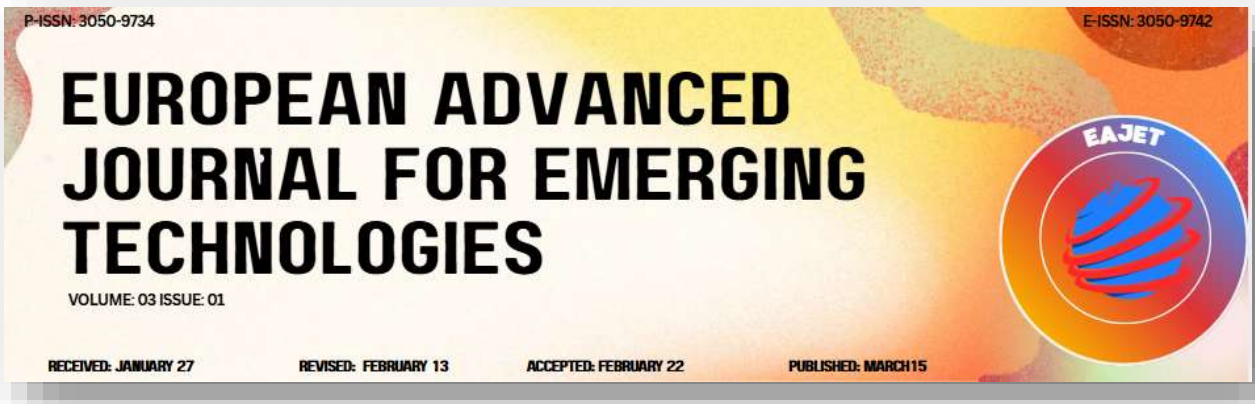



# AI-Powered Autonomous Audit Intelligence for Manufacturing Systems

**Ethan Williams**
Asst Professor

## Abstract

Autonomous Audit Intelligence (AAI) is a specialized form of autonomous artificial intelligence that performs continuous internal audits in complex, data-rich operational environments such as manufacturing. An AAI system operates on data produced by operational systems to verify compliance with requirements. By monitoring requirements such as industry regulations, corporate policies, and best business practices, the monitoring and telemetry capabilities of AAI systems enable the detection of operational anomalies and deviations. Such anomalies in turn trigger investigative audits that seek to isolate and determine the cause of a specific incident. A two-layer architectural framework supports AAI for manufacturing infrastructure. The lower layer represents the telemetry, sensing, and monitoring infrastructure that provides extensive real-time data acquisition. The upper layer addresses data quality, integration, agility, security, and provenance. Several core AI technologies are required for the AAI systems: natural language processing, data quality assurance, information retrieval, case-based reasoning, agent-based tools, and machine learning for anomaly detection.

Several autonomous audit intelligence projects have been implemented in the domain of discrete manufacturing and have been supported by empirical case studies. Otherproject are currently being developed and poineered in utility-scale service industries such as water, power, and transportation. The empirical work has demonstrated the operation and value of autonomous audits using system-generated data but not yet in real-time, with semi-automated analysis of audio-visual data. The methodology and supporting technologies are now being brought to bear in a process industry—risks, compliance, and data quality in a large-scale gas production facility and real-time anomaly detection in an airport terminal.

**Keywords:** Autonomous Audit Intelligence (AAI), Continuous Internal Auditing, Compliance Monitoring Systems, Manufacturing Audit Automation, Operational Anomaly Detection, Investigative Audit Triggering, Telemetry and Monitoring Infrastructure, Real-Time Data Acquisition, Data Quality Assurance, Audit Data Provenance, Secure Industrial Data Integration, Natural Language Processing for Audits, Information Retrieval for Compliance, Case-Based Reasoning Systems, Agent-Based Audit Tools, Machine Learning for Anomaly Detection, Two-Layer Audit Architectures, Industrial Risk and Compliance Management, Autonomous Audits in Process Industries, Empirical Audit Intelligence Case Studies.

## 1. Introduction

The digital transformation of industrial processes and infrastructures is generating increasing amounts of operational data. These data are typically collected for process operation and management purposes, paying little attention to their usability for audit trails, reliability, and compliance reporting. Recent trends propose to capitalize on the data and automatically deliver the audit function as a service, dramatically reducing the cost of periodically conducting compliance audits. This operationalization of the audit function as a service relies on advances in artificial intelligence (AI) that allow precise and interpretable detection of anomalies in the monitored conditions of business services.

The main contribution focuses on the formal definition of autonomous audit intelligence, the core AI technologies needed to build autonomous audit probes, and a detailed architectural framework tailored for deploying such probes in complex manufacturing infrastructures. The work

P-ISSN: 3050-9734
E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 13 ACCEPTED: FEBRUARY 22 PUBLISHED: MARCH15

highlights the main operating modes, explores real-world case studies, and identifies open research challenges. Following the AI approach in the operationalization of autonomous audit probes, the first phase consists of consistently defining the system-to-be. Four specific cases of application are integrated, concentrating mainly on manufacturing settings with bespoke audit automation, satisfying distinct stakeholders' compliance objectives, and delivering value-adding information to external auditors.

### 1.1. Overview of the Study

Audit procedures are fundamentally evidence-gathering activities with monitoring as a key aspect. Innovative companies are applying cutting-edge technological ingredients, such as artificial intelligence (AI), to create autonomous audit systems capable of performing continuous, high-frequency audit activities. Autonomous Audit Intelligence (AAI) represents the application of novel AI techniques for automatic data collection, processing, and interpretation. Autonomous audits increase the accumulation of supporting evidence and provide continuous monitoring of high-risk areas through fact-finding missions.

This work presents a foundational overview of AAI and an architectural framework for operationalizing AAI in manufacturing infrastructure, with specific emphasis on continuous compliance monitoring, anomaly detection, and collaborative investigation of non-conformities and incidents. The overarching aim is to continuously collect and analyze audit-related data from multiple disparate sources to identify risk areas and provide timely alerts for further investigation.


