OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Cognitive Manufacturing: A Hybrid AI-Kepner Tregoe Framework for Predictive Root Cause Analysis in Saudi Arabia's Industry 4.0"

Ramy Abdelmonem Matrawy

Abstract
Background: *Saudi Arabia isn't just upgrading its industrial sector; it is completely rewriting the operational blueprint. Driven by the National Industrial Development and Logistics Program (NIDLP), the push toward Industry 4.0 has placed advanced smart factories at the heart of Vision 2030. These facilities rely entirely on the Industrial Internet of Things (IIoT) and Artificial Intelligence (AI) for predictive maintenance. The problem? AI is largely a "black box." It flags anomalies but rarely explains the logic behind them. This forces engineers into a dangerous cycle: executing costly, unjustified production halts or ignoring critical warnings. Furthermore, merging operational technology (OT) with IT networks exposes sensitive industrial databases to unprecedented cyber risks.*
Objective: *Relying solely on automated AI predictions in high-stakes manufacturing is a critical vulnerability. This paper introduces a customized operational model: the "Hybrid AI-Kepner Tregoe Framework for Predictive Root Cause Analysis (AI-KT PRCA)." The goal is to build a bridge between algorithmic anomaly detection and human rational logic. This ensures that industrial anomalies are verified, resolved, and secured against global IT standards before a multi-million riyal assembly line is shut down.*
Methodology: *Using a qualitative constructive approach, this study evaluates the friction points between AI in manufacturing, the Kepner-Tregoe (KT) rational decision-making process, ITIL Service Operation principles, and ISO/IEC 27001 data security standards within the Saudi context. The proposed AI-KT PRCA framework is then pressure-tested against three archetypal case studies drawn from the realities of Saudi Arabia's advanced manufacturing, petrochemical, and automated logistics sectors.*
Results: *The analysis reveals a stark contrast. Purely AI-driven responses frequently trigger false positives, leading teams to replace expensive hardware when the actual culprit is a software glitch. By applying the AI-KT PRCA framework, engineering teams gain a structured mechanism to bypass the physical symptoms and uncover the true root causes—whether that is a latent SQL database sync error, a corrupted firmware update, or a localized network intrusion.*
Conclusion: *Establishing a formal, hybrid approach to Root Cause Analysis is no longer just an operational upgrade; it is a strategic necessity for the "Year of AI 2026." By integrating human cognitive governance with machine learning, the Kingdom can secure its industrial data pipelines, maximize operational efficiency, and build the investor confidence required to realize its industrial future.*
Keywords: *Artificial Intelligence, Kepner-Tregoe, Root Cause Analysis (RCA), Saudi Vision 2030, Industry 4.0, ISO/IEC 27001, ITIL, Smart Factories.*

Date of Submission: 11-04-2026 Date of acceptance: 23-04-2026

I. Introduction

1.1. The Shift to Digital Industry Under Vision 2030, Saudi Arabia is engineering a massive pivot from a resource-dependent economy to a technology-driven industrial powerhouse. Initiatives like "Project Transcendence" and the development of next-generation hubs like NEOM's Oxagon represent a staggering deployment of Industry 4.0 tech. In these environments, thousands of sensors constantly stream data back to central Microsoft SQL Server databases, generating living "Digital Twins" of the physical plants. We ask AI to monitor these massive data pipelines and predict when a machine is going to fail. But when a modern assembly

line spans both mechanical engineering and complex IT networks, a single anomaly could be a worn bearing, a network latency spike, or a cyber intrusion.

1.2. The "Black Box" Problem The default way most automated facilities handle maintenance right now is fundamentally flawed. When an AI algorithm detects a potential failure, the standard protocol is usually to swap out the flagged hardware to avoid downtime. This creates a dangerous loop. Imagine an AI flags a vibration in a robotic arm. The maintenance team replaces the motor. But what if the root cause wasn't mechanical at all? What if a poorly executed ITIL-managed firmware update altered the machine's torque calibration? Because the AI only sees the physical symptom, the actual problem is ignored. The new motor receives the exact same corrupted update, the vibration returns, and the facility bleeds capital replacing perfectly good hardware. We cannot run billion-riyal infrastructure on AI predictions that lack rational explainability.

