



HARNESSING ARTIFICIAL INTELLIGENCE AND DATA ANALYTICS IN THE SECURITY INDUSTRY TO REDUCE COST DRIVERS AND MEAN TIME TO RESPOND (MTTR): A CASE STUDY OF PT ARA DELVIN

Aled

Institut Teknologi Bandung, Bandung, Indonesia

aled.repository@gmail.com

Abstract

The Indonesian private security industry is undergoing rapid transformation as clients increasingly demand faster response times, greater operational transparency, and visible technological capabilities embedded in service delivery. This study examines how PT ARA DELVIN, a leading integrated security service provider, can leverage Artificial Intelligence (AI), Internet of Things (IoT), and data analytics to address its key cost drivers and reduce its Mean Time to Respond (MTTR). Despite its strong market position, the company's daily operations remain heavily dependent on manpower and rely on a fragmented set of monitoring systems supplied by different vendors that do not integrate with one another. As a result, the current MTTR ranges from 32 to 37 minutes, substantially exceeding the internal target of 17 minutes. The main cost drivers identified include manpower dependency, fragmented multi-vendor systems, manual SROC–field coordination, and limited use of predictive analytics. This study employs an exploratory qualitative case study approach supplemented by a quantitative layer based on the Technology Acceptance Model (TAM) to assess user readiness, while the Define–Measure–Analyze–Improve–Control (DMAIC) framework structures the diagnostic process. Primary data were collected through semi-structured interviews, focus group discussions, field observations, and a structured questionnaire administered to fifty respondents across SROC operators, field coordinators, and management. Internal incident logs, alarm reports, MTTR records, and maintenance logs were reviewed to triangulate the findings. The analysis identifies four core problems: high manpower dependency that inflates the largest cost driver, fragmented multi-vendor systems that prevent integration, manual coordination between the Security Risk Operations Center (SROC) and field teams that lengthens MTTR, and the limited use of predictive analytics that keeps operations reactive. The proposed solution centers on a single integrated platform connecting alarm systems, CCTV, IoT sensors, and access control under one dashboard, complemented by automated dispatching, real-time alerts, mobile reporting, and predictive analytics. The expected impact is twofold: a reduction in the main operational cost drivers and a significant improvement in MTTR toward the 17-minute internal target.

Keywords: Artificial Intelligence; Data Analytics; Cost Drivers; Mean Time to Respond (MTTR); DMAIC; Technology Acceptance Model; Integrated Security Platform

INTRODUCTION

The security industry across Indonesia faces accelerating change driven by rising threats, economic expansion, and growing customer demand for immediate protection services in major cities such as Jakarta. Traditional manned security services have become increasingly expensive for organizations operating within constrained budgets, particularly small and medium-sized enterprises (SMEs) that require cost-efficient security solutions. At the same time, the Asia-Pacific (APAC) security market continues to expand, growing from approximately USD 192 billion in 2021 to USD 239 billion in 2024, an annual growth rate of roughly 8% (CAGR). The Indonesian market alone is forecast to reach USD 7.1 billion in 2025, comprising USD 4.7 billion in guarding services and USD 2.4 billion in technology-enabled security, underscoring the country's continued reliance on physical guarding while signaling the early stages of a digital transition.

PT ARA DELVIN, part of ARA DELVIN Global Group, operates as one of the largest integrated security companies in Indonesia, delivering manned guarding services, integrated electronic systems, risk management, and professional engineering solutions. However, its current operations depend on separate systems that require substantial human intervention for monitoring. The Security Risk Operations Center (SROC) and field teams experience communication breakdowns because the organization lacks a single digital platform, resulting in delayed incident responses and difficulty managing sites with heterogeneous security devices.

Security customers today expect immediate responses, precise situational awareness, and complete reporting transparency. The integration of IoT, AI, cloud computing, and data analytics offers an opportunity to transform security operations from a reactive posture toward predictive, technology-enabled service delivery. For PT ARA DELVIN, such a transformation is critical to preserving market leadership while supporting the broader strategy of building security systems grounded in data analytics. This study therefore investigates how the company can adopt AI and data analytics to reduce its cost drivers and improve its MTTR.