**Fig 1: Autonomous Audit Intelligence (AAI): An Architectural Framework for Continuous Compliance and Anomaly Detection in Manufacturing Infrastructure**

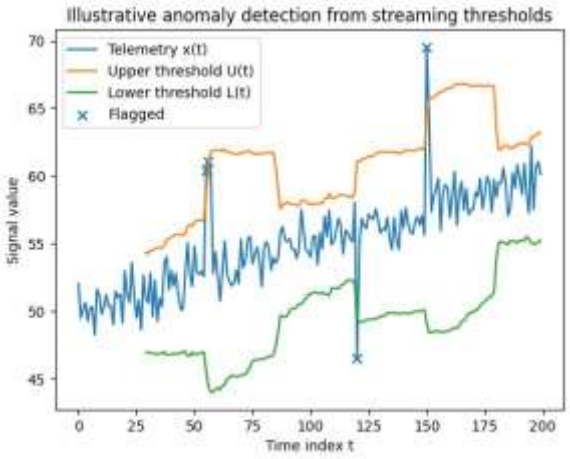
## 2. Theoretical Foundations of Autonomous Audit Intelligence

So-called audit intelligence has the primary function of precisely monitoring the health of an enterprise system with the goal of detecting deviation from established, pre-agreed nominal behavior. While obviously this functionality is analogous to the established supervision role of an empirical approach, audit intelligence is "autonomous," meaning that it operates independently of a human operator—just as AI systems in general are designed to do. More formally, audit intelligence serves as a model-based AI application for supporting auditing and compliance activities by offering a precociously serious view of the expected—rather than the actual—operation of the audited facility. Throughout this narrative, it is also shown that specific approaches and methodologies of empirical approach can naturally serve as engines for autonomously executing distinct classes of audit intelligence. The theme is illustrated through the mining of real audit anomalies that took place in a discrete manufacturing environment over the last decade.

By definition, an audit is an independent examination of financial information of any entity, whether profit oriented

P-ISSN: 3050-9734 E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 13 ACCEPTED: FEBRUARY 22 PUBLISHED: MARCH15

or not, irrespective of its size or legal form, irrespective of its size or legal form. The purpose of an audit is to enable the auditor to express an opinion on these financial statements. The objective of audit intelligence is to extend this concept beyond financial information to the health of manufacturing execution and the ability to deliver product on time and in full.




**Equation A. Multisource signals → consensus estimate**

**Setup**

- Let the true (unobserved) quantity be $x^*$.
- We observe $m$ sources/sensors:

$$x_i = x^* + \varepsilon_i, \quad i = 1, \dots, m$$

Assume:

$$\mathbb{E}[\varepsilon_i] = 0, \quad \mathrm{Var}(\varepsilon_i) = \sigma_i^2$$

**Consensus estimator (weighted mean)**
Take a convex combination:

$$\hat{x} = \sum_{i=1}^{m} w_i \, x_i, \qquad \sum_{i=1}^{m} w_i = 1$$

**Unbiasedness**

$$\mathbb{E}[\hat{x}] = \sum_i w_i \, \mathbb{E}[x_i] = \sum_i w_i \, \mathbb{E}[x^* + \varepsilon_i] = \sum_i w_i \, (x^* + 0) = x^*$$

So $\hat{x}$ is unbiased.

**Variance of the consensus estimator**
If errors are independent:

$$\mathrm{Var}(\hat{x}) = \mathrm{Var}\left(\sum_i w_i \, x_i\right) = \mathrm{Var}\left(\sum_i w_i \, \varepsilon_i\right) = \sum_i w_i^2 \, \sigma_i^2$$

**Choose optimal weights (inverse-variance weighting)**
Minimize $\sum_i w_i^2 \, \sigma_i^2$ subject to $\sum_i w_i = 1$.

Use Lagrange multiplier $\lambda$:

$$\mathcal{L}(w, \lambda) = \sum_i w_i^2 \, \sigma_i^2 - \lambda \left(\sum_i w_i - 1\right)$$

Differentiate:

$$\frac{\partial \mathcal{L}}{\partial w_i} = 2 w_i \sigma_i^2 - \lambda = 0 \Rightarrow w_i = \frac{\lambda}{2\sigma_i^2}$$

Sum constraint:

$$\sum_i w_i = \frac{\lambda}{2} \sum_i \frac{1}{\sigma_i^2} = 1 \Rightarrow \lambda = \frac{2}{\sum_i \frac{1}{\sigma_i^2}}$$

Thus:

$$\boxed{w_i = \frac{\frac{1}{\sigma_i^2}}{\sum_{j=1}^{m} \frac{1}{\sigma_j^2}}}$$

and the minimized variance becomes:

$$\boxed{\mathrm{Var}(\hat{x}) = \frac{1}{\sum_{i=1}^{m} \frac{1}{\sigma_i^2}}}$$

P-ISSN: 3050-9734 E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 13 ACCEPTED: FEBRUARY 22 PUBLISHED: MARCH15

### 2.1. Definitions and scope

The concept of Autonomous Audit Intelligence (AAI) denotes the capacity of an auditing system to self-function without requiring interaction or assistance from human actors during its core processes. The existence of such systems addresses the rising demand for continuous compliance monitoring rather than the periodic assessment of enterprises. On the procedural side, AAI can employ digital technologies to automate the data collection, integration, quality assurance, analysis, and discovery of evidence constituting an audit. Such systems embrace an enlarged notion of audit-ability: rather than being an ex-post examination of an enterprise's activities and supporting records, they continuously accumulate a comprehensive record of data pertaining to a defined production or service delivery process. These data relate either to exposures that can fluctuate over time (e.g., data management, safety and environmental compliance, performance metrics) or to evidential records that support query-driven investigations into specific aspects of operations (e.g., technical incidents, security breaches or failures).

