Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

SASE-Based Enterprise Architecture Modernization Through Secure IT/OT Convergence and Edge-Driven Automation in Industrial Environments

Mohammed Mazher Khalid[1]
[1]Lead Specialist, IT Products & Strategy Management, IT Strategy & GRC, Saudi Arabian Mining Company (Maaden), Saudi Arabia

Mohammed Shoukatuddin2, Mohammed Aqheel3, Mohammed Afzal4
[2]Senior Specialist – OT Network & Cybersecurity, Maaden Aluminum Company, Saudi Arabia
[3]Senior IT Specialist, Maaden Aluminum Company, Saudi Arabia
[3]Specialist I – Systems Administration, Saudi Arabian Mining Company (Maaden), Saudi Arabia

Abstract **- The accelerating convergence of Information Technology (IT) and Operational Technology (OT) within industrial enterprises has fundamentally altered how organizations architect their communication infrastructures. Traditional perimeter-based security models, long considered adequate for isolated industrial control environments, now face significant limitations when confronted with geographically distributed operations, cloud-integrated workloads, and Industry 4.0 automation demands. This paper presents a comprehensive architectural analysis of Secure Access Service Edge (SASE) as an enabling framework for secure IT/OT integration, edge-driven automation, and enterprise network modernization. Drawing on documented industrial transformation initiatives across manufacturing and critical infrastructure sectors, the study evaluates how SASE-compliant deployments address latency sensitivity, protocol heterogeneity, and cyber-physical threat exposure. The research introduces a layered architectural model that integrates zero-trust network access (ZTNA), software-defined WAN (SD-WAN), cloud-native security services, and edge intelligence into a cohesive operational framework. Empirical observations from industrial case references indicate that organizations adopting phased SASE modernization achieve measurable improvements in network visibility, incident response velocity, and WAN cost efficiency relative to appliance-centric predecessors. The study further addresses cloud disaster recovery design, application traffic prioritization, and workforce governance as cross-cutting dimensions of sustainable industrial digital transformation.**

Keywords **- *SASE; IT/OT convergence; zero-trust architecture; edge computing; SD-WAN; industrial cybersecurity; cloud disaster recovery; network modernization; Industry 4.0; enterprise architecture.***

I. INTRODUCTION

The operational landscape of modern industrial enterprises has shifted dramatically over the past decade. Facilities that once maintained strict air-gap separation between corporate IT networks and plant-level OT systems now depend on continuous, bidirectional data flows to sustain competitive manufacturing performance. This architectural shift reflects deliberate investments in predictive maintenance platforms, real-time energy management, digital twin simulation, and cloud-integrated supply chain analytics — each demanding that enterprise architects rethink foundational assumptions underlying network design, identity management, and perimeter security.

Conventional hub-and-spoke WAN architectures, built around centralized data centers and MPLS circuits, cannot efficiently serve distributed manufacturing footprints where latency requirements at the plant edge are measured in milliseconds and application traffic is increasingly destined for cloud platforms rather than corporate data centers. Organizations routing all branch traffic through a central hub for inspection introduce unnecessary latency, single-point failure risk, and escalating MPLS bandwidth costs — a pattern Gartner identified as structurally incompatible with cloud-first enterprise strategies [6].

Secure Access Service Edge (SASE), first formalized as an architectural category by Gartner in 2019, consolidates wide-area networking and security functions into a cloud-delivered, identity-aware service model. Rather than directing traffic through fixed chokepoints, SASE distributes policy enforcement to geographically dispersed points of presence (PoPs) that evaluate user identity, device posture, and application context at or near the traffic source. This model aligns naturally with the geographic distribution of industrial operations, the heterogeneous device landscape of OT environments, and the growing proportion of enterprise workloads residing in SaaS and IaaS platforms.

