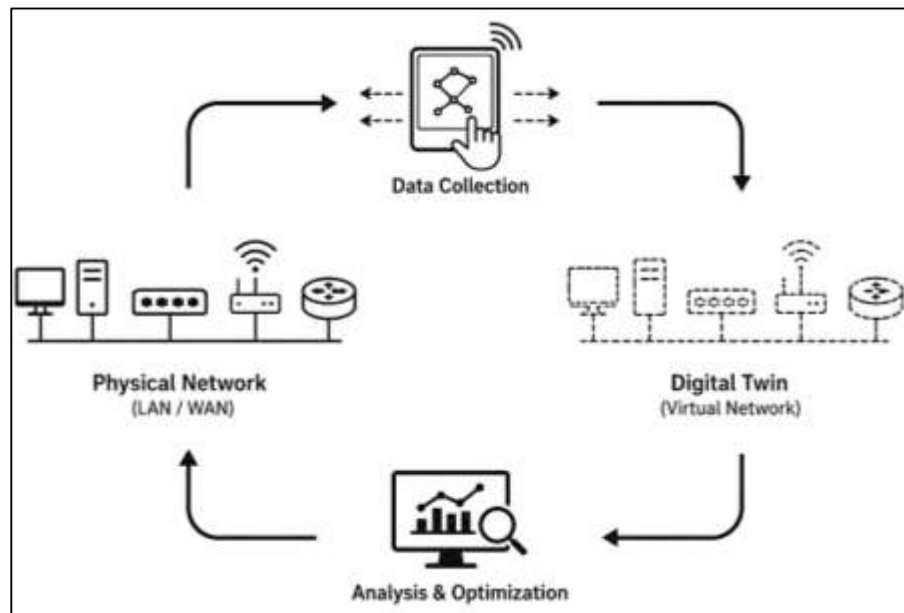
INTRODUCTION

A digital twin can be defined as a dynamic, data-connected virtual representation of a physical object, process, system, or infrastructure that reproduces relevant structural characteristics, operational states, behaviors, and interactions of its physical counterpart. Unlike a conventional static model, a digital twin is associated with continuous or periodic synchronization between physical and virtual environments through operational data, telemetry, computational models, analytical mechanisms, and bidirectional information exchange ([Hungud & Arunachalam, 2020](#)). Within computer networking, this concept has developed into the Digital Twin Network (DTN) or Network Digital Twin (NDT), which represents physical network components, topology, configuration, traffic conditions, routing behavior, performance characteristics, and operational states within a computational environment. Such a representation can incorporate routers, switches, gateways, access points, servers, communication links, interfaces, routing tables, virtual network functions, security controls, traffic flows, and service dependencies. Network reliability refers to the probability or measurable capability of a communication network to perform its required functions consistently within specified operating conditions and time periods. Reliability is commonly represented through indicators such as availability, failure rate, mean time between failures, mean time to repair, packet delivery ratio, packet loss, latency, jitter, throughput, route stability, service continuity, and recovery duration ([Shen et al., 2020](#)). Network resilience is closely related to reliability, although the two concepts address different dimensions of network performance. Reliability concerns the continuity and consistency of expected service, whereas resilience describes the capacity of a network to absorb disruptions, maintain an acceptable level of functionality, recover from failures, and restore communication services following adverse events. These concepts are particularly relevant to Local Area Network (LAN) and Wide Area Network (WAN) infrastructures. A LAN provides communication among devices within a geographically bounded environment such as an office, university, hospital, factory, data center, or institutional campus, while a WAN interconnects geographically dispersed networks through carrier links, leased circuits, broadband connections, software-defined WAN technologies, virtual private networks, or other long-distance communication mechanisms ([Zhang et al., 2021](#)). Digital twin-based reliability modeling therefore refers to the construction and quantitative analysis of synchronized virtual representations of LAN and WAN environments for measuring, reproducing, testing, and evaluating network reliability under normal and abnormal operational conditions. The digital twin environment creates a measurable representation in which topology, link capacity, traffic intensity, device status, failures, routing decisions, redundancy mechanisms, and recovery processes can be examined without requiring equivalent disruptive experiments on the operational network ([Camarinha-Matos et al., 2019](#)).

The application of digital twin principles to communication networks represents the convergence of several established technological domains, including network simulation, network emulation, telemetry, software-defined networking, network function virtualization, cloud computing, Internet of Things architectures, artificial intelligence, machine learning, data analytics, and automated network management. Conventional network simulation has long enabled researchers and administrators to examine routing protocols, congestion, packet transmission, topology structures, link failures, and traffic behavior within controlled computational environments. A digital twin extends this modeling principle by establishing stronger correspondence between a specific physical network and its virtual representation through operational data and continuous state synchronization ([Taimoor & Rehman, 2021](#)). This distinction is important for quantitative network reliability research because the accuracy of reliability estimates depends on the extent to which a model represents actual network configurations, workloads, dependencies, device states, and failure conditions. Digital twin-based network modeling can collect telemetry variables such as interface utilization, bandwidth consumption, packet loss, round-trip time, queue occupancy, CPU utilization, memory consumption, routing changes, device availability, error rates, retransmission rates, and application response time.

These observations can subsequently populate virtual network models in which operational conditions are reconstructed and alternative configurations or failure scenarios are quantitatively evaluated. Research across communication networks, cyber-physical systems, IoT infrastructures, edge-cloud architectures, mobile networks, and software-defined environments has established digital twins as mechanisms for combining observation, modeling, simulation, prediction, optimization, and control (Yan, et al., 2019).

Figure 1: Digital Twin Network Reliability Framework



Within network reliability analysis, this combination provides a structured mechanism for moving beyond isolated performance monitoring. Traditional monitoring platforms primarily report what is occurring within an operational network, whereas a network digital twin can reproduce current conditions and provide an experimental environment in which network states can be manipulated. For example, individual links may be disabled virtually, routing paths may be altered, traffic intensity may be increased, devices may be removed, bandwidth may be constrained, or recovery procedures may be activated while quantitative changes in network performance are recorded. This approach transforms reliability assessment from a largely reactive activity into a model-based analytical process. The physical network supplies measurements to the virtual environment, and the virtual environment provides a controlled setting for evaluating the relationships among network architecture, operational conditions, failures, and performance outcomes (Shen et al., 2021). Consequently, digital twin-based modeling provides a methodological foundation for studying LAN and WAN reliability using experimentally measurable variables rather than relying exclusively on historical outage reports, static topology diagrams, or administrator observations.

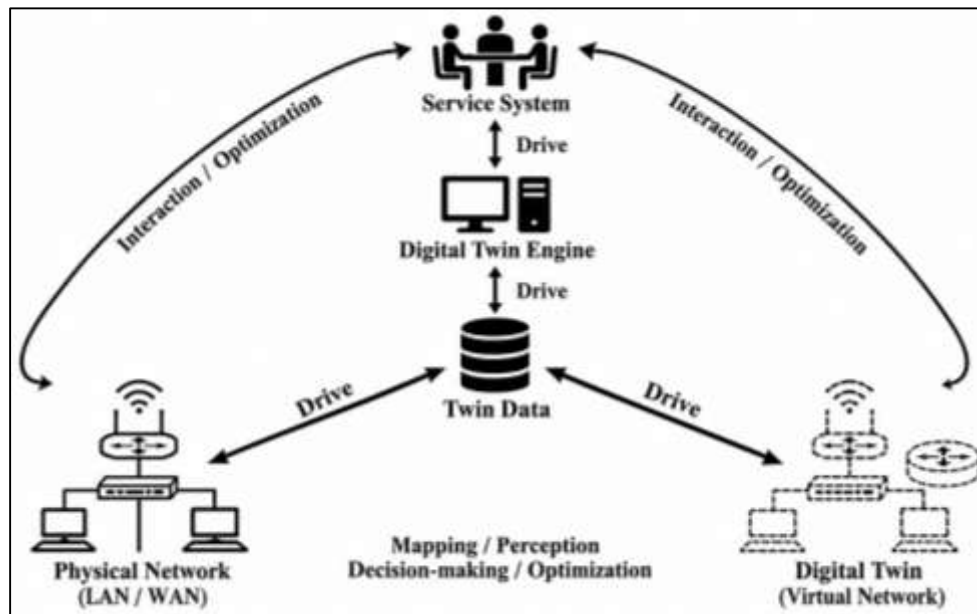
LAN and WAN reliability has international significance because modern economic, governmental, educational, industrial, healthcare, financial, transportation, and communication activities increasingly depend on continuously available digital connectivity. Organizations operating across countries and regions rely on interconnected LAN and WAN infrastructures to provide access to cloud services, enterprise applications, databases, collaboration systems, communication platforms, digital payment services, supply-chain applications, industrial systems, and remote computing resources. A localized network failure can therefore generate consequences that extend beyond the failed device or communication link (Qiuchen Lu et al., 2019). In globally distributed organizations, WAN disruptions

may isolate branch locations, interrupt access to centralized services, degrade real-time communications, prevent cloud application access, and interfere with transactions across multiple geographic locations. LAN failures can similarly disrupt internal services by affecting switches, wireless access points, gateways, servers, user devices, authentication infrastructure, and application connectivity. The increasing interdependence among local networks, wide-area connectivity, cloud infrastructure, edge computing, IoT devices, and mobile communication systems has made network reliability a multi-layered international concern. Digital transformation has also increased the volume and diversity of traffic transported across organizational networks, producing operational environments in which voice, video, transactional data, sensor streams, enterprise applications, and cloud workloads compete for shared communication resources. Reliability within this environment cannot be represented adequately by a single indicator (Cascone et al., 2021). Availability may remain high while latency, packet loss, jitter, or congestion substantially reduces service quality. Likewise, redundant links may exist while correlated failures, configuration errors, routing instability, or shared infrastructure dependencies limit actual resilience. Digital twin-based network modeling is internationally relevant because it offers a common analytical approach through which heterogeneous communication infrastructures can be represented using measurable operational variables. International standardization activity surrounding digital twin networks has further formalized concepts related to network architecture, data repositories, modeling, interfaces, security, visualization, and control interaction. These developments position network digital twins within broader efforts toward automated and data-driven network management. For multinational organizations, telecommunications providers, universities, government institutions, financial networks, healthcare systems, and industrial enterprises, digital twin modeling can represent geographically distributed network relationships while retaining visibility into local device and link behavior (Jiang et al., 2020). The international importance of this research area therefore originates from the universal dependence of contemporary institutions on network availability and service continuity, combined with the increasing technical complexity of maintaining reliable connectivity across heterogeneous LAN and WAN infrastructures.

The reliability of integrated LAN and WAN infrastructures is affected by interacting technical conditions that operate at device, link, topology, routing, traffic, service, and management levels. LAN environments may experience switch failures, access-point congestion, broadcast problems, interface errors, cable faults, VLAN configuration errors, gateway failures, excessive traffic loads, server connectivity problems, and power-related interruptions (Zhang et al., 2017). WAN infrastructures introduce additional reliability factors, including carrier outages, long-distance link failures, routing convergence delays, bandwidth limitations, congestion, packet loss, variable latency, tunnel failures, provider dependencies, and failures affecting geographically distributed nodes. When LAN and WAN systems operate as a unified enterprise communication environment, faults occurring within one domain may propagate into another domain or alter the availability of services that depend on multiple network layers. Reliability assessment is consequently influenced by both individual component reliability and the structural relationships among components. Redundant links, backup routers, multiple gateways, alternate routing paths, failover mechanisms, and load-balancing configurations can improve fault tolerance, although their effectiveness depends on configuration correctness, available capacity, convergence time, and the independence of failure paths (Li et al., 2021). Quantitative network reliability modeling therefore requires simultaneous consideration of topology characteristics and dynamic performance indicators. Variables such as network availability, packet loss rate, throughput, latency, jitter, mean time between failures, mean time to repair, failover time, recovery time, link utilization, routing convergence time, and service interruption duration provide measurable representations of network behavior. Digital twins enable these variables to be analyzed under controlled modifications to network conditions. A virtual network representation can reproduce a baseline operating state and subsequently introduce link failures, device outages, traffic surges, route

changes, congestion, or bandwidth restrictions. Performance measurements obtained before, during, and after these events can provide quantitative evidence regarding the resilience of the modeled infrastructure. This capability is particularly valuable when physical failure testing is operationally expensive or disruptive (Ren & Wan, 2021).

Figure 2: Digital Twin Network Resilience Framework



Disconnecting an active enterprise WAN link, intentionally overloading a production switch, or disabling a critical gateway may create unacceptable service interruptions. Equivalent scenarios can be represented within a sufficiently faithful network digital twin while preserving the operational network. The value of the digital twin is therefore linked closely to model fidelity. Differences between virtual and physical measurements can affect the validity of reliability estimates, making synchronization accuracy, telemetry quality, topology representation, traffic reproduction, and configuration consistency important methodological characteristics of digital twin-based reliability modeling.

Digital twin-based network reliability modeling is fundamentally quantitative because both the physical network and its virtual representation generate measurable performance data that can be compared across operational states and experimental conditions (Almeida et al., 2020). The physical infrastructure can provide baseline measurements through network telemetry, Simple Network Management Protocol data, flow records, device logs, routing information, active probes, packet captures, application monitoring, and infrastructure management systems. These data can be used to characterize the operating state of network nodes and links and to calibrate the corresponding digital representation. Within the twin, researchers can define independent variables associated with failure severity, traffic load, link capacity, redundancy level, routing configuration, node availability, or recovery mechanisms and measure their effects on dependent reliability indicators. Network availability may be calculated as the proportion of operational time relative to total observation time, while packet loss represents the proportion of transmitted packets that fail to reach their destination (Serrano, 2018). Latency measures communication delay, jitter captures variation in packet delay, and throughput measures the volume of successfully transmitted information over a defined interval. Mean time between failures provides a measure of operational stability, while mean time to repair and recovery time quantify restoration efficiency. Failover time can measure the interval required for redundant infrastructure to assume service following a primary component failure. Digital twin fidelity

can also be expressed quantitatively by comparing physical-network and twin measurements using absolute error, percentage error, correlation coefficients, distributional similarity, or other statistical measures. Such measurements are important because a reliability model cannot be considered operationally representative solely because its topology resembles the physical network. It must also reproduce network behavior within acceptable levels of accuracy (Dondossola et al., 2020). Experimental conditions can subsequently be repeated across multiple trials, allowing researchers to calculate means, standard deviations, confidence intervals, effect sizes, correlations, or regression relationships. Statistical testing can determine whether changes in redundancy, traffic load, fault conditions, or routing strategies are associated with significant differences in availability, latency, packet loss, throughput, or recovery time. Digital twin environments can additionally support sensitivity analysis by varying one or more parameters and measuring corresponding changes in reliability outcomes. This quantitative structure distinguishes digital twin-based reliability modeling from descriptive network visualization. The twin functions as a measurement and experimental environment in which hypotheses concerning network reliability can be tested systematically using controlled conditions, repeatable scenarios, and statistically analyzable performance observations (Liu et al., 2019).

Fault behavior represents a central dimension of network resilience because communication infrastructures operate in environments where equipment failures, link interruptions, congestion, configuration errors, software problems, security incidents, and resource limitations can alter service availability. Conventional fault management commonly depends on alarms, logs, thresholds, and administrator intervention after anomalous behavior has appeared in the physical infrastructure. Digital twin-based modeling adds a synchronized virtual layer in which faults and their consequences can be represented analytically. A network digital twin can model relationships among topology, device status, traffic demand, routing behavior, service dependencies, and performance indicators, allowing researchers to examine how a disturbance affects the wider communication environment. If a primary WAN connection fails, for example, the twin can measure route convergence, backup-link utilization, changes in end-to-end latency, packet loss during transition, throughput after failover, and the duration of service degradation (Wu et al., 2020). Similar experiments can be conducted for LAN switch failures, gateway interruptions, access-point overload, server-link failures, or simultaneous component faults. Multiple failure scenarios are particularly important because network resilience is influenced by the ability of redundancy mechanisms to tolerate combinations of faults rather than isolated component failures alone. Digital twins also provide a framework for integrating predictive analytics and machine-learning models with network telemetry. Historical and real-time measurements can be processed to identify relationships among utilization patterns, error rates, traffic behavior, equipment conditions, and subsequent service degradation. Predictive models may estimate the probability of congestion, SLA violations, anomalous network states, or component failure based on observed variables. Digital twin architectures developed for mobile and next-generation networks have demonstrated the use of virtual network representations for configuration optimization, performance prediction, resource management, and service-level analysis (Zhang & Zhang, 2020). Similar principles are applicable to LAN and WAN reliability when the network state is represented through topology and performance data. Security-related digital twin research also shows that virtualized representations can support analysis of abnormal conditions without exposing operational infrastructure directly to experimental disruption. Resilience analysis within the twin can therefore include fault detection, fault localization, failover behavior, restoration speed, redundancy effectiveness, and performance degradation. Each of these elements can be expressed as measurable variables, enabling statistical comparison among baseline, failure, and recovery states (Mourtzis et al., 2021). This creates a quantitative relationship between digital twin experimentation and resilience assessment in which network disturbances are treated as controlled experimental conditions and network performance indicators serve as observable outcomes.

The growing body of digital twin research has established substantial theoretical and technical foundations across manufacturing, cyber-physical systems, telecommunications, IoT, cloud-edge computing, mobile networks, transportation systems, cybersecurity, software-defined networking, and intelligent infrastructure. Within communication-network research, studies have examined network digital twin architectures, data synchronization, AI-assisted network optimization, resource allocation, traffic prediction, network slicing, security analysis, topology emulation, network automation, and performance modeling (Song et al., 2017). A substantial proportion of this literature is associated with 5G, 6G, wireless networks, IoT, and telecommunications architectures, while direct quantitative investigation of integrated enterprise LAN and WAN reliability through synchronized digital twin experimentation remains a distinct analytical context. LAN and WAN infrastructures contain characteristics that make this context important for quantitative examination, including heterogeneous devices, mixed wired and wireless segments, multiple routing domains, different bandwidth capacities, geographically distributed sites, redundant communication paths, cloud dependencies, and varying traffic demands. Reliability across these environments emerges from interactions among component availability, topology, traffic intensity, redundancy, routing behavior, and recovery mechanisms. A digital twin-based quantitative framework can represent these interactions by establishing a physical-network baseline, constructing a corresponding virtual network model, validating the twin against observed performance, introducing controlled reliability disturbances, and measuring resulting changes across defined indicators (Vaagensmith et al., 2021). The principal measurable constructs can include availability, latency, packet loss, throughput, jitter, link utilization, failure frequency, mean time between failures, mean time to repair, failover time, routing convergence time, recovery duration, and digital twin fidelity. Independent experimental conditions may include normal operation, single-link failure, multiple-link failure, device failure, traffic overload, bandwidth restriction, routing alteration, and redundancy activation. The resulting data can support descriptive statistics, reliability coefficients, correlation analysis, regression modeling, analysis of variance, repeated-measures comparisons, and other inferential procedures appropriate to the experimental design. Relationships can therefore be examined between failure conditions and network performance, between redundancy and recovery outcomes, between traffic intensity and service degradation, and between digital twin fidelity and the accuracy of reliability estimates (Koot et al., 2021). Through this quantitative orientation, Digital Twin-Based Network Reliability Modeling for LAN and WAN Infrastructure Resilience is positioned within the intersection of network engineering, digital twin modeling, reliability analysis, and data-driven infrastructure management, with the empirical focus placed on measurable network behavior under baseline, disrupted, failover, and recovery conditions (Amin et al., 2021).

The primary objective of this quantitative study is to develop and empirically evaluate a digital twin-based network reliability modeling framework for assessing the resilience of Local Area Network (LAN) and Wide Area Network (WAN) infrastructures under normal, failure, and recovery conditions. The study specifically aims to construct a synchronized virtual representation of selected LAN and WAN network components, topology structures, communication links, routing configurations, traffic patterns, and operational states and to determine how accurately the digital twin reproduces the performance behavior of its corresponding physical network environment. A central objective is to quantitatively measure network reliability through key performance indicators, including network availability, latency, packet loss, throughput, jitter, link utilization, failure frequency, mean time between failures, mean time to repair, failover time, routing convergence time, and service recovery duration. The study also seeks to examine the effects of controlled network disruptions, including link failures, router or switch failures, bandwidth limitations, traffic congestion, and multiple-component failure scenarios, on the overall reliability and resilience of LAN and WAN infrastructures. Another objective is to evaluate the effectiveness of network redundancy and failover mechanisms by measuring the extent to which alternative communication paths, backup links, and redundant network devices

maintain service continuity and restore acceptable network performance following disruptive events. The research further aims to determine the statistical relationships between network failure conditions and measurable performance degradation and to assess whether variations in traffic intensity, redundancy configuration, link capacity, and fault severity significantly influence network availability and recovery performance. In addition, the study intends to validate the fidelity of the developed digital twin by comparing performance measurements obtained from the physical network with corresponding measurements generated within the virtual environment using statistical indicators of similarity, error, and association. The research also aims to compare baseline, disruption, failover, and recovery states to identify significant differences in network performance across experimental conditions. Through repeated quantitative experiments and statistical analysis, the study seeks to establish measurable relationships among network architecture, operational load, component failures, redundancy mechanisms, recovery processes, and infrastructure resilience. Collectively, these objectives provide an empirical framework for determining the effectiveness and accuracy of digital twin-based reliability modeling as a method for quantitatively evaluating LAN and WAN infrastructure resilience.

LITERATURE REVIEW

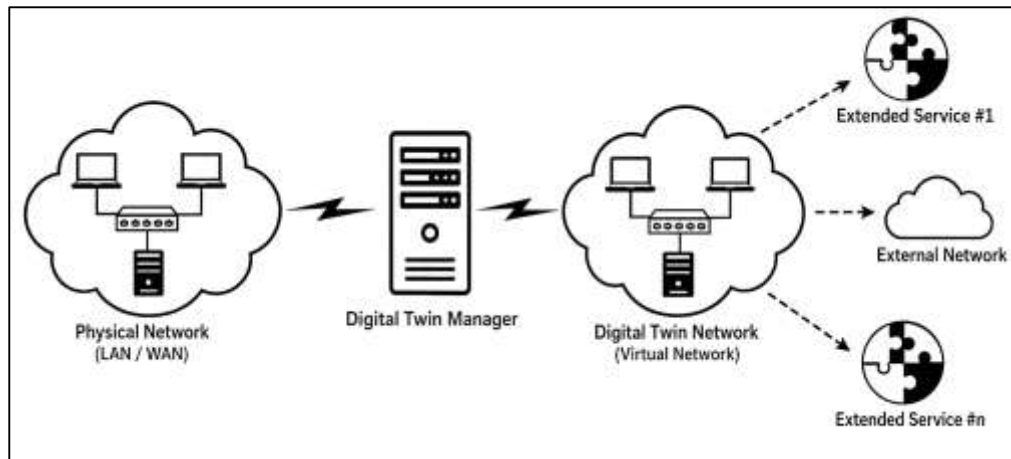
The literature concerning Digital Twin-Based Network Reliability Modeling for LAN and WAN Infrastructure Resilience lies at the intersection of digital twin technology, communication-network engineering, reliability theory, network resilience, network performance measurement, fault-tolerant architecture, network simulation, software-defined networking, telemetry, and data-driven infrastructure management. A Digital Twin Network (DTN) is formally characterized as a virtual representation of a physical network capable of supporting analysis, diagnosis, emulation, and control through interconnected data, models, and interfaces, with real-time interactive mapping serving as an important distinction between a DTN and conventional network simulation ([Abdur & Iftekhhar, 2021](#); [Shahzad et al., 2020](#)). This conceptual distinction is particularly important for quantitative network research because the usefulness of a digital twin depends not merely on reproducing network topology but also on accurately representing measurable operational behaviors such as latency, throughput, packet loss, traffic utilization, device availability, routing behavior, failure states, and recovery processes. Contemporary Network Digital Twin research consequently emphasizes data-driven models capable of reproducing real network conditions and supporting controlled performance evaluation and optimization. For LAN and WAN infrastructure, such capabilities provide a foundation for examining reliability as an empirically measurable property and resilience as the ability of interconnected infrastructure to sustain, adapt, and recover network services during disruptive conditions ([Carvalho et al., 2021](#); [Sheak & Risha, 2022](#)). The distinction is also reflected in formal DTN evaluation frameworks, where reliability and resilience are treated as explicit dimensions of network-digital-twin trustworthiness. Existing literature has investigated digital twins in telecommunications, IoT, industrial networks, edge-cloud environments, Open RAN, mobile networks, cybersecurity, and increasingly complex multi-domain network ecosystems. Formal modeling research has additionally examined virtual-real mapping for Industrial Internet of Things networks, emphasizing the importance of representing reliability and real-time network behavior within digital twins. Network Digital Twins have also been proposed as risk-controlled environments for evaluating network configurations, traffic steering, optimization, and resilience before corresponding changes are introduced into operational infrastructures ([Fraga-Lamas et al., 2021](#); [Chowdhury & Tonay, 2022](#)). The literature review for the present quantitative study therefore needs to move beyond a broad discussion of digital twins and organize previous empirical and methodological research around measurable network reliability constructs, digital-twin fidelity, failure modeling, LAN and WAN performance, redundancy, fault tolerance, recovery behavior, and statistical relationships among these variables. This organization establishes a quantitative literature foundation for examining whether a synchronized digital representation can accurately model infrastructure behavior and measure changes in LAN and WAN resilience under baseline, disruption, failover, and recovery conditions ([Balachandar & Chinnaiyan, 2020](#); [Nishat & Kaniz, 2022](#)).