AAI seeks, in particular, to facilitate automated audits in manufacturing infrastructures deployed in production and process industries where physical assets persist. Such large-scale systems provide services for an extended period, ranging from months to decades. Their complexity typically exceeds that of discrete systems, and audit-ability is traditionally limited to infrequent executive quality assessment cycles. Nevertheless, the manufacturing systems embraced by AAI still sustain substantial flows of risk exposures and noteworthy incidents. Two industry-specific variants are considered: a form that integrates seamlessly into the discrete manufacturing industry and a second type deployed in continuous operation during the production of bulk chemical commodities.

| Component | Equation (symbolic) | What it represents (plain) |
|---|---|---|
| Multisource consensus (sensor fusion) | $\hat{x}=\sum_{i=1}^m w_i x_i,\;\; \sum_i w_i=1$ | Combine multiple telemetry signals into one best estimate using weights. |
| Detection threshold (z-score style) | $z=\frac{x-\mu}{\sigma}$ ; flag if $\|z\|>k$ | Standardize a reading vs expected mean/variance to detect outliers. |
| Rolling threshold (streaming) | $U_t=\mu_t+k\sigma_t,\;L_t=\mu_t-k\sigma_t$ | Streaming upper/lower control limits from rolling window statistics. |

### 2.2. Core AI methodologies for auditing

Within the broad category of AI, some domains of specialization are particularly suitable for systematic deployment in audits and other compliance-related roles. These include goal-directed machine learning techniques such as classification, pattern recognition, and target detection; variational inference and strong generative models; and natural language understanding in domain-specific contexts. Practical and applied areas of intelligence are also relevant, including all forms of temporospatial monitoring and telemetry, predictive maintenance, failure analysis, and computer vision techniques.

Satellites and UAVs with the right sensors are increasingly used for combing more information-rich telemetry services. Terrestrial systems incorporating visible and covert surveillance systems of various types also fall into this

P-ISSN: 3050-9734
E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 13 ACCEPTED: FEBRUARY 22 PUBLISHED: MARCH15

category. Incidentally, any autocratic regime will almost certainly use covert surveillance in all places of assembly and recreation. Current state-of-the-art analytics capabilities in these areas greatly enhance the capture of contextual deviations and anomalies in the physical and natural environment.

## 3. Architectural Framework for Autonomous Audit Systems

Design and deployment approaches for the information systems and networks required to enable autonomous audit intelligence are reviewed. The framework is illustrated with respect to two main considerations: (i) the characteristics of data acquisition and provenance systems, and (ii) the sensing, monitoring, and telemetry systems common to manufacturing environments.

1. Data acquisition and provenance

As signals from the physical world continue to multiply, intelligent inspection and judgment of data acquisition becomes a critical prerequisite for autonomous audit intelligence. Separation of data from fear and trust enables machines to verify the correctness of facts without relying on subjective labels or reputations. Foundational work in game-theoretic mechanism design provides an essential starting point for embedding fault detection directly into data acquisition protocols through appropriately structured incentive and disincentive schemes. Three mechanisms are required: (1) composition of multisource signals into consensus estimates with assurance of performance guarantees; (2) specification of detection and falsification thresholds that avoid misclassification of legitimate, outlying signals; and (3) development of provably incentive-compatible protocols for monitoring establishment of these thresholds.

Rich provenance information enhances understanding and exploitation of the data, leading to findings that are more interpretable and actionable. The absence of provenance associated with signals from the physical world increases reliance on post-hoc forensic explanations by humans. Techniques and tools from provenance research enable automatic augmentation of source data with provenance information that records integrity verification, catfishing detection, and alternate explanation of unusual signals. Application of attributes such as reputation, trust, likeliness, cost, and origin to support realtime decision making and fraud detection have also been demonstrated.

### 3.1. Data acquisition and provenance

Achieving the comprehensive data collection required for continuous audits begins with well-defined provenance processes that protect the origins and integrity of all data objects feeding into the audit systems. Data-sensing, telemetry, and monitoring capabilities vary widely across manufacturing industries and companies. These capabilities can span dedicated sensing and monitoring devices that support custom telemetry and real-time monitoring, through instrumentation of known turbid areas with merged operation-entrepreneurs and digital twinning support released across known non-operational periods, to cloud service-enriched deployments that monitor audio and streaming media of normal-operation capable areas for anomaly detection and preventive support.

Supporting continuous data history for known periods requires preserving the integrity of read-only data feeding into the continuous data history. Such tamper-evidence guarantees are often provided through symmetry private key signed hash fingerprints. Integrated systems often rely on equally defined manifest structures holding reference data to sub يا-indices of all objects held by the storage systems. External systems obtain permission for periodic reads on demand to prevent lock instances of sweep accesses required for tampering detection: only read-only treaty monitored data requires such level of control. Plant and equipment operation data also need guarantees of integrity and source by known sector suppliers. Definition and compliance support of powered memory digital twins provides the needed resources to formalize and support the above definitions, operations, and checks.

P-ISSN: 3050-9734
E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 13 ACCEPTED: FEBRUARY 22 PUBLISHED: MARCH15

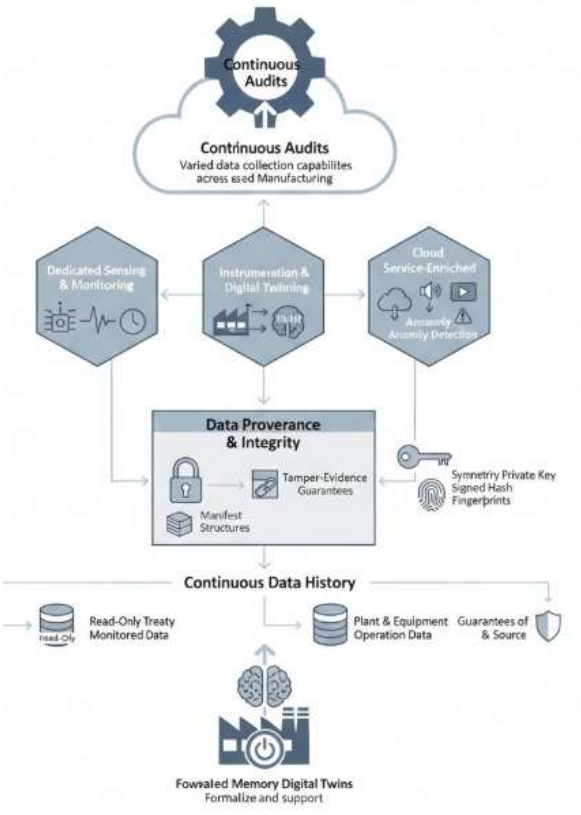



**Fig 2: Ensuring Integrity in Industry 4.0: A Provenance-Based Framework for Tamper-Evident Continuous Auditing and Digital Twin Integration**