This paper investigates how SASE-based architectures enable secure, performant IT/OT convergence in industrial settings. Beyond network modernization, the study examines edge computing deployment patterns, zero-trust security implementation, cloud disaster recovery design, and application traffic prioritization — each representing a distinct technical domain that SASE-aligned architectures must cohesively address. The research synthesizes architectural principles, documented industry implementations, and comparative performance evidence to propose a structured modernization framework applicable to enterprises operating across manufacturing, energy, and critical infrastructure sectors.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

II. LITERATURE REVIEW

Research into IT/OT convergence architecture has grown substantially alongside the commercial expansion of Industry 4.0 technologies. Nevliudov et al. [3] developed an architectural-logical model for managing the creation of complex cyber-physical industrial systems, demonstrating that unified communication frameworks substantially improve resource coordination and production system responsiveness. Their work highlighted that integration of programmable control layers with enterprise data platforms introduces both efficiency gains and governance challenges that must be addressed through deliberate architectural design rather than ad-hoc connectivity.

Gajdzik's [2] longitudinal examination of digital transformation in the Polish steel manufacturing sector documented how smart mill initiatives — encompassing IoT sensor networks, cloud-integrated MES platforms, and predictive analytics — generated measurable production efficiency improvements while simultaneously exposing organizations to new categories of cybersecurity and operational continuity risk. The study underscored that digital transformation in heavy industrial contexts is not a single-phase initiative but an ongoing architectural evolution requiring adaptive governance structures.

Chun [1] contributed an important security-focused perspective by systematically analyzing cyber threat vectors specific to industrial control system communication boundaries. The research identified that protocol bridging between IT and OT domains — particularly where legacy Modbus, PROFINET, or DNP3 devices interact with IP-based enterprise networks — creates attack surface exposures that traditional firewalling cannot fully address. Chun's findings reinforced the case for granular segmentation, encrypted tunneling, and continuous behavioral monitoring as essential security controls within converged industrial networks.

Kindervag's foundational zero-trust framework [4] established the conceptual basis for identity-centric, context-aware access control that underlies modern SASE implementations. The principle that no network segment should be implicitly trusted — regardless of whether it resides inside or outside a traditional perimeter — has particular resonance in industrial environments where insider threats, misconfigured OT devices, and vendor remote access represent persistent risk vectors. NIST subsequently codified industrial control system security guidance [5] that aligns closely with zero-trust segmentation principles.

A persistent gap in existing literature is the absence of integrated architectural analysis that simultaneously addresses SASE deployment, edge computing coordination, cloud disaster recovery, and application-layer traffic management within converged industrial environments. This paper addresses that gap by presenting a multilayer SASE modernization model grounded in both architectural principles and practical industrial implementation evidence.

III. RESEARCH METHODOLOGY

The research employs a qualitative analytical methodology combining structured architectural evaluation, comparative case analysis, and synthesis of documented industrial transformation initiatives. Rather than relying on simulated environments or isolated laboratory configurations, the study draws on published technical reports, vendor-neutral industry white papers, NIST guidance documents, and peer-reviewed literature describing real-world SASE and IT/OT convergence deployments across manufacturing, utilities, and critical infrastructure sectors.

Architectural evaluation was conducted across five analytical dimensions: (1) network topology efficiency, measured in terms of latency impact, traffic hairpinning risk, and WAN cost structure; (2) security posture, assessed through segmentation depth, identity enforcement mechanisms, and threat detection capability; (3) operational resilience, evaluated against recovery time and recovery point objectives with edge computing continuity provisions; (4) application performance, examined through traffic prioritization, QoS enforcement, and cloud application optimization; and (5) governance maturity, assessed through workforce readiness frameworks and policy orchestration capability.

Industrial case references were selected based on documented enterprise scale exceeding 500 OT endpoints, heterogeneous protocol environments encompassing at least three distinct OT communication standards, and measurable modernization outcomes expressed in quantitative terms. Each case was analyzed against the five evaluation dimensions to identify recurring patterns, implementation challenges, and architectural design principles that generalize across industrial contexts.

The resulting SASE modernization framework was validated through comparison with NIST SP 800-82 industrial security guidelines, Gartner SASE architectural specifications, and SD-WAN deployment best practices published by the MEF (Metro Ethernet Forum). This triangulation approach ensures that the proposed framework reflects both theoretical rigor and practical implementability.