This article is organized as follows. Section 2 reviews the relevant literature and theoretical foundations, including cost drivers in service organizations, the Technology Acceptance Model (TAM), Lean wastes, Process Integration Theory, and the Digital Transformation Maturity model. Section 3 describes the research methodology, including the rationale for the mixed qualitative–quantitative case study design and the application of the DMAIC framework. Section 4 presents the results and discussion, organized around the diagnostic findings, the TAM assessment, and the proposed business solution. Section 5 concludes with managerial implications, limitations, and directions for future research.

REVIEW OF LITERATURE

Cost Drivers in Service Organizations

Identifying cost drivers is essential for organizations pursuing operational efficiency and activity-based cost management. In security and similar service industries, costs are shaped by manpower requirements, technology, training needs, and operational complexity. In most cases, labor constitutes the largest cost component due to continuous staffing, supervision, and regulatory compliance. The overall cost structure is further influenced by system maintenance, equipment costs, and the integration of digital platforms. By identifying

these drivers, security firms can pinpoint areas for optimization and design solutions that balance cost efficiency with service reliability (Horngren et al., 2021).

Integrated Security Systems and the Internet of Things

The private security industry is undergoing rapid digital transformation driven by the need for real-time surveillance, integrated monitoring, and efficient resource deployment. Literature on security operations consistently notes that traditional guarding models face limitations, particularly in environments with rising labor costs, device heterogeneity, and manual procedures. Westerman et al. (2014) observe that organizations relying on stand-alone systems struggle to remain operationally efficient because of limited situational awareness and slower decision-making caused by fragmented technologies. In a security context, when CCTV, alarms, and access control are not integrated, operators face information overload and elevated cognitive burden. PT ARA DELVIN's challenge of disconnected systems reinforces the need for unified platforms.

Artificial Intelligence and Data Analytics

Artificial intelligence and data analytics increasingly enable organizations to shift from reactive to predictive operations. In security, AI-based video analytics can automate alarm verification and filter false alarms, reducing operator workload and accelerating response. Predictive analytics, drawing on historical incident and sensor data, allows organizations to anticipate events rather than merely react to them. Davenport and Harris (2017) argue that competing on analytics requires embedding data-driven decision-making into core operational processes, which aligns directly with the transformation PT ARA DELVIN seeks.

Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) explains user adoption of new technologies through two principal constructs: Perceived Usefulness (PU) and Perceived Ease of Use (PEOU), which together shape Behavioral Intention (BI) to adopt. In a labor-intensive organization such as PT ARA DELVIN, where frontline operators and guards must adopt new digital tools, assessing technology readiness is essential. A solution that is technically sound but poorly accepted by its intended users will fail in practice, making TAM a critical complement to the operational diagnosis.

Lean Seven Wastes and Process Integration Theory

The identification of Lean waste aligns closely with the Measure and Analyze stages of the DMAIC methodology. Categorizing waste helps identify operational delays, rework, and points of manual dependency. Studies show that Lean waste reduction supported by digital technology, automation, IoT sensors, and integrated systems can deliver substantial performance improvements. Process Integration Theory further argues that combining disparate monitoring platforms into a single operational interface provides operators with a single source of truth and reduces cognitive overload. For PT ARA DELVIN, digital integration removes unnecessary manual work, shortens processing times, and makes security operations more efficient and less costly.

Digital Transformation Maturity

The literature on digital transformation maturity confirms that traditional-industry organizations advance slowly when they lack integrated systems and standardized workflows. Westerman et al. (2014) describe the maturity phases through which firms must progress, suggesting that reaching higher levels of maturity requires not only unified platforms and data-driven workflows but also the organizational capability to continually

reconfigure them. This perspective frames PT ARA DELVIN's transformation as a staged journey rather than a single technological intervention.

DMAIC Methodology

DMAIC (Define, Measure, Analyze, Improve, Control) is a structured, data-driven problem-solving methodology rooted in Lean Six Sigma. It provides a disciplined sequence for diagnosing operational problems, quantifying their magnitude, identifying root causes, designing improvements, and sustaining gains. In this study, DMAIC structures the entire diagnostic and solution-design process, ensuring that the identification of cost drivers and the MTTR gap leads systematically to an actionable improvement plan.

RESEARCH METHOD

Research Design

This study adopts an exploratory qualitative case study design, complemented by a quantitative layer based on the Technology Acceptance Model (TAM) to assess user readiness. The case study approach is appropriate because the research investigates a contemporary operational phenomenon within its real-life organizational context. The quantitative TAM layer is included because any technology rollout in a labor-intensive organization will fail without sufficient internal capability and acceptance. The DMAIC framework provides the overarching structure that links the diagnosis of cost drivers and the MTTR gap to the proposed solution.