1.3. The Vicious Cycle of Reactive Maintenance The traditional incident management loop in manufacturing prioritizes speed above all else: get the line running again. However, when applied to highly digitized environments, this reactive approach creates a costly cycle:

1. An AI system predicts an anomaly (e.g., abnormal vibration).
2. The maintenance team replaces the physical part to prevent downtime.
3. The underlying root cause (e.g., a software bug) remains untouched because the team treated the symptom, not the disease.
4. The exact same failure reoccurs. This reactive loop wastes physical resources, degrades trust in AI systems, and leaves the facility vulnerable to identical failures.

1.4. Research Objectives and Scope Breaking this cycle requires a disciplined approach that marries the raw processing power of machine learning with structured human logic. The specific objectives of this research are:

1. To critically differentiate between purely automated AI predictions and rationally verified Predictive Root Cause Analysis (PRCA).
2. To review the integration of the Kepner-Tregoe (KT) methodology alongside modern IT Service Management (ITIL V3) and Information Security (ISO 27001) frameworks.
3. To propose a specialized framework, the "Hybrid AI-KT PRCA," tailored for the Saudi industrial ecosystem.
4. To rigorously demonstrate the worth of the framework via extensive, realistic case studies.
5. To analyze the strategic fit of this framework with Vision 2030 and SDAIA objectives, discussing implementation challenges.

II. Literature Review

2.1. Explainable AI and the Kepner-Tregoe Methodology Machine learning algorithms are incredible at finding patterns hidden in noise. But they fail at context. When a decision could cost millions of riyals in halted production, "the algorithm said so" is not an acceptable justification. The Kepner-Tregoe (KT) methodology provides the missing piece. As a globally recognized process for rational decision-making, KT forces investigators to systematically specify the exact parameters of a problem: *What* is the issue? *Where* is it happening? *When* did it start? What is its *Extent*? While current literature heavily covers AI in manufacturing, using KT's structured "Situation Appraisal" and "Problem Analysis" as a cognitive governance layer over AI outputs is a uniquely effective way to solve the AI explainability dilemma.

2.2. Merging ITIL, OT, and the Factory Floor In the past, the factory floor (Operational Technology or OT) and the server room (Information Technology or IT) were entirely separate worlds. Industry 4.0 crushes that divide. Today, an industrial robotic arm is essentially an IT service endpoint. Therefore, ITIL V3 Service Operation principles—specifically Problem Management, which seeks the root cause of software incidents to prevent them from happening again—must physically extend to the machinery. The literature indicates a massive gap in operational frameworks that can seamlessly apply ITIL software problem management to physical IIoT anomalies.

2.3. Information Security (ISO 27001) in Industrial Data The lifeblood of any predictive AI model is data. The Saudi National Cybersecurity Authority (NCA) mandates strict controls over critical infrastructure because compromised data leads to compromised AI. ISO/IEC 27001 serves as the international standard for Information Security Management Systems. In the context of predictive maintenance, ISO 27001 is critical. If the SQL database feeding the AI is breached or altered by a cyber threat, the resulting AI predictions are entirely invalid. Proactive Problem Management must include continuous auditing of data integrity.

III. The Hybrid AI-KT PRCA Framework

To bridge the gap between AI prediction and rational resolution, this paper presents the AI-KT PRCA framework. It is a four-stage, cyclical model designed specifically for the complexities of modern Saudi smart factories.

3.1. Phase 1: AI-Driven Anomaly Detection (The Trigger) This is the entry point, relying on machine processing power to do the heavy lifting.

- **Continuous Monitoring:** IIoT sensors feed real-time operational data into SQL databases.
- **Predictive Flagging:** AI algorithms analyze trends and flag deviations from the digital baseline (e.g., thermal increases, data packet loss, synchronization delays).
- **Output:** The AI generates a Predictive Alert, indicating a high probability of failure. Crucially, it does not automatically initiate a physical shutdown.

3.2. Phase 2: Kepner-Tregoe Problem Analysis (The Human Verification) This is the analytical core where engineers intercept the AI alert to find the true root cause.

- **Specification (IS vs. IS NOT):** The team uses KT to define the anomaly. *What* exactly is the AI flagging? *Where* is it occurring (which specific assembly line)? *When* did the data baseline shift?
- **Distinction and Change Analysis:** The team looks for changes mathematically correlated with the anomaly. If the AI flagged Line A but not Line B, what is distinct about Line A?
- **Hypothesis Testing:** The team tests potential causes against the KT specification. For example: "If the root cause is a worn mechanical bearing, why did the thermal increase happen instantaneously, precisely at 03:00 AM, immediately after an automated network patch?"

3.3. Phase 3: Resolution, ITIL Service Operation, and ISO 27001 Compliance Once the true root cause is rationally identified, this stage dictates the remediation.