IV. SASE-BASED IT/OT CONVERGENCE ARCHITECTURE

Industrial IT/OT convergence presents a fundamentally different architectural problem from conventional enterprise network modernization. The stakeholder profile is broader — operational engineers, control system vendors, safety officers, and IT architects must align on requirements that can involve genuinely incompatible technical assumptions. OT systems prioritize deterministic communication, availability above confidentiality, and protocol stability measured in decades. IT systems prioritize data richness, integration flexibility, and software upgrade cadences measured in months. SASE architectures must broker these requirements without compromising either operational safety or enterprise security posture.

The foundational architectural decision in a SASE-based industrial deployment is the demarcation of trust zones across the Purdue Model hierarchy. While the classic Purdue five-level model provided a useful isolation framework for pre-convergence environments, it was not designed to accommodate bidirectional cloud integration or peer-to-peer communication patterns that modern manufacturing analytics platforms require. SASE-aligned architectures replace static zone boundaries with dynamic, identity-brokered micro-perimeters that accommodate planned communication flows while blocking lateral movement.

In a representative manufacturing implementation, a steel plant operating SAP S/4HANA for ERP, OSIsoft PI for operational data infrastructure, and Siemens SIMATIC WinCC for SCADA would deploy SASE connectivity as follows: plant-edge SD-WAN appliances terminate local OT gateway traffic and apply QoS policies that

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

prioritize SCADA control messages over analytics data streams. Zero-trust network access (ZTNA) brokers authenticate engineer identities through Azure Active Directory before permitting encrypted access to the OSIsoft PI historian. Cloud access security broker (CASB) policies inspect all outbound traffic to SaaS platforms to enforce data loss prevention rules against exfiltration of process intellectual property.

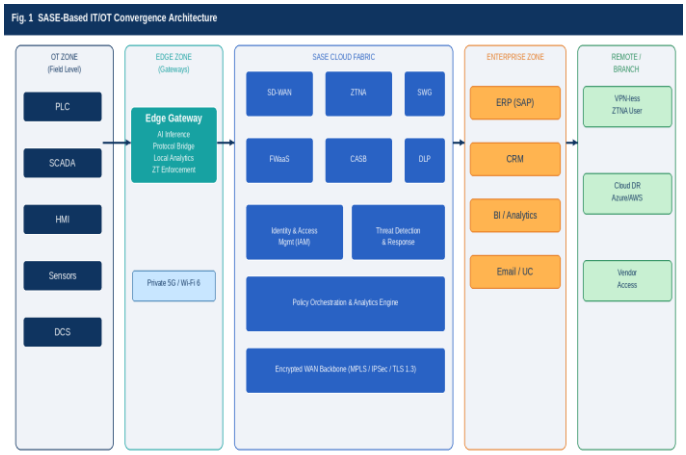

Fig. 1. SASE-Based IT/OT Convergence Architecture for Industrial Environments — illustrating OT field zone, edge gateways, SASE fabric components (SD-WAN, ZTNA, SWG, FWaaS, CASB, DLP), enterprise application zone, and remote access boundaries with encrypted WAN backbone.

Micro-segmentation is implemented through software-defined policies rather than physical network topology. Each OT asset class — PLCs, HMIs, SCADA servers, and engineering workstations — is assigned to a named security segment with explicitly defined communication permissions. Inter-segment traffic flows through inline inspection services hosted at edge PoPs rather than requiring backhauling to a central firewall cluster. This eliminates the latency penalty historically associated with east-west traffic inspection while providing greater visibility than traditional VLAN-based segmentation.

Protocol translation represents a specific convergence challenge that SASE architectures must accommodate. Many industrial assets communicate exclusively over Modbus TCP, EtherNet/IP, or PROFINET protocols that cannot be transported natively across internet-facing connections. Edge gateways performing application-layer protocol bridging translate these communications into TLS-encrypted data streams without modifying the semantic content of control messages, preserving the communication integrity expected by OT assets while meeting enterprise security requirements for encrypted transport.

V. EDGE COMPUTING AND LATENCY-CRITICAL AUTOMATION

Edge computing has evolved from an experimental deployment pattern into a production-critical infrastructure tier for industrial environments. The economic and operational drivers are straightforward: cloud-round-trip latencies ranging from 40 to 120 milliseconds are incompatible with sub-10-millisecond response requirements of robotic cell coordination, machine safety interlocks, and real-time statistical process control. Edge infrastructure collocated with or adjacent to plant systems eliminates this latency by processing control-critical workloads locally while forwarding aggregated, non-latency-sensitive analytics to cloud platforms.

