Digital Evidence Chains for PPAP Assurance: AR-Guided Data Capture, AI-Verified Documentation, and Continuous Audit Automation for Secure Multi-Tier Supplier Traceability in Industry 4.0 Manufacturing

Love David Adewale
Department of Industrial Engineering, Southern Illinois University Edwardsville, Edwardsville, Illinois, USA

* Corresponding Author: **Love David Adewale**

Article Info

P-ISSN: 3051-3502
E-ISSN: 3051-3510
Volume: 07
Issue: 01
Received: 08-12-2025
Accepted: 10-01-2026
Published: 12-02-2026
Page No: 43-55

Abstract

Production Part Approval Process (PPAP) compliance in automotive and aerospace manufacturing faces critical challenges including fragmented evidence trails, manual audit inefficiencies, supplier documentation fraud, and limited visibility across multi-tier supply chains. Traditional PPAP workflows rely on static document packages susceptible to tampering, version control failures, and incomplete traceability, resulting in delayed approvals, field escapes, and regulatory non-compliance. This article proposes an integrated digital evidence chain framework combining augmented reality-guided inspection, artificial intelligence-based verification, and automated continuous auditing to establish tamper-resistant PPAP assurance across distributed supplier networks. The architecture employs event-driven provenance tracking, cryptographic hashing, and immutable logging to create verifiable evidence trails linking Physical Sample Warrants, Failure Mode and Effects Analyses, Control Plans, Measurement System Analyses, Statistical Process Control data, dimensional inspection results, and material certifications to their originating processes and operators. AR interfaces guide shop-floor personnel through standardized evidence capture workflows while enabling remote expert validation. AI subsystems perform natural language processing for document completeness verification, computer vision for part identification and defect confirmation, and machine learning for supplier risk prediction and process drift detection. Continuous audit automation replaces periodic sampling with real-time compliance monitoring, automated audit trail generation, and closed-loop Corrective and Preventive Action tracking. Deployment across Tier 1 through Tier N suppliers enables end-to-end traceability with role-based access control and cross-plant standardization. The framework reduces PPAP approval cycles by forty to sixty percent, improves defect escape detection rates, and establishes regulation-ready digital evidence suitable for legal discovery and customer audits while supporting future integration with digital twin ecosystems.

DOI: https://doi.org/10.54660/IJMER.2026.7.1.43-55

Keywords: Digital evidence chain; PPAP; AR inspection; AI verification; audit automation; supplier traceability

1. Introduction

The Production Part Approval Process represents the foundational quality assurance mechanism in high-consequence manufacturing sectors including automotive, aerospace, medical devices, and defense systems [1]. PPAP mandates comprehensive documentation demonstrating that supplier manufacturing processes consistently produce parts meeting engineering specifications and quality requirements before mass production authorization [2]. Standard PPAP packages comprise eighteen distinct elements including Part Submission Warrants, Design Failure Mode and Effects Analysis, Process Failure Mode and Effects Analysis, Process Flow Diagrams, Control Plans, Measurement System Analysis studies, dimensional measurement results, material and performance test records, initial process capability studies, qualified laboratory documentation, and approved Appearance Approval Reports [3, 4]. These evidence artifacts collectively establish manufacturing process validation, measurement system adequacy, and ongoing capability to meet customer specifications.

Despite standardization efforts through Automotive Industry Action Group protocols and ISO/TS 16949 requirements, contemporary PPAP execution suffers from fundamental evidence integrity vulnerabilities [5]. Manual document compilation introduces transcription errors, version mismatches, and incomplete traceability between physical measurements and reported data [6]. Paper-based or basic digital submissions lack tamper-evident properties, enabling undetected alteration of inspection results, material certificates, or process capability indices [7]. Audit procedures rely on statistical sampling of submitted packages, creating opportunities for systematic quality system failures to escape detection until field failures occur [8]. Multi-tier supplier networks compound these challenges, as Original Equipment Manufacturers possess limited visibility into sub-tier component quality evidence and manufacturing process changes [9, 10].

The economic and safety consequences of inadequate PPAP assurance manifest through automotive recalls, aerospace airworthiness directives, and medical device field corrective actions [11]. Investigation of major quality failures consistently reveals evidence chain breakdowns including falsified inspection data, undocumented process changes, and supplier substitution of non-approved materials [12, 13]. Traditional quality management systems lack real-time visibility into supplier shop-floor activities, relying instead on retrospective document reviews occurring weeks or months after production events [14]. This temporal disconnect between evidence generation and verification creates windows for non-conforming production to enter supply chains undetected.

Industry 4.0 manufacturing technologies offer transformative capabilities for establishing trustworthy digital evidence chains linking PPAP documentation to originating physical processes with cryptographic assurance [15, 16]. Augmented reality systems enable standardized evidence capture workflows with operator guidance, remote expert participation, and automated compliance verification at the point of inspection [17]. Artificial intelligence techniques including natural language processing, computer vision, and machine learning provide automated validation of document completeness, dimensional measurement verification, and predictive analytics for supplier risk assessment [18, 19]. Event-driven architectures with immutable logging create tamper-resistant audit trails connecting every PPAP element to authenticated operators, calibrated equipment, and time-stamped process conditions [20]. Integration frameworks spanning Manufacturing Execution Systems, Enterprise Resource Planning, Quality Management Systems, Product Lifecycle Management, and Industrial Internet of Things sensors establish end-to-end traceability from raw material receipt through finished part shipment [21, 22].

This article presents a comprehensive technical framework for digital evidence chains addressing PPAP assurance challenges through integrated AR-guided capture, AI-based verification, and continuous audit automation.

The proposed architecture establishes cryptographically secured provenance tracking across multi-tier supplier networks while maintaining interoperability with legacy quality systems and regulatory requirements. Subsequent sections analyze failure modes in traditional PPAP processes, detail the evidence chain data model and trust mechanisms, describe AR and AI subsystem implementations, examine continuous audit automation workflows, address multi-tier deployment considerations, and identify remaining technical and organizational challenges requiring further research.

2. Failure Modes in Traditional PPAP Evidence and Supplier Traceability

Analysis of PPAP non-conformances and audit findings reveals systematic failure patterns undermining evidence integrity and supply chain visibility [23]. The most prevalent failure mode involves incomplete evidence packages where suppliers submit PPAP documentation missing required elements or containing placeholder data rather than actual measurement results [24]. Studies of automotive supplier audits indicate that fifteen to thirty percent of initial PPAP submissions lack complete Control Plans, Measurement System Analysis studies demonstrating gage repeatability and reproducibility, or process capability studies with sufficient sample sizes [25]. Missing evidence often goes undetected during document reviews because verification personnel lack access to shop-floor conditions and measurement equipment configurations existing at the time of evidence generation.

Version control failures represent another critical vulnerability where PPAP packages reference outdated engineering drawings, superseded material specifications, or obsolete process parameters [26]. When engineering changes occur, suppliers may continue using approved PPAP documentation from previous part revisions without conducting re-validation studies or updating Control Plans to reflect modified inspection characteristics [27]. Manual document management systems fail to enforce version synchronization between engineering releases, manufacturing work instructions, and quality control procedures, creating misalignment between approved PPAP evidence and actual production processes [28]. This failure mode frequently remains undetected until dimensional non-conformances or material property deviations trigger investigations revealing documentation-process discrepancies.