### 3.2. Sensing, monitoring, and telemetry in manufacturing environments

Automation systems for monitoring and control are the predominant information sources in man- ufacturing environments. These systems—often comprising hundreds or thousands of interconnected controllers, sensors, actuators, and user interfaces—interoperate with a wide variety of automated machines and pieces of equipment within manufacturing and factory environments. Technologies such as programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, distributed control systems, monitoring and control information systems, and complex event processing tools serve to monitor vital parameters, guarantee production and equipment safety, and control and refine production flows. Recent trends see such systems being complemented by smart sensors that are capable of performing complex computations and behaviors at lower cost. Multi-sensor data fusion and data-driven anomaly detection approaches enable the detection of unforeseen events, facilitating online fault detection in equipment or processes.

Audit systems for utility-scale assets (e.g., energy networks and process industries), on the other hand, have not yet been integrated in a similar way. Rather, many energy and process assets are equipped with disparate systems and devices for sensing, monitoring, and telemetry; fulfil their own functionality in hostile and inaccessible environments; and act as standalone systems for dedicated purposes. Although data from these devices is gathered, correlated, and analyzed in ad hoc manners for specific investigations, the concept of continuous risk- and compliance-oriented audit systems for such facilities has not yet been developed. Recent, yet limited, advances in the Internet of Things (IoT) and Industry 4.0 areas advocate the use of low-cost, smart, distributed sensors for data collection and anomaly detection in such environments.

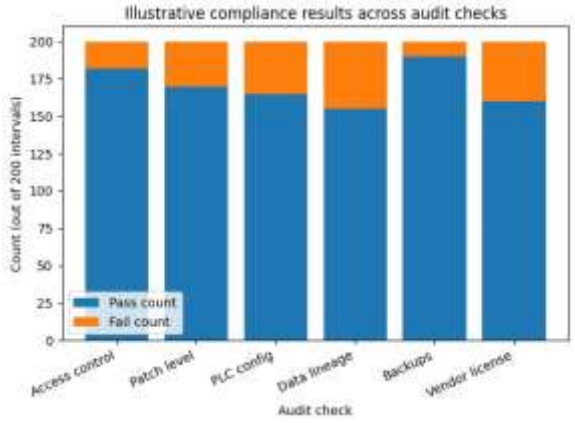
## 4. Data Management and Quality Assurance

Surveys of enterprise data show that up to 90 percent of data is waste. Redundant, inconsistent, and otherwise low-quality data diminish every business function that relies on it, including audits. Therefore, independent, transparent, automated, and regular assessments of the quality of data and systems that underpin audits can create a real impact. Audit problems often arise not from the lack of data but rather from misalignment of signals across the IT landscape. A mismatch of labels of known-good data results in erroneous categorical data, sometimes with dire effects. Ensuring that signs indicate the same thing implies

P-ISSN: 3050-9734
E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 13 ACCEPTED: FEBRUARY 22 PUBLISHED: MARCH15

sending data upstream for better scoring and aligning classification using supervised learning.

No corporate resource today is immune to data-quality updates—from regulatory changes to a cascading, high-impact special event that damages governance and security, compliance, EMS, quality, reliability, execution, and other audits. The intelligent systems governing the direct control of many processes rely on cookies that indicate the health and performance of controllers, as well as cookies on physical equipment that indicate normal and abnormal behavior, such that performance can easily be detected using these signals. Auditors can check that such cookies reside in the expected places, have the correct status, and have proper management protocols and responsibilities defined.




**Equation B. Detection thresholds**

**Assume nominal behavior**

Let $X$ be a metric under normal operation:

$$X \sim \mathcal{N}(\mu, \sigma^2)$$

Given an observation $x$, define the z-score:

$$\boxed{z = \frac{x - \mu}{\sigma}}$$

**Threshold rule**

Flag anomaly if:

$$\boxed{|z| > k}$$

Equivalently:

$$x > \mu + k\sigma \quad \text{or} \quad x < \mu - k\sigma$$

So:

$$\boxed{U = \mu + k\sigma, \qquad L = \mu - k\sigma}$$

**False-alarm rate (why $k$ matters)**

Under normality:

$$\mathbb{P}(|Z| > k) = 2\big(1 - \Phi(k)\big)$$

**4.1. Data integration across heterogeneous systems**

A key goal of autonomous audit intelligence is to provide a high level of assurance that evidence from various operations—compliance with policies, process benchmarks, and designated operational behaviours—has not been tampered with. This assurance is inherently linked to the provenance of the evidence data and metadata. In applied systems where data are acquired from audit sources that focus on different lines of business, operations, or systems of record, the challenge becomes one of integrating these separate data sets. It is highly likely that different technologies and vendors define and maintain these separate systems in their own ways. The challenge of combining these separate data pools depends on provenance.