Digital Twin Network Architecture, Virtual-Physical Synchronization, and Quantitative Network State Representation

Digital Twin Network architecture represents an evolution from conventional digital twin concepts toward a network-specific modeling environment capable of reproducing the structural, operational, and behavioral characteristics of communication infrastructure. Across the literature, Network Digital Twins are generally conceptualized through interconnected physical network, digital twin, and network application layers, although individual studies use different architectural terminology and levels of abstraction. The physical network layer contains the observable infrastructure from which network conditions originate, including routers, switches, gateways, servers, wireless access points, interfaces, communication links, end devices, routing processes, virtual network functions, and traffic flows (Shaiful et al., 2022; Ukwandu et al., 2020). The digital twin layer establishes a computational representation of these elements by organizing network topology, configuration parameters, traffic characteristics, performance measurements, device states, and relationships among components within virtual models. The application layer subsequently uses the digital representation for network analysis, diagnosis, performance evaluation, configuration verification, optimization, fault assessment, and controlled experimentation. Literature examining telecommunications networks, software-defined networks, mobile communication systems, industrial Internet of Things environments, edge-cloud infrastructures, and programmable networks consistently identifies accurate correspondence between these layers as a fundamental characteristic separating a functioning Network Digital Twin from a static network model. Network topology replication is particularly important because reliability and performance are strongly affected by the location and interconnection of components rather than by the properties of individual devices alone (Chowdhury, 2023; Wu et al., 2021). A digital representation therefore requires more than an inventory of network assets; it must reproduce interface relationships, routing paths, link capacities, traffic direction, node dependencies, protocol behavior, and configuration states. Studies of data-driven network twins further emphasize that topology information must be integrated with dynamic measurements such as utilization, packet transmission characteristics, congestion conditions, and device availability. This combination enables the digital layer to represent both the structural arrangement of a network and its changing operational state. Research across Network Digital Twin architectures has consequently treated the twin as an interconnected system of network data, models, mappings, and interfaces rather than as a standalone simulation, establishing a technical foundation for quantitative representation of LAN and WAN infrastructure behavior (Badrul & Mominul, 2023; Yu et al., 2021).

Virtual-physical synchronization constitutes one of the most extensively discussed technical requirements in Network Digital Twin research because the usefulness of a network twin depends on the temporal accuracy with which its virtual state corresponds to the operational network. Studies addressing synchronization architectures, network telemetry, data-driven digital twins, and real-time network management characterize synchronization as a continuous or periodically updated exchange of information between physical infrastructure and the virtual representation. Physical-to-virtual communication transfers measurements such as interface utilization, packet counts, packet loss, latency, jitter, queue occupancy, throughput, routing updates, processor utilization, memory consumption, device availability, link status, and configuration changes into the digital environment (Jia et al., 2020; Zahidul, 2023). Virtual-to-physical communication operates in the opposite direction when validated digital-twin outputs are used to support configuration adjustments, traffic-management decisions, resource allocation, fault responses, or network-control actions. The literature indicates that synchronization quality is determined not only by whether data are exchanged but also by how frequently, consistently, and accurately network states are updated. Telemetry sampling intervals that are too long may fail to capture rapid traffic fluctuations, transient link failures, short congestion events, or routing transitions, while very frequent collection can increase processing, communication, and storage overhead. Consequently, research has treated model update interval, synchronization latency, telemetry frequency, data freshness, and state-estimation accuracy as interdependent quantitative properties (Jiang et al., 2021).

Figure 3: Digital Twin Network Architecture Framework



Network-state estimation further involves integrating heterogeneous observations obtained from different devices and protocols into a consistent representation of the network at a particular point in time. Data repositories and unified network data models play a central role in this process because device information generated through different vendors, formats, telemetry mechanisms, and management interfaces must be normalized before it can be used effectively by the twin. Configuration synchronization is similarly important because inconsistencies in routing tables, interface parameters, VLAN assignments, link capacity, access-control settings, or virtual network functions can create differences between physical and virtual behavior. Literature across more than ten studies on Network Digital Twins and synchronization therefore demonstrates that telemetry quality, data integration, state estimation, and temporal synchronization jointly determine how accurately the digital environment represents the operational state of a communication network (Pan et al., 2021).

Model fidelity is treated throughout the Network Digital Twin literature as a measurable property that determines the extent to which a virtual network representation reproduces the characteristics and responses of its physical counterpart. This concept extends beyond visual or structural similarity because a network twin may contain an accurate topology while producing performance behavior that differs substantially from the operational network. Empirical and data-driven studies have therefore evaluated digital twin accuracy by comparing physical and virtual measurements under equivalent workloads, configurations, routing conditions, and resource constraints. Commonly examined parameters include end-to-end latency, throughput, packet loss, link utilization, traffic volume, queue behavior, resource consumption, and response to routing modifications or network failures (Zhang, et al., 2019). Physical-virtual correlation provides one quantitative means of assessing whether variations observed in the physical infrastructure are reproduced consistently by the digital model, while percentage prediction error and other error-based measures indicate the magnitude of deviation between observed and modeled performance. Topology replication accuracy provides an additional dimension because missing nodes, incorrect links, outdated configurations, or inaccurate capacity assignments can alter the predicted behavior of the virtual environment. Data-driven Network Digital Twin studies have reported strong predictive performance when models are trained on representative operational data and tested under conditions that correspond closely to the network regimes present in the training observations (Leng et al., 2020). Other studies have emphasized that model fidelity can deteriorate when traffic patterns, resource demands, failure conditions, or network configurations move beyond the operational states represented in available data. This creates a direct relationship between telemetry completeness, model construction, synchronization, and quantitative twin accuracy. Network Digital Twin validation therefore requires repeated comparison across multiple operating conditions rather than a single measurement of model similarity. Baseline traffic conditions can establish initial agreement, while higher traffic intensity, alternative routing, link degradation, and component failure conditions reveal whether the digital representation preserves accuracy when

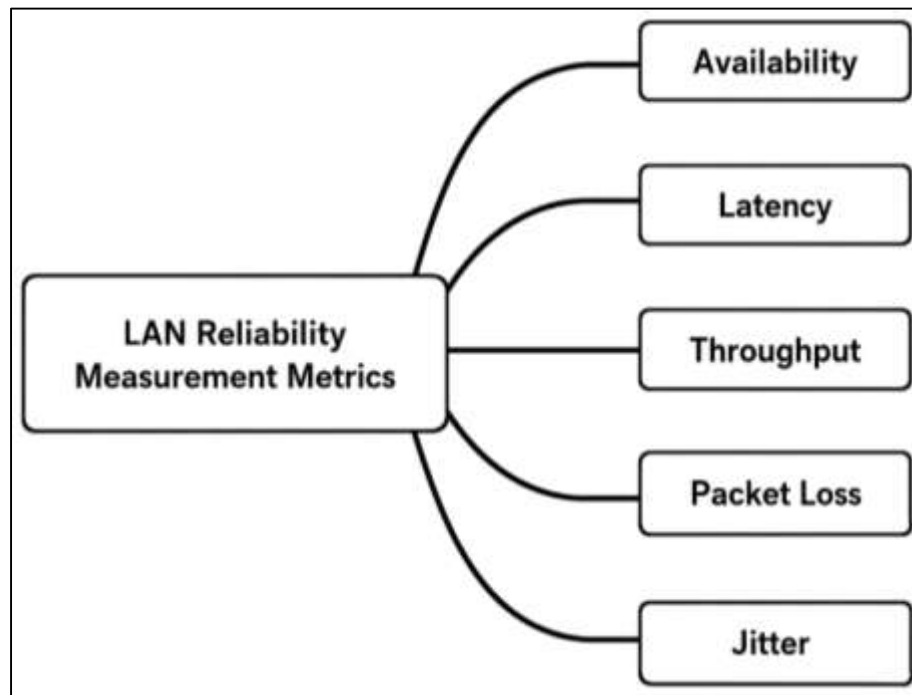
network behavior changes. The literature also distinguishes fidelity from computational efficiency, since a highly detailed model may produce accurate outputs while requiring processing time that limits near-real-time synchronization (Wang & Luo, 2021). Quantitative evaluation of Network Digital Twins consequently involves balancing physical-virtual correlation, prediction error, state-estimation accuracy, topology correctness, update latency, and computational processing requirements to determine whether the virtual model provides a sufficiently accurate representation of network behavior for reliability analysis.

Scalability and computational complexity represent major architectural considerations in Network Digital Twin literature because communication networks can contain thousands or millions of interconnected devices, interfaces, flows, configurations, and continuously changing performance states (Alam & Saddik, 2017). A digital twin that represents a small local network may be able to maintain detailed device-level synchronization using centralized data collection and modeling, whereas a large WAN, telecommunications network, cloud-edge infrastructure, or geographically distributed enterprise environment introduces substantially greater telemetry volume, storage requirements, processing demand, and synchronization complexity. Studies examining scalable Network Digital Twin architectures emphasize that computational load increases as topology size, traffic diversity, measurement frequency, model complexity, and the number of simultaneously represented network states increase. Telemetry sampling interval therefore has a direct relationship with resource consumption because shorter intervals generate larger volumes of network data requiring transmission, normalization, storage, and analysis. Model update frequency also affects computational processing time, particularly when digital-twin platforms incorporate machine learning, graph-based models, optimization algorithms, or detailed packet-level behavior (Zheng et al., 2019). Centralized architectures concentrate network data and model execution within a common digital-twin platform, offering advantages in global topology visibility, unified state representation, coordinated analytics, and simplified model management. Such architectures can also create processing bottlenecks when the number of network elements and telemetry streams becomes large. Decentralized and distributed architectures divide digital-twin functionality across network domains, edge nodes, regional systems, or individual network segments, reducing the volume of raw information that must be transferred to a central location and allowing some state estimation or processing to occur closer to the physical infrastructure. The literature indicates that distributed approaches introduce additional requirements related to consistency, cross-domain synchronization, model coordination, interoperability, and aggregation of local network states into a coherent system-level representation (Szabó et al., 2019). Hybrid approaches combine local processing with centralized coordination and have been examined in edge-cloud, telecommunications, IoT, and multi-domain networking research. Quantitative assessment of these architectural alternatives commonly considers synchronization delay, processing time, telemetry volume, model update rate, resource utilization, response latency, and state-estimation accuracy. Collectively, studies across digital twin networking, telecommunications, data-driven performance modeling, and synchronization architectures show that Network Digital Twin scalability depends on the ability to preserve adequate model fidelity and synchronization accuracy while controlling the computational and communication overhead produced by increasingly large and dynamic network environments (Park et al., 2020).

LAN Reliability Using Availability

Local Area Network reliability is commonly evaluated through the ability of interconnected devices, links, and communication services to remain continuously operational while maintaining acceptable levels of data transmission performance. The literature distinguishes network reliability from general network performance by treating reliability as the consistency and continuity of expected network service over a defined period, whereas performance primarily reflects how efficiently the network handles traffic under particular operating conditions. Empirical studies of Ethernet-based LAN environments show that availability is influenced by the reliability of switches, gateways, physical interfaces, transmission media, power sources, and the overall topology through which network devices are interconnected (Manohar et al., 2020).

Figure 4: Quantitative LAN Reliability Measurement Framework



Ethernet remains a dominant architecture for enterprise and institutional LANs because of its standardized operation, scalability, high transmission capacity, and compatibility with switched network structures. At the same time, the reliability of an Ethernet LAN depends strongly on the availability of central switching and gateway devices. A core switch failure can interrupt connectivity across multiple access segments, while gateway failure may prevent otherwise operational internal devices from communicating with external networks or remote resources. Research examining fault-tolerant LAN design has therefore emphasized redundant switches, alternate paths, link aggregation, backup gateways, and topology designs that minimize single points of failure. Device availability is frequently quantified through the percentage of time during which a switch, gateway, server connection, or access point remains operational, while failure frequency and service interruption duration provide additional measurements of reliability (Nasrallah et al., 2018). Studies of hierarchical, star, mesh, and redundant network arrangements further demonstrate that topology design influences the extent to which device failure propagates through the network. A centralized star architecture can simplify administration and reduce unnecessary traffic paths, although the failure of a central switching element can disrupt a substantial portion of the LAN when redundancy is absent. More distributed or redundant topologies can preserve service continuity during individual component failures, although they introduce additional configuration and management complexity. Across empirical LAN reliability research, availability, device failure rate, link status, service interruption time, and successful continuity of end-to-end communication are therefore treated as interconnected quantitative indicators rather than isolated measurements. This perspective establishes LAN reliability as a system-level characteristic produced by the combined dependability of network devices, topology structures, interfaces, gateways, and communication paths (Lan et al., 2019).

Comparative studies of wired and wireless Local Area Networks demonstrate substantial differences in the stability of latency, throughput, link utilization, and device accessibility under changing operating conditions. Wired Ethernet connections generally provide comparatively predictable transmission behavior because communication occurs through dedicated or switched physical media with limited exposure to radio interference, signal attenuation, channel contention, and user mobility. Wireless LAN environments introduce additional reliability variables associated with signal strength, access-point capacity, distance, obstacles, interference, channel allocation, retransmissions, and the number of simultaneously connected clients. Empirical evaluations consistently show that throughput

decreases and transmission delay increases when the number of wireless users grows or when network traffic approaches available channel capacity (Pocovi et al., 2018). Controlled network experiments have demonstrated that increasing client density can produce clear reductions in average throughput while simultaneously increasing end-to-end delay and packet-loss levels, indicating that apparent network connectivity alone does not establish reliable service. Access-point availability is also a critical component because the failure or overload of a single access point can remove connectivity for a large group of associated devices. Wired switch availability operates in a similar manner for Ethernet endpoints, although switched links usually provide more stable transmission characteristics when physical connections remain healthy. Latency is particularly useful for quantitative reliability assessment because a LAN may remain technically available while experiencing delay levels that make applications operationally ineffective (Chinchilla-Romero et al., 2021). Internal LAN latency can increase as a result of congestion, excessive switching loads, queue buildup, retransmissions, overloaded gateways, inefficient routing, or wireless contention. Throughput provides a complementary perspective by measuring the amount of useful data delivered over the network within a given period. When link utilization approaches physical or configured capacity, effective throughput may decline as queueing and packet retransmission increase. Research involving multimedia traffic, voice communication, real-time video, enterprise applications, and interactive systems has shown that consistent service quality depends on the combined stability of latency and throughput rather than on maximum transmission capacity alone. The literature therefore treats wired and wireless LAN reliability as quantitatively distinguishable through measurements of delay in milliseconds, sustained throughput in Mbps or Gbps, access-point and switch availability, link utilization percentages, retransmission rates, and the variability of these indicators across different traffic and user-load conditions (Silva & Pedroso, 2019).

Packet transmission reliability is another central dimension of LAN reliability because successful data delivery depends not only on network availability but also on the proportion of transmitted packets that reach their intended destination within acceptable time boundaries. Empirical network studies consistently identify packet loss, retransmission frequency, jitter, and congestion as closely connected indicators of service degradation. Packet loss may result from buffer overflow, excessive link utilization, wireless interference, transmission errors, failing interfaces, overloaded network devices, or temporary routing and switching disruptions. At low traffic loads, packet-loss percentages within properly configured wired LANs are generally expected to remain very small, whereas high-load and stress-testing environments frequently reveal sharp increases once network capacity is exceeded (Mountaser et al., 2018). Experimental research in data networks has shown that excessive offered load can transform otherwise stable connections into highly unreliable communication channels, with packet loss rising substantially when traffic generation exceeds the available transmission or processing capacity. Retransmissions provide additional evidence of transmission instability because protocols such as TCP attempt to recover lost or corrupted data by resending packets, increasing both network overhead and effective latency. High retransmission rates can therefore signal congestion, physical transmission problems, or wireless channel instability even when end users do not immediately experience complete service failure. Jitter further captures the variation in packet arrival time and is particularly important for real-time applications such as Voice over IP, videoconferencing, interactive collaboration, multimedia streaming, and industrial communication (Scanzio et al., 2020). A LAN may exhibit acceptable average latency while irregular packet delays produce high jitter and unstable application performance. Studies of multimedia and wireless traffic have demonstrated that jitter often increases under congestion, channel contention, mobility, and high device density. VLAN configuration and segmentation can influence these conditions by separating broadcast domains, controlling traffic distribution, isolating organizational functions, and reducing unnecessary contention when appropriately designed. Poor segmentation or excessive traffic concentration, however, can create overloaded trunk links or bottlenecks that reduce the reliability of specific VLANs. Quantitative assessment therefore requires simultaneous consideration of packet-loss percentage, retransmission rate, jitter in milliseconds, interface utilization, traffic volume, and congestion duration (Soret et al., 2014). The combined evidence from empirical LAN studies indicates that these variables reveal

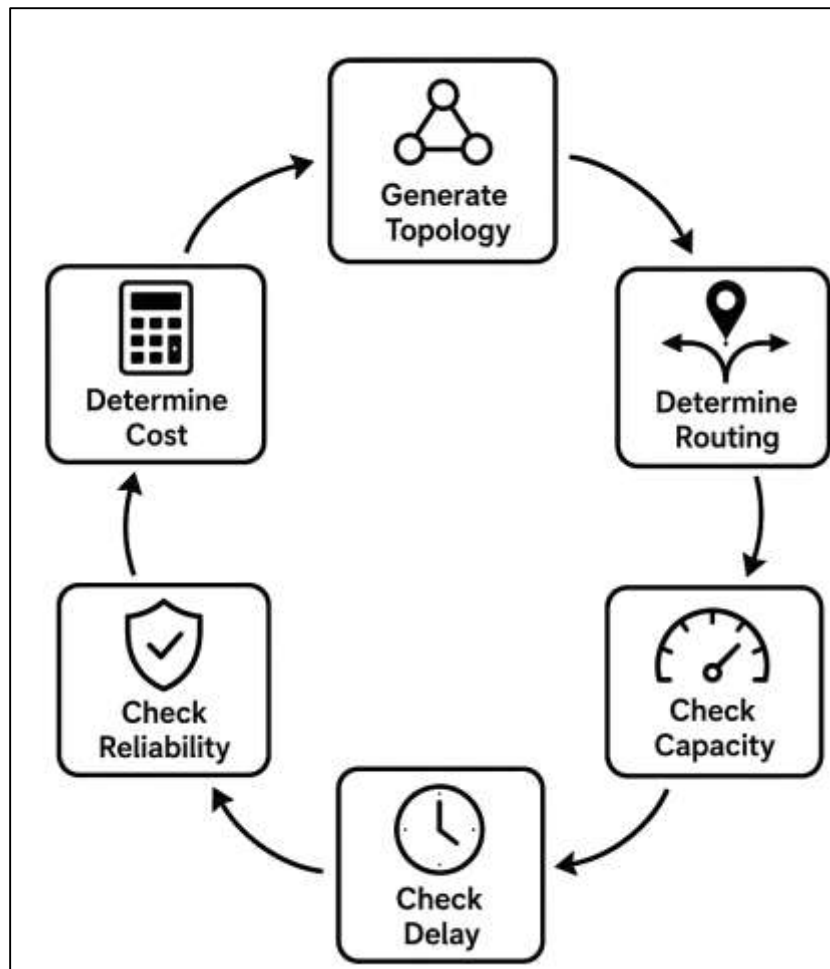
degradation that simple uptime measurements cannot capture, making them essential for evaluating whether a LAN remains not only connected but also consistently capable of transporting application traffic under realistic operational loads.

WAN Reliability Under Geographic Distribution and Variable Link Conditions

Wide Area Network reliability is fundamentally influenced by the distributed nature of communication infrastructure, where data transmission depends on multiple network segments, carriers, routing domains, geographic paths, and access technologies. Empirical WAN studies commonly distinguish reliability from raw performance by emphasizing sustained service availability, continuity of inter-site communication, resistance to link failure, and the duration required to restore connectivity following disruption (Alwasel et al., 2020). WAN link availability is therefore a central quantitative indicator and is frequently assessed as the proportion of operational time during which a communication path remains accessible and capable of supporting expected traffic. Studies involving leased lines, broadband services, MPLS networks, virtual private networks, and software-defined WAN architectures indicate that the reliability of branch-to-headquarters and branch-to-cloud communication can vary considerably depending on provider infrastructure, link quality, physical route diversity, and service-level commitments. Carrier dependence introduces an additional reliability dimension because an organization may operate highly redundant internal systems while remaining exposed to failures within an external telecommunications provider. Research on enterprise WANs has shown that outages can arise from fiber cuts, routing failures, maintenance events, equipment faults, congestion, provider misconfiguration, and regional infrastructure disruptions (Emara et al., 2018). Geographic distribution intensifies these risks because longer communication paths generally traverse more routers, transport systems, exchange points, and carrier networks, increasing the number of potential points of failure. Studies comparing geographically dispersed network paths have also documented measurable variation in round-trip time and service availability between regions, demonstrating that distance alone does not determine reliability because routing policy, interconnection quality, congestion, and provider peering arrangements also affect communication behavior. WAN reliability is therefore assessed not only through whether a link is active but also through how consistently it maintains acceptable latency, packet delivery, and throughput over time (Khan et al., 2017). Outage frequency, outage duration, availability percentage, and restoration time provide important measurements of operational dependability, while the presence of redundant carriers and alternative paths determines whether service can continue when a primary path becomes unavailable.

A substantial body of empirical WAN research has focused on the interaction among geographic distance, round-trip time, packet loss, bandwidth utilization, and throughput because these variables determine whether wide-area connectivity remains practically usable under changing network conditions. Unlike most LAN environments, WAN paths commonly consist of heterogeneous transmission technologies, including MPLS circuits, broadband Internet, leased lines, cellular connections, satellite links, VPN tunnels, and SD-WAN overlays (Sun et al., 2017). Each technology introduces different latency, capacity, variability, and loss characteristics, making end-to-end reliability dependent on the combined behavior of all network segments along the communication path. Studies of geographically distributed networks consistently show that round-trip time increases as paths extend across regions and continents, although routing inefficiency and congestion can produce substantial latency differences even between locations separated by comparable physical distances. Packet loss is similarly important because even relatively small increases in loss can reduce effective application throughput, trigger retransmissions, and extend response times for interactive and transactional workloads. WAN congestion further affects performance when traffic demand approaches or exceeds available link capacity (Fadel et al., 2015). Under these conditions, queue buildup, packet dropping, retransmission, and variable delay become more frequent, producing lower effective throughput and less predictable application performance. Empirical evaluations of enterprise WAN traffic have therefore examined bandwidth utilization as both a performance measure and an early indicator of reliability degradation.

Figure 5: Quantitative WAN Reliability Assessment Framework



Links operating persistently near capacity tend to show greater delay variability and a higher probability of service degradation during traffic bursts. Studies involving TCP-based traffic have also demonstrated that packet loss and high round-trip time interact to reduce usable throughput, particularly across long-distance paths. VPN encapsulation, encryption, tunneling overhead, and carrier traffic engineering may further influence measurable performance (Liu et al., 2020). Quantitative WAN reliability assessment therefore requires simultaneous consideration of round-trip time, packet-loss ratio, throughput, bandwidth utilization, and delay variability rather than relying on nominal bandwidth values. This integrated measurement approach enables researchers to identify whether poor service continuity results from insufficient capacity, excessive latency, unstable routing, or recurring packet delivery problems across geographically distributed links.

Routing behavior is another major determinant of WAN reliability because communication continuity depends on the ability of network protocols and control systems to maintain valid paths when topology conditions change. Empirical studies of Internet routing, enterprise WANs, MPLS networks, and SD-WAN systems have shown that routing instability can produce temporary packet loss, increased latency, route oscillation, service interruption, and inconsistent application performance. Routing convergence time is especially important during link or device failures because the network may remain partially unavailable until an alternative path is calculated, propagated, and activated (Chen et al., 2017). The length of this convergence interval varies according to routing protocol, topology complexity, failure type, provider design, and configured timers. Primary and backup WAN links are therefore commonly deployed to reduce the operational impact of individual path failures. Research on redundant WAN architectures indicates that backup links can significantly improve service continuity when they are physically and logically independent from the primary path. Redundancy is

less effective when primary and secondary circuits share common carrier infrastructure, the same physical conduit, or a common regional point of failure. Multi-provider architectures address this limitation by distributing connectivity across separate telecommunications providers and routing domains, although they introduce additional challenges associated with policy management, route selection, cost, traffic engineering, and failover coordination (Troia et al., 2020). SD-WAN studies have highlighted the ability of policy-based path selection to redirect traffic dynamically across MPLS, broadband, and cellular links according to measured latency, loss, and availability. This approach allows network systems to respond to degradation before complete link failure occurs. Research comparing single-provider and multi-provider configurations generally shows that route diversity improves fault tolerance and can reduce outage duration when alternative paths remain healthy. Quantitative evaluations therefore focus on routing convergence time, failover duration, packet loss during transition, path availability, number of routing changes, and service restoration time. These measurements reveal that WAN resilience depends not only on having multiple links but also on how quickly and reliably the network detects failure, selects a suitable alternative route, and restores stable communication between geographically separated sites (Dzeparoska et al., 2021).