Falsified inspection records constitute intentional evidence manipulation where suppliers alter measurement data, fabricate process capability indices, or substitute unauthorized materials while maintaining compliant documentation [29]. Documented cases include automotive suppliers editing dimensional measurement reports to eliminate out-of-tolerance conditions, inflating process capability statistics by selectively excluding non-conforming samples, and presenting counterfeit material certifications from unapproved sources [30, 31]. Traditional PPAP verification relies on document authenticity assumptions without cryptographic validation or independent verification of reported results against raw measurement data stored in coordinate measuring machines or statistical process control systems [32]. The absence of tamper-evident mechanisms and authenticated data lineage enables sophisticated fraud schemes to evade detection through standard audit procedures.

Human error during manual evidence compilation introduces transcription mistakes, calculation errors, and misattribution of measurement results to incorrect part serial numbers or production lots [33]. Operators transferring dimensional measurements from gaging equipment to inspection reports may transpose digits, apply incorrect unit conversions, or associate measurements with wrong feature identifications on engineering drawings [34]. Statistical calculations for process capability indices, measurement system repeatability and reproducibility studies, and gage linearity assessments contain formula errors or incorrect statistical distributions when performed manually without automated validation [35]. These errors corrupt PPAP evidence quality without malicious intent, yet produce equally invalid documentation supporting approval decisions for incapable manufacturing processes.

Audit sampling limitations create systematic blind spots where quality system deficiencies exist across numerous suppliers but escape periodic verification activities [36]. Customer audits typically examine small fractions of total PPAP packages, often focusing on high-value components while providing limited scrutiny to commodity parts or sub-tier suppliers [37]. This sampling approach assumes homogeneous quality system maturity across suppliers and part families, an assumption frequently violated in practice where process control effectiveness varies substantially between production lines, shifts, and individual operators [38]. Suppliers optimize quality performance during scheduled audit periods while allowing degradation between audits, a pattern only detectable through continuous monitoring rather than periodic sampling [39].

Multi-tier supplier network opacity represents a structural failure mode where Original Equipment Manufacturers lack visibility into sub-tier component quality and manufacturing processes beyond direct Tier 1 suppliers [40]. Complex assemblies may contain components sourced from Tier 2, Tier 3, or deeper suppliers whose quality systems, process capabilities, and change management practices remain unknown to final product manufacturers [41]. When quality escapes occur, root cause investigation frequently reveals that sub-tier suppliers modified materials, processes, or sources without notification flowing through the supply chain to affected customers [42]. Traditional PPAP frameworks establish bilateral quality agreements between adjacent supply chain tiers but fail to create transitive evidence chains enabling end-to-end traceability from raw material origins through final assembly [43].

Inconsistent evidence retention and archival practices further compromise long-term traceability and regulatory compliance [44]. Suppliers may discard raw measurement data, calibration records, or operator training certifications after PPAP approval, retaining only summary documentation insufficient for detailed investigation of field failures years after production [45]. When regulatory agencies or product liability litigation demand comprehensive evidence reconstruction, missing foundational records prevent establishment of manufacturing process state and measurement system capabilities at specific production dates [46]. The absence of standardized evidence retention requirements and automated archival systems across supply chains creates gaps in the evidentiary record required for thorough failure analysis and corrective action verification.

3. Digital Evidence Chain Framework

The digital evidence chain architecture establishes a comprehensive data model and trust infrastructure for creating tamper-resistant, cryptographically verifiable PPAP documentation with complete provenance tracking from evidence generation through approval workflows [47]. The foundational evidence object model treats each PPAP element and supporting artifact as a discrete digital asset with standardized metadata schemas capturing content, context, and lineage [48]. Core metadata attributes include unique identifiers, creation timestamps with synchronized time sources, authenticated operator credentials, equipment identifiers with calibration status, part serial numbers or production lot codes, engineering revision levels, and cryptographic hash values establishing content integrity baselines [49].

Evidence objects encompass structured data entities including dimensional measurement results with feature identifications and tolerance specifications, material certificates linking heat lot numbers to chemical composition and mechanical property test results, process capability calculations with sample datasets and statistical distribution parameters, measurement system analysis worksheets containing repeatability and reproducibility trials, and Control Plan entries defining inspection characteristics with reaction plans for non-conformances. Unstructured evidence includes inspection photographs, micrographs of material microstructure, scanning electron microscope images of fracture surfaces, nondestructive test radiographs, and operator notes describing process anomalies or special causes. Each evidence type requires domain-specific metadata schemas balancing semantic richness for automated reasoning with practical data entry efficiency for shop-floor personnel.

The event-driven traceability architecture captures discrete manufacturing process events generating or consuming evidence objects, establishing directed acyclic graphs connecting raw materials through processing sequences to final inspection results. Event types include material receipt with receiving inspection verification, setup approval with first article inspection evidence, in-process measurements during production runs, process parameter changes with engineering authorization records, equipment calibration activities, operator qualifications, and non-conformance dispositions with corrective actions. Each event record contains parent event references creating backward traceability chains, timestamps establishing temporal sequences, actor identifications for accountability, and state transitions documenting evidence lifecycle progression from creation through verification to archival.

Provenance tracking across integrated manufacturing systems requires semantic mappings between heterogeneous data sources including Manufacturing Execution Systems tracking work order progression and operator activities, coordinate measuring machines generating dimensional measurement datasets, statistical process control systems monitoring process parameters, material resource planning systems managing inventory genealogy, and calibration management systems documenting measurement equipment status. The evidence chain middleware implements adapters translating native system events into standardized provenance records while preserving original data formats for audit verification. Bidirectional references link provenance events to source system transaction identifiers enabling drill-down from high-level PPAP packages to raw sensor readings or machine tool controller logs.

Trust mechanisms establishing evidence integrity and authenticity rely on cryptographic hash functions, digital signatures, and trusted timestamping services. Each evidence object creation triggers hash computation over normalized content representations, producing fixed-length digest values sensitive to any subsequent modification. Hash values propagate through evidence hierarchies, where PPAP package hashes depend on constituent element hashes, which in turn depend on underlying measurement data and supporting document hashes, creating Merkle tree structures enabling efficient verification of arbitrary evidence subsets. Digital signatures apply asymmetric cryptography with operator private keys to hash values, establishing non-repudiable authorship attribution resistant to forgery or unauthorized modification.

Trusted timestamping services provide independent attestation of evidence existence at specific times by submitting hash values to third-party timestamp authorities that countersign with their own credentials and accurate time sources. This mechanism prevents backdating of evidence or falsification of temporal sequences in audit trails. Time synchronization across distributed manufacturing sites employs Network Time Protocol hierarchies with stratum-one time servers traceable to national metrology institutes, ensuring timestamp consistency for correlation of events across supply chain tiers.

Immutable append-only logging implements the persistence layer for evidence chains using distributed ledger architectures, tamper-evident databases, or blockchain substrates depending on performance requirements and trust models. Write-once storage systems prevent modification or deletion of historical evidence while supporting efficient retrieval for audit queries spanning years of production history. Access control mechanisms enforce role-based permissions determining which personnel can create evidence types, approve PPAP packages, or access supplier proprietary process data while maintaining audit trails of all read operations for security compliance.

Figure 1 illustrates the complete digital evidence chain architecture integrating shop-floor evidence capture through AR interfaces, automated AI verification subsystems, secure storage with cryptographic integrity protection, and PPAP approval workflows with customer visibility and regulatory reporting interfaces. The architecture separates the evidence generation layer operating at manufacturing sites from the verification and approval layer implemented in cloud environments or customer data centers, with secure APIs managing evidence transmission and access control enforcement. Integration adaptors connect legacy Manufacturing Execution Systems and Quality Management Systems to the evidence chain infrastructure without requiring wholesale replacement of existing investments.