Data Collection

Primary data were collected through semi-structured interviews with management and operational personnel, focus group discussions, field observations, and a structured questionnaire administered to fifty respondents drawn from SROC operators, field coordinators, and management. The TAM questionnaire used a five-point Likert scale to measure Perceived Usefulness, Perceived Ease of Use, and Behavioral Intention. Secondary data, including incident logs, alarm reports, MTTR records, and maintenance logs, were reviewed in parallel to triangulate the findings and identify cost-related inefficiencies.

Data Analysis

Qualitative data were analyzed thematically, while descriptive statistics were computed for the TAM scores. The DMAIC framework structured the analysis: the Define phase scoped the operational problems based on internal pain points and the external market context faced by PT ARA DELVIN; the Measure phase quantified fragmentation, response-time delays, and cost inefficiencies; the Analyze phase combined Fishbone analysis with Lean waste identification to detect underlying causes across people, process, technology, environment, materials, and management dimensions; the Improve phase formulated alternative solutions; and the Control phase translated those solutions into KPIs, dashboards, and standardized procedures. Triangulation across interviews, observations, internal documents, and literature was applied throughout to enhance the validity of the findings.

RESULTS AND DISCUSSION

Current Condition and MTTR Diagnosis

Information provided by management and operational units reveals that PT ARA DELVIN currently relies on a manpower-intensive security model with labor costs rising year over year. The SROC manages security monitoring and incident response across several disconnected systems, requiring operators to switch between multiple alarm platforms,

ticketing systems, and communication channels to handle a single incident. This fragmentation directly lengthens response time.

Table 1. MTTR Phase Breakdown (Current Baseline)

Phase	Description	Time
Detection & Alarm	Trigger to operator awareness	7 min
Verification	Manual confirmation of incident	10 min
Dispatch & Coordination	SROC–field communication	~9 min
Field Response	Guard mobilization	~6 min
Total MTTR	From trigger to first response	32 min (exceeds 17 min KPI)

Source: Author, based on internal MTTR records.

Decomposing the Mean Time to Respond into its four phases reveals where automation would yield the greatest operational return. The current baseline of 32 minutes exceeds the KPI target of 17 minutes by roughly 88%, exposing the organization to contractual penalty clauses and reputational risk. The verification and dispatch phases, which depend heavily on manual confirmation and SROC–field communication, represent the largest addressable delays.

Cost Structure and Manpower Dependency

Interviews with managers and field officers identify excessive dependence on manpower as a dominant issue. Financial analysis indicates that labor represents the largest component of operational expenditure, with scaling for new clients typically requiring additional guards and producing linear cost growth. This manpower-heavy model limits scalability and exposes the organization to wage inflation and labor regulation risk. PT ARA DELVIN's current concentration of roughly 72% labor cost represents an easily imitable resource configuration; the proposed solution rebalances the cost base toward a unique bundle of integrated technological capabilities that is harder for competitors to replicate.

Table 2. Indicative Cost Structure Rebalancing

Cost Component	Current	Target	Change
Manpower (salaries & benefits)	72%	45%	–27
Technology & integration	18%	38%	+20
Maintenance & rework	10%	17%	+7

Source: Author (indicative; detailed financial modelling is outside the study scope).

The reallocation reduces dependence on linearly scaling manpower and increases investment in technology and analytics capabilities that, once developed, become difficult for competitors to replicate. This shift directly reduces the largest cost driver of the operation and supports a long-term cost base built on organization-specific bundles of knowledge, data, analytics capability, and digital infrastructure.

Root Cause Analysis: Lean Wastes

Applying Lean waste analysis within the DMAIC Analyze phase highlights the principal sources of inefficiency. Waiting carries the highest aggregate impact and is directly addressable by AI auto-verification, which removes manual confirmation latency. Over-processing, caused by duplicate data entry across CCTV, alarm, and ticketing platforms, is resolved by API-based system integration. The data-silo form of inventory waste is mitigated by a unified data layer that enables analytics and predictive maintenance. Transportation

waste, in the form of manual communication loops over radio and messaging applications, lengthens MTTR and is reduced through automated dispatching and mobile digital reporting.