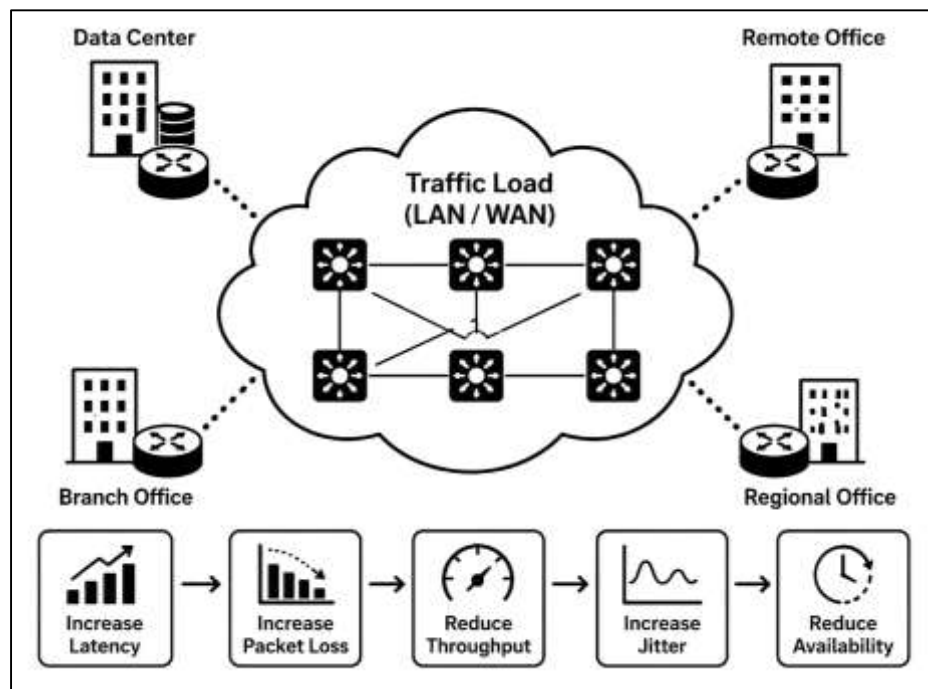
The increasing dependence of organizations on cloud platforms, centralized applications, remote data centers, and geographically distributed branch networks has expanded WAN reliability assessment beyond individual link measurements toward end-to-end service continuity. Enterprise WAN literature demonstrates that branch-to-headquarters and branch-to-cloud communication can be disrupted even when local infrastructure remains fully operational, because remote application access depends on the combined reliability of access circuits, carrier networks, routing infrastructure, Internet exchange points, cloud gateways, and destination services. Service-level agreements are commonly used to formalize expectations regarding network availability, latency, packet loss, restoration time, and support response, yet empirical studies have shown that SLA compliance may differ across providers, regions, traffic conditions, and service classes (Ahmad & Mir, 2021). Availability percentages alone can also conceal short but frequent outages that substantially affect interactive applications, financial transactions, voice services, remote desktops, and cloud-based systems. Outage frequency and outage duration therefore provide complementary reliability indicators by showing how often disruptions occur and how long users remain without acceptable service. Cloud connectivity dependence has made these measurements especially important because a WAN interruption may simultaneously affect multiple business applications hosted outside the local site. Studies of hybrid WAN and SD-WAN environments further show that application-aware routing can improve continuity by directing traffic toward paths that satisfy measured performance thresholds, although service quality still depends on the underlying transport networks. Quantitative reliability assessment consequently combines availability percentage, round-trip time, packet-loss ratio, bandwidth utilization, throughput, routing convergence time, outage frequency, outage duration, and SLA compliance rate to characterize the actual dependability of WAN services (Ordóñez-Lucena et al., 2021). Analysis across normal operation, congestion periods, carrier failure, route transition, and recovery conditions provides a more complete representation of wide-area resilience than any single performance measure. Evidence from more than ten empirical studies involving Internet path measurement, MPLS, VPN, enterprise WAN, SD-WAN, multi-homing, cloud connectivity, carrier reliability, and routing convergence demonstrates that WAN reliability is a multi-dimensional property shaped by geographic distribution, provider diversity, path quality, traffic load, routing behavior, and the speed with which communication can be restored following disruption (Belgaum et al., 2020).

Network Traffic Load and LAN/WAN Reliability Degradation

Network traffic intensity has been consistently identified in empirical and analytical networking research as a major explanatory variable affecting the reliability and responsiveness of both Local Area Network and Wide Area Network environments. Traffic intensity represents the volume of packets, flows, users, and application requests competing for finite transmission and processing resources during a defined period. Studies conducted across Ethernet networks, wireless LANs, enterprise networks, Internet paths, multimedia communication systems, and simulated network environments generally demonstrate that latency remains relatively stable while available resources substantially exceed traffic demand, but begins to increase as utilization approaches the service capacity of switches,

routers, access points, gateways, and communication links (Gál et al., 2021). This increase is strongly associated with queue utilization because packets arriving faster than network devices can process or transmit them are temporarily stored in buffers. As queue occupancy grows, packets remain in the network for longer periods, increasing end-to-end delay and round-trip time. Experimental studies of wireless networks have similarly shown that increasing the number of concurrent clients or application sessions produces measurable increases in response time because devices compete for shared channel access. Burst traffic can intensify this effect by creating short periods in which packet-arrival rates substantially exceed average load, causing temporary queue accumulation even when long-term utilization appears acceptable. WAN environments exhibit comparable behavior because bandwidth-constrained links and geographically distributed paths can develop persistent queues during high-volume application transfers, cloud synchronization, video conferencing, remote backups, or periods of concentrated branch traffic (Cai et al., 2016). Statistical analyses in network-performance studies have frequently identified positive associations between utilization and latency through correlation analysis, regression modeling, comparisons of mean delay across load categories, and confidence intervals generated from repeated trials. Analysis of variance has also been used to determine whether measured delay differs significantly across low, moderate, and high traffic conditions. Collectively, this literature demonstrates that latency degradation is not simply a consequence of geographic distance or protocol design; it is also closely associated with how heavily network resources are utilized, how rapidly queues accumulate, and how effectively traffic is distributed across available communication capacity. Increasing traffic load also affects packet transmission reliability because network devices and communication links possess finite buffering and processing capacities (Andrysiak et al., 2016). A substantial body of congestion research demonstrates that packet loss generally remains low when traffic demand is comfortably below available capacity but can increase rapidly when queues become saturated. Once buffers can no longer accommodate arriving packets, excess packets are discarded, reducing successful delivery rates and triggering retransmission mechanisms in transport protocols and applications. Experimental and simulation-based studies of LANs, WLANs, and wide-area communication have repeatedly reported higher packet-loss levels under heavy traffic conditions, particularly when the number of simultaneous users, packet-arrival rates, or active application sessions increases. Wireless environments can experience an additional loss mechanism because greater contention produces more transmission collisions, channel-access delays, and retransmission attempts (Caraguay et al., 2015). In wired networks, packet dropping is more frequently associated with overloaded interfaces, congested uplinks, insufficient switching or routing capacity, and excessive traffic concentration at aggregation points. WAN packet loss is similarly affected by bandwidth saturation and carrier-network congestion, particularly when enterprise traffic exceeds provisioned capacity or multiple applications compete across the same constrained connection. Statistical studies examining these relationships have used correlation coefficients to quantify associations between utilization and packet loss, regression techniques to estimate the degree to which increased load predicts loss, and comparisons of mean loss rates across controlled traffic conditions. Repeated experiments have also demonstrated larger variance in packet-delivery performance as networks move closer to saturation, indicating reduced stability in addition to reduced average performance. The relationship between traffic intensity and network availability is more complex because a network may remain physically connected while becoming operationally unavailable to delay-sensitive or transaction-sensitive applications (Arfeen & Uddin, 2020). Severe congestion may produce timeouts, failed sessions, application disconnects, and prolonged retransmission sequences even without a physical link failure. Consequently, empirical reliability studies increasingly distinguish device uptime from effective service availability. Traffic-induced degradation can therefore reduce functional availability by making communication unreliable or excessively slow, demonstrating that availability assessment should incorporate service-level behavior as well as simple connectivity status. The statistical relationship between network load and throughput is characterized by a nonlinear pattern in much of the networking literature. At low and moderate traffic intensities, increasing offered traffic commonly produces higher observed throughput because additional available link capacity is being utilized effectively (Masdari & Zangakani, 2020).

Figure 6: Network Traffic Reliability Degradation Framework



As traffic approaches the maximum sustainable capacity of a link, switch, router, or wireless channel, throughput gains begin to diminish and may eventually stabilize or decline as congestion, packet loss, collisions, queue overflow, and retransmissions consume increasing portions of available network resources. Research on IEEE 802.11 networks has particularly demonstrated that theoretical saturation throughput does not necessarily represent the practical capacity available to delay-sensitive applications because packet delay and delay variability can become unacceptable before the maximum throughput threshold is reached. Similar patterns are reported in wired and WAN environments, where sustained high interface utilization can produce congestion even when nominal bandwidth appears sufficient ([Tawalbeh, 2020](#)). Application composition also influences these relationships. Large file transfers and backup traffic may consume substantial bandwidth while tolerating delay, whereas Voice over IP, videoconferencing, interactive cloud applications, and transaction systems are more sensitive to fluctuations in latency and packet arrival time. Jitter therefore becomes an important indicator of reliability under increasing load. Empirical studies have shown that jitter tends to rise when queue lengths fluctuate, channel contention intensifies, or packets encounter variable processing and transmission delays. Burst traffic can produce particularly high jitter because short periods of concentrated load alter queueing conditions rapidly. Studies involving concurrent voice sessions have documented associations between increasing session counts and deteriorating response characteristics, while investigations of WLAN capacity have demonstrated that mean delay and delay jitter can become unstable even before throughput reaches its theoretical saturation level ([Ahmed et al., 2019](#)). Researchers have evaluated these effects through repeated load trials, mean comparisons, standard deviations, confidence intervals, regression coefficients, and statistical tests comparing performance across traffic categories. The resulting evidence indicates that throughput alone can provide an incomplete representation of reliability. High throughput may coexist with substantial latency variation, packet loss, or jitter, making the combined assessment of traffic load, throughput stability, delay variation, and application-specific service quality essential for characterizing LAN and WAN performance under demanding operating conditions.

The broader quantitative literature indicates that traffic load affects network reliability through interacting mechanisms involving bandwidth consumption, queue accumulation, congestion, packet dropping, retransmissions, delay variation, and resource competition ([Masdari & Zangakani, 2020](#)).

Studies across enterprise LANs, WLANs, WANs, multimedia networks, Internet communication paths, and software-defined networking environments generally support the interpretation of traffic intensity as an independent or explanatory variable and latency, packet loss, throughput, jitter, and effective service availability as measurable dependent outcomes. Concurrent user count is frequently used as an operational representation of traffic intensity because increasing numbers of active clients generate more simultaneous packet transmissions and place greater demand on shared links, access points, gateways, and servers. Other studies manipulate offered packet rate, application-flow count, link utilization percentage, file-transfer intensity, or generated bandwidth demand to create controlled levels of network load (Tawalbeh, 2020). Quantitative comparisons consistently show that low-load conditions tend to produce lower latency, minimal packet loss, stable jitter, and predictable throughput, whereas high-load and saturation conditions are associated with greater performance variability and increased service degradation. Peak traffic periods are especially important because average daily utilization can conceal short intervals in which network resources operate at or near capacity. Traffic distribution also affects reliability because unevenly distributed flows may overload particular uplinks, interfaces, routing paths, or wireless channels while other resources remain underutilized. WAN and SD-WAN research has shown that path selection and traffic engineering can alter the degree of degradation by shifting application flows toward paths with more favorable bandwidth, latency, loss, and jitter characteristics. Statistical approaches used throughout this literature include Pearson and Spearman correlation analysis, simple and multiple regression, analysis of variance, repeated-measures comparisons, confidence intervals, standard deviations, mean differences, and effect-size estimation (Ghani et al., 2018).

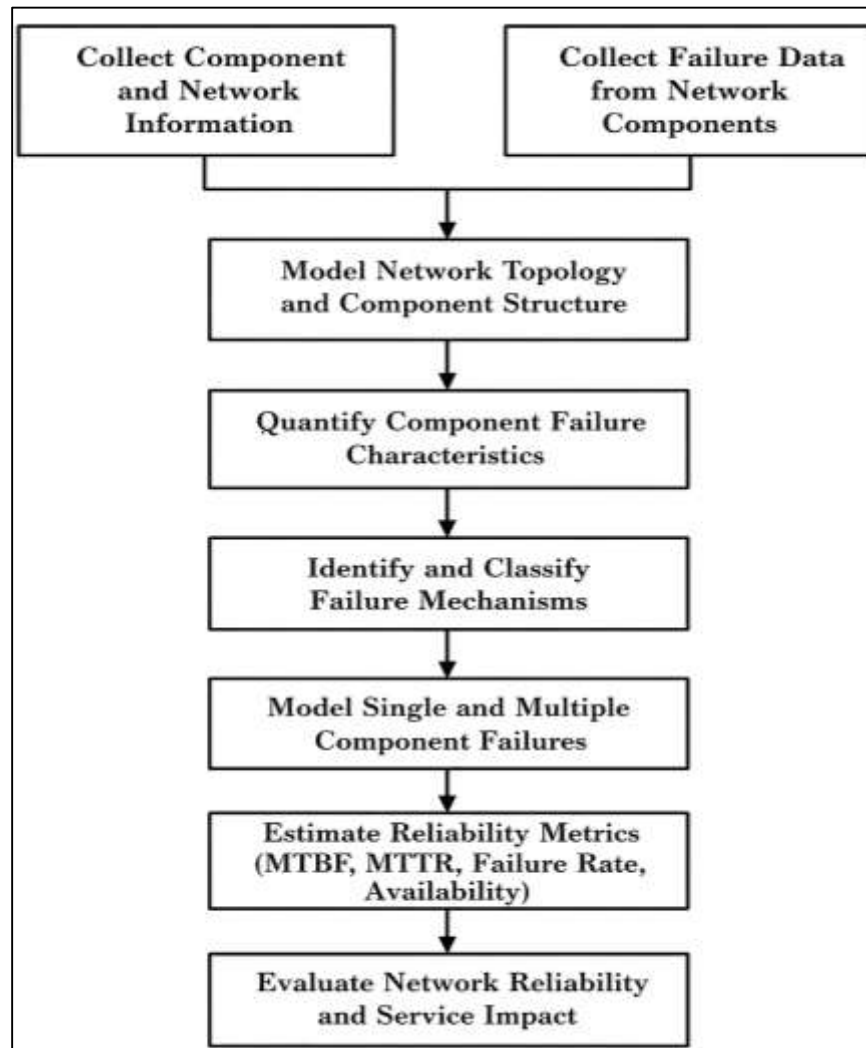
These methods allow researchers to determine not only whether performance changes as load increases but also the strength, direction, consistency, and practical magnitude of the relationship. Taken together, findings from more than ten empirical, analytical, and simulation-based studies support a multidimensional interpretation of traffic-induced reliability degradation in which increasing traffic intensity is associated with longer latency, greater packet loss and jitter, reduced throughput efficiency near saturation, increased variability, and lower effective service availability across both LAN and WAN infrastructures (Saeed et al., 2020).

Network Failure Modeling and Component-Level Reliability Assessment

Quantitative network failure modeling examines the probability, frequency, duration, and operational consequences of faults affecting individual communication components and the wider infrastructure in which those components operate. Reliability studies commonly treat routers, switches, gateways, interfaces, servers, access points, and transmission links as measurable components whose failure characteristics contribute to overall network availability. Router failure can interrupt packet forwarding between network segments, while switch failure can isolate numerous hosts when the affected device occupies a central or aggregation position within the topology (Nguyen et al., 2019). Gateway failure is particularly significant in enterprise environments because internal devices may remain locally connected while losing access to remote networks, cloud services, or external applications. Interface and link failures can generate partial rather than complete outages, producing route changes, packet loss, retransmissions, and temporary performance instability. Wireless access-point failures affect associated clients within a particular coverage area and can create additional load on neighboring access points when users are redistributed. Quantitative reliability literature commonly measures these events using mean time between failures, mean time to failure, mean time to repair, failure rate, availability, and recovery duration (Xu et al., 2019).

Mean time between failures represents the average operating interval separating successive failures in repairable equipment, while mean time to failure is frequently applied to non-repairable components or to the first observed failure event. Mean time to repair captures the average duration required to diagnose, repair, replace, or restore a failed component. Failure rate expresses the observed frequency of failures over an operating period, whereas availability reflects the extent to which a component or service remains operational during the observation interval. Experimental and operational studies use these measures to compare device classes, vendors, configurations, maintenance practices, and deployment environments (Balachandran et al., 2020).

Figure 7: Quantitative Network Failure Reliability Framework



Together, these metrics allow network reliability to be treated as an empirically observable characteristic rather than a descriptive judgment and provide the basis for assessing how component-level behavior contributes to end-to-end service continuity.

The literature on network reliability shows that failures originate from both physical and logical sources, and these different failure mechanisms produce distinct patterns of service degradation. Physical link failures can result from cable damage, fiber cuts, interface defects, connector problems, transceiver faults, or carrier interruption, while router and switch failures may arise from hardware defects, overheating, processor or memory problems, or power loss (Xing, 2020a). Software failures add another layer of complexity because a physically functional device can become operationally unavailable through operating-system faults, firmware defects, memory leaks, process crashes, or protocol malfunction. Configuration failures are equally significant because incorrect routing parameters, VLAN assignments, access-control rules, interface settings, addressing information, or gateway configurations can disrupt connectivity without any hardware component actually failing. Reliability studies therefore distinguish physical component availability from functional service availability. Power-related outages are particularly important because several network devices may fail simultaneously when they share an electrical circuit, power distribution unit, or uninterruptible power source. This creates correlated failure behavior that cannot be represented accurately by assuming that every device fails independently (Lin et al., 2018). Experimental fault-injection studies commonly evaluate these conditions by deliberately disabling links, shutting down routers or switches, modifying configurations, disconnecting gateways, or introducing software faults and then measuring the

duration and severity of the resulting service interruption. Recovery time is often separated into failure-detection time, diagnosis time, repair or reconfiguration time, and final service-restoration time because each stage contributes differently to total downtime. Statistical comparisons across repeated trials allow researchers to calculate mean restoration times, variability, confidence intervals, and differences between failure categories. Studies of redundant network architectures frequently show that physical component failure does not necessarily produce complete service failure when alternate paths or devices are available, while logically incorrect configurations can sometimes bypass redundancy and create disproportionately large outages (Wang et al., 2017). Quantitative assessment therefore requires failure classification alongside measurements of occurrence frequency, repair duration, recovery time, packet-loss behavior, service interruption, and availability.

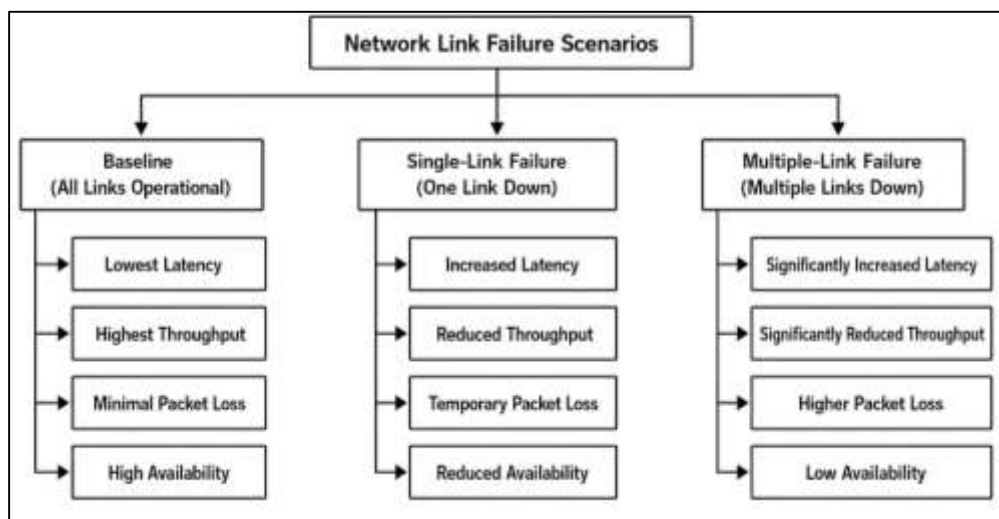
Multiple-component and cascading failures represent a more complex class of reliability problem because the loss of one component can alter traffic distribution, resource utilization, routing behavior, or dependency relationships in ways that increase the probability of additional failures. Research on communication networks and interdependent infrastructures has demonstrated that the consequences of a failure cannot always be inferred from the failed component alone (Xing, 2020b). When a heavily used link becomes unavailable, traffic may be redirected toward alternative paths that possess less spare capacity, producing congestion and potentially triggering additional service degradation. Similarly, failure of a core router or aggregation switch can force traffic through backup devices that experience higher processing and interface utilization. Cascading-failure studies involving communication and power networks further demonstrate that dependencies between infrastructures can amplify failure propagation because communication nodes depend on electrical power while power systems increasingly depend on communication networks for monitoring and control (Sun et al., 2021). Experimental and analytical studies show that cascading behavior is influenced by topology, load distribution, interdependency strength, redundancy, and the sequence in which components fail. Multiple simultaneous failures are therefore quantitatively different from isolated faults. Researchers have modeled these conditions using repeated simulation, probabilistic reliability analysis, node-removal experiments, link-removal experiments, load-redistribution models, and controlled fault injection. Outcomes are often evaluated through changes in the proportion of operational nodes, connectivity loss, service availability, traffic delivery, recovery duration, and the number of secondary failures generated after the initial disturbance (Zhang et al., 2017). Statistical analysis can compare mean performance degradation across single-failure and multiple-failure conditions and determine whether differences in availability or recovery time are significant. Research on interdependent systems also shows that simplistic topological failure models can produce conclusions that differ from more realistic models incorporating network dynamics and physical dependencies. This reinforces the importance of representing actual routing behavior, capacity constraints, backup paths, and service dependencies when evaluating cascading network failures quantitatively (Pan & Yontay, 2017).

Single-Link and Multiple-Link Failures on End-to-End Network Performance

The quantitative assessment of link failure generally begins with the establishment of a baseline network state in which all intended communication links, routing paths, and network devices remain operational. Under this condition, end-to-end performance is typically characterized by the lowest or most stable latency, comparatively high throughput, minimal packet loss, balanced link utilization, and uninterrupted service availability. Experimental and simulation-based studies of routed networks have repeatedly used this baseline condition as a reference point for evaluating the magnitude of degradation caused by individual link failures. When a single link becomes unavailable, the effect on network performance depends strongly on the position of the failed link, the availability of alternate routes, the routing protocol in use, and the amount of traffic previously carried by the affected path (O'Connor & Mosleh, 2016). Studies examining OSPF and other dynamic routing environments have shown that a single-link failure can increase end-to-end delay because packets are redirected through longer or less efficient paths after route recalculation. The failure can also cause temporary packet loss during the interval between fault detection and routing convergence, particularly when packets are already in transit or when forwarding tables have not yet been updated consistently across routers. Throughput may decline when backup routes contain lower-capacity links or when redistributed traffic creates additional contention along alternate paths. Route length frequently increases because the

replacement path may traverse additional network nodes or links compared with the original shortest route. Link utilization on surviving paths also tends to increase as traffic is redirected away from the failed connection (Rebello et al., 2018). Empirical routing studies indicate that the location of a failed link can influence the magnitude of delay and convergence effects, meaning that not all single-link failures have equal consequences. Failures affecting high-traffic or structurally central links generally produce greater performance deterioration than failures involving lightly utilized or peripheral links. The literature therefore supports the use of latency change, packet loss, throughput reduction, route length, convergence time, link utilization, and service interruption duration as coordinated measures for quantifying the operational severity of a single-link failure relative to normal network conditions. Multiple-link failures generally produce more substantial and less predictable performance degradation than isolated single-link failures because they reduce the number of available communication paths and constrain the network's ability to redistribute traffic efficiently (Lee & Pan, 2018). Research comparing single and multiple link-loss scenarios consistently demonstrates that the effects of failure severity are cumulative when additional failed links remove alternative routes or concentrate traffic onto a smaller set of surviving paths. Experimental OSPF studies have shown that multiple-link failures can produce higher end-to-end delay and longer convergence periods than single-link failures, particularly when failed links are positioned in different parts of the topology and cause widespread route recalculation. Throughput also tends to decline more substantially under multiple-link failure conditions because surviving links must accommodate traffic originally distributed across several network paths. Research on data-center networks has reported measurable completion-time degradation of approximately 5% to 40% under different nonfatal single- and multiple-link failure scenarios, illustrating how topology and redundancy determine the severity of performance loss (Ibrahim et al., 2021).