In environments where multiple operations or systems contribute data for inclusion in a common audit trail, common operational-day segments may be established to enable time-slicing of the data and auditing across the multiple operations or systems. However, when the operations or systems product spans are required to be included, the challenge is one of semantic alignment between the different data pools. It is at the earliest plausible moment in the operational value chain that the surveillance data should be recorded within an evidence repository. In enterprise IT infrastructure, the captured data for operations enabling functions are also becoming increasingly granular. The integrated message bus within

P-ISSN: 3050-9734 E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 13 ACCEPTED: FEBRUARY 22 PUBLISHED: MARCH15

the IT infrastructure becomes a central data feed for continuous security monitoring. Integrating the supply-chain data operations-hosted near real time is also many times possible through the use of common suppliers feeding multiple verticals.

**4.2. Data quality, lineage, and tamper-evidence**

Continuous compliance monitoring can determine whether the current state of any system complies with defined requirements and standards. While this information can be used for inspection or auditing purposes, it is also suitable for detecting anomalies: violations that need to be investigated. Anomalies can involve an immediate security threat or a deterioration of a system within acceptable ranges, which however requires immediate attention to be resolved before exceeding the tolerable limits. The response to an anomaly can be handled independently or by triggering a formal investigation process that makes use of multiple sources of evidence, actors, and dimensions. Implementing continuous compliance monitoring of production infrastructures is critical, yet challenging. It involves environments where both production and maintenance systems play a relevant role. The integration of the information available in the respective systems must therefore account for their heterogeneity, management of data quality, provenance, supervision of data entry and updating, and need for monitoring coverage beyond the physical interconnections already managed by the monitored systems. The specific case of Information Technology–Operational Technology convergence is also relevant: a topic of extensive research and experimentation, involving cloud-based infrastructures, Distributed Ledger Technology, and the integration of physical and virtual layer—a dimension, however, not affording the funnelling of evidence from operations into business, and by-pass auditing over Proprietary Network.

## 5. Operationalizing Autonomous Audits in Manufacturing

The implementation of autonomous audit intelligence in discrete manufacturing and the process industries aims to establish a continuous compliance monitoring capability that uses data provenance to automatically ingest authoritative data sources from across the facility, to monitor these sources for supporting vendor compliance and license limitations, and to direct focused investigative efforts based on the telemetry of other systems affecting operational quality or performance.

The continuous compliance capability grounds subsequent objectives, starting with continual alignment of audit checks with company priorities, supported by engineering and database-aware visualizations. Anomaly detection becomes self-sustaining, with emerging telemetry adaptive to supporting facility operations and enterprise resource planning. Audit support for data generation expands from simple data integrity verifications during synchronizations to full-fledged evidencing of data quality and flow throughout system linage, monitoring data quality with telemetry from command-and-control systems and integrating alert mechanisms that close mismatch loops. Where utilities scale cloud powers operational resource generation, Azure Data Factory operates front-end data movement and telemetry. The fabric underlies the joint auditing of security, management, and business processes supporting a renewed investigation into Microsoft Azure and Power BI usage patterns, building on Microsoft's Azure Data Factory for the large-scale operational support of cloud services across other interested process and chemical engineering case studies.

**5.1. Continuous compliance monitoring**

Many of the aforementioned AI techniques can be deployed to support continuous compliance monitoring tasks in manufacturing environments. Thanks to the availability of process telemetry, control signals, and related documents, it is increasingly common to translate regulatory requirements—such as the US FDA Title 21, Part 11, which assures confidence in electronic records—into formal rules, audit points, and templates that can be continuously monitored and tested for compliance. Rigorously implemented, such automation supports the

P-ISSN: 3050-9734
E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 13 ACCEPTED: FEBRUARY 22 PUBLISHED: MARCH15

business-proof posture concept by allowing an organization to double-check that the required conditions are fulfilled. Detecting and notifying non-fulfillment in real time reduces the burden on personnel and clients while enabling transparent operations.

British Gas, for example, is developing a bank of assurance templates that can be continually monitored, flagged if they are about to fall out of compliance, and automatically and periodically tested by personnel using "robotic process automation" technologies. Automatic firmware and security patch updates on Internet-connected assets are also regularly monitored and evaluated. Changes made on operators' desktops in the wider supply chain are validated by scanning operator registry entries. In the Commonwealth of Virginia's COVID-19 Response and Recovery programs, AI audit agents monitor data collected from programs administering funds made available by the federal CARES Act and identify areas of non-compliance with existing policies and procedures. In another case, a specialized AI agent enables real-time alerting and remediating of vulnerabilities in Azure cloud deployments. More broadly, recent advances in real-time database technologies enable the continuous monitoring of compliance with rules specified in business process modeling-related notations—such as the Business Process Model and Notation (BPMN) language. Recent works also describe the use of a robotic process automation tool to conduct audit tests defined in an audit command language supplied by leading auditors.


**Fig 3: Automated Assurance: AI-Driven Continuous Compliance Monitoring and Business-Proof Governance in Industrial Systems**

**5.2. Anomaly detection and investigative workflows**

Anomaly detection and investigative workflows provide additional capabilities for operationalizing autonomous audits in manufacturing systems. Audit anomalies are identified by comparing actual data with audit requirements and expected data; the audit requirements of the business are defined based on regulations, risks, or industry best practices. Data from compliance checks and other sources can help detect audit violations, and an anomaly detection capability can either use supervised models that recognize specific violations or perform unsupervised detection based on data learning. A general-purpose anomaly detection product can be incorporated into a specific autonomous audit setting.

Anomalies highlighted by these audit-capable tools can serve as input for investigative workflows. Data and model-driven processes can then offer support for translating detected business process anomalies into specific Audit Research Questions that focus on identifying the root cause

P-ISSN: 3050-9734
E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 13 ACCEPTED: FEBRUARY 22 PUBLISHED: MARCH15

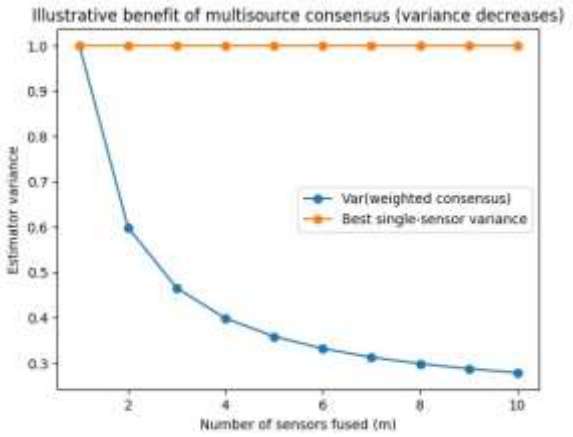
and possible corrective actions. This capability is illustrated through a practical example involving the recommendation or simplification of an investigation for a storage tank fire incident.