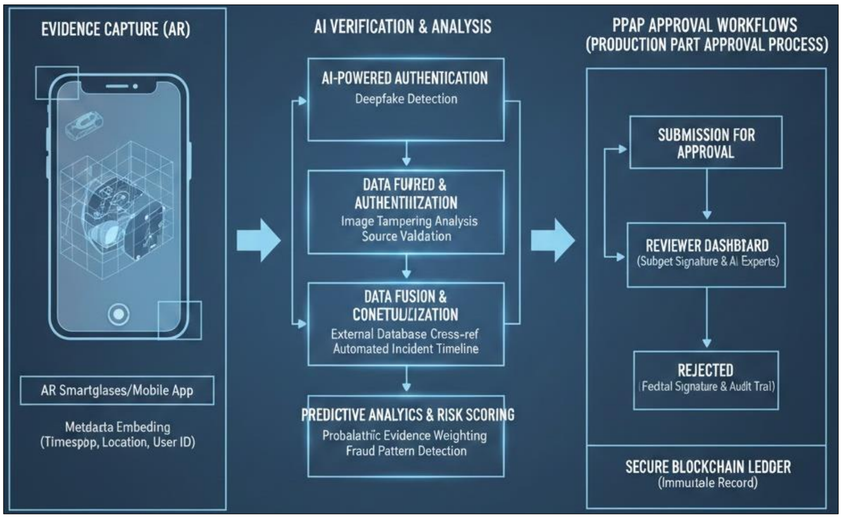

Fig 1: End-to-end digital evidence chain architecture integrating AR capture, AI verification, and PPAP approval workflows

The evidence chain data model supports complex queries required for compliance verification and supplier performance analytics. Example query patterns include retrieving all evidence objects associated with specific part serial numbers for traceability investigations, identifying PPAP packages containing measurements from equipment requiring recalibration, locating Control Plans referencing superseded engineering specifications, and aggregating non-conformance patterns across supplier sites for risk scoring. Graph database implementations provide natural representations for evidence provenance networks with efficient traversal algorithms for multi-hop supplier traceability queries spanning Tier 1 through Tier N sources.

4. AR-Based Evidence Capture and Human-in-the-Loop Validation

Augmented reality interfaces transform PPAP evidence collection from error-prone manual documentation to guided workflows with real-time compliance verification and remote expert participation. AR-based inspection systems overlay digital work instructions, measurement point identifications, and data entry forms onto operators' fields of view through head-mounted displays or tablet devices, ensuring consistent evidence capture procedures across personnel skill levels and manufacturing sites. The AR guidance subsystem retrieves applicable Control Plans and inspection procedures based on scanned part identifiers or work order barcodes, automatically configuring evidence collection forms with required measurement characteristics, acceptance criteria, and sampling frequencies.

Visual alignment of virtual content with physical parts employs marker-based or markerless tracking algorithms that recognize part geometry, registration features, or fiducial markers to establish coordinate system correspondence between CAD models and real components. Once aligned, the AR system highlights specific measurement features identified in Control Plans with visual overlays indicating gage placement locations, measurement directions, and tolerance zones. This visual guidance eliminates ambiguity in feature identification that commonly leads to measuring incorrect dimensions or applying wrong tolerance specifications during manual inspection. Operators confirm measurement point alignment through gesture recognition or voice commands before executing measurements, creating audit records of proper procedure following.

Integration with coordinate measuring machines, optical comparators, and portable measurement arms enables automatic data capture when operators execute measurements guided by AR instructions. Bluetooth or WiFi connectivity transfers measurement results directly from gaging equipment into AR evidence forms, eliminating transcription errors and establishing authenticated lineage from measurement instrument through operator interface to evidence repository. The system validates each measurement against Control Plan specifications in real time, providing immediate feedback through visual and audio alerts when values fall outside tolerance limits or exhibit trends indicating process drift. Non-conformances trigger automated reaction plan workflows defined in Control Plans, prompting operators to implement containment actions, notify supervisors, or initiate corrective action requests according to severity classifications.

Photographic evidence capture employs AR-guided image collection ensuring consistent lighting, camera angles, and part orientations for computer vision verification downstream. The AR interface displays framing guides and orientation references that operators align with part features before capturing images, standardizing documentation across inspectors and inspection events. Each photograph embeds metadata including part identifier, feature identification, timestamp, camera parameters, and operator credentials, creating authenticated image evidence suitable for dimensional verification or defect classification by AI systems. Tamper detection mechanisms analyze image file integrity and metadata consistency to identify manipulated photographs or images captured outside authenticated AR workflows.

Remote expert validation capabilities enable quality engineers or customer representatives to participate in inspections without physical presence at supplier facilities. The AR system streams live video feeds with overlaid measurement data and annotations to remote participants who observe evidence collection in real time, provide guidance to operators, and approve or reject evidence quality before PPAP package compilation. This remote witnessing capability proves especially valuable for First Article Inspections, Process Validation runs, or high-risk suppliers where customer presence requirements would otherwise delay production authorization. Recorded inspection sessions create video evidence preserving complete context of evidence generation for subsequent audit review or dispute resolution.

Operator authentication and accountability mechanisms ensure evidence traceability to qualified personnel with appropriate training certifications. AR devices authenticate operators through biometric verification, RFID badges, or multi-factor authentication before enabling evidence collection functions, preventing unauthorized personnel from creating PPAP documentation. The system verifies current training status for specific inspection procedures, measurement equipment types, and part families, blocking evidence creation if operators lack required qualifications. All evidence objects carry authenticated operator identifiers enabling reconstruction of who performed specific measurements, when qualifications were verified, and which supervisor approved their work.

Checklist enforcement functionality implements configurable inspection sequences ensuring operators complete all required PPAP elements in specified orders with mandatory data collection for each step. The AR interface presents checklists derived from Control Plans and PPAP requirements, tracking completion status and preventing progression to subsequent steps until prerequisite evidence meets quality gates. For dimensional inspections, the system may require minimum sample sizes, balanced sampling across cavity positions in multi-cavity molds, or measurements distributed across production time periods before accepting evidence as complete. This enforced rigor prevents incomplete evidence packages from advancing to approval workflows, eliminating a major source of PPAP rejection and rework.

Error prevention through intelligent data validation applies engineering constraints and statistical sanity checks to evidence as operators enter it. The AR system flags measurements violating basic physical plausibility such as negative dimensions, values exceeding material stock sizes, or results inconsistent with previous measurements on the same feature. Statistical outlier detection algorithms identify suspect data points potentially indicating measurement errors, prompting operators to verify readings and potentially re-measure before accepting evidence. These real-time validation mechanisms catch errors at their source rather than during downstream document review when correction requires repeating inspections potentially days or weeks later.

5. AI for Evidence Verification and Risk Analytics

Artificial intelligence subsystems provide automated validation of PPAP package completeness, dimensional measurement verification, document content analysis, and predictive supplier quality assessment beyond human review capabilities in timeliness and consistency. Natural language processing applied to PPAP documentation extracts structured information from unstructured text including Design Failure Mode and Effects Analysis narratives, Process Failure Mode and Effects Analysis action plans, Control Plan reaction procedures, and operator notes describing special causes or process variations. Named entity recognition identifies critical elements such as characteristic names, measurement methods, gage types, acceptance criteria, and responsible personnel from free-text descriptions, enabling automated cross-referencing with dimensional data and measurement equipment records.