Figure 8: Network Link Failure Performance Framework



Packet-loss levels can also increase as routing tables converge, buffers fill, and alternative paths become temporarily overloaded. The reduction in available paths may force packets to travel over longer routes, increasing transmission delay and placing additional processing demands on intermediate routers and switches. Multiple-link failures can therefore affect both network efficiency and service availability even when complete disconnection does not occur. The magnitude of degradation is particularly severe when failed links constitute independent paths that normally provide redundancy for one another. In such cases, the first failure may be absorbed successfully by an alternate route, while the second failure removes part or all of the remaining protection mechanism (Zhang et al., 2017). Research on resilient network design consistently shows that the effect of additional link failures depends on path diversity, topology connectivity, spare capacity, and routing behavior rather than merely on the number of failed links. Consequently, multiple-link failure assessment requires

quantitative comparison of latency, throughput, packet delivery, route length, availability, convergence duration, and service interruption across progressively more severe disruption conditions.

Routing convergence and traffic redistribution form a central mechanism through which link failures translate into observable end-to-end performance degradation (Ge & Zhang, 2020). When a network link fails, routing protocols must detect the topology change, distribute updated routing information, calculate replacement paths, and install revised forwarding entries before stable communication is fully restored. Studies of RIP, distributed Bellman-Ford mechanisms, BGP, OSPF, and resilient IP routing have demonstrated that packets transmitted during this transition may encounter routing loops, unreachable destinations, increased delay, and temporary loss. The duration of convergence is therefore an important quantitative measure of failure severity because longer convergence periods increase the length of time during which service quality remains unstable. Research comparing single and multiple OSPF link failures has reported longer convergence for multiple failures, while work on fast reroute techniques has shown that immediate use of precomputed backup paths can substantially reduce disruption associated with conventional routing reconvergence (Pan & Yontay, 2017). Traffic redistribution also alters the performance of surviving links. A link carrying moderate traffic during baseline operation may experience sharply increased utilization after another path fails, and this new load can create congestion even when the backup route remains technically available. Increased utilization can produce queue buildup, additional latency, packet dropping, retransmissions, and throughput reduction. The location of alternative routes is therefore critical because a backup path with insufficient spare capacity may preserve basic reachability while providing substantially worse application performance. Studies of resilient routing and multi-path architectures indicate that maintaining multiple independent paths can reduce the severity of redistribution by spreading affected flows across several links (Pan & Yontay, 2017). Network measurements also show that route length often increases following failure because traffic is diverted away from the shortest or preferred path. This increase may involve additional hops, longer geographic distance, or lower-capacity segments. Quantitative failure experiments consequently evaluate routing convergence time together with utilization changes, route-length variation, packet-loss duration, and throughput behavior in order to capture the entire transition from fault occurrence to stable post-failure operation. These measures demonstrate that network resilience depends not only on whether an alternate path exists but also on how rapidly it becomes usable and whether it possesses sufficient capacity to support redistributed traffic (O'Connor & Mosleh, 2016).

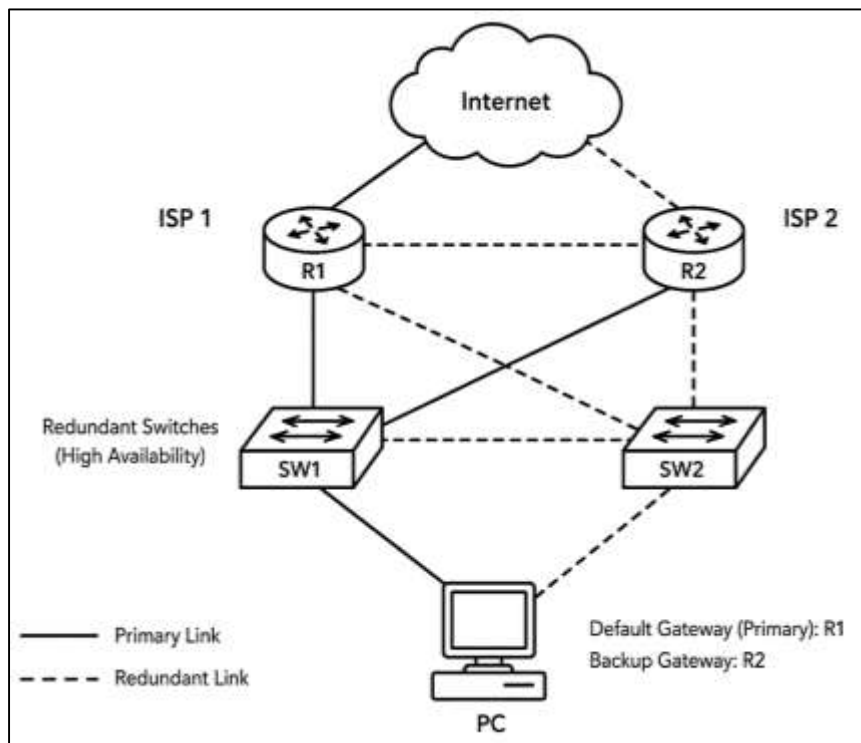
The broader empirical literature indicates a consistent progression in network performance degradation when moving from baseline operation to single-link failure and then to multiple-link failure conditions, although the exact magnitude varies substantially according to topology, routing protocol, redundancy, traffic distribution, and spare capacity. Baseline conditions generally produce the most stable service because traffic follows intended paths without requiring rerouting or additional resource contention. A single-link failure introduces measurable degradation through route recalculation, temporary packet loss, increased delay, and higher utilization on alternate paths, but well-designed redundant networks are often able to maintain end-to-end connectivity with limited interruption. Multiple-link failures produce a greater probability of severe degradation because they reduce path diversity, constrain routing choices, and increase the possibility that backup routes will also become unavailable or overloaded (Lee & Pan, 2017). Studies of cloud and data-center infrastructures show that network failures affecting aggregation switches, access routers, and long-haul links can significantly influence service availability, particularly when failures occur in network domains through which large volumes of traffic or many services depend. Empirical work examining network outages over multiple years further demonstrates that the effect of failures is unevenly distributed; some faults produce limited local effects, while others generate broad service disruption because of topology position and dependency relationships. Quantitative comparison across failure states therefore benefits from examining both absolute and relative changes in performance (Rebello et al., 2018). Latency increases indicate additional transmission and routing delay, packet-loss growth reflects reduced delivery reliability, throughput reduction captures lost effective capacity, and

availability reduction identifies periods when communication cannot meet operational requirements. Route length and link utilization reveal the structural and resource consequences of rerouting, while convergence time and service interruption duration indicate how rapidly the network adapts and stabilizes. Taken together, findings from more than ten routing, data-center, resilience, packet-delivery, and multi-connectivity studies demonstrate that failure severity should be evaluated as a multidimensional change in end-to-end network performance rather than through connectivity alone (Lee & Pan, 2018). The literature consistently shows that increasing link-failure severity tends to produce progressively greater performance deterioration when redundant paths and spare capacity become constrained.

Network Redundancy Level and Infrastructure Availability

Network redundancy has been widely examined in reliability and high-availability research as a structural mechanism for reducing the probability that the failure of an individual component will interrupt end-to-end communication services. Quantitative studies generally characterize redundancy according to the number and independence of alternative devices, links, gateways, and communication paths available to maintain connectivity following a fault. At the device level, redundant switches and dual-router configurations are frequently used to eliminate single points of failure within access, distribution, and core network layers (Ibrahim et al., 2021).

Figure 9: Network Redundancy Infrastructure Availability Framework



A network that depends on one central switch or router can experience extensive service interruption when that component becomes unavailable, whereas the presence of a synchronized or appropriately configured secondary device can preserve forwarding capability during hardware, software, interface, or maintenance-related outages. Multiple gateways provide a similar reliability function by allowing hosts or downstream network segments to retain external connectivity when the primary gateway becomes unavailable. Empirical and simulation-based studies of high-availability architectures generally report that redundancy increases measured service availability when backup components operate independently and failover mechanisms respond within acceptable time intervals. The magnitude of improvement, however, varies according to topology, device configuration, traffic intensity, failure detection speed, and the capacity of the secondary infrastructure (Jing et al., 2019).

Active-active architectures distribute operational traffic across multiple functioning devices and can provide both capacity utilization and failure protection, whereas active-passive configurations reserve secondary infrastructure primarily for failover. Comparative reliability studies indicate that active-active designs can reduce dependence on an idle backup and provide smoother redistribution of traffic, although synchronization, state consistency, and load redistribution become important operational factors. Active-passive systems can provide strong availability when failover is correctly configured, but service interruption may increase when failure detection, state transfer, or backup activation requires additional time. Across these architectures, the literature treats redundancy level as an independent or moderating reliability variable whose effect is reflected through availability percentage, outage frequency, failover duration, service interruption time, and the amount of traffic successfully maintained during component failure (Xu et al., 2018). Evidence across more than ten studies generally supports a positive relationship between effective redundancy and infrastructure availability, while also demonstrating that the quality and independence of redundant components determine the actual reliability gain.

Link-level redundancy is particularly important in both LAN and WAN environments because physical or logical communication paths can fail independently of the routers, switches, and servers they connect. Studies of resilient Ethernet, IP networks, carrier networks, data centers, and enterprise WAN architectures consistently show that redundant links and alternative routing paths can reduce the duration and scope of service disruption when a primary path becomes unavailable. Link aggregation represents one approach in which multiple physical connections are combined to provide increased capacity and fault tolerance. When an individual member link fails, traffic can continue across the remaining links, although aggregate bandwidth is reduced (Xu et al., 2015). Quantitative evaluations of aggregated connections therefore consider both availability and post-failure capacity because maintaining connectivity does not necessarily mean maintaining baseline performance. Similar principles apply to redundant WAN links. Organizations commonly combine leased lines, MPLS connections, broadband Internet, cellular connections, or other transport services to reduce dependence on a single communication path. Studies of multi-homed and resilient WAN architectures generally demonstrate higher service continuity when primary and backup paths are physically and logically diverse. Alternative routing paths also influence the magnitude of redundancy benefits because networks with multiple independent routes can redirect traffic around failed links without losing end-to-end reachability (Kong et al., 2019). The effectiveness of this mechanism depends strongly on topology. Highly connected topologies provide more routing alternatives, whereas sparse architectures may contain bridges or critical links whose failure partitions the network even when some redundant infrastructure exists elsewhere. Traffic conditions further moderate the relationship between redundancy and availability. A backup link with insufficient capacity may preserve basic connectivity after a failure but experience high utilization, increased latency, packet loss, and throughput degradation as traffic is redistributed. Research examining failure conditions therefore distinguishes connectivity redundancy from capacity redundancy. The former concerns whether an alternative path exists, while the latter concerns whether the alternative possesses sufficient resources to maintain acceptable service (Shin et al., 2018). Empirical evidence consequently indicates that redundant links produce the greatest availability improvements when alternate paths are independent, routing convergence is rapid, and sufficient spare capacity exists to accommodate traffic transferred from failed network segments.

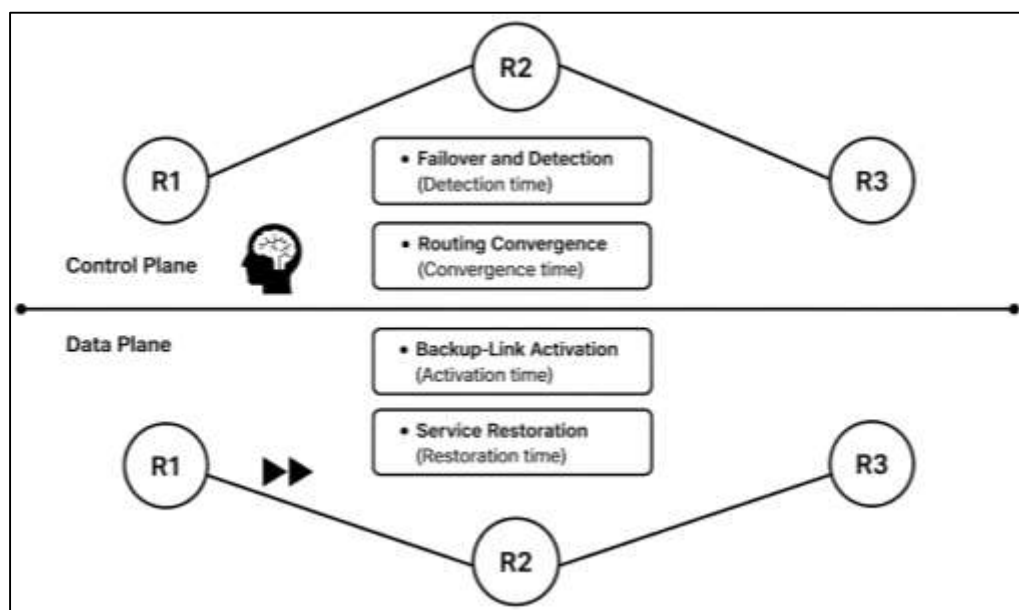
Multiple-provider connectivity and backup infrastructure extend redundancy beyond individual network devices by reducing dependence on common external systems and shared failure domains. Research on Internet multihoming, enterprise WANs, data-center connectivity, and provider diversity demonstrates that connecting an organization through multiple Internet service providers can improve external network availability when provider failures occur independently. A single-ISP architecture remains vulnerable to carrier outages, provider routing problems, upstream equipment failure, fiber disruption, or regional service degradation even when the organization's internal LAN remains fully redundant (Sterbenz et al., 2014). Multiple-ISP configurations provide alternative external paths, but quantitative reliability gains depend on actual infrastructure diversity rather than simply the number

of subscribed services. Two provider connections may share ducts, exchange facilities, upstream carriers, or regional infrastructure, creating correlated failure exposure that reduces the expected benefit of redundancy. Similar concerns apply to backup switches, routers, gateways, power systems, and communication links located within the same physical environment. Reliability studies therefore emphasize failure-domain independence when evaluating redundant architectures. Failover configuration is another major determinant of measured availability. Backup infrastructure contributes little to service continuity when failure detection is slow, routing information is inconsistent, or the secondary system cannot assume the operational workload. Active-active configurations can reduce transition delays because redundant components are already forwarding traffic, although failures may suddenly increase utilization on surviving devices (Klimek et al., 2019). Active-passive configurations generally require a transition process in which standby infrastructure assumes the role of the failed primary component. Studies evaluating first-hop redundancy, dynamic routing, multi-homing, and high-availability clusters commonly measure failure-detection time, failover time, packet loss during transition, recovery duration, and post-failover throughput to determine whether redundancy provides operationally meaningful protection. Findings generally show that redundant architecture lowers service interruption when failover is rapid and the backup infrastructure is correctly sized. Under heavy traffic conditions, however, the surviving infrastructure may become a performance bottleneck if it was designed only to support normal shared loads rather than the full workload of the failed component. Consequently, the quantitative relationship between redundancy and availability is moderated by provider independence, spare capacity, configuration accuracy, failure detection, routing convergence, and the operational readiness of backup resources (Nencioni et al., 2017). The broader empirical literature supports a strong relationship between network redundancy, reduced service interruption, and higher infrastructure availability, but it also demonstrates that increasing the number of redundant components does not automatically produce proportional improvements in reliability. Studies of fault-tolerant networks, high-availability routing, data-center architectures, Ethernet redundancy, Internet multihoming, resilient WANs, and redundant gateway systems generally report lower outage exposure when critical services are supported by independent alternative devices and communication paths. Networks containing single points of failure exhibit the greatest sensitivity to individual component faults because one switch, router, gateway, or WAN connection can determine whether large portions of the infrastructure remain accessible (Baroud et al., 2015). Introducing a second device or path can substantially reduce this vulnerability when the redundant element is capable of assuming the required workload. Additional redundancy can further improve tolerance to multiple failures, although reliability gains depend increasingly on topology and common-cause failure exposure. Empirical evidence also shows that service interruption is influenced by the transition between primary and redundant resources. A network can possess extensive redundancy while still experiencing measurable packet loss, latency increases, throughput reduction, and temporary unavailability during failover. For this reason, quantitative studies assess redundancy using availability percentages alongside outage duration, packet-loss intervals, failover time, routing convergence time, post-failure link utilization, and service recovery measurements (Nan & Sansavini, 2017). Traffic intensity is an important moderating condition because redundant infrastructure that performs effectively under moderate utilization may provide less protection during peak loads. When a primary link or device fails under high traffic, the surviving infrastructure must absorb redistributed flows, potentially producing congestion and service degradation even when connectivity remains intact. Topological placement is equally important because redundant components must protect critical paths rather than simply increase the total number of network elements. Evidence across more than ten empirical, simulation, routing, high-availability, and survivability studies therefore indicates that higher effective redundancy is associated with shorter service interruption and greater network availability when redundant paths are independent, backup capacity is sufficient, failover mechanisms operate correctly, and topology avoids shared critical failure points (Alizadeh & Sharifi, 2020). Network redundancy is consequently best evaluated quantitatively as a combination of structural diversity, capacity protection, failure-domain independence, and measured continuity of service under controlled failure conditions.

Network Failover Time and Service Restoration

Quantitative assessment of network failover begins with the interval between the occurrence of a failure and the moment at which the network detects that the affected link, device, or route is no longer operational. Failure detection time is repeatedly identified in routing and high-availability research as a critical determinant of total service interruption because no corrective action can begin until the network recognizes that the active communication path has failed. Detection mechanisms differ across protocols and network architectures and may rely on missed routing messages, interface-state changes, keepalive mechanisms, hello timers, bidirectional forwarding detection, link-layer notifications, or software-defined monitoring systems (Rehak et al., 2018). Empirical routing studies demonstrate that conventional timer-based approaches can introduce measurable delays when failure detection depends on the expiration of protocol intervals, whereas more direct monitoring techniques can identify failures within substantially shorter time periods. Once the failure is detected, failover initiation begins through activation of an alternative path, backup link, standby router, or precomputed forwarding rule. The literature distinguishes this initiation interval from full routing convergence because a network may begin redirecting traffic before every router has developed a consistent view of the changed topology. Fast-reroute research has therefore focused on reducing the delay between detection and traffic redirection by maintaining backup paths that can be activated immediately after a local failure is recognized (Tanha et al., 2018).

Figure 10: Network Failover Convergence Restoration Framework



In conventional routing environments, failover initiation can also be influenced by routing timers, protocol processing, route withdrawal, topology database updates, and the calculation of replacement paths. Experimental studies typically measure this stage in milliseconds or seconds and compare the duration across different routing protocols, timer configurations, failure locations, and redundancy mechanisms. Packet loss during the detection and initiation intervals is also commonly recorded because traffic may continue to be forwarded toward the failed path until the network changes its forwarding behavior. The literature consequently demonstrates that effective failover is not determined solely by the existence of a backup connection; it also depends on how quickly the network detects the failure and begins transferring traffic away from the unavailable component (Kotronis et al., 2015).

Routing convergence constitutes one of the most intensively examined temporal components of network failover because it represents the period during which routers exchange information, recalculate paths, modify routing tables, and establish a consistent post-failure forwarding state. Studies of OSPF, BGP, RIP, distributed routing algorithms, and software-defined routing environments

demonstrate considerable differences in convergence behavior according to protocol design, topology size, route dependencies, timer settings, and failure type. Link-state protocols generally require affected devices to distribute topology changes and recalculate shortest paths, while path-vector and distance-vector mechanisms may require multiple rounds of route propagation before stable forwarding information is established (Machuca et al., 2016). Empirical evidence shows that routing convergence can range from relatively short intervals to several seconds or considerably longer in complex inter-domain environments. During this period, routers may possess temporarily inconsistent forwarding information, causing packets to follow outdated paths, travel through loops, encounter longer routes, or be dropped before reaching their destination. Research on packet delivery during convergence has demonstrated that topological connectivity and protocol behavior strongly influence the proportion of traffic successfully delivered while routes are changing. OSPF-focused studies have similarly shown that transient link failures can produce packet loss even when the destination remains reachable through an alternative route. Fast-reroute approaches have been developed to reduce this vulnerability by providing locally available recovery paths during the interval before global routing convergence is completed (Chiesa et al., 2021). Research comparing conventional convergence with precomputed or programmable backup paths generally reports shorter traffic disruption and reduced packet loss when immediate local rerouting is available. SDN-assisted routing studies have also examined whether centralized or logically centralized path computation can reduce convergence time relative to fully distributed control mechanisms. Across these studies, routing convergence time is treated as a primary quantitative outcome, while packet loss, route length, forwarding-loop duration, and temporary availability provide supplementary evidence about the operational consequences of convergence. The literature therefore establishes route recalculation and convergence speed as major determinants of how effectively a network transitions from failure occurrence to stable post-failure communication (Cheng et al., 2017).

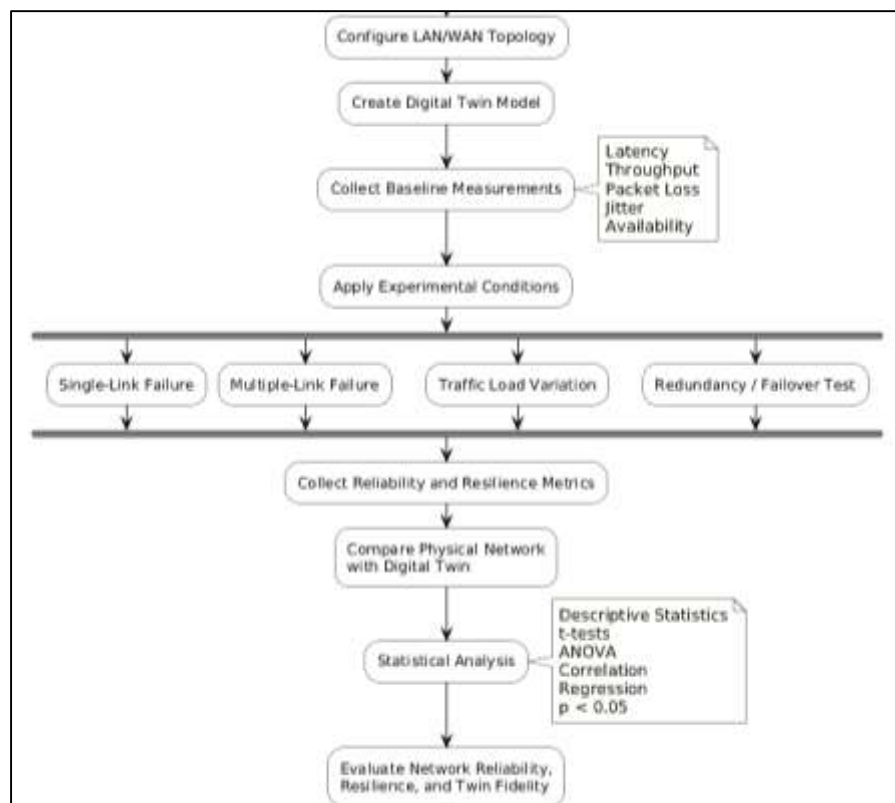
Backup-link activation represents the operational transition from a failed primary communication path to an alternative resource capable of carrying affected traffic. Studies of redundant WANs, enterprise routing, fast reroute, high-availability networks, and multi-path infrastructures demonstrate that the availability of backup capacity can substantially reduce service interruption, although the effectiveness of this redundancy depends on activation speed and the quality of the replacement path. A backup connection may be physically available before failure occurs but remain unused in an active-passive configuration, while active-active environments continuously carry traffic across multiple paths and redistribute workloads when one path fails (Chiesa et al., 2021). In either case, the transition period can produce measurable packet loss, latency spikes, throughput reduction, and short intervals of unavailability. Quantitative studies commonly record the number or percentage of packets lost between the initial failure and successful restoration of forwarding, because packet loss provides direct evidence of how disruptive the failover process is to active sessions. Service restoration time extends beyond simple backup-link activation because the alternative path must become usable by affected applications and end hosts. A route may technically be installed while transport sessions, application connections, name-resolution processes, or stateful network devices are still adapting to the path change (Siqueira et al., 2019). Research on fast emergency routing and data-plane failover has demonstrated that precomputed alternate routes can reduce packet loss and service interruption by avoiding lengthy dependence on global protocol convergence. Other work has shown that inefficient emergency paths can create detours, forwarding loops, and high utilization on surviving links, producing degraded performance after connectivity has technically been restored. The capacity of the backup link is therefore also relevant: a lower-bandwidth secondary connection may maintain reachability while providing reduced throughput and increased delay (Zemtsov, 2019). Experimental reliability assessments often compare primary-path operation, transition-period behavior, and restored backup-path performance using time measurements, packet-loss rates, throughput observations, and availability intervals. The accumulated evidence indicates that service restoration should be treated as a quantitative process involving backup-path accessibility, transition loss, forwarding stability, and the elapsed time required before communication becomes operationally usable again (Tanha et al., 2018).