## 6. Case Studies and Empirical Evidence

Two case studies highlight the operationalization of autonomous audit intelligence in a discrete manufacturing enterprise and a massively parallel chemical production facility. Discrete Manufacturing. A stealth-mode company that manufactures high-performance semiconductors served as a proof-of-concept facility for autonomous audit intelligence, primarily in the context of risk management for the US Department of Defense. Operating as a subcontractor for a Defence Advanced Research Projects Agency program, the company received a US$92 million injection to demonstrate continuous compliance with a US DOD Cybersecurity Maturity Model Certification Level II. Meeting this standard requires combining people, processes, and technology to prevent cyberattacks or detect them early so that recovery is very quick or the damage is minimal.

An interdisciplinary team drafted a continuous compliance strategy that combines process-centric and risk-centric approaches. The process-centric approach identifies the people, processes, and machines involved in information technology processes. The risk-centric method interrogates technical vulnerabilities using exploitability risk assessment. The union of the two approaches informs audit monitoring, recording, alerting, and reporting decisions. The monitoring, recording, alerting, and reporting functions require technology-based audit volunteers that gather requisite evidence on a routine basis. Autonomous audit intelligence provides a framework for the design and deployment of these audit volunteers.

Utilities and Process Industries. The full generic solution set was instantiated on the massively parallel operations of the Main Water Company of Suez, which provides water in many forms (drinking, industrial, cooling, etc.) for different sectors, including food, textile, energetic, and tourism. Both water and sewage circulate in different treatment avenues according to the final destination required. Assets and operations are monitored by a geographically dispersed, heterogeneous multiservice supervisory control and data acquisition system. Data collection and integration occur in an asset management evolutionary approach. The combination of assurance-based enterprise risk management, continuous assurance, and continuous audit also supports the water operations.




**Equation C. Streaming / real-time thresholds (rolling window)**

AAI emphasizes continuous monitoring and telemetry , so $\mu, \sigma$ must often be estimated online.

For a rolling window of size $W$, at time $t$:

$$\mu_t = \frac{1}{W}\sum_{j=t-W+1}^{t} x_j \;\; \sigma_t = \sqrt{\frac{1}{W-1}\sum_{j=t-W+1}^{t}\left(x_j - \mu_t\right)^2}$$

Then thresholds are:

$$\boxed{U_t = \mu_t + k\sigma_t, \qquad L_t = \mu_t - k\sigma_t}$$

Flag if $x_t \notin [L_t, U_t]$.

### 6.1. Autonomous audits in discrete manufacturing


The use of AI supports autonomous audits of discrete manufacturing assets such as supply and production systems in an automotive factory environment. Operations are replete with constraints, and their violation creates numerous operational incidents. Deviations and incidents typically occur at a low frequency; many lay hidden in large volumes of logs and incident records, though they can have serious long-term impacts or require extensive incident-remediation resources. Monitoring for deviations in real time generally results in excessive false alarms, while delayed investigations are often idle because the conditions driving them no longer hold. Autonomous audits promise to improve these situations by providing just-in-time investigations of incident precursors and root causes. Artificially Intelligent Autonomous Audit Systems reside in the background and continuously examine audit objectives, data, and task execution to improve decision-making, monitoring, and maintenance over time. They learn from human-led investigations of deviations or incidents typical of quality degradation, efficiency decrease, or high resource consumption and provide require-and-supply views of manufacturing operations. Autonomous audits serve as audits a human auditor is not aware of but executes nevertheless. Automating extensive operation monitoring may not be feasible, but a portfolio of autonomous audits can cover the main concerns of deviation and incident monitoring and investigation.

**6.2. Process industries and utility-scale facilities**

Continuous monitoring of emerging data sources—such as digital twin environments and external events, including source code commits—provides organizations operating process industries and utility-scale facilities with a unique opportunity to more efficiently deploy audit resources while maintaining assurance over an up-to-date set of operational processes within a Compliance-as-a-Service model. Such proactive monitoring reduces the overall effort and associated costs of service-oriented auditing activities. Just-in-time triggering of full audits is possible when specific anomalies arise based on the broader context of assets whose underlying status has changed. Information technology-based techniques also have an important role to play in more granular monitoring of alert-like conditions identified by sensors in the physical world.

The DevOps change management paradigm, applied in manufacturing environments where hardware change is not a regular occurrence, combined with virtualization, infrastructure-as-code, continuous integration/continuous deployment, and other techniques, identifies configuration status that is different from expected values. These alerts catalyze further investigation by specialized team members, drawing on not only technology-based information but enabling human intelligence to evaluate process changes and external events too. Within process-oriented environments, such alarm-like anomalies correspond to the velocity dimension of Big Data. This provides much deeper and more precise examination than the traditional anemic audit checklist approach on a 12- or 18-month cycle.