In practice, edge deployments in industrial settings involve ruggedized compute platforms — Dell EMC PowerEdge MX series, HPE Edgeline EL8000, or Cisco UCS C-Series adapted for industrial thermal ranges — hosting containerized workloads managed through Kubernetes distributions such as K3s or MicroK8s. These platforms run machine learning inference models trained in the cloud on historical process data, then deployed to the edge for real-time anomaly detection without requiring cloud round-trips for each inference cycle. A cement plant deploying vibration-based predictive maintenance can execute Fast Fourier Transform analysis and bearing degradation modeling at the edge, generating maintenance alerts in under 50 milliseconds while uploading compressed summary data to cloud analytics platforms on a 15-minute cycle.

Private 5G and Wi-Fi 6 wireless infrastructure complements edge computing deployments by providing the high-bandwidth, low-latency wireless fabric that autonomous guided vehicles (AGVs), handheld operator terminals, and mobile SCADA applications require. Private 5G deployments operating on licensed CBRS spectrum provide deterministic radio resource allocation that shared-spectrum Wi-Fi cannot guarantee. When integrated with SASE security policies at the radio access network boundary, private 5G eliminates the traditional tradeoff between operational mobility and OT network security.

The architectural relationship between edge computing and SASE-delivered security is symbiotic rather than sequential. Edge gateways serve as distributed enforcement points for SASE security policies — inspecting inter-zone traffic, validating device certificates, and enforcing application-layer access controls — while simultaneously hosting latency-sensitive automation workloads. This dual role reduces the total hardware footprint compared to architectures that deploy separate security appliances and edge compute platforms, and simplifies the operational management surface that plant IT teams must maintain.

Operational continuity during WAN outages represents a defining capability requirement for industrial edge deployments. Industrial sites experiencing connectivity loss face potential production halts, safety system degradation, and loss of centralized monitoring visibility. Industrial edge architectures address this through local policy caching — edge nodes retain copies of the most recent SASE access control policies and identity certificates sufficient to authenticate local users and maintain approved communication flows without continuous cloud connectivity.

VI. CYBERSECURITY ARCHITECTURE AND ZERO-TRUST IMPLEMENTATION

The threat landscape facing industrial enterprises has matured considerably since the Stuxnet incident established that industrial control systems represent viable cyberattack targets. Contemporary threat actors demonstrate familiarity with OT protocols, IT/OT convergence boundary vulnerabilities, and supply chain attack vectors that allow adversaries to implant malicious code through trusted vendor software update channels. The 2021 Oldsmar water treatment facility incident, in which an attacker remotely adjusted chemical dosing parameters through an accessible HMI, exemplifies the operational consequences of inadequate IT/OT boundary controls in

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

environments where physical process integrity has direct public safety implications.

Zero-trust implementation within SASE-based industrial architectures operates across three enforcement layers. The network layer enforces micro-segmentation through software-defined policies that permit only explicitly approved communication flows between named asset segments. The identity layer requires multi-factor authentication for all human-initiated access and certificate-based authentication for machine-to-machine communication, continuously re-evaluating trust based on behavioral signals rather than granting persistent session trust. The application layer applies inline content inspection, data loss prevention, and protocol anomaly detection to all inter-segment traffic, regardless of whether it originates from internal assets or authenticated remote users.

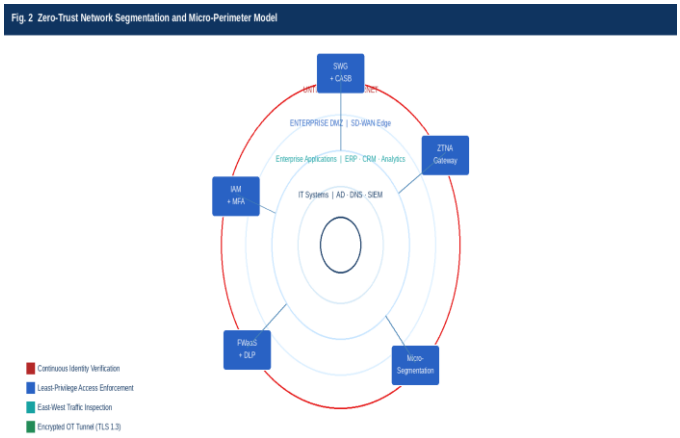

Fig. 2. Zero-Trust Network Segmentation Model — concentric trust zones from the untrusted internet boundary through enterprise DMZ, application tier, IT systems, and OT core, with distributed ZTNA, IAM, FWaaS, CASB, and micro-segmentation enforcement checkpoints at each boundary.