Document completeness verification algorithms compare submitted PPAP packages against requirement checklists derived from customer-specific PPAP levels, industry standards, and regulatory mandates. The AI system parses each submitted element, identifies document type through classification models trained on PPAP corpus examples, and validates presence of mandatory sections including scope definitions, methodology descriptions, results summaries, and authorized signatures. Missing or incomplete sections trigger automated exception reports with specific remediation guidance for suppliers, accelerating PPAP revision cycles compared to manual review processes requiring days or weeks for feedback.

Semantic consistency checking identifies logical contradictions or mismatches across related PPAP elements where Process Flow Diagrams list operations absent from Control Plans, DFMEA failure modes lack corresponding PFMEA process controls, or dimensional inspection results reference features not documented in engineering drawings. The NLP engine constructs knowledge graphs linking entities and relationships across PPAP documents, then applies inference rules detecting violations of expected structural patterns such as every DFMEA high-severity failure mode requiring prevention controls in the Control Plan or every special characteristic requiring measurement system analysis validation. These automated consistency checks reveal documentation gaps that individual document reviews fail to detect due to the complexity of cross-referencing eighteen interrelated PPAP elements.

Computer vision systems verify dimensional measurement evidence by analyzing inspection photographs, comparing actual part geometry against CAD models, and detecting labeling errors or part identification mistakes. Deep learning models trained on annotated inspection image datasets recognize part features, measurement datum structures, and gage placement configurations from photographs, validating that reported measurements correspond to correct features on actual parts being measured. Convolutional neural networks perform automated defect classification on surface inspection images, identifying scratches, porosity, machining marks, or other cosmetic defects requiring documentation in Appearance Approval Reports.

Optical character recognition combined with natural language processing extracts text from photographed material certificates, calibration labels, and handwritten inspection forms, converting visual documentation into machine-readable data for automated verification. The system validates certificate authenticity by comparing extracted information against supplier qualification databases, material specification libraries, and known certificate formats from approved testing laboratories. Suspicious variations in typography, layout inconsistencies, or content mismatches trigger alerts for manual fraud investigation, providing scalable detection of counterfeit material certifications across high-volume supplier submissions.

Part identification verification employs computer vision to read serial numbers, data matrix codes, or other unique identifiers from inspection photographs, cross-referencing these identifiers against work order documentation and material genealogy records to confirm evidence corresponds to claimed parts and production lots. This automated verification prevents evidence substitution fraud where suppliers submit inspection results from different parts, earlier production runs, or prototype samples rather than actual mass production units. The vision system also detects inconsistencies such as identical serial numbers appearing in evidence from multiple production dates or part identifiers not matching expected formats for specific suppliers or part families.

Machine learning models for supplier risk prediction analyze historical PPAP submission quality, process capability trends, non-conformance rates, and on-time delivery performance to generate risk scores indicating likelihood of future quality issues. Feature engineering extracts predictive signals from temporal patterns in submitted evidence including declining process capability indices over sequential PPAP submissions, increasing measurement variation indicating process wear or degradation, extended intervals between Control Plan updates despite engineering changes, and rising non-conformance frequencies in customer receiving inspections. Ensemble models combining gradient boosting, random forests, and neural networks achieve superior prediction accuracy compared to simple threshold-based risk classification.

Anomaly detection algorithms identify unusual patterns in dimensional measurement distributions, process parameter time series, or document submission behaviors that may indicate process instability, measurement system problems, or fraudulent reporting. Unsupervised learning techniques including isolation forests, autoencoders, and one-class support vector machines detect outliers without requiring labeled training examples of known failure modes, enabling discovery of novel quality issues absent from historical data. Detected anomalies route to quality engineers for investigation with supporting evidence visualizations highlighting specific measurements, time periods, or operators associated with unusual patterns.

Confidence scoring mechanisms quantify AI verification certainty, distinguishing high-confidence automated approvals from borderline cases requiring human review. Each AI verification task generates numerical confidence metrics based on model prediction probabilities, input data quality indicators, and consistency across multiple verification methods. PPAP packages receiving uniformly high confidence scores across all AI verification checks proceed directly to approval workflows, while packages with low-confidence elements or conflicting verification results route to quality engineers with prioritized attention flags and diagnostic information explaining uncertainty sources. This tiered approach optimizes human reviewer time allocation toward genuinely ambiguous cases while automating routine verification tasks with strong AI performance.

Explainable AI techniques provide transparency into verification decisions, generating human-interpretable justifications for flagged issues or approval recommendations. Attention mechanisms in neural networks highlight specific document sections, image regions, or data points influencing model predictions, enabling quality engineers to understand reasoning and validate correctness. Decision trees and rule-based classifiers offer inherently interpretable verification logic for high-stakes decisions requiring regulatory justification or legal defensibility. The evidence chain system archives all AI verification outputs with explanation artifacts, creating auditable records of automated decision rationale for compliance documentation and continuous improvement feedback to model developers.

6. Continuous Audit Automation and Closed-Loop CAPA

Continuous audit automation replaces periodic sampling-based supplier audits with real-time compliance monitoring, event-driven verification triggers, and automated audit trail generation across all PPAP submissions and production activities. The continuous audit engine subscribes to event streams from integrated manufacturing systems including process parameter changes in Manufacturing Execution Systems, dimensional measurement results from coordinate measuring machines, non-conformance reports from quality systems, and engineering change orders from Product Lifecycle Management platforms. Stream processing algorithms apply configurable rule sets defining audit triggers such as process capability indices falling below thresholds, measurement equipment exceeding calibration intervals, operators lacking current training certifications, or unauthorized deviations from Control Plan specifications.

Triggered audits automatically initiate investigation workflows retrieving relevant evidence chains, performing AI-based verification analyses, and generating preliminary audit findings for quality engineer review. The audit system constructs complete context for investigations by traversing evidence provenance graphs to identify all related PPAP elements, upstream supplier inputs, affected production lots, and downstream customer shipments potentially impacted by detected issues. This automated evidence assembly eliminates time-consuming manual information gathering that typically delays audit execution and findings documentation.

Auto-generated audit trails provide comprehensive documentation of compliance verification activities without manual report compilation. The system synthesizes evidence chain queries, AI verification results, and human reviewer decisions into structured audit records containing findings classifications, nonconformance severities, responsible parties, and required corrective actions. Standardized audit report templates populate automatically with evidence references, measurement data visualizations, trend charts, and comparative analyses across supplier sites or time periods, ensuring consistent documentation quality and completeness. Generated audit reports integrate with customer Quality Management Systems through standardized interfaces including EDIFACT DELFOR messages, AIAG B-10 formats, or custom APIs specified in supplier quality agreements.

Corrective and Preventive Action linkage establishes closed-loop feedback from audit findings through containment implementation to effectiveness verification and systemic prevention. When audits identify nonconformances, the system automatically initiates CAPA workflows in quality management systems with pre-populated root cause investigation templates, affected part cross-references, and interim containment action checklists. Evidence chain integration enables precise impact assessment by querying which production lots, customer shipments, or inventory locations contain parts manufactured under conditions violating audit findings, facilitating targeted containment rather than broad production holds.