## 7. Conclusion

Integrating research in information systems security and assurance, data quality, data provenance, continuous auditability, and artificial intelligence yields Autonomous Audit Intelligence (A2I) for continuous oversight of cyber-physical manufacturing infrastructure and processes. Aerospace, automotive, and other discrete manufacturers are adopting Computer Numerical Control (CNC) systems with integrated computing and communication; complex embedded systems; and complex supply chains, deploying a Continuous Digital Thread (CDT) that facilitates cyber-physical convergence, where internal and external systems are integrated. Simultaneously, new legislation demands continuous compliance, monitoring, and reporting of the trading and environmental performance of product-realizing services and infrastructures. A2I enables Audit-as-a-Service of Infrastructure-as-Code, focused primarily on data quality and privacy, to enhance CAIQ and CAIS. Software agents that audit based on rules and roles defined in the blockchain of the Integrated Digital Environment (IDE) of a Digital Pilot Plant (DPP) realize a Digital Twin Enterprise (DTE). Empirical evidence from the DTE of a Baden-Württemberg-based German supplier to the

P-ISSN: 3050-9734
E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 13 ACCEPTED: FEBRUARY 22 PUBLISHED: MARCH15

aerospace industry, and the Integrated Instrumentation Architecture (IIA) of the Digital Twin Laboratory (DTL) of an Indian utility-scale wind energy developer, further empirically validate Autonomous Audit Intelligence for manufacturing, Continuous Auditability of Cyber-Physical Systems, and Audit-as-a-Service of Manufacturing Infrastructure as Autonomous Audit Intelligence-as-a-Service.

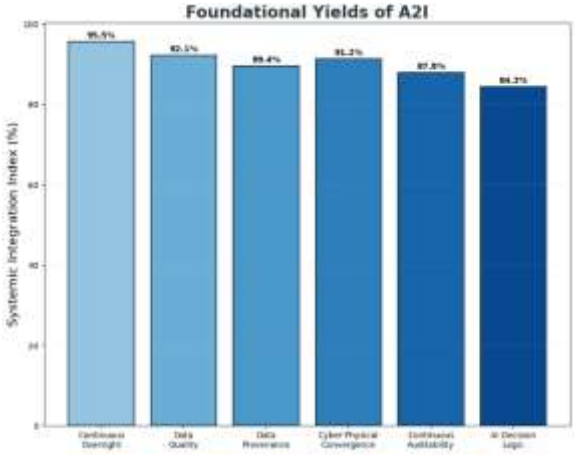



**Fig 4: Foundational Yields of A2I**

**7.1. Summary of Findings and Future Directions**

Autonomous Audit Intelligence for Manufacturing Infrastructure presents an overview of the study, followed by theoretical foundations and definitions. Core methodologies for auditing are described, and an architectural framework proposed. Sections then cover data acquisition, provenance and quality, integration across heterogeneous systems, and operationalization in manufacturing. Continuous compliance monitoring and anomaly detection are explored, with empirical evidence from discrete manufacturing, process industries, and utility-scale facilities.

As data proliferates in manufacturing infrastructure and autonomous systems, new data quality challenges arise, together with opportunities for intelligent analysis. Autonomous Audit Intelligence routinely checks that data sources and sinks, as well as data provenance, support system requirements. Autonomous Audit Intelligence delivers evidence-based insights about these checks, detecting data quality issues and supporting operational investigations. Closed-loop solutions apply such insights in real time, while open-loop implementations introduce new audit workflows. Automated or semiautomated audit approaches are termed Autonomous Audit Intelligence.

## 8. References

1. Lee, C., & Lim, C. (2021). From technological development to social advance: A review of Industry 4.0 through machine learning. Technological Forecasting and Social Change, 167, 120653.
2. Mi, S., Feng, Y., Zheng, H., Wang, Y., Gao, Y., & Tan, J. (2021). Prediction maintenance integrated decision-making approach supported by digital twin-driven cooperative awareness and interconnection framework. Journal of Manufacturing Systems, 58, 329–345.
3. Kolla, S. H., & Mattaparthi, R. (2025). Hybrid Gen AI Systems: Integrating Small LMs with Large Language Models for Cost-Efficient Enterprise Automation and Decision Intelligence. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(6), 13345-13357.
4. Savolainen, J., & Urbani, M. (2021). Maintenance optimization for a multi-unit system with digital twin simulation: Example from the mining industry. Journal of Intelligent Manufacturing, 32, 1953–1973.
5. Wang, Y., Tao, F., Zhang, M., Wang, L., & Zuo, Y. (2021). Digital twin enhanced fault prediction for the autoclave with insufficient data. Journal of Manufacturing Systems, 60, 350–359.
6. Magnanini, M. C., & Tolio, T. A. M. (2021). A model-based Digital Twin to support responsive manufacturing systems. CIRP Annals, 70(1), 353–356.
7. Zhai, S., Gehring, B., & Reinhart, G. (2021). Enabling predictive maintenance integrated production scheduling by operation-specific health prognostics