- **Error Control:** If the issue is software-based (e.g., a flawed configuration), an ITIL Change Management request is formally raised to roll back or patch the system safely.
- **Security Auditing:** If the root cause involved unauthorized access or corrupted data schemas, ISO 27001 incident response protocols are triggered to quarantine the affected SQL database segment and conduct a forensic review.
- **Workarounds:** A Known Error Record is created in the ITIL database to speed up future resolutions while permanent architectural fixes are deployed.

3.4. Phase 4: Machine Learning Optimization (The Feedback Loop) The final stage ensures the AI system learns from human rational logic.

- **Algorithm Tuning:** The AI is updated with the KT-verified root cause. It learns to differentiate between a mechanical thermal increase and a software-induced thermal increase.
- **Systemic Prevention:** The verified findings are shared across the industrial network, updating preventive maintenance schedules and IT access policies across the entire manufacturing ecosystem.

IV. Illustrative Case Study Analysis

To demonstrate the framework's practical applicability, we analyze three archetypal scenarios in Saudi Arabia's industrial landscape, comparing traditional incident responses against the AI-KT PRCA framework.

Case Study 1: Predictive Anomaly in an Oxagon Advanced Component Plant

- **Scenario:** An AI monitoring system in a NEOM Oxagon facility predicts an 85% chance of imminent failure in a critical robotic assembly arm due to abnormal micro-vibrations.
- **Traditional Response:** * *Action:* The production line is immediately halted. Engineers physically replace the robotic arm's servo motors.
    - *Outcome:* It costs $50,000 in parts and $200,000 in lost production time. 48 hours later, the new arm exhibits the exact same vibration. The root cause was entirely missed.
- **AI-KT PRCA Application:**
    - *Phase 1:* The AI flags the vibration.
    - *Phase 2 (KT):* Engineers apply the Kepner-Tregoe process. The specification reveals the vibration *IS* occurring on Arm 4, but *IS NOT* occurring on Arms 1-3. It started precisely at 00:15 AM. The distinction? Arm 4 is the only unit that received an over-the-air firmware update at midnight.

- *Phase 3:* The root cause is identified as a software calibration error, not a hardware failure. An ITIL service rollback is executed. Total cost: zero dollars in parts, 15 minutes of scheduled downtime.
- *Phase 4:* The AI is retrained to cross-reference firmware update logs against vibration signatures before issuing future alerts.

Case Study 2: Database Latency in a Jubail Petrochemical Facility

- **Scenario:** AI detects a critical delay in pressure valve response times across a major refinery, predicting an imminent physical over-pressurization event.
- **Traditional Response:**
  - *Action:* Emergency physical venting protocols are triggered. Maintenance teams dismantle and inspect the physical pneumatic valves, finding absolutely no mechanical faults.
  - *Outcome:* The facility suffers massive production disruption and the flaring of valuable chemicals, yet the underlying system latency remains unresolved.
- **AI-KT PRCA Application:**
  - *Phase 1:* AI flags the response delay.
  - *Phase 2 (KT):* KT analysis reveals the delay *IS* affecting all valves globally, but *IS NOT* localized to any specific physical sector. The key distinction is that the latency correlates exactly with a scheduled backup of the central SQL Server database.
  - *Phase 3:* Utilizing ISO 27001 audit controls, the team discovers that a recent, unapproved change to the SQL indexing caused the database to lock during backups, delaying the IT-to-OT signal transmission.
  - *Phase 4:* Database indexing is corrected under ITIL Change Management. The AI is updated to monitor SQL server load balancing as a precursor to physical valve latency.

Case Study 3: Data Integrity Breach in an Automated Logistics Hub

- **Scenario:** In a fully automated port facility on the Red Sea, AI flags erratic behavior in autonomous guided vehicles (AGVs), suggesting rapid sensor degradation.
- **Traditional Response:**
  - *Action:* AGVs are continuously pulled from service for sensor recalibration, reducing port throughput by 30%.
  - *Outcome:* Recalibrated AGVs return to service but continue to exhibit erratic routing, causing logistical bottlenecks.
- **AI-KT PRCA Application:**
  - *Phase 1:* AI flags AGV routing anomalies.
  - *Phase 2 (KT):* KT specifies that the erratic behavior only occurs when AGVs enter Sector 4. The physical sensors are identical to those in Sector 3.
  - *Phase 3:* Investigation shifts away from physical sensors and toward data integrity. ISO 27001 protocols reveal that a compromised edge server in Sector 4 is feeding corrupted spatial coordinates to the AGV's SQL-based routing tables. The root cause is a localized cyber intrusion, not failing hardware.
  - *Phase 4:* The compromised server is isolated and patched. The AGVs immediately resume normal operation. The AI is integrated with SIEM (Security Information and Event Management) to cross-reference physical anomalies with network security alerts.