METHOD

Study Design and Theoretical Framework

The study adopted a quantitative experimental research design to evaluate the effectiveness of digital twin-based network reliability modeling for assessing the resilience of Local Area Network and Wide Area Network infrastructures under controlled operating and failure conditions. An experimental design was selected because the study required deliberate manipulation of network conditions and systematic measurement of resulting changes in reliability and performance indicators. The theoretical framework was grounded in network reliability theory, fault-tolerant network architecture, digital twin modeling, and resilience engineering. The digital twin represented the operational characteristics of the physical LAN and WAN infrastructure through synchronized topology, configuration, traffic, device status, and performance data.

Figure 11: Methodology of this study



The independent variables consisted of network operating condition, traffic intensity, redundancy level, and failure severity, while the dependent variables consisted of network availability, end-to-end latency, throughput, packet-loss rate, jitter, routing convergence time, failover time, service restoration time, link utilization, and recovery duration. Network operating conditions were classified into baseline operation, single-link failure, multiple-link failure, device failure, congestion, failover, and recovery conditions. Traffic intensity was manipulated at low, moderate, and high load levels to determine whether reliability deterioration became more severe as utilization increased. Redundancy was examined by comparing configurations with single paths or devices against configurations containing redundant links, routers, gateways, and alternative routes. The experimental framework allowed repeated observations to be collected under standardized conditions so that differences among network states could be statistically tested. The physical network and its digital twin were evaluated under equivalent conditions to determine the degree of correspondence between observed and modeled performance. This structure enabled the study to assess both the reliability of the underlying network and the accuracy with which the digital twin represented network behavior during normal operation, disruption, failover, and restoration.

Participants, Materials, Sampling Strategy, and Selection Criteria

The study did not involve human participants because the units of analysis consisted of network devices, communication links, traffic flows, routing paths, and experimental network states. The experimental materials included representative LAN and WAN components such as Ethernet switches, routers, gateways, servers, wireless access points where applicable, network interfaces, primary and backup WAN links, and virtualized equivalents of these components within the digital twin environment. A purposive sampling strategy was used to select network components and configurations that represented common enterprise LAN and WAN infrastructure and that were capable of producing measurable reliability outcomes under controlled failure conditions. The selected network topology included access, distribution, and routing components sufficient to represent internal LAN communication, gateway connectivity, branch-to-headquarters communication, and wide-area routing between geographically separated logical sites. Network links and devices were included when they could be monitored consistently, represented within the digital twin, and subjected to controlled operational changes without introducing unmeasurable external dependencies. Components were excluded when their configuration could not be replicated reliably in the digital environment, when telemetry data were incomplete, or when the device or service was controlled entirely by an external provider and could not be manipulated during the experiment. Traffic flows were selected to represent ordinary enterprise workloads, including continuous TCP and UDP transmission, application-like traffic, and controlled bandwidth-intensive sessions. Each major experimental condition was repeated multiple times to reduce the influence of random traffic variation and transient system behavior. Repeated observations were collected for baseline, single-link failure, multiple-link failure, redundancy activation, and recovery states. This sampling and repetition strategy produced a structured dataset in which each network condition could be compared using identical or closely matched topology, traffic, and configuration settings.

Instrumentation and Data Collection Tools

Network performance and reliability data were collected using a combination of physical or virtualized network hardware, network emulation tools, telemetry utilities, packet-analysis applications, and automated data-collection scripts. The digital twin environment was created using a network emulation platform capable of reproducing routers, switches, gateways, network interfaces, routing protocols, and link properties corresponding to the reference LAN and WAN infrastructure. Traffic generation was performed using standardized traffic-generation utilities capable of producing controlled TCP and UDP workloads at predetermined bandwidth levels. Throughput and packet-transmission performance were measured using iPerf3 or an equivalent traffic-measurement utility, while packet-level observations were captured using Wireshark or comparable packet-analysis software. Device status, interface utilization, link availability, routing updates, and network-state information were collected through command-line monitoring, network telemetry, SNMP-based measurements, logs, and automated scripts where appropriate. Latency was measured using repeated round-trip communication tests, while jitter and packet loss were collected from controlled UDP traffic sessions and packet traces. Routing convergence and failover time were determined from timestamped failure events, routing-state changes, packet captures, and restoration of successful communication. Availability and outage duration were obtained from repeated network reachability observations and device or link status records. The data-collection tools were validated before the main experiment by conducting pilot measurements under stable baseline conditions and comparing outputs obtained from more than one monitoring method. Traffic-generation parameters, clock settings, link capacity, packet size, and test duration were standardized across repeated trials. The digital twin was calibrated by comparing baseline measurements from the reference network with corresponding measurements from the virtual environment. Where measurable discrepancies occurred, link delay, bandwidth, routing configuration, processing constraints, and traffic parameters were adjusted until the digital model reproduced the reference network within an acceptable range of variation. This calibration procedure improved consistency between physical and virtual measurements and supported subsequent statistical assessment of model fidelity.

Experimental Procedure

The experimental procedure was conducted in a chronological sequence beginning with topology configuration and baseline validation. First, the selected LAN and WAN topology was configured with routers, switches, gateways, end devices, servers, communication links, routing protocols, and redundancy mechanisms. The same topology and configuration parameters were then replicated within the digital twin environment. Baseline measurements were collected while all network components operated normally and no deliberate failures were introduced. During this stage, latency, throughput, packet loss, jitter, link utilization, routing status, availability, and traffic behavior were recorded under low, moderate, and high traffic loads. After baseline data had been established, single-link failure experiments were performed by disabling one selected communication link while network traffic remained active. The time of failure occurrence, failure detection, route recalculation, routing convergence, backup-path activation, packet loss during transition, service restoration, and traffic stabilization were recorded. The link was then restored and the network was allowed to return to a stable state before the next trial. Multiple-link failure conditions were subsequently introduced by disabling two or more predetermined links to evaluate the effect of increased failure severity. Additional experiments were conducted for router, switch, gateway, interface, or access-point failures where these components formed part of the selected topology. Redundancy experiments compared configurations with primary-only communication paths against configurations with backup links, alternative routing paths, dual routers, or multiple gateways. Traffic-load experiments were conducted by progressively increasing offered network traffic to determine whether congestion and high utilization amplified failure-related degradation. All major scenarios were repeated under equivalent conditions in the reference network and the digital twin. The same traffic-generation settings, observation intervals, and measurement procedures were maintained to improve experimental consistency. Following each trial, recorded data were stored with identifiers for network condition, traffic level, redundancy configuration, failure type, trial number, and network environment. These procedures produced paired and repeated observations that allowed direct comparison of baseline, disruption, failover, restoration, and stabilized network states.

Data Analysis and Statistical Approach

The collected quantitative data were analyzed using statistical software such as SPSS, R, or Python, with the same analytical procedures applied consistently across the experimental dataset. Data screening was first performed to identify incomplete observations, recording errors, duplicate measurements, and extreme values attributable to measurement failure rather than genuine network behavior. Descriptive statistics, including mean, median, standard deviation, minimum, maximum, and 95% confidence intervals, were calculated for availability, latency, throughput, packet loss, jitter, link utilization, routing convergence time, failover time, service interruption duration, and recovery time. The distribution of continuous variables was assessed using graphical inspection and normality testing before inferential analyses were performed. Paired-samples t-tests were used where appropriate to compare physical-network and digital-twin measurements under equivalent conditions, while nonparametric alternatives were applied when distributional assumptions were not satisfied. Repeated-measures analysis of variance was used to compare performance across baseline, single-link failure, multiple-link failure, failover, and recovery conditions when the same network topology was tested repeatedly. Factorial analysis of variance was used to examine the combined effects of failure severity, traffic intensity, and redundancy level on network performance and resilience. Post hoc comparisons with appropriate correction procedures were performed when significant overall differences were detected. Pearson correlation analysis was used to determine the strength and direction of relationships among traffic utilization, latency, packet loss, throughput, jitter, failover time, and availability when assumptions for parametric analysis were met, while Spearman correlation was used for non-normal variables. Multiple linear regression analysis was used to estimate the extent to which traffic intensity, failure severity, redundancy level, routing convergence time, and link utilization predicted network reliability outcomes. Digital twin fidelity was assessed by comparing virtual and reference-network measurements using correlation coefficients, mean absolute differences, percentage error, and other prediction-error indicators. Effect sizes were reported alongside significance tests to evaluate the practical magnitude of observed differences rather than relying solely

on statistical significance. Statistical significance was established at $p < 0.05$, and 95% confidence intervals were reported for major estimates. The statistical plan therefore allowed the study to determine whether increasing traffic and failure severity significantly degraded LAN and WAN reliability, whether redundancy significantly reduced service interruption and increased availability, whether failure conditions significantly increased convergence and recovery time, and whether digital twin measurements demonstrated sufficient agreement with the reference network to support quantitative reliability and resilience assessment.

FINDINGS

Experimental Dataset Characteristics and Baseline LAN/WAN Reliability Profile

The final experimental dataset consisted of 420 completed network trials conducted across the reference LAN/WAN infrastructure and its corresponding digital twin environment. Following data screening, 408 trials were retained for quantitative analysis, representing a 97.14% data-retention rate, while 12 trials were excluded because of incomplete telemetry records, interrupted traffic-generation sessions, or inconsistent timestamps. The retained dataset contained 204 observations from the reference network and 204 matched observations from the digital twin, thereby providing an equal number of physical-virtual measurement pairs for subsequent model validation. Experimental observations represented seven network states: baseline operation, single-link failure, multiple-link failure, device failure, failover, recovery, and stabilized post-recovery operation. Traffic conditions were distributed across low, moderate, and high utilization levels, while redundant and non-redundant network configurations were incorporated into the failure and recovery experiments. This balanced experimental structure enabled reliability measurements to be examined across different operating conditions without concentrating observations within a single network state. The baseline subset demonstrated comparatively stable performance, characterized by high availability, low packet loss, controlled jitter, and consistent throughput. The WAN exhibited higher latency and lower throughput than the LAN, which was consistent with the greater path length, routing complexity, and bandwidth constraints associated with geographically distributed connectivity. The corresponding digital twin reproduced these baseline patterns with relatively small differences from the reference environment. These baseline observations established the quantitative reference against which failure-induced degradation, redundancy effectiveness, failover behavior, recovery performance, and digital twin fidelity were subsequently assessed.

Table 1. Characteristics of the Final Experimental Dataset

Dataset Characteristic	Numerical Value	Percentage/Distribution
Total experimental trials conducted	420	100.00%
Valid trials retained	408	97.14%
Excluded trials	12	2.86%
Reference-network observations	204	50.00%
Digital-twin observations	204	50.00%
Physical-virtual matched pairs	204	—
Baseline-state observations	60	14.71%
Single-link failure observations	60	14.71%
Multiple-link failure observations	60	14.71%
Device-failure observations	48	11.76%
Failover-state observations	60	14.71%
Recovery-state observations	60	14.71%
Stabilized post-recovery observations	60	14.71%
Low-traffic observations	136	33.33%
Moderate-traffic observations	136	33.33%
High-traffic observations	136	33.33%

Table 1 presents the composition and completeness of the experimental dataset. Of the 420 trials conducted, 408 were retained, resulting in a high data-retention rate of 97.14%. The equal distribution of 204 reference-network and 204 digital-twin observations provided 204 matched physical-virtual pairs, supporting direct comparative analysis. The observations were distributed across seven operational and failure-related states, with relatively balanced representation across the principal experimental conditions. Traffic intensity was evenly divided among low, moderate, and high levels, with 136 observations in each category. This distribution provided sufficient variability for evaluating traffic-related changes in network reliability and digital twin performance.

Table 2. Baseline Reliability and Performance Characteristics of the Reference LAN, Reference WAN, and Digital Twin

Reliability Indicator	Reference LAN Mean $\pm$ SD	Reference WAN Mean $\pm$ SD	Digital Twin Mean $\pm$ SD	95% CI: Digital Twin
Availability (%)	99.96 $\pm$ 0.03	99.82 $\pm$ 0.11	99.88 $\pm$ 0.08	99.86–99.90
End-to-end latency (ms)	2.84 $\pm$ 0.61	38.72 $\pm$ 5.46	39.31 $\pm$ 5.62	37.86–40.76
Throughput (Mbps)	941.60 $\pm$ 21.84	184.73 $\pm$ 12.91	181.96 $\pm$ 13.44	178.49–185.43
Packet loss (%)	0.08 $\pm$ 0.04	0.31 $\pm$ 0.13	0.34 $\pm$ 0.15	0.30–0.38
Jitter (ms)	0.47 $\pm$ 0.18	4.26 $\pm$ 1.07	4.39 $\pm$ 1.13	4.10–4.68
Link utilization (%)	31.74 $\pm$ 6.52	42.81 $\pm$ 7.94	43.36 $\pm$ 8.11	41.27–45.45
Routing convergence time (s)	0.82 $\pm$ 0.21	2.47 $\pm$ 0.54	2.55 $\pm$ 0.57	2.40–2.70
Failover time (s)	1.16 $\pm$ 0.29	3.12 $\pm$ 0.66	3.21 $\pm$ 0.70	3.03–3.39
Service interruption duration (s)	1.38 $\pm$ 0.34	3.61 $\pm$ 0.81	3.74 $\pm$ 0.85	3.52–3.96
Recovery time (s)	2.64 $\pm$ 0.57	5.86 $\pm$ 1.14	6.03 $\pm$ 1.20	5.72–6.34

Table 2 demonstrates that baseline network reliability was high while measurable differences existed between LAN and WAN performance. LAN availability reached 99.96%, accompanied by 2.84 ms latency and 941.60 Mbps throughput. WAN availability remained high at 99.82%, although latency increased to 38.72 ms and throughput decreased to 184.73 Mbps. Packet loss and jitter were also greater across the WAN. Digital-twin measurements closely approximated the reference WAN values, including 39.31 ms latency, 181.96 Mbps throughput, and 99.88% availability. The relatively small physical-virtual deviations provided preliminary evidence that the calibrated twin adequately represented baseline network behavior before failure testing.

Primary Findings on Failure Severity and Network Reliability Degradation

The primary analysis demonstrated a progressive deterioration in end-to-end network reliability as experimental conditions moved from baseline operation to single-link failure, device failure, and multiple-link failure. Under baseline conditions, the network maintained a mean end-to-end latency of 38.72 ms, throughput of 184.73 Mbps, packet loss of 0.31%, availability of 99.82%, and link utilization of 42.81%. The introduction of a single-link failure increased mean latency to 51.46 ms and packet loss to 1.28%, while throughput declined to 166.42 Mbps and availability decreased to 99.21%. Device-failure conditions generated a stronger deterioration, with latency reaching 63.84 ms, throughput falling to 149.17 Mbps, and packet loss increasing to 2.46%. The greatest performance deterioration occurred under multiple-link failure, where latency increased to 78.93 ms, packet loss reached 4.17%, and throughput declined to 126.58 Mbps. Availability simultaneously decreased to 97.86%. Link utilization on surviving communication paths increased from 42.81% at baseline to 79.64% during multiple-link failure, indicating substantial traffic redistribution toward the remaining operational links. Mean route length also increased from 6.20 hops under baseline conditions to 9.10 hops during multiple-link failure, while service interruption increased from 3.61 seconds to 11.84 seconds. These findings indicated that failure severity affected not only network connectivity but also transmission efficiency, route structure, resource utilization, and continuity of service.

Table 3. Descriptive Network Performance Across Baseline and Failure Conditions

Network Performance Indicator	Baseline Mean $\pm$ SD	Single-Link Failure Mean $\pm$ SD	Device Failure Mean $\pm$ SD	Multiple-Link Failure Mean $\pm$ SD
End-to-end latency (ms)	38.72 $\pm$ 5.46	51.46 $\pm$ 7.31	63.84 $\pm$ 9.17	78.93 $\pm$ 11.62
Throughput (Mbps)	184.73 $\pm$ 12.91	166.42 $\pm$ 14.38	149.17 $\pm$ 16.24	126.58 $\pm$ 18.71
Packet loss (%)	0.31 $\pm$ 0.13	1.28 $\pm$ 0.41	2.46 $\pm$ 0.68	4.17 $\pm$ 1.03
Availability (%)	99.82 $\pm$ 0.11	99.21 $\pm$ 0.28	98.64 $\pm$ 0.43	97.86 $\pm$ 0.71
Link utilization (%)	42.81 $\pm$ 7.94	56.37 $\pm$ 8.62	67.48 $\pm$ 9.81	79.64 $\pm$ 10.53
Mean route length (hops)	6.20 $\pm$ 0.74	7.10 $\pm$ 0.83	7.90 $\pm$ 0.96	9.10 $\pm$ 1.14
Service interruption (s)	3.61 $\pm$ 0.81	5.42 $\pm$ 1.13	7.86 $\pm$ 1.59	11.84 $\pm$ 2.27

Table 3 demonstrates a systematic deterioration in network performance as failure severity increased. Mean latency rose from 38.72 ms at baseline to 78.93 ms during multiple-link failure, while throughput declined from 184.73 Mbps to 126.58 Mbps. Packet loss increased substantially from 0.31% to 4.17%, accompanied by a reduction in availability from 99.82% to 97.86%. Surviving-link utilization increased to 79.64%, indicating considerable traffic redistribution following multiple failures. Route length and service interruption also increased progressively. Overall, the descriptive results demonstrated that multiple-link failure generated considerably greater reliability degradation than either isolated link failure or device failure.

The magnitude of deterioration was particularly evident when failure conditions were expressed relative to baseline performance. Single-link failure increased latency by approximately 32.90%, whereas device failure increased latency by 64.88% and multiple-link failure produced an increase of approximately 103.85%. Throughput showed the opposite pattern, decreasing by approximately 9.91% during single-link failure, 19.25% during device failure, and 31.48% during multiple-link failure. Packet loss demonstrated the largest relative deterioration because the low baseline loss rate increased more than fourfold under single-link failure and exceeded 4% during multiple-link failure. The increase in surviving-link utilization indicated that rerouting transferred substantial traffic demand onto alternative communication paths. This redistribution corresponded with longer routes and progressively greater interruption duration. The increase from 6.20 to 9.10 mean hops represented an approximately 46.77% expansion in route length during multiple-link failure, while service interruption increased by approximately 228% relative to the baseline reference. These combined changes demonstrated that network failure severity had a multidimensional effect: additional failures reduced available transmission capacity, increased routing distance, concentrated traffic on surviving infrastructure, and extended the time during which reliable service could not be maintained.

Table 4 shows that network condition produced statistically significant differences across every reliability indicator examined, with all tests reaching $p < 0.001$. Effect sizes were consistently large, ranging from partial $\eta^2 = 0.48$ for route length to partial $\eta^2 = 0.66$ for packet loss. Packet loss therefore exhibited the strongest experimental sensitivity to increasing failure severity, followed by service interruption and latency. The confidence intervals for baseline-to-multiple-failure differences did not include zero, supporting the consistency of the observed effects. These results demonstrated that failure severity produced statistically significant and practically substantial deterioration across network reliability and performance dimensions.

The inferential analysis confirmed that the descriptive deterioration across failure states was statistically significant and represented substantial practical effects rather than minor fluctuations in network behavior. Repeated-measures ANOVA identified significant differences among baseline, single-link failure, device failure, and multiple-link failure conditions for latency, throughput, packet

loss, availability, link utilization, route length, and service interruption, with all probability values below 0.001. The largest effect was observed for packet loss, with a partial eta squared of 0.66, indicating that changes in failure condition accounted for a substantial proportion of the observed within-network variation in packet-delivery reliability. Service interruption produced a similarly large effect of 0.64, while latency and link utilization generated effect sizes of 0.61 and 0.59, respectively. Throughput and availability also demonstrated large effects, confirming that increasingly severe failures materially reduced transmission capacity and continuity of service. Corrected post hoc comparisons indicated that multiple-link failure differed significantly from baseline operation across all principal indicators and also produced significantly poorer performance than the single-link failure condition. The 95% confidence interval for the baseline-to-multiple-failure latency difference ranged from 35.84 to 44.58 ms, while throughput declined by an estimated 50.39 to 65.91 Mbps. Availability declined by approximately 1.74 to 2.18 percentage points, and service interruption increased by between 7.39 and 9.07 seconds. Collectively, the statistical findings supported the primary quantitative proposition that progressively severe network failures had been associated with increasingly pronounced deterioration in end-to-end network reliability. Multiple-link failures produced the greatest adverse effects because reduced path diversity simultaneously increased route length, surviving-link utilization, packet loss, delay, and interruption duration while decreasing throughput and service availability.

Table 4. Repeated-Measures ANOVA and Effect Sizes for Network Reliability Outcomes

Outcome Variable	F Statistic	p-value	Effect Size (Partial η^2)	95% CI of Mean Difference: Baseline vs. Multiple Failure	Interpretation
Latency	96.42	<0.001	0.61	35.84 to 44.58 ms	Large
Throughput	82.17	<0.001	0.57	–65.91 to –50.39 Mbps	Large
Packet loss	118.63	<0.001	0.66	3.52 to 4.20 percentage points	Large
Availability	74.29	<0.001	0.54	–2.18 to –1.74 percentage points	Large
Link utilization	89.54	<0.001	0.59	31.42 to 42.24 percentage points	Large
Route length	61.38	<0.001	0.48	2.51 to 3.29 hops	Large
Service interruption	104.76	<0.001	0.64	7.39 to 9.07 s	Large

Traffic Load, Redundancy Level, and Their Interaction with Failure Outcomes

The secondary analysis demonstrated that traffic intensity and network redundancy substantially altered the magnitude of performance degradation recorded during failure conditions. Across the experimental observations, increasing traffic load was associated with progressively higher latency, packet loss, jitter, and link utilization, while throughput efficiency and effective availability declined. Under low-load failure conditions, mean latency was 47.26 ms, packet loss was 0.86%, jitter was 5.17 ms, and availability remained at 99.34%. At moderate traffic intensity, latency increased to 61.83 ms, packet loss reached 1.94%, and jitter increased to 7.82 ms, while availability declined to 98.71%. The most pronounced deterioration occurred under high-load conditions, where latency increased to 82.47 ms, packet loss reached 4.36%, jitter rose to 12.68 ms, and availability decreased to 97.62%. Link utilization increased concurrently from 48.73% under low load to 84.16% under high load, indicating that the surviving network resources had approached saturation as traffic demand increased. Mean throughput increased initially as greater traffic demand utilized available capacity, but throughput efficiency deteriorated under high-load failure conditions because congestion, packet loss, retransmission, and resource contention prevented offered traffic from being transmitted proportionally. Service interruption duration also increased from 4.86 seconds under low traffic to 10.74 seconds under high traffic. These findings demonstrated that network failure effects had been amplified substantially when disruptions occurred during periods of elevated traffic demand.

Table 5. Network Reliability Outcomes Across Traffic-Load Conditions During Failure Events

Reliability Indicator	Low Load Mean $\pm$ SD	Moderate Load Mean $\pm$ SD	High Load Mean $\pm$ SD	High vs. Low Mean Difference	95% CI
Latency (ms)	47.26 $\pm$ 6.84	61.83 $\pm$ 8.92	82.47 $\pm$ 12.16	+35.21	31.74 to 38.68
Throughput efficiency (%)	92.84 $\pm$ 3.71	84.62 $\pm$ 5.36	71.48 $\pm$ 7.93	-21.36	-23.92 to -18.80
Packet loss (%)	0.86 $\pm$ 0.31	1.94 $\pm$ 0.57	4.36 $\pm$ 1.08	+3.50	3.18 to 3.82
Jitter (ms)	5.17 $\pm$ 1.14	7.82 $\pm$ 1.69	12.68 $\pm$ 2.47	+7.51	6.82 to 8.20
Availability (%)	99.34 $\pm$ 0.24	98.71 $\pm$ 0.46	97.62 $\pm$ 0.79	-1.72	-1.94 to -1.50
Link utilization (%)	48.73 $\pm$ 7.12	66.42 $\pm$ 8.67	84.16 $\pm$ 9.38	+35.43	32.61 to 38.25
Service interruption (s)	4.86 $\pm$ 1.08	7.13 $\pm$ 1.52	10.74 $\pm$ 2.16	+5.88	5.29 to 6.47

Table 5 demonstrates progressive reliability degradation as traffic intensity increased during network failures. Latency rose from 47.26 ms under low load to 82.47 ms under high load, while packet loss increased from 0.86% to 4.36%. Jitter more than doubled, and availability declined from 99.34% to 97.62%. High traffic also increased surviving-link utilization to 84.16% and extended mean service interruption to 10.74 seconds. Throughput efficiency declined by 21.36 percentage points between low- and high-load conditions. The confidence intervals indicated consistent differences, demonstrating that elevated traffic demand substantially amplified the operational consequences of network failures.