P-ISSN: 3050-9734 E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 13 ACCEPTED: FEBRUARY 22 PUBLISHED: MARCH15

with generative deep learning. Journal of Manufacturing Systems, 61, 830–855.
8. Davuluri, P. S. L. (2023). AI-Augmented Sanctions Screening: Enhancing Accuracy and Latency in Real Time Compliance Systems. AI-Augmented Sanctions Screening: Enhancing Accuracy and Latency in Real Time Compliance Systems (December 15, 2023).
9. Wu, J.-Y., Wu, M., Chen, Z., Li, X., & Yan, R. (2021). A joint classification-regression method for multi-stage remaining useful life prediction. Journal of Manufacturing Systems, 58, 109–119.
10. Kim, S. W., Kong, J. H., Lee, S. W., & Lee, S. (2022). Recent advances of artificial intelligence in manufacturing industrial sectors: A review. International Journal of Precision Engineering and Manufacturing, 23, 111–129.
11. Tercan, H., & Meisen, T. (2022). Machine learning and deep learning based predictive quality in manufacturing: A systematic review. Journal of Intelligent Manufacturing, 33, 1879–1905.
12. Xia, L., Zheng, P., Li, X., Gao, R. X., & Wang, L. (2022). Toward cognitive predictive maintenance: A survey of graph-based approaches. Journal of Manufacturing Systems, 64, 107–120.
13. Reddy.V.A.R Domain-Driven Design in Enterprise Healthcare Applications: A Practitioner's Analysis. J Rare Cardiovasc Dis. 2025;5(3):402–422.
14. Zonta, T., da Costa, C. A., Zeiser, F. A., Ramos, G. de O., Kunst, R., & Righi, R. da R. (2022). A predictive maintenance model for optimizing production schedule using deep neural networks. Journal of Manufacturing Systems, 62, 450–462.
15. Zhu, Q., Huang, S., Wang, G., Moghaddam, S. K., Lu, Y., & Yan, Y. (2022). Dynamic reconfiguration optimization of intelligent manufacturing system with human-robot collaboration based on digital twin. Journal of Manufacturing Systems, 65, 330–338.
16. Naqvi, S. M. R., Ghufran, M., Meraghni, S., Varnier, C., Nicod, J.-M., & Zerhouni, N. (2022). Human knowledge centered maintenance decision support in digital twin environment. Journal of Manufacturing Systems, 65, 528–537.
17. Liang, Z., Wang, S., Peng, Y., Mao, X., Yuan, X., Yang, A., & Yin, L. (2022). The process correlation interaction construction of Digital Twin for dynamic characteristics of machine tool structures with multi-dimensional variables. Journal of Manufacturing Systems, 63, 78–94.
18. Arnarson, H., Mahdi, H., Solvang, B., & Bremdal, B. A. (2022). Towards automatic configuration and programming of a manufacturing cell. Journal of Manufacturing Systems, 64, 225–235.
19. Müller, D., März, M., Scheele, S., & Schmid, U. (2022). An interactive explanatory AI system for industrial quality control. Proceedings of the AAAI Conference on Artificial Intelligence, 36(11), 12580–12586.
20. Sridhar Mahadevan. (2024). Intelligent Serverless Process Automation for Scalable Cloud Operations and Dynamic Resource Optimization. Journal of Computational Analysis and Applications (JoCAAA), 33(06), 4207–4221. Retrieved from https://www.eudoxuspress.com/index.php/pub/article/view/5787
21. Maddikunta, P. K. R., Pham, Q.-V., Prabadevi, B., Deepa, N., Dev, K., Gadekallu, T. R., Ruby, R., & Liyanage, M. (2022). Industry 5.0: A survey on enabling technologies and potential applications. Journal of Industrial Information Integration, 26, 100257.
22. Fordal, J. M., Schjølberg, P., Helgetun, H., Skjermo, T. Ø., Wang, Y., & Wang, C. (2023). Application of sensor data based predictive maintenance and artificial neural networks to enable Industry 4.0. Advances in Manufacturing, 11, 248–263.
23. Mypati, O., Mukherjee, A., Mishra, D., Pal, S. K., Chakrabarti, P. P., & Pal, A. (2023). A critical review on applications of artificial intelligence in manufacturing. Artificial Intelligence Review, 56(S1), 661–768.
24. Castañé, G., Dolgui, A., Kousi, N., Meyers, B., Thevenin, S., Vyhmeister, E., & Östberg, P.-O. (2023). The ASSISTANT project: AI for high level

P-ISSN: 3050-9734 E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 13 ACCEPTED: FEBRUARY 22 PUBLISHED: MARCH15

decisions in manufacturing. International Journal of Production Research, 61(7), 2288–2306.
25. Farahani, M. A., McCormick, M. R., Gianinny, R., Hudacheck, F., Harik, R., Liu, Z., & Wuest, T. (2023). Time-series pattern recognition in Smart Manufacturing Systems: A literature review and ontology. Journal of Manufacturing Systems, 69, 208–241.
26. Zhang, M., Tao, F., Zuo, Y., Xiang, F., Wang, L., & Nee, A. Y. C. (2023). Top ten intelligent algorithms towards smart manufacturing. Journal of Manufacturing Systems, 71, 158–171.
27. Liu, S., Bao, J., & Zheng, P. (2023). A review of digital twin-driven machining: From digitization to intellectualization. Journal of Manufacturing Systems, 67, 361–378.
28. Xiao, Y., Zheng, S., Shi, J., Du, X., & Hong, J. (2023). Knowledge graph-based manufacturing process planning: A state-of-the-art review. Journal of Manufacturing Systems, 70, 417–435.
29. Loganathan, R. (2025). AGENTIC AI FRAMEWORKS FOR AUTONOMOUS RISK DETECTION AND COMPLIANCE REMEDIATION IN ENTERPRISE DATA CENTER OPERATIONS. Lex Localis-Journal of Local Self-Government, 23 (S6), 9672–9697.
30. Gunraj, H., Guerrier, P., Fernandez, S., & Wong, A. (2023). SolderNet: Towards trustworthy visual inspection of solder joints in electronics manufacturing using explainable artificial intelligence. Proceedings of the AAAI Conference on Artificial Intelligence, 37(13).
31. Alexander, Z., Chau, D. H. P., Saldaña, C., & others. (2024). An interrogative survey of explainable AI in manufacturing. IEEE Transactions on Industrial Informatics, 20(5), 7069–7081.
32. Gao, R. X., Krüger, J., Merklein, M., Möhring, H.-C., & Váncza, J. (2024). Artificial intelligence in manufacturing: State of the art, perspectives, and future directions. CIRP Annals, 73(2), 723–749.
33. Liu, Z., Lang, Z.-Q., Gui, Y., Zhu, Y.-P., & Laalej, H. (2024). Digital twin-based anomaly detection for real-time tool condition monitoring in machining. Journal of Manufacturing Systems, 75, 163–173.
34. Li, D., Liu, S., Wang, B., Yu, C., Zheng, P., & Li, W. (2025). Trustworthy AI for human-centric smart manufacturing: A survey. Journal of Manufacturing Systems, 78, 308–327.
35. Keramati Feyz Abadi, M. M., Liu, C., Zhang, M., Hu, Y., & Xu, Y. (2025). Leveraging AI for energy-efficient manufacturing systems: Review and future prospectives. Journal of Manufacturing Systems, 78, 153–177.