V. Discussion: Strategic Implications for Vision 2030

The institution of a mature AI-KT PRCA discipline has profound strategic implications that directly impact the Kingdom's national goals.

5.1. Realizing the "Year of AI 2026" Objectives The Saudi Data and AI Authority (SDAIA) strongly emphasizes the concept of "Responsible AI." The integration of Kepner-Tregoe provides the necessary cognitive governance to make industrial AI explainable and accountable. By ensuring that algorithmic predictions are subjected to rigorous human rational analysis before executing critical operational changes, this framework builds trust in automation. That trust is a strict prerequisite for the broader adoption of AI across the Kingdom's economy.

5.2. Maximizing OPEX Efficiency in NIDLP Projects The National Industrial Development and Logistics Program aims to transform Saudi Arabia into a leading global industrial powerhouse. This requires maximizing the uptime of incredibly expensive, high-tech manufacturing assets. As demonstrated in the case studies, purely reactive or unverified AI responses lead to wasted capital expenditure on unnecessary hardware replacements.

The PRCA framework drastically reduces Operational Expenditure (OPEX) by pinpointing the true—often software-based or network-based—root causes of industrial anomalies.

5.3. Challenges in Implementation Transitioning to this hybrid model presents very specific challenges:

- **The IT/OT Skills Gap:** The framework requires professionals who understand both physical engineering (electronic engineering, OT) and sophisticated IT service management (SQL, ITIL, ISO 27001). Developing cross-trained "Digital Industrial Architects" is a critical human capital challenge for Saudi universities and enterprises.
- **Cultural Resistance to Rational Process:** In high-pressure manufacturing environments, there is an immense temptation to "just trust the AI" or "just replace the part." Enforcing the discipline of taking the time to run a Kepner-Tregoe analysis requires strong leadership. It demands a systemic shift in organizational culture from reactive firefighting to proactive, logical investigation.

VI. Conclusion

The digital industrial revolution driving Saudi Vision 2030 presents an unprecedented opportunity to leapfrog traditional manufacturing paradigms. However, deploying AI without a structured framework for logical validation and data security creates fragile ecosystems prone to costly, misdiagnosed disruptions.

This research establishes that integrating the Kepner-Tregoe rational process with AI predictive models, governed heavily by ITIL and ISO 27001 standards, provides the optimal operational architecture for Industry 4.0. The Proactive Root Cause Analysis (PRCA) framework empowers engineers to move beyond the physical symptoms of mechanical failure to uncover complex systemic, digital, and cybersecurity root causes.

A culture of forward-thinking problem-solving is the operational engine that will safeguard the Kingdom's industrial assets. This hybrid approach ensures that the advanced smart factories being built from Jubail to NEOM are not only highly automated but resilient, secure, and economically efficient, firmly supporting the ambitious horizons of Vision 2030.

References

[1]. AXELOS. (2011). *ITIL Service Operation: ITIL V3 Edition*. TSO (The Stationery Office).
[2]. International Organization for Standardization. (2022). *ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems*.
[3]. Kepner, C. H., & Tregoe, B. B. (1981). *The New Rational Manager*. Princeton Research Press.
[4]. National Cybersecurity Authority (NCA), Kingdom of Saudi Arabia. (2022). *Essential Cybersecurity Controls (ECC-1: 2022)*. Retrieved from nca.gov.sa.
[5]. National Industrial Development and Logistics Program (NIDLP). (2023). *Accelerating the Fourth Industrial Revolution in the Kingdom: A Strategic Overview*. Vision 2030 Publications.
[6]. Saudi Data & AI Authority (SDAIA). (2024). *National Principles for Artificial Intelligence Ethics and Explainability in Industrial Applications*.
[7]. Al-Zahrani, K., & Smith, J. (2023). Integrating Information Security (ISO 27001) in Industry 4.0: Challenges in Saudi Arabian Smart Factories. *Journal of Industrial Information Integration*, 12(4), 315-330.
[8]. Vision 2030, Kingdom of Saudi Arabia. *Official Website and Documentation*. Retrieved from vision2030.gov.sa.