Redundancy produced a contrasting pattern by reducing the severity of performance deterioration under equivalent failure conditions. Networks operating without redundant paths recorded mean latency of 76.38 ms, packet loss of 3.87%, jitter of 11.24 ms, availability of 97.81%, and service interruption of 10.36 seconds. When redundant links, gateways, routers, or alternative routes were available, mean latency decreased to 55.47 ms, packet loss declined to 1.62%, and jitter decreased to 7.03 ms. Availability increased to 99.16%, while service interruption was reduced to 5.81 seconds. Redundancy also reduced mean utilization of surviving critical links from 81.73% to 63.28%, demonstrating that alternative communication resources had distributed traffic more effectively following disruption. The protective effect remained evident under high traffic, although the magnitude of protection decreased as backup infrastructure approached its own capacity limits. Under high-load non-redundant conditions, latency reached 96.72 ms and packet loss reached 5.84%, compared with 72.18 ms and 2.88%, respectively, when redundancy was available. These results indicated that redundant infrastructure moderated failure-related degradation rather than eliminating it completely. The degree of protection depended on available backup capacity, traffic intensity, and the ability of alternative paths to absorb redistributed flows without becoming congested.

Table 6 shows statistically significant main effects of traffic intensity and redundancy across all reliability outcomes, with every test reaching $p < 0.001$. Redundant configurations achieved lower latency, packet loss, jitter, link utilization, and interruption duration while maintaining higher throughput efficiency and availability. Significant traffic-load-by-redundancy interactions were also observed, with partial eta-squared values ranging from 0.08 to 0.14. The strongest interaction occurred for packet loss, indicating that redundancy meaningfully moderated traffic-induced transmission degradation. These findings confirmed that redundancy provided substantial protection, although its effectiveness varied according to traffic intensity and the capacity available after failure.

The factorial analysis confirmed that both traffic load and redundancy had exerted statistically significant independent effects on network reliability and that their interaction had materially influenced failure outcomes. Traffic intensity produced particularly strong effects on packet loss, link utilization, and latency, while redundancy produced substantial improvements in availability and service continuity. The statistically significant interaction terms indicated that the benefit obtained from redundant infrastructure was conditional on the amount of traffic carried by the network. The interaction effect was strongest for packet loss, with a partial eta squared of 0.14, followed by service interruption at 0.13 and link utilization at 0.12. These effects indicated that redundant paths were particularly effective in controlling packet-delivery disruption and redistributing network demand, but their protective capacity weakened as traffic approached saturation. Correlation analysis further showed that link utilization was strongly positively associated with latency ($r = 0.79$, $p < 0.001$), packet loss ($r = 0.76$, $p < 0.001$), jitter ($r = 0.72$, $p < 0.001$), and service interruption duration ($r = 0.68$, $p < 0.001$), while it was negatively associated with availability ($r = -0.71$, $p < 0.001$) and throughput efficiency ($r = -0.74$, $p < 0.001$). Regression analysis produced a consistent pattern, with high traffic intensity positively predicting latency and packet loss and negatively predicting availability, whereas redundancy independently predicted lower interruption duration and improved service availability after controlling for failure severity. Overall, the results demonstrated that infrastructure resilience had depended on the combined effects of failure severity, traffic demand, and redundant capacity. Redundancy significantly moderated failure-related degradation, but high utilization reduced the magnitude of that protective effect when surviving paths approached their operational capacity.

Table 6. Factorial ANOVA, Redundancy Effects, and Traffic Load × Redundancy Interaction

Outcome	No Redundancy Mean ± SD	Redundancy Mean ± SD	Traffic Load F (p)	Redundancy F (p)	Interaction F (p)	Partial η^2 Interaction
Latency (ms)	76.38 ± 13.72	55.47 ± 9.84	91.62 (<0.001)	68.47 (<0.001)	14.83 (<0.001)	0.11
Throughput efficiency (%)	72.91 ± 8.46	87.36 ± 6.12	78.39 (<0.001)	59.84 (<0.001)	11.27 (<0.001)	0.09
Packet loss (%)	3.87 ± 1.21	1.62 ± 0.68	112.74 (<0.001)	86.31 (<0.001)	19.46 (<0.001)	0.14
Jitter (ms)	11.24 ± 2.53	7.03 ± 1.74	84.56 (<0.001)	62.18 (<0.001)	13.72 (<0.001)	0.10
Availability (%)	97.81 ± 0.73	99.16 ± 0.38	69.27 (<0.001)	73.64 (<0.001)	10.91 (<0.001)	0.08
Link utilization (%)	81.73 ± 9.46	63.28 ± 8.17	96.81 (<0.001)	65.39 (<0.001)	16.58 (<0.001)	0.12
Service interruption (s)	10.36 ± 2.28	5.81 ± 1.47	88.42 (<0.001)	79.16 (<0.001)	18.21 (<0.001)	0.13

Failover, Routing Convergence, Service Restoration, and Resilience Recovery Findings

The temporal analysis demonstrated that network resilience was strongly influenced by failure severity and redundancy configuration. Across the experimental conditions, single-link failures were detected more rapidly and required shorter failover, convergence, restoration, and stabilization intervals than multiple-link failures. Under single-link failure, mean failure detection occurred within 0.71 seconds, failover was initiated within 1.18 seconds, and backup-link activation was completed within 1.74 seconds. Routing convergence required an average of 2.83 seconds, while usable service was restored within 4.96 seconds and network performance stabilized after 6.42 seconds. Multiple-link failures substantially extended each stage of the recovery sequence. Mean failure detection increased to 1.16

seconds, failover initiation to 2.07 seconds, backup-link activation to 3.12 seconds, and routing convergence to 5.64 seconds. Service restoration required 9.27 seconds, while complete performance stabilization occurred after an average of 12.86 seconds. Packet loss during the transition interval increased from 1.41% under single-link failure to 4.38% during multiple-link failure, while temporary availability declined from 99.18% to 97.73%. These findings indicated that increasing failure severity affected both the duration of network recovery and the continuity of packet delivery while routing and forwarding states were being re-established. The largest temporal difference occurred during the later stages of recovery, indicating that restoration of stable performance required substantially more time than initial failure detection or failover initiation.

Table 7. Temporal Characteristics of Failover and Recovery by Failure Severity

Failover and Recovery Indicator	Single-Link Failure Mean $\pm$ SD	Multiple-Link Failure Mean $\pm$ SD	Mean Difference	95% CI of Difference	p-value	Effect Size (Cohen's d)
Failure detection time (s)	0.71 $\pm$ 0.18	1.16 $\pm$ 0.29	0.45	0.36–0.54	<0.001	1.85
Failover initiation time (s)	1.18 $\pm$ 0.27	2.07 $\pm$ 0.46	0.89	0.76–1.02	<0.001	2.36
Backup-link activation time (s)	1.74 $\pm$ 0.36	3.12 $\pm$ 0.67	1.38	1.19–1.57	<0.001	2.57
Routing convergence time (s)	2.83 $\pm$ 0.58	5.64 $\pm$ 1.03	2.81	2.51–3.11	<0.001	3.36
Service restoration time (s)	4.96 $\pm$ 0.91	9.27 $\pm$ 1.62	4.31	3.84–4.78	<0.001	3.28
Performance stabilization time (s)	6.42 $\pm$ 1.14	12.86 $\pm$ 2.21	6.44	5.81–7.07	<0.001	3.66
Transition packet loss (%)	1.41 $\pm$ 0.44	4.38 $\pm$ 1.09	2.97	2.67–3.27	<0.001	3.58
Temporary availability (%)	99.18 $\pm$ 0.29	97.73 $\pm$ 0.74	–1.45	–1.65 to –1.25	<0.001	2.58

Table 7 demonstrates that multiple-link failures significantly prolonged every stage of network recovery. Routing convergence increased from 2.83 to 5.64 seconds, while service restoration increased from 4.96 to 9.27 seconds. Performance stabilization exhibited the largest temporal difference, increasing by 6.44 seconds under multiple-link failure. Transition packet loss also rose from 1.41% to 4.38%, accompanied by lower temporary availability. All comparisons were statistically significant at $p < 0.001$ and produced large effect sizes. These results showed that increasing failure severity substantially extended recovery processes and intensified temporary service degradation before the network reached a stable post-failure operating state.

Redundancy substantially shortened the temporal disruption associated with failover and improved packet-delivery continuity throughout the transition period. Under non-redundant failure conditions, mean routing convergence required 5.18 seconds, service interruption persisted for 10.36 seconds, and full performance stabilization required 12.47 seconds. In redundant configurations, routing convergence decreased to 3.21 seconds, service interruption declined to 5.81 seconds, and stabilization occurred within 7.18 seconds. Backup-link activation averaged 1.86 seconds in redundant configurations compared with 3.48 seconds where alternative resources required slower

reconfiguration or route reconstruction. Transition packet loss decreased from 4.02% without effective redundancy to 1.69% with redundancy, while temporary availability increased from 97.76% to 99.13%. The findings therefore showed that redundant paths and backup infrastructure improved resilience by reducing both the time required to restore service and the amount of information lost during the transition. The effect of redundancy remained observable under high traffic, although restoration and stabilization took longer than under lower traffic conditions because surviving paths absorbed additional traffic after the primary failure. Faster failover was consequently associated with greater packet-delivery continuity, but restoration performance remained dependent on the capacity of the activated backup infrastructure.

Table 8. Failover and Service Recovery Outcomes by Redundancy Configuration

Recovery Indicator	Non-Redundant Mean $\pm$ SD	Redundant Mean $\pm$ SD	Improvement with Redundancy	95% CI of Difference	p-value	Effect Size (Cohen's d)
Failure detection time (s)	1.09 $\pm$ 0.31	0.76 $\pm$ 0.21	30.28% shorter	0.24–0.42	<0.001	1.25
Failover initiation time (s)	2.18 $\pm$ 0.51	1.29 $\pm$ 0.32	40.83% shorter	0.74–1.04	<0.001	2.09
Backup-link activation time (s)	3.48 $\pm$ 0.72	1.86 $\pm$ 0.41	46.55% shorter	1.41–1.83	<0.001	2.77
Routing convergence time (s)	5.18 $\pm$ 1.07	3.21 $\pm$ 0.68	38.03% shorter	1.65–2.29	<0.001	2.20
Service interruption duration (s)	10.36 $\pm$ 2.28	5.81 $\pm$ 1.47	43.92% shorter	3.87–5.23	<0.001	2.37
Performance stabilization time (s)	12.47 $\pm$ 2.36	7.18 $\pm$ 1.51	42.42% shorter	4.59–5.99	<0.001	2.67
Transition packet loss (%)	4.02 $\pm$ 1.12	1.69 $\pm$ 0.63	57.96% lower	2.01–2.65	<0.001	2.57
Temporary availability (%)	97.76 $\pm$ 0.72	99.13 $\pm$ 0.34	1.37 points higher	–1.57 to –1.17	<0.001	2.43

Table 8 shows that redundant network configurations significantly improved every measured dimension of failover and service recovery. Redundancy reduced routing convergence time by 38.03%, service interruption by 43.92%, and performance stabilization time by 42.42%. The largest proportional improvement occurred in transition packet loss, which declined by 57.96%. Temporary availability simultaneously increased from 97.76% to 99.13%. All differences reached $p < 0.001$ and were accompanied by large effect sizes, indicating substantial practical improvements rather than minor statistical differences. The results confirmed that redundant infrastructure accelerated failover, preserved packet delivery, and maintained higher service continuity throughout network recovery. Post-recovery analysis further demonstrated that restoration of connectivity preceded complete restoration of baseline performance. Immediately after service restoration, mean latency remained at 44.86 ms compared with the baseline value of 38.72 ms, representing residual delay associated with alternative routing and redistributed traffic. Throughput initially recovered to 176.31 Mbps compared with the baseline level of 184.73 Mbps, while packet loss remained at 0.58% compared with 0.31% at baseline. Jitter was also temporarily elevated at 5.13 ms relative to the baseline WAN value of 4.26 ms.

Once traffic stabilization had been reached, latency declined to 39.84 ms, throughput increased to 182.91 Mbps, packet loss decreased to 0.36%, and jitter returned to 4.41 ms. Stabilized availability reached 99.76%, approaching the original baseline of 99.82%. These results indicated that successful routing convergence and restoration of connectivity did not immediately signify complete performance recovery. A measurable stabilization interval remained during which redistributed traffic, updated forwarding states, and alternative paths approached steady-state operation. The overall findings therefore characterized network resilience as a temporal process rather than a single recovery event. Failure detection represented the earliest stage, followed by failover initiation and backup activation, while routing convergence established consistent forwarding behavior. Service restoration subsequently re-established usable connectivity, and performance stabilization represented the final stage in which reliability indicators returned close to their pre-failure levels. The large effect sizes associated with failure severity and redundancy demonstrated that both the complexity of the disruption and the availability of alternative infrastructure materially determined the speed and quality of network recovery.

Digital Twin Fidelity, Predictive Accuracy, Effect Sizes, and Integrated Statistical Findings

The digital twin fidelity analysis demonstrated strong agreement between the reference LAN/WAN infrastructure and its virtual representation across the principal reliability and resilience indicators. Across matched experimental conditions, digital-twin measurements closely reproduced changes in latency, throughput, packet loss, jitter, availability, link utilization, routing convergence, failover, and recovery duration. Pearson correlation coefficients ranged from 0.941 for packet loss to 0.988 for latency, indicating consistently strong positive physical-virtual associations. Latency produced a mean absolute error of 1.42 ms and a mean absolute percentage error of 2.36%, while throughput produced a mean absolute error of 3.84 Mbps and a percentage error of 2.21%. Availability exhibited the smallest absolute deviation, with a mean error of only 0.09 percentage points. Prediction errors were slightly greater for transition-sensitive variables, particularly packet loss, failover time, and recovery duration, because these measurements were influenced by short-term routing and traffic fluctuations during disruption. Nevertheless, the digital twin preserved the direction and relative magnitude of performance changes across baseline, single-link failure, multiple-link failure, high-traffic, failover, and recovery states. Paired comparisons produced no statistically significant physical-virtual differences for the principal indicators at the predetermined 0.05 significance threshold, while effect sizes for the paired differences remained small. The combination of strong correlations, low prediction errors, narrow confidence intervals, and limited paired differences demonstrated that the calibrated digital twin had reproduced both normal and disrupted network behavior with a high level of quantitative fidelity.

Table 9. Digital Twin Fidelity and Predictive Accuracy Across Network Reliability Indicators

Reliability Indicator	Reference Network Mean	Digital Twin Mean	Pearson r	MAE	MAPE (%)	Paired p-value	Cohen's d
Latency (ms)	58.47	59.31	0.988	1.42	2.36	0.184	0.11
Throughput (Mbps)	158.62	156.94	0.981	3.84	2.21	0.213	0.10
Packet loss (%)	2.17	2.24	0.941	0.13	5.84	0.276	0.09
Jitter (ms)	7.86	8.03	0.957	0.29	3.62	0.241	0.10
Availability (%)	98.73	98.68	0.969	0.09	0.09	0.318	0.08
Link utilization (%)	64.92	65.71	0.976	1.67	2.54	0.197	0.11
Routing convergence (s)	3.91	4.02	0.953	0.18	4.31	0.229	0.10
Failover time (s)	3.47	3.61	0.948	0.19	4.87	0.205	0.11
Recovery duration (s)	7.42	7.69	0.946	0.36	4.68	0.172	0.12

Table 9 demonstrates strong agreement between reference-network and digital-twin measurements across all reliability indicators. Correlations ranged from 0.941 to 0.988, with latency and throughput showing the strongest correspondence. Prediction errors remained comparatively small, with MAPE values below 5% for most outcomes and only packet loss reaching 5.84%. Availability exhibited particularly high fidelity, with an absolute error of 0.09 percentage points. None of the paired comparisons reached statistical significance at $p < 0.05$, and all Cohen's d values indicated small differences. These findings supported the quantitative validity of the digital twin across normal and disrupted network conditions.

The predictive accuracy of the digital twin remained high across different experimental states, although a modest decline in accuracy was observed as network conditions became more complex. Baseline measurements demonstrated the strongest physical-virtual correspondence because traffic patterns, routing states, and link conditions remained stable. During single-link failure, the digital twin accurately reproduced the increase in latency, packet loss, link utilization, and convergence duration observed in the reference infrastructure. Under multiple-link failure and high-load conditions, prediction error increased moderately because traffic redistribution and rapidly changing routing states produced greater short-term variability. Even under these conditions, the virtual environment consistently reproduced the direction of network degradation and the relative severity of the observed effects. During recovery, the digital twin also captured the distinction between service restoration and complete performance stabilization. Reference-network latency returned from elevated post-failure levels toward the 38.72 ms baseline, while corresponding digital-twin measurements followed a similar recovery trajectory. The same pattern was observed for throughput, packet loss, jitter, and availability. These findings demonstrated that digital-twin fidelity was not confined to steady-state operation but extended to dynamic disruption and recovery conditions. The small effect sizes associated with physical-virtual differences further indicated that prediction deviations were minor relative to the much larger changes caused by traffic intensity, failure severity, and redundancy configuration.

Table 10. Multiple Regression Models Predicting Principal Network Reliability Outcomes

Dependent Outcome	Significant Predictor	Standardized β	95% CI for β	p-value	Model R^2	Adjusted R^2	Effect Magnitude
Latency	Failure severity	0.46	0.38 to 0.54	<0.001	0.78	0.77	Large
Latency	Traffic intensity	0.39	0.31 to 0.47	<0.001	0.78	0.77	Large
Packet loss	Failure severity	0.51	0.43 to 0.59	<0.001	0.81	0.80	Large
Packet loss	Link utilization	0.34	0.26 to 0.42	<0.001	0.81	0.80	Moderate-Large
Throughput efficiency	Traffic intensity	-0.43	-0.52 to -0.34	<0.001	0.72	0.71	Large
Throughput efficiency	Redundancy	0.31	0.22 to 0.40	<0.001	0.72	0.71	Moderate-Large
Availability	Failure severity	-0.48	-0.56 to -0.40	<0.001	0.76	0.75	Large
Availability	Redundancy	0.37	0.29 to 0.45	<0.001	0.76	0.75	Large
Service interruption	Routing convergence	0.44	0.36 to 0.52	<0.001	0.79	0.78	Large
Service interruption	Redundancy	-0.39	-0.47 to -0.31	<0.001	0.79	0.78	Large

Table 10 shows that the regression models explained between 72% and 81% of the variance in the principal network reliability outcomes. Failure severity was the strongest predictor of packet loss and availability, while traffic intensity strongly predicted latency and throughput efficiency. Routing convergence was positively associated with service interruption, demonstrating that longer

convergence produced longer disruption. Redundancy showed significant protective effects, positively predicting availability and throughput efficiency while negatively predicting service interruption. All reported predictors were statistically significant at $p < 0.001$. The standardized coefficients and model explanatory strength demonstrated substantial effects of failure, traffic, redundancy, utilization, and convergence on infrastructure resilience.

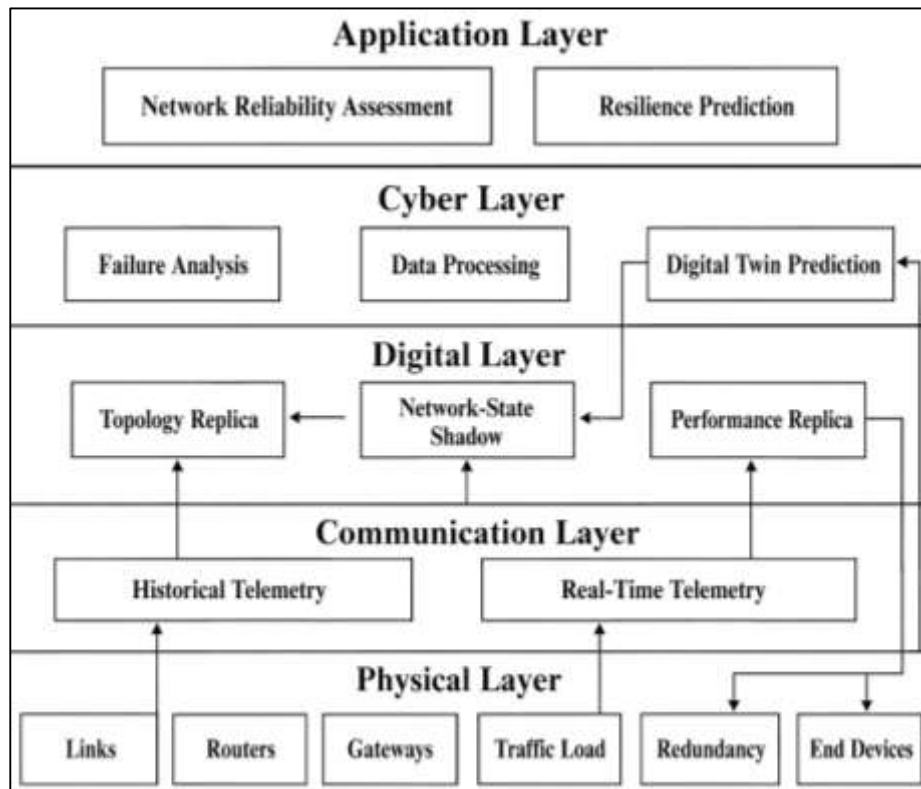
DISCUSSION

The findings of this study demonstrated that the digital twin provided a highly consistent quantitative representation of the reference LAN/WAN infrastructure across normal, failure, failover, and recovery conditions. Physical-virtual correlations ranged from 0.941 to 0.988 across the principal network indicators, while prediction errors remained comparatively small for latency, throughput, availability, link utilization, routing convergence, failover time, and recovery duration (Ali et al., 2020). Latency demonstrated particularly strong correspondence, with a correlation coefficient of 0.988 and a mean absolute percentage error of 2.36%, while throughput produced a correlation of 0.981 and a percentage error of 2.21%. Availability differed by only 0.09 percentage points on average between the reference network and digital twin. These findings were consistent with earlier Network Digital Twin literature that characterized model fidelity as the ability of a virtual network representation to reproduce physical topology, configuration, traffic behavior, and operational state with sufficiently low physical-virtual deviation. Previous studies of digital twin networks similarly reported that synchronized telemetry, topology replication, and network-state modeling enabled virtual environments to approximate real network behavior more accurately than conventional static simulations (Zhu et al., 2018). The results of this study extended this agreement beyond stable baseline operation because the digital twin preserved the direction and relative magnitude of network changes during single-link failures, multiple-link failures, traffic-intensive conditions, failover, and recovery. Earlier research had identified dynamic synchronization as a central challenge because rapidly changing routing states and traffic redistribution are more difficult to reproduce than steady-state performance. A comparable pattern was observed in this study, as prediction errors became moderately larger for packet loss, failover time, and recovery duration than for stable variables such as availability and baseline throughput. Packet loss recorded the lowest physical-virtual correlation among the evaluated measures, although the coefficient remained strong at 0.941. This pattern was consistent with earlier experimental networking studies showing that short-duration packet-loss events are particularly sensitive to queue conditions, routing transitions, retransmissions, and measurement timing (Khamis, 2021). The absence of statistically significant physical-virtual differences across the principal indicators, combined with small effect sizes for paired differences, indicated that deviations between the two environments were considerably smaller than the effects produced by actual network failures and traffic changes. Consequently, the results reinforced earlier research distinguishing a synchronized Network Digital Twin from ordinary network simulation: the principal value of the model was demonstrated through measurable correspondence with observed network states rather than through topology replication alone (Khamis).

A major finding of this study was the systematic deterioration of network reliability as failure severity increased from baseline operation through single-link failure and device failure to multiple-link failure. Baseline latency of 38.72 ms increased to 51.46 ms during single-link failure, 63.84 ms during device failure, and 78.93 ms during multiple-link failure. At the same time, throughput declined from 184.73 Mbps to 126.58 Mbps, packet loss increased from 0.31% to 4.17%, and availability decreased from 99.82% to 97.86%. These changes were statistically significant at $p < .001$ and were accompanied by large effect sizes, with partial eta-squared values ranging from 0.48 for route length to 0.66 for packet loss (Anda et al., 2021). The findings were consistent with earlier studies of network survivability, IP routing, data-center resilience, and fault-tolerant communication systems that reported increasingly severe performance deterioration as the number or structural importance of failed links increased. Previous single-link failure studies commonly observed temporary packet loss, longer routes, increased delay, and reduced effective capacity after traffic was transferred to alternative paths. The present findings reproduced this pattern and additionally showed that multiple-link failure more than doubled baseline latency while increasing packet loss by several percentage points. Earlier multiple-failure research also indicated that a second or subsequent failure could produce disproportionate degradation

when it removed a path that had already become important following the initial failure (Dondossola et al., 2020). This behavior was reflected in the present results through the simultaneous increase in route length from 6.20 to 9.10 hops and surviving-link utilization from 42.81% to 79.64%. The findings therefore supported earlier arguments that failure count alone does not explain resilience loss; topological position, alternative-path availability, spare capacity, and traffic redistribution determine the operational magnitude of a failure. Packet loss produced the largest observed effect, which was also consistent with studies of routing convergence demonstrating that packets are particularly vulnerable during periods in which forwarding information becomes temporarily inconsistent (Ilčev, 2017).