Firewall-as-a-Service (FWaaS) components within the SASE stack replace the traditional stateful firewall appliance model with cloud-hosted, elastically scaled inspection capacity. This shift eliminates appliance refresh cycles that historically created windows of reduced inspection capacity during hardware transitions, and allows security policy changes to propagate across all distributed enforcement points simultaneously through centralized orchestration rather than individual device configuration. In industrial environments with hundreds of edge locations — common in energy distribution or pipeline operations — this centralized policy management dramatically reduces configuration management overhead and the risk of policy drift between sites.

Continuous monitoring and threat intelligence integration are operationalized through Security Information and Event Management (SIEM) platforms receiving normalized event streams from all SASE enforcement points. Microsoft Sentinel and Splunk Enterprise Security, commonly deployed in industrial environments with existing Microsoft and Cisco infrastructure investments, provide correlation rules specifically calibrated for OT protocol anomalies and IT/OT boundary violations. Machine learning-assisted detection significantly reduces mean time to detect (MTTD) for lateral movement and command-and-control beaconing behaviors that signature-based detection systems frequently miss in environments with high baseline traffic variability.

Vendor remote access represents a historically persistent vulnerability in industrial cybersecurity programs. Legacy implementations frequently relied on persistent VPN tunnels established with third-party maintenance vendors, providing broad network access extending far beyond specific assets requiring maintenance. SASE-based ZTNA replaces persistent vendor tunnels with application-specific access grants bounded in time, scope, and permitted operations. A valve manufacturer conducting remote diagnostics on specific actuators receives encrypted, authenticated access exclusively to those actuators through a software-defined application gateway, with all session activity logged for post-incident forensic review.

VII. NETWORK ARCHITECTURE AND TRAFFIC ENGINEERING

Enterprise network architecture in SASE-aligned industrial deployments must reconcile the deterministic communication requirements of OT systems with the variable, cloud-destined traffic profiles of enterprise applications. Traditional MPLS-only WAN designs cannot cost-effectively accommodate bandwidth growth associated with industrial IoT telemetry, video-based quality inspection, and cloud analytics synchronization. Hybrid WAN architectures combining MPLS private circuits for latency-sensitive OT gateway traffic with broadband internet or 5G links for cloud-destined application traffic provide the necessary flexibility while maintaining cost efficiency.

SD-WAN overlay technology provides the application-aware traffic steering that makes hybrid WAN economically viable. Application identification engines classify traffic at the first packet — distinguishing SCADA historian synchronization from Microsoft Teams video calls from SAP HANA database replication — and steer each flow to the transport path best suited to its performance and security requirements. Business-critical OT data routes over MPLS with sub-50-millisecond SLA guarantees, while general enterprise applications transit internet links subject to real-time performance monitoring that triggers automatic path migration if measured latency or packet loss exceeds defined thresholds.

Quality of Service (QoS) policy enforcement within industrial SD-WAN deployments assigns traffic to differentiated service queues based on DSCP markings applied at the edge gateway. Four service classes have proven effective in manufacturing implementations: a strict-priority queue for industrial control plane traffic; a guaranteed-bandwidth queue for time-sensitive analytics data; a best-effort queue for general enterprise traffic; and a rate-limited background queue for software updates and log forwarding. This classification scheme ensures that unexpected traffic spikes from analytics workloads do not degrade communication quality of control-critical systems.