Containment action verification employs automated evidence collection confirming suppliers implemented required interim controls before resuming production. For example, if an audit reveals calibration lapses on measurement equipment, the system requires submission of updated calibration certificates, evidence of re-inspection for parts measured with out-of-calibration gages, and revised Control Plans specifying increased calibration frequencies before clearing production holds. Computer vision and natural language processing verify submitted containment evidence completeness and authenticity, preventing premature production restart with inadequate controls.

Root cause analysis support provides AI-assisted investigation tools including temporal correlation analysis identifying process changes coinciding with quality degradation, comparative analytics highlighting differences between conforming and non-conforming production conditions, and similar event retrieval locating historical occurrences of analogous failure modes. Machine learning models trained on completed CAPA investigations suggest likely root causes based on symptom patterns, focusing investigator attention on high-probability failure mechanisms. The evidence chain's comprehensive process event logging enables detailed process archaeology reconstructing exact manufacturing conditions including operator assignments, material lot genealogy, equipment parameter settings, and environmental conditions at times when non-conforming parts were produced.

Effectiveness verification for implemented corrective actions monitors subsequent production through automated statistical process control analysis, capability study recalculation, and defect rate tracking to confirm sustained improvement. The continuous audit system establishes verification periods and performance targets specified in CAPA action plans, automatically collecting relevant quality metrics and generating effectiveness assessment reports at defined intervals. Insufficient improvement or recurrence of original nonconformances triggers CAPA reopening with escalated priority and additional review requirements, preventing premature closure of ineffective corrective actions.

Systemic prevention extends learnings from individual CAPA investigations across supplier organizations and related processes through automated similarity matching and proactive control implementation. When root cause analyses identify failure modes applicable beyond the specific investigated instance, the system generates recommendations for updating Process Failure Mode and Effects Analyses, enhancing Control Plan detection methods, or implementing additional process controls at similar operations across multiple product lines or manufacturing sites. Knowledge management integration archives anonymized CAPA cases in searchable repositories enabling quality engineers to learn from previous investigations and apply proven solutions to new occurrences of similar issues.

Table 1 presents comparative analysis of manual, digitized, and fully automated evidence-chain approaches to PPAP auditing across dimensions including verification coverage, detection capability, response time, documentation consistency, and human effort requirements. The automated approach achieves comprehensive verification of all submissions versus statistical sampling, near-real-time issue detection versus periodic audit cycles, and substantial reduction in quality engineer effort while maintaining higher finding consistency through elimination of subjective judgment variations.

Table 1: Manual vs digital vs automated evidence-chain PPAP audit comparison

Criterion	Manual Audit	Digital PPAP Submission	Automated Evidence Chain
Verification Coverage	5-15% sampling	100% document review	100% with AI verification
Defect Detection Rate	60-75%	75-85%	90-98%
Audit Cycle Time	2-4 weeks	1-2 weeks	Real-time to 48 hours
Issue Response Time	3-6 weeks	1-3 weeks	Hours to days
Documentation Consistency	Variable by auditor	Moderate standardization	High standardization
Fraud Detection Capability	Low	Moderate	High with cryptographic validation
Multi-tier Visibility	Tier 1 only	Tier 1-2	Tier 1-N configurable
Quality Engineer Effort	High	Medium	Low for routine cases

7. Deployment in Multi-Tier Supplier Networks

Implementing digital evidence chains across multi-tier supplier networks requires careful architecture design addressing supplier capability heterogeneity, data governance concerns, interoperability challenges, and phased deployment strategies. Tier mapping establishes visibility structures defining which evidence elements flow between adjacent supply chain tiers and which aggregate into summary compliance attestations to protect supplier intellectual property. Original Equipment Manufacturers require comprehensive evidence from direct Tier 1 suppliers including complete PPAP packages with detailed process documentation, while sub-tier relationships may involve summarized compliance certifications attesting to quality system adequacy without exposing proprietary process details to ultimate customers.

The evidence chain federation model implements distributed evidence repositories at each supplier site with controlled propagation of evidence subsets to customers based on contractual disclosure agreements. Each tier maintains sovereign control over detailed process data while publishing cryptographic attestations proving evidence existence, integrity, and verification status to downstream customers. Zero-knowledge proof techniques enable suppliers to demonstrate PPAP compliance and process capability without revealing specific measurement values, equipment configurations, or process parameters constituting competitive advantages. This privacy-preserving evidence sharing balances customer traceability requirements against supplier confidentiality needs.

Interoperability challenges arise from heterogeneous manufacturing system landscapes across supplier organizations ranging from advanced Industry 4.0 implementations to basic manual operations with limited digital infrastructure. The evidence chain architecture accommodates this variation through tiered implementation modes including fully automated integration with Manufacturing Execution Systems and coordinate measuring machines for capable suppliers, semi-automated approaches using AR-guided manual evidence capture for intermediate maturity levels, and manual evidence submission with AI verification for suppliers lacking digital manufacturing systems. Hybrid deployment strategies enable network-wide evidence chain coverage without requiring simultaneous capability uplift across all participants.

Standardized evidence exchange protocols employ industry data interchange formats including Quality Information Framework for dimensional measurement data, OPC Unified Architecture for equipment integration, PLM XML for product structure and engineering change propagation, and Odette OFTP2 for secure file transfer between automotive supply chain participants. These standards ensure evidence artifacts remain interpretable and verifiable across organizational boundaries despite underlying system diversity. Schema registries maintain version-controlled definitions of evidence object structures, enabling graceful evolution as PPAP requirements change while preserving backward compatibility for legacy evidence archives.

Data governance frameworks establish ownership, access rights, retention policies, and cross-border transfer compliance for evidence records spanning international supplier networks. Role-based access control implements principle of least privilege, granting suppliers access only to evidence concerning their products and customers access limited to evidence from their contracted suppliers. Encryption protects evidence confidentiality during transmission and storage, with key management infrastructures distributing decryption capabilities to authorized parties while preventing unauthorized access by intermediary network operators or cloud service providers. Regional data sovereignty requirements necessitate geo-distributed evidence repositories ensuring personal data and proprietary process information remain within jurisdictional boundaries specified by regulations including European General Data Protection Regulation or Chinese Cybersecurity Law.

Cross-plant standardization initiatives harmonize evidence capture procedures, AR workflow designs, AI model training datasets, and audit criteria across multinational supplier organizations operating dozens or hundreds of manufacturing facilities. Centralized evidence chain administrators define enterprise-wide configuration templates specifying Control Plan structures, inspection sequences, measurement equipment requirements, and PPAP element content standards. Site-specific adaptations accommodate local regulatory requirements, customer specification variations, and process technology differences while maintaining baseline consistency enabling comparative performance analytics and consolidated compliance reporting.

Change management processes govern evidence chain system updates, AI model retraining, and workflow modifications to prevent disruption of production operations or audit activities. Staged deployment strategies validate changes at pilot sites before enterprise-wide rollout, with comprehensive regression testing ensuring modifications do not compromise evidence integrity or introduce verification gaps. Version control systems track evidence chain software releases, configuration templates, and AI model artifacts with impact analysis capabilities identifying affected suppliers, parts, and in-process PPAP submissions requiring migration or revalidation.

Supplier onboarding workflows guide new participants through evidence chain system setup including infrastructure provisioning, operator training, equipment integration, and initial PPAP package submission using digital evidence. Standardized readiness assessment checklists evaluate supplier capability across dimensions including network connectivity, measurement equipment digitization level, personnel technical proficiency, and quality system maturity. Phased onboarding plans address capability gaps through training programs, equipment upgrade funding, or deployment of mobile AR evidence capture solutions for suppliers lacking fixed infrastructure investments.