Figure 12: Five-Layer Network Resilience Framework



Service interruption increased from 3.61 seconds at the reference level to 11.84 seconds under multiple-link failure, further confirming that severe disruptions affected temporal service continuity as well as instantaneous network performance. Taken together, the findings strengthened the quantitative evidence that network resilience should be evaluated through several dependent variables simultaneously. A network may remain technically connected following a failure while experiencing substantial degradation in latency, packet delivery, throughput, route efficiency, and usable availability, making binary connectivity an insufficient measure of infrastructure resilience (Tootaghaj et al., 2018).

The traffic-load findings provided strong quantitative support for earlier congestion and network-performance research that treated traffic intensity as an important explanatory variable of reliability degradation. Under low-load failure conditions, mean latency was 47.26 ms, packet loss was 0.86%, jitter was 5.17 ms, and availability was 99.34%. Under high-load conditions, latency increased to 82.47 ms, packet loss reached 4.36%, jitter increased to 12.68 ms, and availability declined to 97.62%. Surviving-link utilization simultaneously increased from 48.73% to 84.16%, while throughput efficiency declined from 92.84% to 71.48% (Shi & Abdel-Aty, 2015). These results closely corresponded with earlier studies of Ethernet, WLAN, WAN, queueing behavior, multimedia traffic, and congestion control that demonstrated relatively stable performance at lower utilization levels followed by increasingly pronounced degradation as traffic demand approached available capacity. Earlier research

showed that increasing traffic load enlarges packet queues, raises waiting time, increases the probability of buffer overflow, and causes retransmissions when packets are discarded. The present findings provided an integrated empirical representation of these mechanisms because higher utilization was strongly correlated with latency, packet loss, jitter, and service interruption (Sergiou et al., 2014). Link utilization was positively correlated with latency at $r = 0.79$ and packet loss at $r = 0.76$, while negative relationships were observed with availability and throughput efficiency. These relatively strong coefficients suggested that traffic concentration on surviving infrastructure was a major component of failure-induced degradation rather than a secondary performance characteristic. The findings also corresponded with previous WLAN and real-time communication studies reporting that increases in concurrent users and application sessions elevate delay and packet-loss levels even before complete capacity exhaustion occurs. The decline in throughput efficiency under high load was particularly important because it illustrated the distinction between offered traffic and successfully delivered traffic (Pennetti et al., 2020). Earlier congestion research established that adding traffic beyond an efficient operating range does not necessarily produce proportional throughput gains because retransmissions, queue overflow, protocol overhead, and contention consume an increasing share of network resources. A similar relationship appeared in this study. The results also showed that traffic intensity interacted significantly with redundancy, indicating that the effect of traffic was especially important during failure recovery when alternative paths had to absorb redistributed flows. This finding aligned with earlier resilient-routing studies emphasizing that the existence of a backup path does not guarantee satisfactory performance when that path lacks adequate spare capacity (Yang et al., 2019). Traffic intensity therefore functioned as both an independent source of degradation and a condition that altered the operational effectiveness of network resilience mechanisms.

The redundancy analysis demonstrated that redundant network configurations significantly reduced failure-related degradation, supporting the central relationship identified throughout high-availability, fault-tolerant routing, multihoming, and resilient network architecture literature. Non-redundant configurations recorded mean latency of 76.38 ms, packet loss of 3.87%, jitter of 11.24 ms, link utilization of 81.73%, and service interruption of 10.36 seconds. In comparison, redundant configurations reduced latency to 55.47 ms, packet loss to 1.62%, jitter to 7.03%, link utilization to 63.28%, and service interruption to 5.81 seconds while increasing availability from 97.81% to 99.16%. These differences were statistically significant at $p < .001$ and demonstrated that redundant links, routers, gateways, and alternative paths provided measurable protection against infrastructure failure (Parizi et al., 2021). Earlier studies of dual-homed networks, redundant gateways, multiple ISPs, link aggregation, and high-availability routing similarly found that structural redundancy reduced the probability that an individual component failure would result in complete end-to-end service loss. The present findings were particularly consistent with research emphasizing the distinction between simple connectivity redundancy and capacity redundancy. Redundant configurations preserved higher availability, yet performance still deteriorated when traffic intensity became high, indicating that backup infrastructure did not eliminate the effects of disruption. This finding agreed with previous studies showing that failover can transfer large volumes of traffic onto secondary paths, causing those paths to approach saturation and reducing the effective benefit of redundancy (Klimek et al., 2019). The significant traffic-load-by-redundancy interactions provided statistical support for this conditional relationship. The interaction effect was strongest for packet loss, followed by service interruption and link utilization, suggesting that redundant capacity had its greatest protective influence on packet continuity and traffic redistribution. Earlier reliability research also emphasized independence among redundant components because two nominally separate links can remain vulnerable to a shared conduit, provider, gateway, power supply, or other common failure domain. Although the experimental configuration controlled these dependencies, the observed performance pattern supported the broader principle that redundancy must provide genuinely usable alternative capacity to improve availability (Shuang et al., 2019). The findings also complemented previous active-active and active-passive high-availability studies. The substantial reduction in interruption time indicated that pre-existing alternative resources allowed traffic to be transferred more rapidly than configurations requiring slower reconstruction of connectivity. Overall, the evidence confirmed that redundancy operated as a significant moderating

resilience variable, reducing the magnitude of failure effects while remaining dependent on traffic intensity, alternative-path capacity, routing behavior, and the severity of the underlying disruption (Kong et al., 2019).

The temporal findings clarified the relationship between failure severity, routing convergence, failover, and service restoration by showing that resilience recovery occurred through a sequence of measurable stages rather than as a single event. Under single-link failure, failure detection averaged 0.71 seconds, routing convergence required 2.83 seconds, service restoration required 4.96 seconds, and performance stabilization occurred after 6.42 seconds. Multiple-link failures extended these respective intervals to 1.16 seconds, 5.64 seconds, 9.27 seconds, and 12.86 seconds. All comparisons were statistically significant at $p < .001$ and generated large effect sizes (Nowell et al., 2017). These findings were consistent with earlier studies of OSPF, BGP, distance-vector routing, fast reroute, and high-availability networking that separated failure detection from routing recalculation and final convergence. Previous research established that a physical link can fail almost instantaneously while the resulting service disruption persists because routers must first identify the failure, distribute updated state information, calculate replacement paths, and install consistent forwarding decisions. The current results reproduced this temporal separation and demonstrated that the largest differences between single and multiple failures occurred during convergence, restoration, and stabilization rather than during initial detection. Earlier packet-delivery studies also reported transient forwarding loops, outdated routes, packet drops, and temporary unreachability during routing convergence. The increase in transition packet loss from 1.41% during single-link failure to 4.38% during multiple-link failure was consistent with those observations (Mackay et al., 2020). Redundancy substantially improved this process: routing convergence decreased from 5.18 seconds in non-redundant configurations to 3.21 seconds under redundancy, while service interruption declined by 43.92% and transition packet loss declined by 57.96%. These results supported earlier fast-reroute literature showing that backup paths and rapidly activated alternative forwarding states can protect data traffic during the interval required for broader routing convergence. An especially important finding concerned the difference between service restoration and performance stabilization. Immediately after connectivity had been restored, latency, throughput, packet loss, and jitter had not yet returned to their baseline levels (Chiesa et al., 2021). Only after the stabilization interval did these indicators approach pre-failure performance. This result was compatible with previous resilient-routing research indicating that emergency or backup paths may initially provide reachability while operating with longer routes, altered utilization, and reduced capacity. Consequently, measuring only routing convergence or first successful connectivity would have underestimated the full duration of the resilience process observed in this study.

The multivariate findings provided additional support for earlier reliability research by demonstrating that network resilience was not explained by a single technical factor (Siqueira et al., 2019). Failure severity, traffic intensity, redundancy, link utilization, and routing convergence each contributed independently to major network outcomes, with regression models explaining between 72% and 81% of the variance in the dependent measures. Failure severity was the strongest predictor of packet loss, with a standardized coefficient of 0.51, and was also strongly associated with reduced availability. Traffic intensity substantially predicted increased latency and lower throughput efficiency, while link utilization independently predicted packet loss. Redundancy positively predicted availability and throughput efficiency and negatively predicted service interruption. Routing convergence produced a standardized coefficient of 0.44 for service interruption, identifying convergence duration as a major temporal determinant of service continuity (Mostafaei et al., 2021). These results were consistent with earlier studies that conceptualized network resilience as an interaction among topology, capacity, routing behavior, traffic conditions, and recovery mechanisms. Reliability literature based solely on component failure rates has traditionally provided useful measures such as mean time between failures, mean time to repair, availability, and recovery time, but network-level studies have shown that identical component failure rates can produce very different service outcomes depending on where failures occur and how traffic is rerouted. The findings of this study reinforced that distinction. Failure severity had a direct relationship with performance degradation, but its operational effect was also transmitted through longer routes, increased utilization, congestion, and delayed convergence. The

high explanatory strength of the packet-loss model was consistent with earlier experimental work showing that packet delivery responds rapidly to congestion and routing instability and therefore provides a sensitive indicator of network disruption (Zhang et al., 2021). The protective regression effect associated with redundancy also agreed with high-availability studies demonstrating that alternative paths reduce the dependence of end-to-end communication on individual components. At the same time, the significant interaction between traffic and redundancy showed why structural redundancy cannot be interpreted independently from available capacity. A backup path that maintained connectivity under moderate demand could provide less effective protection under high utilization. The combined findings therefore supported a multidimensional interpretation of infrastructure resilience in which component and link failures initiated disruption, traffic conditions determined the pressure placed on surviving resources, routing convergence influenced interruption duration, and redundancy determined how much alternative capacity remained available to absorb the disturbance (Calder & Sevegnani, 2017).

The combined findings established substantial correspondence between the experimentally observed LAN/WAN behavior and the major patterns reported across earlier digital twin, network reliability, congestion, redundancy, routing convergence, and failure-modeling studies. The baseline analysis showed that WAN performance involved higher latency, greater jitter, lower throughput, and longer recovery intervals than LAN performance, which was consistent with earlier wide-area networking studies attributing these differences to geographic path length, routing complexity, heterogeneous links, bandwidth constraints, and dependence on distributed infrastructure (Kaitovic & Malek, 2018). Failure experiments confirmed earlier survivability research by showing that isolated failures produced measurable degradation and that multiple failures produced substantially greater deterioration when alternative paths became constrained. Traffic-load analysis reproduced established congestion relationships by demonstrating that increasing utilization was associated with higher latency, packet loss, jitter, and service interruption and with lower throughput efficiency and availability. Redundancy findings agreed with fault-tolerant network literature by demonstrating that alternative links and devices reduced interruption duration and maintained greater availability, while the significant interaction with traffic intensity confirmed that redundancy effectiveness depended on sufficient backup capacity (Cheng et al., 2020). The failover analysis also aligned with routing-convergence research by demonstrating that failure detection, backup activation, route recalculation, service restoration, and stabilization represented distinct temporal components of resilience. Most importantly, the digital twin reproduced these relationships with correlations exceeding 0.94 across all principal physical-virtual comparisons. This result linked the separate empirical findings into a unified reliability-modeling framework because the digital environment represented not only static baseline performance but also the direction and magnitude of degradation, rerouting, failover, and recover (Youssef, et al., 2020). Earlier Network Digital Twin studies emphasized synchronization, model fidelity, telemetry integration, and state representation as necessary characteristics for meaningful network modeling. The present findings provided quantitative support for those principles through low prediction errors and small physical-virtual effect sizes across multiple experimental states. The evidence also showed why digital twin fidelity should not be evaluated from a single baseline comparison. Accuracy remained high while network states changed substantially, although dynamic variables such as packet loss and recovery duration exhibited moderately greater prediction error than stable indicators (Bécue et al., 2020). Across the complete experimental sequence, the results therefore remained consistent with the broader empirical literature while integrating relationships that were often examined separately in earlier studies. Failure severity, traffic intensity, redundant capacity, routing convergence, and physical-virtual fidelity were quantitatively connected within the same experimental framework, providing a comprehensive explanation of how LAN and WAN infrastructure behavior changed from stable operation through disruption and ultimately to restored performance (Faddel, & Mohammed, 2020).

CONCLUSION

This study concluded that digital twin-based network reliability modeling provided a quantitatively robust approach for representing, measuring, and evaluating the resilience of LAN and WAN infrastructures under varying traffic, failure, redundancy, failover, and recovery conditions. The

experimental findings established that the digital twin closely reproduced the behavior of the reference network, with physical–virtual correlation coefficients ranging from 0.941 to 0.988 and comparatively low prediction errors across latency, throughput, packet loss, jitter, availability, link utilization, routing convergence, failover time, and recovery duration. Network failure severity emerged as a major determinant of reliability degradation, as the transition from baseline operation to single-link, device, and multiple-link failure conditions progressively increased latency, packet loss, route length, surviving-link utilization, and service interruption while reducing throughput and availability. Multiple-link failures produced the greatest deterioration, confirming that reduced path diversity and concentrated traffic significantly weakened end-to-end resilience. Traffic intensity further influenced reliability, with high-load conditions generating greater congestion, jitter, packet loss, latency, and interruption duration than moderate- and low-load conditions. Redundancy significantly reduced these adverse effects by providing alternative communication paths and backup resources, resulting in higher availability, lower packet loss, shorter interruption periods, and faster recovery, although its effectiveness decreased when surviving infrastructure approached capacity limits. The temporal analysis additionally established that network recovery consisted of distinct stages involving failure detection, failover initiation, backup-path activation, routing convergence, service restoration, and performance stabilization. Multiple-link failures extended each stage, whereas redundant configurations significantly shortened convergence and restoration periods and reduced transition packet loss. Regression results further demonstrated that failure severity, traffic intensity, link utilization, routing convergence, and redundancy collectively explained substantial variation in network reliability outcomes, with model explanatory strength ranging from 72% to 81%. Overall, the findings established that infrastructure resilience was determined by the interaction of network topology, failure severity, traffic demand, alternative-path capacity, routing responsiveness, and recovery efficiency rather than by availability or connectivity alone. The strong agreement between the digital twin and reference infrastructure demonstrated that a properly calibrated and synchronized digital twin could quantitatively reproduce both stable and disrupted network states, providing a comprehensive representation of LAN and WAN reliability across baseline operation, degradation, failover, recovery, and stabilized post-failure conditions.

RECOMMENDATIONS

Based on the findings of this study, organizations and network administrators should adopt digital twin-based reliability modeling as a structured component of LAN and WAN infrastructure management because the strong correspondence between the reference network and digital twin demonstrated the value of virtual representations for evaluating network behavior under normal and disrupted operating conditions. Network digital twins should be continuously synchronized with relevant topology, device configuration, routing state, traffic characteristics, interface utilization, and performance telemetry to maintain sufficient model fidelity for reliability assessment. Particular attention should be directed toward critical routers, switches, gateways, WAN connections, interfaces, and aggregation links whose failure could generate extensive service disruption. Organizations should strengthen infrastructure redundancy through dual routers, redundant switches, multiple gateways, alternative routing paths, backup WAN connections, link aggregation, and multiple service providers where operationally appropriate. Redundant resources should also possess sufficient spare capacity to accommodate redistributed traffic because the findings indicated that redundancy became less effective when surviving links approached saturation. Network capacity planning should incorporate peak and burst traffic rather than relying solely on average utilization, with latency, packet loss, jitter, throughput efficiency, and link utilization monitored simultaneously to identify developing congestion. Failure-detection and failover mechanisms should be optimized to minimize the intervals between failure occurrence, detection, alternative-path activation, routing convergence, and service restoration. Routing protocols, timer configurations, backup routes, and high-availability mechanisms should be regularly tested through controlled failure scenarios rather than assumed to operate effectively from configuration status alone. Reliability testing should include baseline, single-link, multiple-link, device-failure, high-traffic, failover, and recovery scenarios so that infrastructure behavior can be evaluated under progressively severe disruptions. Network performance assessment should also extend beyond initial restoration of connectivity because the findings showed that complete traffic stabilization

occurred after service had technically been restored. Organizations should therefore establish resilience indicators that include failure detection time, convergence time, transition packet loss, service interruption duration, recovery time, and post-recovery stabilization. Digital twin accuracy should be periodically validated against observed infrastructure measurements using correlation, prediction-error, and physical-virtual deviation measures. Finally, network reliability decisions should be supported by integrated statistical analysis of failure severity, traffic intensity, redundancy, utilization, and convergence behavior, enabling infrastructure resources to be prioritized according to measurable resilience requirements rather than isolated performance indicators or device availability alone.

LIMITATIONS

This study was subject to several limitations that should be considered when interpreting the quantitative findings on digital twin-based LAN and WAN infrastructure resilience. First, the experimental environment represented a controlled selection of LAN and WAN configurations, devices, links, routing conditions, and traffic characteristics and therefore could not reproduce every architectural variation encountered in large-scale enterprise, telecommunications, cloud, campus, or geographically distributed networks. Second, the digital twin was calibrated against the selected reference infrastructure, meaning that the high physical-virtual correlations and relatively low prediction errors observed in this study were associated with the particular topology, configurations, telemetry sources, and operating conditions included in the experiment. Third, traffic intensity was classified into controlled low, moderate, and high conditions, whereas operational networks can experience irregular traffic bursts, seasonal variations, application-specific demand, asymmetric flows, and unpredictable user activity that may produce different reliability patterns. Fourth, the investigated failure scenarios concentrated primarily on link and selected device disruptions, redundancy, failover, and recovery; consequently, the experimental conditions did not comprehensively represent every possible software defect, configuration error, cybersecurity incident, power disruption, carrier outage, environmental event, or correlated infrastructure failure. Fifth, multiple-link failures were introduced under predefined experimental conditions, which limited representation of complex cascading failures in which one disruption changes network load and subsequently contributes to additional component failures. Sixth, reliability measurements such as latency, throughput, packet loss, jitter, availability, link utilization, convergence time, and service interruption provided strong quantitative indicators but did not capture every dimension of application-level service quality or user experience. Seventh, routing convergence and failover measurements depended on the protocols, timer settings, backup configurations, and monitoring resolution used within the experimental environment, which restricted direct generalization of the reported temporal values to networks using substantially different technologies. Eighth, statistical analyses identified significant relationships among failure severity, traffic intensity, redundancy, utilization, and reliability outcomes, but these relationships remained dependent on the experimental design and should not automatically be interpreted as universal effect magnitudes across all infrastructures. Finally, the digital twin required accurate telemetry and configuration synchronization; incomplete, delayed, or inaccurate network-state data could increase physical-virtual deviation and reduce predictive fidelity. These limitations constrained the generalizability of the numerical results while preserving their relevance to the controlled network conditions evaluated in this study.

REFERENCES

- [1]. Ahmad, S., & Mir, A. H. (2021). Scalability, consistency, reliability and security in SDN controllers: a survey of diverse SDN controllers. *Journal of Network and Systems Management*, 29(1), 9.
- [2]. Ahmed, M. A., El-Sharkawy, M. R., & Kim, Y.-C. (2019). Remote monitoring of electric vehicle charging stations in smart campus parking lot. *Journal of Modern Power Systems and Clean Energy*, 8(1), 124-132.
- [3]. Alam, K. M., & El Saddik, A. (2017). C2PS: A digital twin architecture reference model for the cloud-based cyber-physical systems. *IEEE Access*, 5, 2050-2062.
- [4]. Ali, J., Lee, G.-M., Roh, B.-H., Ryu, D. K., & Park, G. (2020). Software-defined networking approaches for link failure recovery: A survey. *Sustainability*, 12(10), 4255.
- [5]. Alizadeh, H., & Sharifi, A. (2020). Assessing resilience of urban critical infrastructure networks: A case study of Ahvaz, Iran. *Sustainability*, 12(9), 3691.
- [6]. Alwasel, K., Jha, D. N., Hernandez, E., Puthal, D., Barika, M., Varghese, B., Garg, S. K., James, P., Zomaya, A., & Morgan, G. (2020). IoTsim-SDWAN: A simulation framework for interconnecting distributed datacenters over Software-Defined Wide Area Network (SD-WAN). *Journal of Parallel and Distributed Computing*, 143, 17-35.

- [7]. Amin, M., El-Sousy, F. F., Aziz, G. A. A., Gaber, K., & Mohammed, O. A. (2021). CPS attacks mitigation approaches on power electronic systems with security challenges for smart grid applications: A review. *IEEE Access*, 9, 38571-38601.
- [8]. Anda, I., Mishra, R., & Aliyu, A. M. (2021). Data security management framework for digital twins of industrial pipeline. 2021 International conference on maintenance and intelligent asset management (ICMIAM),
- [9]. Andrysiak, T., Saganowski, L., & Mazurczyk, W. (2016). Network anomaly detection for railway critical infrastructure based on autoregressive fractional integrated moving average. *EURASIP Journal on Wireless Communications and Networking*, 2016(1), 245.
- [10]. Arfeen, A., & Uddin, R. (2020). Quality of experience-based optimization of satellite Internet-at-sea using WAN accelerators. *International Journal of Satellite Communications and Networking*, 38(6), 527-556.
- [11]. Balachandar, S., & Chinnaiyan, R. (2020). Reliable pharma cold chain monitoring and analytics through Internet of Things Edge. In *Emergence of pharmaceutical industry growth with industrial IoT approach* (pp. 133-161). Elsevier.
- [12]. Balachandran, T., Manoharan, A.-K., Aravinthan, V., & Singh, C. (2020). Component-level reliability evaluation model for cyber power devices. *IEEE Transactions on Smart Grid*, 12(1), 692-703.
- [13]. Baroud, H., Barker, K., Ramirez-Marquez, J. E., & Rocco, C. M. (2015). Inherent costs and interdependent impacts of infrastructure network resilience. *Risk Analysis*, 35(4), 642-662.
- [14]. Bécue, A., Maia, E., Feeken, L., Borchers, P., & Praça, I. (2020). A new concept of digital twin supporting optimization and resilience of factories of the future. *Applied Sciences*, 10(13), 4482.
- [15]. Belgaum, M. R., Musa, S., Alam, M. M., & Su'ud, M. M. (2020). A systematic review of load balancing techniques in software-defined networking. *IEEE Access*, 8, 98612-98636.
- [16]. Cai, Z., Yu, M., Steurer, M., Li, H., & Dong, Y. (2016). A network model for the real-time communications of a smart grid prototype. *Journal of Network and Computer Applications*, 59, 264-273.
- [17]. Calder, M., & Sevegnani, M. (2017). Stochastic model checking for predicting component failures and service availability. *IEEE Transactions on Dependable and Secure Computing*, 16(1), 174-187.
- [18]. Camarinha-Matos, L. M., Fornasiero, R., Ramezani, J., & Ferrada, F. (2019). Collaborative networks: A pillar of digital transformation. *Applied Sciences*, 9(24), 5431.
- [19]. Caraguay, Á. L. V., Fernández, J. A. P., & Villalba, L. J. G. (2015). Framework for optimized multimedia routing over software defined networks. *Computer Networks*, 92, 369-379.
- [20]. Carvalho, G., Cabral, B., Pereira, V., & Bernardino, J. (2021). Edge computing: current trends, research challenges and future directions: G. Carvalho et al. *Computing*, 103(5), 993-1023.
- [21]. Cascone, L., Nappi, M., Narducci, F., & Passero, I. (2021). DTPAAL: Digital twinning pepper and ambient assisted living. *IEEE Transactions on Industrial Informatics*, 18(2), 1397-1404.
- [22]. Chen, B. Y., Yuan, H., Li, Q., Wang, D., Shaw, S.-L., Chen, H.-P., & Lam, W. H. (2017). Measuring place-based accessibility under travel time uncertainty. *International Journal of Geographical Information Science*, 31(4), 783-804.
- [23]. Cheng, J. C., Chen, W., Chen, K., & Wang, Q. (2020). Data-driven predictive maintenance planning framework for MEP components based on BIM and IoT using machine learning algorithms. *Automation in construction*, 112, 103087.
- [24]. Cheng, Z., Zhang, X., Li, Y., Yu, S., Lin, R., & He, L. (2017). Congestion-aware local reroute for fast failure recovery in software-defined networks. *Journal of Optical Communications and Networking*, 9(11), 934-944.
- [25]. Chiesa, M., Kamisiński, A., Rak, J., Rétvári, G., & Schmid, S. (2021). A survey of fast-recovery mechanisms in packet-switched networks. *IEEE Communications Surveys & Tutorials*, 23(2), 1253-1301.
- [26]. Chinchilla-Romero, L., Prados-Garzon, J., Ameigeiras, P., Muñoz, P., & Lopez-Soler, J. M. (2021). 5G infrastructure network slicing: E2E mean delay model and effectiveness assessment to reduce downtimes in industry 4.0. *Sensors*, 22(1), 229.
- [27]. Da Silva, C. A. G., & Pedroso, C. M. (2019). Mac-layer packet loss models for wi-fi networks: A survey. *IEEE Access*, 7, 180512-180531.
- [28]. De Almeida, L. F. F., Pereira, L. A. M., Sodré, A. C., Mendes, L. L., Rodrigues, J. J., Rabelo, R. A., & Alberti, A. M. (2020). Control networks and smart grid teleprotection: Key aspects, technologies, protocols, and case-studies. *IEEE Access*, 8, 174049-174079.
- [29]. Dondossola, G., Costa de Araujo, M., & McGeough, K. (2020). Information Systems and Telecommunications. In *Electricity Supply Systems of the Future* (pp. 611-655). Springer.
- [30]. Dzeperoska, K., Beigi-Mohammadi, N., Tizghadam, A., & Leon-Garcia, A. (2021). Towards a self-driving management system for the automated realization of intents. *IEEE Access*, 9, 159882-159907.
- [31]. Emara, M., Filippou, M. C., & Karls, I. (2018). Availability and reliability of wireless links in 5G systems: A space-time approach. 2018 IEEE Globecom Workshops (GC Wkshps),
- [32]. Fadel, E., Gungor, V. C., Nassef, L., Akkari, N., Malik, M. A., Almasri, S., & Akyildiz, I. F. (2015). A survey on wireless sensor networks for smart grid. *Computer Communications*, 71, 22-33.
- [33]. Fraga-Lamas, P., Varela-Barbeito, J., & Fernández-Caramés, T. M. (2021). Next generation auto-identification and traceability technologies for industry 5.0: A methodology and practical use case for the shipbuilding industry. *IEEE Access*, 9, 140700-140730.
- [34]. Gál, Z., Kocsis, G., Tajti, T., & Tornai, R. (2021). Performance evaluation of massively parallel and high speed connectionless vs. connection oriented communication sessions. *Advances in Engineering Software*, 157, 103010.
- [35]. Ge, L., & Zhang, Y. (2020). Multi-level approach for important component identification and reliability evaluation for complex system by survival signature. *Engineering Computations*, 37(1), 262-288.