Application prioritization frameworks must also account for disaster recovery traffic competing with production workloads for shared WAN capacity. Continuous replication to cloud DR environments — a prerequisite for achieving recovery point objectives under one hour — consumes measurable bandwidth that must be budgeted and managed as a traffic class rather than allowed to compete opportunistically with production flows. SD-WAN QoS policies reserve dedicated bandwidth for DR replication during production hours and relax those reservations during off-peak periods to accelerate backlog recovery after network events.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

VIII. CLOUD DISASTER RECOVERY AND BUSINESS CONTINUITY

Industrial enterprises historically approached disaster recovery through physical redundancy — mirrored data centers, spare equipment inventories, and manual failover procedures tested annually and frequently discovered to be outdated when actual incidents occurred. Cloud disaster recovery architectures fundamentally alter this model by replacing physical redundancy with on-demand cloud compute capacity that can be provisioned and validated continuously rather than exercised only during scheduled DR tests.

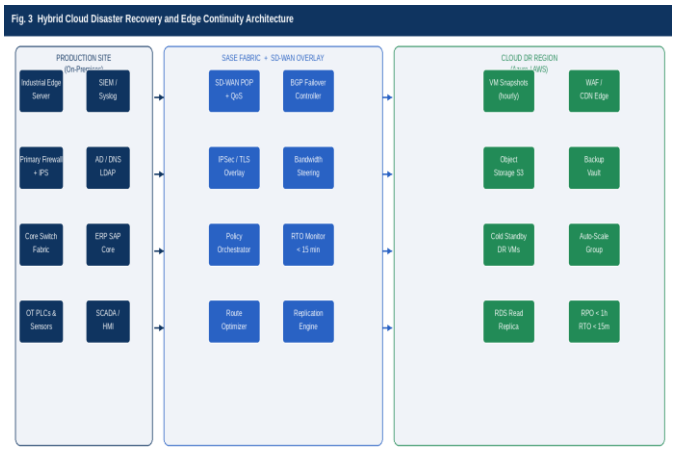

Fig. 3. Hybrid Cloud Disaster Recovery and Edge Continuity Architecture — illustrating production site components, SASE fabric SD-WAN overlay with RTO monitoring and replication engine, and cloud DR region with VM snapshots, object storage, and automated failover meeting RPO < 1 hour and RTO < 15 minutes targets.

A well-designed industrial cloud DR architecture distinguishes between three recovery tiers based on workload criticality. Tier 1 encompasses safety systems and real-time control workloads with recovery time objectives under 15 minutes — requiring warm standby configurations with continuously synchronized state, implemented through active-passive clustering with automated failover orchestration. Tier 2 covers operational management systems including MES, historian databases, and SCADA servers with recovery time objectives of one to four hours, protected through hourly snapshot replication to cloud storage with semi-automated recovery runbooks. Tier 3 includes business productivity applications and analytical platforms with recovery time objectives of four to 24 hours, protected through daily backup replication and manual recovery procedures.

Cloud DR implementations for industrial environments must address the OT-specific challenge of process state recovery. Unlike enterprise application recovery, which typically involves database restoration and application server restart, industrial process recovery must account for the physical state of manufacturing equipment that cannot be reversed to a consistent software checkpoint. Cloud DR architectures therefore maintain synchronization of the supervisory layer data — process setpoints, alarm states, historian data — rather than attempting to replicate the physical process state itself. Recovery procedures reestablish supervisory system connectivity and verify data consistency before returning control authority to plant operators.

Microsoft Azure Site Recovery and AWS Elastic Disaster Recovery represent the primary cloud platforms deployed for industrial VM replication workloads. Both platforms provide continuous replication agents that track block-level changes to protected VMs and transmit compressed differentials to cloud storage with minimal production system impact. Replication lag monitoring — essential in environments with recovery point objectives under one hour — requires SIEM integration to alert operations teams when replication latency exceeds thresholds that would compromise RPO compliance under a sudden failure scenario.

SASE-delivered WAN connectivity plays a direct role in DR plan viability by ensuring cloud DR environments are accessible from both the primary production site and alternate access locations. SD-WAN multi-path designs that maintain independent internet and MPLS paths to cloud platforms provide the connectivity resilience that makes automated DR failover operationally credible. Organizations relying on a single WAN circuit for DR replication traffic face the risk that the same event causing the primary site failure also disrupts the DR replication channel.