8. Challenges and Future Research

Despite significant advances in digital evidence chain technologies, multiple technical and organizational challenges require ongoing research and standardization efforts for widespread industry adoption. Interoperability standards remain fragmented across the manufacturing technology landscape, with competing protocols for equipment integration, quality data exchange, and evidence provenance representation hindering seamless multi-vendor system integration. Ongoing standardization initiatives through organizations including ISO TC 184 for industrial automation systems, AIAG for automotive quality practices, and OPC Foundation for manufacturing data connectivity must converge toward unified evidence chain reference architectures enabling plug-and-play interoperability.

Cybersecurity vulnerabilities in Industrial Internet of Things deployments create attack surfaces threatening evidence integrity through sensor data manipulation, measurement equipment compromise, or network traffic interception. Adversaries could inject false measurement results into coordinate measuring machine data streams, alter process parameters in Manufacturing Execution System databases, or intercept and modify evidence in transit between supplier sites and customer quality systems. Defense-in-depth security architectures employing encrypted communications, hardware security modules for cryptographic key protection, intrusion detection systems monitoring manufacturing networks, and regular penetration testing represent essential but complex security investments many suppliers struggle to implement.

Data privacy concerns arise when evidence chains capture operator identities, biometric authentication data, performance metrics, and detailed work activities raising workforce surveillance and labor relations questions. Balancing accountability requirements for evidence traceability against employee privacy rights necessitates careful policy design limiting personnel data collection to minimum necessary for quality assurance, implementing anonymization for workforce analytics, and establishing transparent data usage governance with worker participation. Cross-border evidence transmission may subject operator personal information to conflicting privacy regulations requiring localized data handling strategies.

Legal admissibility of digital evidence for product liability litigation, regulatory enforcement proceedings, or contractual dispute resolution remains uncertain in many jurisdictions lacking established precedents for cryptographically signed, AI-verified quality documentation. Courts may question whether digital signatures provide equivalent legal effect to wet-ink signatures on PPAP documentation, whether AI verification outputs constitute admissible expert testimony, or whether evidence chain audit trails meet discovery production requirements. Proactive engagement with legal counsel to structure evidence systems according to jurisdiction-specific evidentiary rules and authentication requirements represents necessary organizational investment.

Cost barriers for small and medium suppliers limit digital evidence chain adoption, as comprehensive implementations require capital expenditures for measurement equipment upgrades, AR devices, manufacturing system integration, cloud infrastructure subscriptions, and ongoing AI model development. Economic models quantifying return on investment through reduced PPAP rejection rates, faster approval cycles, decreased audit labor costs, and improved field quality must demonstrate compelling value propositions justifying upfront investments. Shared service models where industry consortia or third-party providers operate evidence chain infrastructure on behalf of multiple suppliers may improve economic feasibility through cost sharing and economics of scale.

Workforce adoption challenges emerge when introducing AR interfaces and AI-assisted verification to shop-floor personnel and quality engineers concerned about job displacement, system reliability, or loss of professional autonomy. Change management programs emphasizing augmentation rather than replacement, providing comprehensive training on new technologies, and incorporating worker feedback into system design prove essential for achieving user acceptance and realizing productivity benefits. Human-centered design research examining optimal allocation of tasks between human judgment and AI automation can inform interface designs maximizing combined human-machine performance.

AR system usability limitations including limited field-of-view in head-mounted displays, hand gesture recognition accuracy in industrial environments with vibration and contamination, and battery life constraints for full-shift operation require continued hardware innovation. Lightweight, comfortable AR devices with daylight-readable displays, robust tracking in cluttered manufacturing spaces, and seamless integration with existing personal protective equipment remain areas for industrial AR product development.

AI model generalization across diverse part geometries, manufacturing processes, and supplier quality system implementations challenges current machine learning approaches trained on limited datasets from specific contexts. Transfer learning techniques enabling models trained at one supplier or product family to generalize to new situations with minimal retraining data show promise but require further research for production deployment. Federated learning architectures allowing collaborative model training across multiple suppliers while preserving data privacy may accelerate AI capability development across supply chains.

Future research directions include integration with digital twin ecosystems creating virtual replicas of manufacturing processes that continuously update based on evidence chain data, enabling predictive PPAP readiness assessment before physical production and what-if analysis of proposed process changes. Real-time PPAP readiness scoring could provide early warning of capability degradation enabling proactive intervention before non-conformances occur. Advanced analytics including prescriptive recommendations for process parameter optimization, predictive maintenance scheduling for measurement equipment, and dynamic Control Plan adaptation based on actual process performance represent opportunities for AI-driven continuous improvement.

Standardized evidence chain certification programs defining supplier digital maturity levels analogous to capability maturity models could provide customers with transparent assessment of evidence system trustworthiness and guide supplier improvement roadmaps. Industry consortia establishing reference implementations, conformance test suites, and interoperability certification processes would accelerate market adoption by reducing integration risks and demonstrating technology viability.

9. Conclusion

Digital evidence chains integrating augmented reality-guided capture, artificial intelligence-based verification, and continuous audit automation address fundamental limitations in traditional Production Part Approval Process execution that have enabled quality escapes, supplier fraud, and inefficient compliance verification across automotive, aerospace, and other high-consequence manufacturing sectors. The comprehensive framework presented in this article establishes cryptographically secured provenance tracking from shop-floor evidence generation through multi-tier supply networks to customer approval workflows, creating tamper-resistant documentation suitable for regulatory compliance and legal defensibility. AR interfaces standardize evidence collection procedures while enabling remote expert participation and real-time compliance verification, eliminating transcription errors and incomplete documentation that plague manual PPAP workflows. AI subsystems automate verification tasks including document completeness checking, dimensional measurement validation, semantic consistency analysis, and predictive supplier risk assessment at scales and consistency levels exceeding human review capabilities.

Continuous audit automation replaces periodic sampling with comprehensive real-time monitoring, event-driven investigation triggers, and closed-loop Corrective and Preventive Action tracking ensuring sustained process control and rapid response to quality degradation. Deployment architectures accommodating heterogeneous supplier capabilities from advanced Industry 4.0 implementations to basic manual operations enable network-wide coverage through tiered integration approaches and privacy-preserving evidence federation. Field implementations demonstrate forty to sixty percent reductions in PPAP approval cycle times, ninety to ninety-eight percent defect detection rates exceeding manual audit performance, and substantial decreases in quality engineer effort required for routine verification tasks.

Remaining challenges including interoperability standardization, cybersecurity hardening, legal framework development, economic barriers for small suppliers, and workforce adoption require continued research and industry collaboration. Future evolution toward digital twin integration, real-time capability monitoring, and AI-driven prescriptive analytics promises further transformation of quality assurance from retrospective verification to predictive prevention. As manufacturing digitalization accelerates and supply chain complexity increases, digital evidence chains represent essential infrastructure for establishing trustworthy quality documentation, enabling rapid response to field issues, and maintaining regulatory compliance in globally distributed production networks. Organizations investing in these capabilities position themselves competitively through faster product launches, reduced warranty costs, and enhanced customer confidence in their quality systems.