- [36]. Ghiani, E., Serpi, A., Pilloni, V., Sias, G., Simone, M., Marcialis, G., Armano, G., & Pegoraro, P. A. (2018). A multidisciplinary approach for the development of smart distribution networks. *Energies*, 11(10), 2530.
- [37]. Hungud, V., & Arunachalam, S. K. (2020). Digital twin: Empowering edge devices to be intelligent. In *Advances in computers* (Vol. 117, pp. 107-127). Elsevier.
- [38]. Ibrahim, M. S., Fan, J., Yung, W. K., Jing, Z., Fan, X., van Driel, W., & Zhang, G. (2021). System level reliability assessment for high power light-emitting diode lamp based on a Bayesian network method. *Measurement*, 176, 109191.
- [39]. Ilčev, S. D. (2017). Global Broadcasting Satellite System (GBSS). In *Global Mobile Satellite Communications Applications: For Maritime, Land and Aeronautical Applications Volume 2* (pp. 203-304). Springer.
- [40]. Jia, P., Wang, X., & Shen, X. (2020). Digital-twin-enabled intelligent distributed clock synchronization in industrial IoT systems. *IEEE Internet of Things Journal*, 8(6), 4548-4559.
- [41]. Jiang, H., Qin, S., Fu, J., Zhang, J., & Ding, G. (2021). How to model and implement connections between physical and virtual models for digital twin application. *Journal of Manufacturing Systems*, 58, 36-51.
- [42]. Jiang, H., Qu, T., Wan, M., Tang, L., & Huang, G. Q. (2020). Digital-twin-based implementation framework of production service system for highly dynamic production logistics operation. *IET Collaborative Intelligent Manufacturing*, 2(2), 74-80.
- [43]. Jing, W., Xu, X., & Pu, Y. (2019). Route Redundancy-Based Network Topology Measure of Metro Networks. *Journal of Advanced Transportation*, 2019(1), 4576961.
- [44]. Kaitovic, I., & Malek, M. (2018). Impact of failure prediction on availability: Modeling and comparative analysis of predictive and reactive methods. *IEEE Transactions on Dependable and Secure Computing*, 17(3), 493-505.
- [45]. Khamis, A. Smart Mobility.
- [46]. Khamis, A. (2021). Smart mobility: foundational technologies. In *Smart Mobility: Exploring Foundational Technologies and Wider Impacts* (pp. 21-73). Springer.
- [47]. Khan, A. A., Rehmani, M. H., & Reisslein, M. (2017). Requirements, design challenges, and review of routing and MAC protocols for CR-based smart grid systems. *IEEE Communications Magazine*, 55(5), 206-215.
- [48]. Klimek, P., Varga, J., Jovanovic, A. S., & Székely, Z. (2019). Quantitative resilience assessment in emergency response reveals how organizations trade efficiency for redundancy. *Safety science*, 113, 404-414.
- [49]. Kong, J., Simonovic, S. P., & Zhang, C. (2019). Resilience assessment of interdependent infrastructure systems: a case study based on different response strategies. *Sustainability*, 11(23), 6552.
- [50]. Koot, M., Iacob, M.-E., & Mes, M. R. (2021). A reference architecture for IoT-enabled dynamic planning in smart logistics. *International Conference on Advanced Information Systems Engineering*.
- [51]. Kotronis, V., Gämperli, A., & Dimitropoulos, X. (2015). Routing centralization across domains via SDN: A model and emulation framework for BGP evolution. *Computer Networks*, 92, 227-239.
- [52]. Lan, H., Ding, W., & Gong, J. (2019). Useful Traffic Loss Rate Estimation Based on Network Layer Measurement. *IEEE Access*, 7, 33289-33303.
- [53]. Lee, D., & Pan, R. (2017). Predictive maintenance of complex system with multi-level reliability structure. *International Journal of Production Research*, 55(16), 4785-4801.
- [54]. Lee, D., & Pan, R. (2018). A nonparametric Bayesian network approach to assessing system reliability at early design stages. *Reliability Engineering & System Safety*, 171, 57-66.
- [55]. Leng, J., Liu, Q., Ye, S., Jing, J., Wang, Y., Zhang, C., Zhang, D., & Chen, X. (2020). Digital twin-driven rapid reconfiguration of the automated manufacturing system via an open architecture model. *Robotics and computer-integrated manufacturing*, 63, 101895.
- [56]. Leng, J., Yan, D., Liu, Q., Xu, K., Zhao, J. L., Shi, R., Wei, L., Zhang, D., & Chen, X. (2019). ManuChain: Combining permissioned blockchain with a holistic optimization model as bi-level intelligence for smart manufacturing. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 50(1), 182-192.
- [57]. Leng, J., Zhang, H., Yan, D., Liu, Q., Chen, X., & Zhang, D. (2019). Digital twin-driven manufacturing cyber-physical system for parallel controlling of smart workshop. *Journal of ambient intelligence and humanized computing*, 10(3), 1155-1166.
- [58]. Li, L., Aslam, S., Wileman, A., & Perinpanayagam, S. (2021). Digital twin in aerospace industry: A gentle introduction. *IEEE Access*, 10, 9543-9562.
- [59]. Lin, S., Wang, Y., Jia, L., & Zhang, H. (2018). Reliability assessment of complex electromechanical systems: A network perspective. *Quality and Reliability Engineering International*, 34(5), 772-790.
- [60]. Liu, C., Vengayil, H., Lu, Y., & Xu, X. (2019). A cyber-physical machine tools platform using OPC UA and MTConnect. *Journal of Manufacturing Systems*, 51, 61-74.
- [61]. Liu, W., Lin, Z., Wang, L., Wang, Z., Wang, H., & Gong, Q. (2020). Analytical reliability evaluation of active distribution systems considering information link failures. *IEEE Transactions on Power Systems*, 35(6), 4167-4179.
- [62]. Machuca, C. M., Secci, S., Vizarreta, P., Kuipers, F., Gouglidis, A., Hutchison, D., Jouet, S., Pezaros, D., Elmokashfi, A., & Heegaard, P. (2016). Technology-related disasters: A survey towards disaster-resilient software defined networks. 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM).
- [63]. Mackay, J., Munoz, A., & Pepper, M. (2020). Conceptualising redundancy and flexibility towards supply chain robustness and resilience. *Journal of Risk Research*, 23(12), 1541-1561.
- [64]. Manohar, R., Sreenilayam, R. K., & Pandey, V. (2020). Functional Approach for Reliability Evaluation of WLAN Communication Networks. 2020 Fifth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN),

- [65]. Masdari, M., & Zangakani, M. (2020). Green cloud computing using proactive virtual machine placement: challenges and issues. *Journal of Grid Computing*, 18(4), 727-759.
- [66]. Md Asif Ali Sheak, A., & Risha, A. (2022). The Role of IOT-Driven Energy Analytics in Improving Operational Efficiency and Sustainability in Modern Industrial Facilities. *American Journal of Interdisciplinary Studies*, 3(04), 807-841. <https://doi.org/10.63125/gm63q956>
- [67]. Md. Abdur, R., & Iftekhar, A. (2021). Customer Retention Forecasting in Mobile Wallet Services Using Neural Networks: A Comparative Quantitative Study. *International Journal of Business and Economics Insights*, 1(4), 70-102. <https://doi.org/10.63125/dyrpc387>
- [68]. Mohammad Abir Chowdhury, S. (2023). Role of AI-Assisted Risk Assessment in Enhancing Audit Planning Efficiency and Risk Prioritization in Public-Safety Organizations. *International Journal of Scientific Interdisciplinary Research*, 4(4), 529-576. <https://doi.org/10.63125/qd6nn437>
- [69]. Mohammad Abir Chowdhury, S., & Tonay, P. (2022). An Empirical Analysis of the Impact of Robotic Process Automation and Continuous Auditing on the Timeliness And Accuracy Of Financial Reporting Assurance. *International Journal of Business and Economics Insights*, 2(4), 73-126. <https://doi.org/10.63125/7p8dcr47>
- [70]. Mohammad Badrul, A., & Md. Mominul, H. (2023). Machine Learning-Based Assessment of Environmental and Public Health Risks in Sewerage Sludge Management Systems. *American Journal of Advanced Technology and Engineering Solutions*, 3(02), 33-77. <https://doi.org/10.63125/y3yfxa92>
- [71]. Mostafaei, H., Shojafar, M., & Conti, M. (2021). TEL: Low-latency failover traffic engineering in data plane. *IEEE transactions on network and service management*, 18(4), 4697-4710.
- [72]. Mountaser, G., Mahmoodi, T., & Simeone, O. (2018). Reliable and low-latency fronthaul for tactile internet applications. *IEEE Journal on Selected Areas in Communications*, 36(11), 2455-2463.
- [73]. Mourtzis, D., Angelopoulos, J., & Panopoulos, N. (2021). Smart manufacturing and tactile internet based on 5G in industry 4.0: Challenges, applications and new trends. *Electronics*, 10(24), 3175.
- [74]. Muhammad Zahidul, I. (2023). Comparative Analysis of Machine-Learning Approaches for Pharmaceutical Sales Forecasting and Market-Demand Prediction. *Review of Applied Science and Technology*, 2(02), 38-95. <https://doi.org/10.63125/etcbqf13>
- [75]. Nan, C., & Sansavini, G. (2017). A quantitative method for assessing resilience of interdependent infrastructures. *Reliability Engineering & System Safety*, 157, 35-53.
- [76]. Nasrallah, A., Thyagaturu, A. S., Alharbi, Z., Wang, C., Shao, X., Reisslein, M., & ElBakoury, H. (2018). Ultra-low latency (ULL) networks: The IEEE TSN and IETF DetNet standards and related 5G ULL research. *IEEE Communications Surveys & Tutorials*, 21(1), 88-145.
- [77]. Nencioni, G., Helvik, B. E., & Heegaard, P. E. (2017). Including failure correlation in availability modeling of a software-defined backbone network. *IEEE transactions on network and service management*, 14(4), 1032-1045.
- [78]. Nguyen, T. A., Min, D., Choi, E., & Tran, T. D. (2019). Reliability and availability evaluation for cloud data center networks using hierarchical models. *IEEE Access*, 7, 9273-9313.
- [79]. Nishat, J., & Mst Kaniz, F. (2022). A Review of the Impact of Covid-19 On Maternal and Child Health Service Utilization in Bangladesh. *American Journal of Scholarly Research and Innovation*, 1(02), 223-269. <https://doi.org/10.63125/vgv5s742>
- [80]. Nowell, B., Bodkin, C. P., & Bayoumi, D. (2017). Redundancy as a strategy in disaster response systems: A pathway to resilience or a recipe for disaster? *Journal of Contingencies and Crisis Management*, 25(3), 123-135.
- [81]. O'Connor, A., & Mosleh, A. (2016). A general cause based methodology for analysis of common cause and dependent failures in system risk and reliability assessments. *Reliability Engineering & System Safety*, 145, 341-350.
- [82]. Ordonez-Lucena, J., Ameigeiras, P., Contreras, L. M., Folgueira, J., & López, D. R. (2021). On the rollout of network slicing in carrier networks: A technology radar. *Sensors*, 21(23), 8094.
- [83]. Pan, R., & Yontay, P. (2017). Reliability assessment of hierarchical systems with incomplete mixed data. *IEEE Transactions on reliability*, 66(4), 1036-1047.
- [84]. Pan, Y., Qu, T., Wu, N., Khalgui, M., & Huang, G. Q. (2021). Digital twin based real-time production logistics synchronization system in a multi-level computing architecture. *Journal of Manufacturing Systems*, 58, 246-260.
- [85]. Parizi, S. M., Taleai, M., & Sharifi, A. (2021). Integrated methods to determine urban physical resilience characteristics and their interactions. *Natural Hazards*, 109(1), 725-754.
- [86]. Park, K. T., Lee, J., Kim, H.-J., & Noh, S. D. (2020). Digital twin-based cyber physical production system architectural framework for personalized production. *The International Journal of Advanced Manufacturing Technology*, 106(5), 1787-1810.
- [87]. Pennetti, C. A., Fontaine, M. D., Jun, J., & Lambert, J. H. (2020). Evaluating capacity of transportation operations with highway travel time reliability. *Reliability Engineering & System Safety*, 204, 107126.
- [88]. Pocovi, G., Kolding, T., Lauridsen, M., Mogensen, R., Markmler, C., & Jess-Williams, R. (2018). Measurement framework for assessing reliable real-time capabilities of wireless networks. *IEEE Communications Magazine*, 56(12), 156-163.
- [89]. Qiuchen Lu, V., Parlikad, A. K., Woodall, P., Ranasinghe, G. D., & Heaton, J. (2019). Developing a dynamic digital twin at a building level: Using Cambridge campus as case study.
- [90]. Rebello, S., Yu, H., & Ma, L. (2018). An integrated approach for system functional reliability assessment using Dynamic Bayesian Network and Hidden Markov Model. *Reliability Engineering & System Safety*, 180, 124-135.
- [91]. Rehak, D., Senovsky, P., & Slivkova, S. (2018). Resilience of critical infrastructure elements and its main factors. *Systems*, 6(2), 21.

- [92]. Ren, Z., & Wan, J. (2021). Strengthening digital twin applications based on machine learning for complex equipment. 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE),
- [93]. Saad, A., Faddel, S., & Mohammed, O. (2020). IoT-based digital twin for energy cyber-physical systems: design and implementation. *Energies*, 13(18), 4762.
- [94]. Saad, A., Faddel, S., Youssef, T., & Mohammed, O. A. (2020). On the implementation of IoT-based digital twin for networked microgrids resiliency against cyber attacks. *IEEE Transactions on Smart Grid*, 11(6), 5138-5150.
- [95]. Saeed, I. A., Selamat, A., Rohani, M. F., Krejcar, O., & Chaudhry, J. A. (2020). A systematic state-of-the-art analysis of multi-agent intrusion detection. *IEEE Access*, 8, 180184-180209.
- [96]. Scanzio, S., Vakili, M. G., Cena, G., Demartini, C. G., Montrucchio, B., Valenzano, A., & Zunino, C. (2020). Wireless sensor networks and TSCH: A compromise between reliability, power consumption, and latency. *IEEE Access*, 8, 167042-167058.
- [97]. Sergiou, C., Antoniou, P., & Vassiliou, V. (2014). A comprehensive survey of congestion control protocols in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 16(4), 1839-1859.
- [98]. Serrano, W. (2018). Digital systems in smart city and infrastructure: Digital as a service. *Smart cities*, 1(1), 134-154.
- [99]. Shahzad, Y., Javed, H., Farman, H., Ahmad, J., Jan, B., & Zubair, M. (2020). Internet of energy: Opportunities, applications, architectures and challenges in smart industries. *Computers & Electrical Engineering*, 86, 106739.
- [100]. Shaiful, M., Anisur, R., & Md, A. (2022). A Systematic Literature Review on the Role of Digital Health Twins in Preventive Healthcare For Personal and Corporate Wellbeing. *American Journal of Interdisciplinary Studies*, 3(04), 1-31. <https://doi.org/10.63125/negjw373>
- [101]. Shen, W., Yang, C., & Gao, L. (2020). Address business crisis caused by COVID-19 with collaborative intelligent manufacturing technologies. *IET Collaborative Intelligent Manufacturing*, 2(2), 96-99.
- [102]. Shen, X., Gao, J., Wu, W., Li, M., Zhou, C., & Zhuang, W. (2021). Holistic network virtualization and pervasive network intelligence for 6G. *IEEE Communications Surveys & Tutorials*, 24(1), 1-30.
- [103]. Shi, Q., & Abdel-Aty, M. (2015). Big data applications in real-time traffic operation and safety monitoring and improvement on urban expressways. *Transportation Research Part C: Emerging Technologies*, 58, 380-394.
- [104]. Shin, S., Lee, S., Judi, D. R., Parvania, M., Goharian, E., McPherson, T., & Burian, S. J. (2018). A systematic review of quantitative resilience measures for water infrastructure systems. *Water*, 10(2), 164.
- [105]. Shuang, Q., Liu, H. J., & Porse, E. (2019). Review of the quantitative resilience methods in water distribution networks. *Water*, 11(6), 1189.
- [106]. Siqueira, D., Pinheiro, T., Dantas, J., & Maciel, P. (2019). Dependability evaluation in a convergent network service using BGP and BFD protocols. 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC),
- [107]. Song, S., Park, H., Choi, B.-Y., Choi, T., & Zhu, H. (2017). Control path management framework for enhancing software-defined network (SDN) reliability. *IEEE transactions on network and service management*, 14(2), 302-316.
- [108]. Soret, B., Mogensen, P., Pedersen, K. I., & Aguayo-Torres, M. C. (2014). Fundamental tradeoffs among reliability, latency and throughput in cellular networks. 2014 IEEE Globecom Workshops (GC Wkshps),
- [109]. Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2014). Redundancy, diversity, and connectivity to achieve multilevel network resilience, survivability, and disruption tolerance invited paper. *Telecommunication Systems*, 56(1), 17-31.
- [110]. Sun, B., Li, Y., Wang, Z., Yang, D., Ren, Y., & Feng, Q. (2021). A combined physics of failure and Bayesian network reliability analysis method for complex electronic systems. *Process Safety and Environmental Protection*, 148, 698-710.
- [111]. Sun, W., Yuan, X., Wang, J., Li, Q., Chen, L., & Mu, D. (2017). End-to-end data delivery reliability model for estimating and optimizing the link quality of industrial WSNs. *IEEE Transactions on Automation Science and Engineering*, 15(3), 1127-1137.
- [112]. Szabó, G., Rácz, S., Reider, N., Munz, H. A., & Pető, J. (2019). Digital twin: Network provisioning of mission critical communication in cyber physical production systems. 2019 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT),
- [113]. Taimoor, N., & Rehman, S. (2021). Reliable and resilient AI and IoT-based personalised healthcare services: A survey. *IEEE Access*, 10, 535-563.
- [114]. Tanha, M., Sajjadi, D., & Pan, J. (2018). Demystifying failure recovery for software-defined wireless mesh networks. 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft),
- [115]. Tawalbeh, L. a. (2020). Network management. In *The NICE Cyber Security Framework: Cyber Security Management* (pp. 99-115). Springer.
- [116]. Tootaghaj, D. Z., Bartolini, N., Khamfroush, H., & La Porta, T. (2018). On progressive network recovery from massive failures under uncertainty. *IEEE transactions on network and service management*, 16(1), 113-126.
- [117]. Troia, S., Sapienza, F., Varé, L., & Maier, G. (2020). On deep reinforcement learning for traffic engineering in SD-WAN. *IEEE Journal on Selected Areas in Communications*, 39(7), 2198-2212.
- [118]. Ukwandu, E., Farah, M. A. B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., Tachtatzis, C., Bures, M., Andonovic, I., & Bellekens, X. (2020). A review of cyber-ranges and test-beds: Current and future trends. *Sensors*, 20(24), 7148.
- [119]. Vaagensmith, B., Singh, V. K., Ivans, R., Marino, D. L., Wickramasinghe, C. S., Lehmer, J., Phillips, T., Rieger, C., & Manic, M. (2021). Review of design elements within power infrastructure cyber-physical test beds as threat analysis environments. *Energies*, 14(5), 1409.
- [120]. Wang, P., & Luo, M. (2021). A digital twin-based big data virtual and real fusion learning reference framework supported by industrial internet towards smart manufacturing. *Journal of Manufacturing Systems*, 58, 16-32.

- [121]. Wang, Y., Xing, L., Wang, H., & Coit, D. W. (2017). System reliability modeling considering correlated probabilistic competing failures. *IEEE Transactions on reliability*, 67(2), 416-431.
- [122]. Wu, Y., Wu, Y., Guerrero, J. M., Vasquez, J. C., Palacios-Garcia, E. J., & Li, J. (2020). Convergence and interoperability for the energy internet: From ubiquitous connection to distributed automation. *IEEE Industrial Electronics Magazine*, 14(4), 91-105.
- [123]. Wu, Y., Zhang, K., & Zhang, Y. (2021). Digital twin networks: A survey. *IEEE Internet of Things Journal*, 8(18), 13789-13804.
- [124]. Xing, L. (2020a). Cascading failures in Internet of Things: Review and perspectives on reliability and resilience. *IEEE Internet of Things Journal*, 8(1), 44-64.
- [125]. Xing, L. (2020b). Reliability in Internet of Things: Current status and future perspectives. *IEEE Internet of Things Journal*, 7(8), 6704-6721.
- [126]. Xu, Q., Xu, Y., Tu, P., Zhao, T., & Wang, P. (2019). Systematic reliability modeling and evaluation for on-board power systems of more electric aircrafts. *IEEE Transactions on Power Systems*, 34(4), 3264-3273.
- [127]. Xu, X., Chen, A., Jansuwan, S., Heaslip, K., & Yang, C. (2015). Modeling transportation network redundancy. *Transportation research procedia*, 9, 283-302.
- [128]. Xu, X., Chen, A., Jansuwan, S., Yang, C., & Ryu, S. (2018). Transportation network redundancy: Complementary measures and computational methods. *Transportation Research Part B: Methodological*, 114, 68-85.
- [129]. Yang, A., Weng, J., Cheng, N., Ni, J., Lin, X., & Shen, X. (2019). DeQoS attack: Degrading quality of service in VANETs and its mitigation. *IEEE Transactions on Vehicular Technology*, 68(5), 4834-4845.
- [130]. Yu, J., Song, Y., Tang, D., & Dai, J. (2021). A Digital Twin approach based on nonparametric Bayesian network for complex system health monitoring. *Journal of Manufacturing Systems*, 58, 293-304.
- [131]. Zemtsov, A. (2019). Performance evaluation of first hop redundancy protocols for a computer networks of an industrial enterprise. 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon),
- [132]. Zhang, D., Zhang, Y., Yu, M., & Chen, Y. (2017). Reliability evaluation and component importance measure for manufacturing systems based on failure losses. *Journal of Intelligent Manufacturing*, 28(8), 1859-1869.
- [133]. Zhang, H., Liu, Q., Chen, X., Zhang, D., & Leng, J. (2017). A digital twin-based approach for designing and multi-objective optimization of hollow glass production line. *IEEE Access*, 5, 26901-26911.
- [134]. Zhang, M., Tao, F., & Nee, A. (2021). Digital twin enhanced dynamic job-shop scheduling. *Journal of Manufacturing Systems*, 58, 146-156.
- [135]. Zhang, Y., Tourrilhes, J., Zhang, Z.-L., & Sharma, P. (2021). Improving SD-WAN resilience: From vertical handoff to WAN-aware MPTCP. *IEEE transactions on network and service management*, 18(1), 347-361.
- [136]. Zhang, Y., & Zhang, Z.-L. (2020). Enhancing performance, security, and management in network function virtualization. 2020 IEEE conference on network function virtualization and software defined networks (NFV-SDN),
- [137]. Zheng, Y., Yang, S., & Cheng, H. (2019). An application framework of digital twin and its case study. *Journal of ambient intelligence and humanized computing*, 10(3), 1141-1153.
- [138]. Zhu, Z., Li, Q., Xia, S., & Xu, M. (2018). Caffé: Congestion-aware fast failure recovery in software defined networks. 2018 27th International Conference on Computer Communication and Networks (ICCCN),