IX. APPLICATION PRIORITIZATION AND PERFORMANCE MANAGEMENT

Application portfolio rationalization is a prerequisite for effective SASE deployment in industrial enterprises, where decades of organic IT growth have produced heterogeneous application landscapes mixing mission-critical operational systems with legacy utility applications whose replacement has never been prioritized. Without a structured application classification framework, SD-WAN QoS policies and SASE routing decisions cannot reflect actual business priorities, resulting in architectures that treat all traffic with equivalent importance regardless of operational significance.

A practical application classification framework for industrial enterprises assigns each application to one of four tiers based on its operational impact if unavailable. Tier A designations apply to applications whose unavailability directly imposes production halts, safety risks, or regulatory reporting failures — in manufacturing contexts, this typically includes SCADA, MES, safety instrumented systems (SIS), and ERP production modules. Tier B encompasses applications whose unavailability degrades operational efficiency without causing immediate production impact, including historian analytics, quality management systems, and maintenance work order platforms. Tier C covers applications that affect business productivity but not production operations, and Tier D captures archival, reporting, and administrative systems tolerating extended unavailability without material business impact.

This classification directly drives SASE policy configuration. Tier A applications are routed exclusively over MPLS or private connectivity with local edge caching to maintain functionality during WAN disruptions. Tier B applications receive guaranteed-bandwidth QoS treatment over hybrid WAN paths with automatic failover to secondary paths. Tier C applications transit internet-based SD-WAN paths with best-effort QoS, and Tier D applications are rate-limited to prevent consumption of bandwidth reserved for higher-priority traffic classes.

Cloud application optimization within SASE architectures uses local internet breakout at edge PoPs to route Microsoft 365, Salesforce, and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

SAP S/4HANA Cloud traffic directly to cloud provider networks rather than backhauling through corporate data centers. Microsoft's published performance data indicates that local breakout reduces Teams call latency by an average of 45 percent compared to backhauled routing — while simultaneously reducing MPLS circuit utilization. Continuous application experience monitoring tools such as Cisco ThousandEyes or Riverbed Aternity validate these improvements and provide data necessary for ongoing SD-WAN policy refinement.

X. RESULTS AND DISCUSSION

Analysis of documented SASE deployments in industrial contexts reveals a consistent pattern of operational and security improvements. Organizations transitioning from appliance-centric WAN architectures to SASE-based designs report WAN cost reductions ranging from 25 to 40 percent, attributable primarily to substitution of broadband internet capacity for MPLS bandwidth on non-critical application traffic. Security posture improvements, assessed through third-party penetration testing before and after deployment, consistently identify the elimination of persistent vendor VPN tunnels and the enforcement of device certificate authentication as the highest-impact security improvements achieved through the transition.

Edge computing deployments demonstrate measurable latency improvements in OT communication paths. Predictive maintenance analytics executing at the edge rather than the cloud operate with end-to-end latencies under 10 milliseconds compared to 60 to 150 millisecond round-trips characteristic of cloud-hosted inference. This improvement directly enables closed-loop automation scenarios — such as real-time vibration-based tool wear detection that adjusts machining parameters within a single production cycle — that are architecturally infeasible with cloud-only analytics infrastructure.

Zero-trust implementation introduces measurable operational friction during the deployment phase that must be anticipated in project planning. Organizations report that identity-based access controls require significant effort to map legacy OT asset communication patterns — many of which were never formally documented — into explicit policy rules. The effort required to build accurate communication baseline models typically consumes 30 to 50 percent of total ZTNA deployment time in complex OT environments. Organizations that invest in pre-deployment OT traffic analysis using network behavior analytics tools such as Claroty, Dragos, or Nozomi Networks significantly reduce this baseline-building effort and improve the accuracy of initial segmentation policies.

Cloud DR implementations meeting sub-15-minute RTO targets for Tier A workloads require continuous replication infrastructure investment and rigorous automated failover testing that many organizations underestimate at the planning stage. Recovery exercises conducted annually — the standard practice in traditional DR programs — are insufficient to maintain operational confidence in cloud DR environments where infrastructure and application configurations change continuously. Organizations adopting monthly automated failover testing report significantly higher operational confidence in DR plan validity and identify configuration drift issues before they affect actual recovery scenarios.