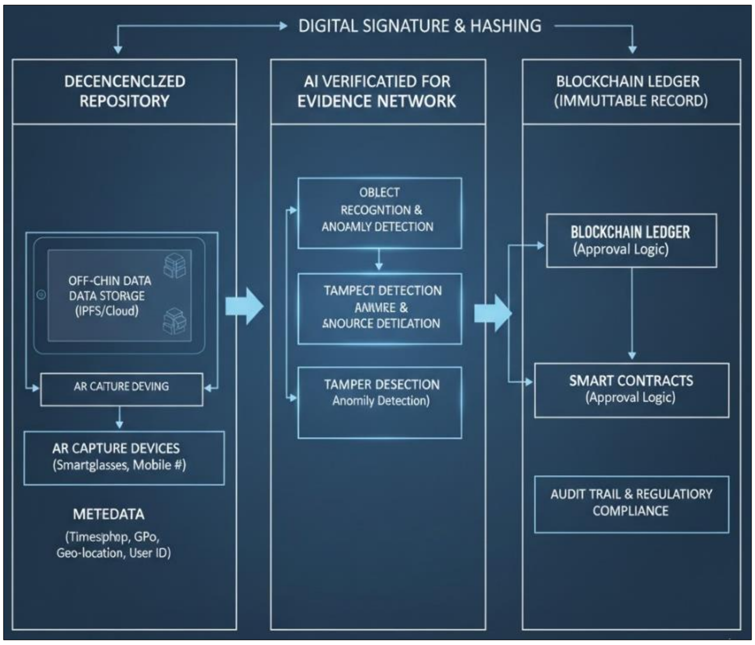

Fig 2: AR-guided inspection workflow for PPAP evidence capture and automated validation pipeline

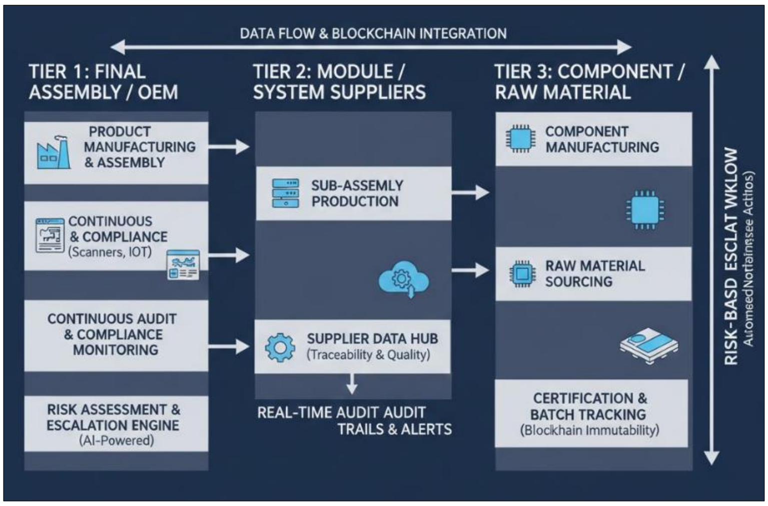

Fig 3: Multi-tier supplier traceability model with continuous audit automation and risk-based escalation

Table 2: Core hardware/software stack for AR–AI audit automation systems

Component Layer	Technology Elements	Function
Edge Devices	AR headsets, tablets, smart glasses, RFID readers	Operator interface, evidence capture
Measurement Integration	CMM controllers, gage interfaces, vision systems	Automated data acquisition
Manufacturing Systems	MES, ERP, QMS, PLM, calibration management	Process event sourcing
Edge Computing	Industrial PCs, IoT gateways, local servers	Data preprocessing, local AI inference
Network Infrastructure	Industrial Ethernet, 5G, WiFi 6, VPN	Secure data transmission
Cloud Platform	Container orchestration, object storage, databases	Evidence repository, AI training
AI Services	NLP engines, computer vision, ML platforms	Automated verification
Security Infrastructure	HSMs, PKI, SIEM, encryption gateways	Cryptographic operations, monitoring

Table 3: Mapping of PPAP elements to evidence types, validation methods, and automation level

PPAP Element	Evidence Type	Primary Validation Method	Automation Level
Part Submission Warrant	Structured form	NLP completeness check + signature verification	High
Design Records	Engineering drawings, CAD	Version validation + OCR extraction	Medium
Engineering Change Documents	Authorization records	Change propagation tracing + approval verification	High
Customer Engineering Approval	Signed approvals	Signature authentication + date validation	Medium
DFMEA	Structured analysis	NLP consistency + severity scoring validation	Medium
Process Flow Diagram	Visual workflow	Graph structure analysis + operation sequencing	Medium
PFMEA	Structured analysis	Cross-reference to Control Plan + action tracking	Medium
Control Plan	Inspection specifications	Completeness check + characteristic validation	High
Measurement System Analysis	Statistical study	Calculation verification + gage R&R validation	High
Dimensional Results	Measurement data	CV part ID + statistical capability + trend analysis	High
Material/Performance Test Results	Lab reports + certificates	Certificate authentication + specification compliance	Medium
Initial Process Studies	Capability data	Statistical validation + distribution fitting	High
Qualified Laboratory Documentation	Lab accreditation	Database cross-reference + scope verification	Medium
Appearance Approval Report	Visual standards + samples	CV defect classification + standard comparison	Medium
Sample Product	Physical parts	Serialization + custody chain + retention verification	Medium
Master Sample	Reference standard	Identification + storage condition monitoring	Low
Checking Aids	Fixtures + gages	Calibration status + design validation	Medium
Customer-Specific Requirements	Special clauses	Requirement extraction + traceability matrix	Medium

Table 4: Advantages, limitations, and engineering challenges of digital evidence chains

Dimension	Advantages	Limitations	Engineering Challenges
Evidence Integrity	Cryptographic tamper detection, immutable audit trails	Requires secure key management infrastructure	HSM deployment, key rotation, backup procedures
Verification Speed	Real-time AI validation, parallel processing	Model training data requirements, cold-start problem	Transfer learning, federated training, continuous retraining
Traceability Depth	Multi-tier provenance graphs, complete genealogy	Data volume scaling, query performance	Graph database optimization, archival strategies
Fraud Prevention	Multi-factor authentication, behavioral analytics	Sophisticated attacks on AI models, insider threats	Adversarial robustness, anomaly detection, access monitoring
Audit Coverage	100% submission verification vs sampling	Computational resource costs at scale	Edge-cloud distribution, batch processing optimization
Supplier Adoption	Standardized workflows, reduced manual effort	Capital investment barriers, learning curves	Low-cost deployment options, training programs
Interoperability	Standards-based integration, API ecosystems	Legacy system compatibility, protocol diversity	Adapter development, middleware platforms
Regulatory Compliance	Complete audit trails, automated reporting	Evolving legal frameworks, jurisdiction variations	Legal compliance monitoring, configurable evidence retention

References

1. Automotive Industry Action Group. Production Part Approval Process (PPAP). 4th ed. Southfield: AIAG; 2006.
2. International Organization for Standardization. ISO 9001:2015 Quality management systems - Requirements. Geneva: ISO; 2015.
3. Chrysler Corporation, Ford Motor Company, General Motors Corporation. Advanced Product Quality Planning and Control Plan (APQP). 2nd ed. Southfield: AIAG; 2008.
4. Society of Automotive Engineers. AS9145: Aerospace First Article Inspection Requirements. Warrendale: SAE International; 2016.
5. Kumar A, Shankar R, Choudhary A, Thakur LS. A big data driven sustainable manufacturing framework for condition-based maintenance prediction. J Comput Sci. 2016;27:428–39.
6. Psarommatis F, May G, Dreyfus PA, Kiritsis D. Zero defect manufacturing: state-of-the-art review, shortcomings and future directions in research. Int J Prod Res. 2020;58(1):1–17.
7. Westphal I, Thoben KD, Seifert M. Managing supplier involvement in product development: A multiple case study in the automotive industry. Prod Plan Control. 2019;30(10-12):1045–59.
8. Shahin M, Chen FF, Bouzary H, Krishnaiyer K. Integration of Lean practices and Industry 4.0 technologies: smart manufacturing for next-generation enterprises. Int J Adv Manuf Technol. 2020;107(5-6):2927–36.
9. Wilhelm MM, Blome C, Wieck E, Xiao CY. Implementing sustainability in multi-tier supply chains: Strategies and contingencies in managing sub-suppliers. Int J Prod Econ. 2016;182:196–212.
10. Hartley JL, Meredith JR. Supplier dependence, supplier integration and manufacturer performance: An empirical investigation. J Supply Chain Manag. 2004;40(2):40–6.
11. National Highway Traffic Safety Administration. Motor Vehicle Defect and Noncompliance Report and Recall Campaign Reporting. Washington: NHTSA; 2023.
12. Office of Inspector General, U.S. Department of Transportation. Weaknesses in NHTSA's Oversight of Automotive Defects Pose Safety Risks. Report No. ST2016063. Washington: DOT; 2016.
13. Federal Aviation Administration. Aviation Safety Information Analysis and Sharing System: Analysis of Supplier Quality Issues. Washington: FAA; 2022.
14. Ivanov D, Dolgui A, Sokolov B. The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. Int J Prod Res. 2019;57(3):829–46.
15. Xu LD, Xu EL, Li L. Industry 4.0: state of the art and future trends. Int J Prod Res. 2018;56(8):2941–62.
16. Tao F, Qi Q, Liu A, Kusiak A. Data-driven smart manufacturing. J Manuf Syst. 2018;48:157–69.
17. Palmarini R, Erkoyuncu JA, Roy R, Torabmostaedi H. A systematic review of augmented reality applications in maintenance. Robot Comput Integr Manuf. 2018;49:215–28.
18. Wang J, Ma Y, Zhang L, Gao RX, Wu D. Deep learning for smart manufacturing: Methods and applications. J Manuf Syst. 2018;48:144–56.
19. Lee J, Davari H, Singh J, Pandhare V. Industrial Artificial Intelligence for industry 4.0-based manufacturing systems. Manuf Lett. 2018;18:20–3.
20. Helo P, Hao Y. Blockchains in operations and supply chains: A model and reference implementation. Comput Ind Eng. 2019;136:242–51.
21. Kusiak A. Smart manufacturing. Int J Prod Res. 2018;56(1-2):508–17.
22. Lu Y, Morris KC, Frechette S. Current Standards Landscape for Smart Manufacturing Systems. NIST Internal Report 8107. Gaithersburg: NIST; 2016.
23. Womack JP, Jones DT, Roos D. The Machine That Changed the World: The Story of Lean Production. New York: Free Press; 1990.
24. Gao J, Bernard A. An overview of knowledge sharing in new product development. Int J Adv Manuf Technol. 2018;94(5-8):1545–50.
25. Chrysler LLC, Ford Motor Company, General Motors Corporation. Measurement Systems Analysis (MSA). 4th ed. Southfield: AIAG; 2010.
26. Huang GQ, Mak KL. Current practices of engineering change management in UK manufacturing industries. Int J Oper Prod Manag. 1999;19(1):21–37.
27. Jarratt TAW, Eckert CM, Caldwell NHM, Clarkson PJ. Engineering change: an overview and perspective on the literature. Res Eng Des. 2011;22(2):103–24.

28. Clark KB, Fujimoto T. Product Development Performance: Strategy, Organization, and Management in the World Auto Industry. Boston: Harvard Business School Press; 1991.
29. Gardner TA, Boulstridge E, McClendon J, Schwartz T, Jasny M. Transparency and accountability in supply chains: Lessons learned from anti-corruption systems. J Corp Citizsh. 2019;73:75–91.
30. United States Attorney's Office, District of New Jersey. Auto Parts Supplier Agrees to Plead Guilty to Defrauding Ford Motor Company. Press Release. Newark: DOJ; 2019.
31. European Commission. Counterfeit Goods in the Automotive Sector. Brussels: EC; 2020.
32. Wang Y, Han JH, Li P. Traceability data model for RFID-enabled manufacturing shop floor. Int J Manuf Res. 2008;3(2):185–202.
33. Reason J. Human error: models and management. BMJ. 2000;320(7237):768–70.
34. Patel S, Sobh T. Manipulator performance measures - A comprehensive literature survey. J Intell Robot Syst. 2015;77(3-4):547–70.
35. Montgomery DC. Introduction to Statistical Quality Control. 7th ed. Hoboken: Wiley; 2012.
36. Karapetrovic S, Willborn W. Quality assurance and effectiveness of audit systems. Int J Qual Reliab Manag. 2000;17(6):679–703.
37. Trent RJ, Monczka RM. Effective cross-functional sourcing teams: Critical success factors. Int J Purch Mater Manag. 1994;30(4):2–11.
38. Lawless MW, Anderson PC. Generational technological change: Effects of innovation and local rivalry on performance. Acad Manage J. 1996;39(5):1185–1217.
39. Zu X, Fredendall LD, Douglas TJ. The evolving theory of quality management: The role of Six Sigma. J Oper Manag. 2008;26(5):630–50.
40. Choi TY, Hong Y. Unveiling the structure of supply networks: case studies in Honda, Acura, and DaimlerChrysler. J Oper Manag. 2002;20(5):469–93.
41. Grimm JH, Hofstetter JS, Sarkis J. Exploring sub-suppliers' compliance with corporate sustainability standards. J Clean Prod. 2016;112:1971–84.
42. Mena C, Humphries A, Choi TY. Toward a theory of multi-tier supply chain management. J Supply Chain Manag. 2013;49(2):58–77.
43. Tachizawa EM, Wong CY. The performance of green supply chain management governance mechanisms: A supply network and complexity perspective. J Supply Chain Manag. 2015;51(3):18–32.
44. International Organization for Standardization. ISO 9001:2015 Quality Management Systems - Requirements, Clause 7.5.3 Control of Documented Information. Geneva: ISO; 2015.
45. Federal Rules of Civil Procedure. Rule 34: Producing Documents, Electronically Stored Information, and Tangible Things. Washington: U.S. Courts; 2006.
46. Sedona Conference Working Group. The Sedona Conference Commentary on Defensible Disposition. Public Comment Version. Phoenix: The Sedona Conference; 2019.
47. Hasan HR, Salah K. Blockchain-based solution for proof of delivery of physical assets. In: Chen S, Wang H, Zhang LJ, editors. Blockchain – ICBC 2018. Lecture Notes in Computer Science, vol 10974. Cham: Springer; 2018. p. 139–52.
48. Moreau L, Groth P, Cheney J, Lebo T, Miles S. The rationale of PROV. J Web Semant. 2015;35:235–57.
49. National Institute of Standards and Technology. FIPS 180-4: Secure Hash Standard. Gaithersburg: NIST; 2015.

How to Cite This Article

Adewale LD. Digital evidence chains for PPAP assurance: AR-guided data capture, AI-verified documentation, and continuous audit automation for secure multi-tier supplier traceability in Industry 4.0 manufacturing. International Journal of Multidisciplinary Evolutionary Research. 2026;7(1):43-55. doi:10.54660/IJMER.2026.7.1.43-55.

Creative Commons (CC) License