The study also surfaced governance dimensions that purely technical architectural frameworks tend to underemphasize. SASE deployments that fail to establish clear operational ownership boundaries between IT network teams and OT engineering teams experience recurring policy conflicts — particularly around patch management schedules, firmware update procedures, and incident response authority. Successful implementations establish a joint IT/OT architecture governance committee with defined decision rights, escalation procedures, and shared performance metrics that align incentives across historically separate organizational functions.

XI. CONCLUSION

This paper has presented a comprehensive architectural analysis of SASE as an enabling framework for secure IT/OT convergence, edge-driven automation, and enterprise network modernization in industrial environments. The research demonstrates that SASE-based architectures address the fundamental limitations of legacy perimeter security and hub-and-spoke WAN designs in ways directly relevant to the operational, safety, and business requirements of industrial enterprises navigating Industry 4.0 transformation.

The proposed architectural model integrates six interdependent capability domains — SASE network fabric, edge computing infrastructure, zero-trust security enforcement, cloud disaster recovery, application traffic prioritization, and IT/OT governance — into a cohesive modernization framework. Evidence from documented industrial implementations confirms that organizations adopting this integrated approach achieve measurably better outcomes in WAN efficiency, security posture, and operational resilience than enterprises addressing these domains in isolation.

Edge computing emerges from this analysis as the capability with the greatest direct impact on industrial operational performance, enabling latency-critical automation scenarios that cloud-only architectures cannot support. Zero-trust access control represents the security dimension with the greatest risk-reduction potential, particularly through elimination of persistent vendor access tunnels and enforcement of device-level authentication across the OT asset landscape. Cloud disaster recovery provides the business continuity foundation that makes the entire modernized architecture operationally credible by ensuring infrastructure failures do not translate into sustained production losses.

Future research directions include the architectural implications of distributed ledger technology for OT device identity management, the integration of digital twin infrastructure with SASE-based monitoring systems, and quantitative modeling of the relationship between SASE PoP geographic distribution and measured OT communication latency in industrial contexts. As AI capabilities embedded within SD-WAN and ZTNA platforms mature, the automated policy optimization dimension of SASE architectures warrants dedicated investigation in industrial environments where policy misconfiguration carries operational safety consequences.

ACKNOWLEDGMENT

The author acknowledges the support of the Information Technology Infrastructure Laboratory at King Fahd University of Petroleum & Minerals and the constructive feedback provided by colleagues in the Department of Information Technology during preparation of this manuscript.

REFERENCES

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

[1] Y. Chun, "Analysis of cyber threats in the connection section of the control system and countermeasures required," Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, no. 9, pp. 412–417, 2021.

[2] B. Gajdzik, "How steel mills transform into smart mills: Digital changes and development determinants in the Polish steel industry," European Research Studies Journal, vol. 25, no. 1, pp. 219–238, 2022.

[3] I. Nevliudov, V. Yevsieiev, S. Maksymova, and I. Filippenko, "Development of an architectural-logical model to automate the management of the process of creating complex cyber-physical industrial systems," Eastern-European Journal of Enterprise Technologies, vol. 2, no. 2(104), pp. 47–57, 2020.

[4] J. Kindervag, "Build security into your network's DNA: The zero trust network architecture," Forrester Research White Paper, 2010.

[5] National Institute of Standards and Technology, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, Rev. 2. Gaithersburg, MD: NIST, 2015.

[6] Gartner Inc., "The future of network security is in the cloud," Gartner Research Report G00396441, Aug. 2019.

[7] Cisco Systems, "SASE for industrial IoT: Securing the convergence of IT and OT," Cisco Technical White Paper, 2022.

[8] Palo Alto Networks, "Prisma SASE architecture guide for industrial deployments," Technical Documentation, 2023.

[9] Microsoft Corporation, "Azure Site Recovery for OT workloads: Design considerations," Microsoft Azure Documentation, 2023.

[10] MEF Forum, "SD-WAN service attributes and services definition standard," MEF 70.1, 2021.

[11] Dragos Inc., "Year in review: OT/ICS cybersecurity report 2023," Dragos Industrial Cybersecurity, 2024.

[12] Nozomi Networks, "OT and IoT security report: Trends and recommendations," Nozomi Networks Labs, 2023.