TAM Assessment of User Readiness

The TAM assessment confirms that the workforce is highly ready to adopt the proposed platform, with a high Perceived Usefulness score of 4.52 and a Behavioral Intention score of 4.26. However, the Perceived Ease of Use score among SROC operators was lower, at 3.64, indicating concern about the complexity of new tools. This finding implies that adoption hinges less on convincing staff of the platform's value, which they already recognize, and more on ensuring the system is easy to use through intuitive interface design and intensive training. The TAM results therefore directly inform the change-management emphasis of the implementation plan.

Proposed Business Solution

The proposed solution centers on a unified Integrated Platform powered by AI-based analytics and IoT connectivity. In line with Process Integration Theory, combining different monitoring platforms into one operational interface provides SROC operators with a single source of truth and reduces cognitive overload. AI-backed video analytics enables automated alarm verification and threat filtering, while automated dispatching and mobile digital reporting replace manual communication loops, substantially lowering MTTR. The platform also establishes the foundation for predictive analytics, allowing the company to act before incidents escalate.

Implementation Plan

The Control element of DMAIC is operationalized as a seven-month implementation plan divided into four strategic phases:

1. Phase 1 (Months 1–2): Foundation & System Integration. Develop a standardized API architecture and deploy a common SROC dashboard, unifying CCTV, alarm, and access control under one interface to eliminate over-processing and duplicate data entry.
2. Phase 2 (Months 3–4): AI Enablement & Automation. Implement AI video analytics for predictive triage and automated alarm verification, and automate mobile dispatch workflows to remove communication waste and shorten MTTR.
3. Phase 3 (Months 5–6): Workforce Enablement & Change Management. Address the lower PEOU score (3.64) through intensive, user-centric training for SROC operators and field personnel, ensuring high adoption and low resistance to change.
4. Phase 4 (Month 7): Control & Sustained Monitoring. Formalize digital-first Standard Operating Procedures (SOP) and deploy performance dashboards to track MTTR reductions and sustained cost efficiency.

CONCLUSION

This study answers three research questions. First, regarding cost drivers, PT ARA DELVIN's principal cost driver is its heavy reliance on a manpower-intensive security model; as operations expand, the guard workforce grows proportionally, making labor the largest line item and exposing the firm to wage inflation and margin contraction. Fragmented, heterogeneous technologies that do not communicate with one another compound the problem by forcing manual communication loops and duplicate data entry, generating Lean

wastes such as waiting and communication waste that lengthen MTTR to 32–37 minutes and raise operational costs.

Second, regarding technology-based solutions, a unified Integrated Platform powered by AI-based analytics and IoT connectivity is the most suitable means of overcoming manual inefficiencies and reducing reliance on human resources. Consolidating monitoring platforms provides a single source of truth, AI-backed video analytics automates alarm verification, and automated dispatching with mobile reporting markedly reduces MTTR. The TAM analysis confirms strong workforce readiness, with a Perceived Usefulness score of 4.52 and a Behavioral Intention score of 4.26.

Third, regarding the implementation plan, the Control element of DMAIC is realized through a structured seven-month program across four phases: foundation and system integration; AI enablement and automation; workforce enablement and change management; and control with sustained monitoring. Together these phases translate the diagnosed root causes into a coherent transformation roadmap whose expected impact is twofold: a reduction in the main operational cost drivers and a significant improvement in MTTR toward the 17-minute internal target.

Managerial Implications

Effective change management is critical to a successful rollout. Although the TAM analysis indicates a high intention to adopt, personnel remain cautious about the complexity of new tools, as reflected in the PEOU score of 3.64. Management should pair the technology rollout with robust on-the-job training that moves guards from manual processes to mobile reporting applications. During the Control phase, PT ARA DELVIN should formally rewrite its SOPs to require full use of the Integrated Platform and phase out duplicated effort such as manual ticketing and dispatch via messaging applications. Finally, the company should consider extending the platform beyond internal use toward a multisided API ecosystem that responsibly monetizes anonymized analytics, creating new revenue streams that reinforce its competitive position.

Limitations and Future Research

This study has several limitations that open avenues for future research. The qualitative case study design limits the generalizability of findings beyond the specific organizational context of PT ARA DELVIN, and the absence of a detailed financial model means that quantitative ROI and TCO outcomes remain projections rather than verified results. Importantly, this study does not include a detailed quantitative analysis of how to achieve the 25% cost reduction target; it focuses on identifying the key cost drivers, proposing AI- and data analytics-based solutions, and outlining their qualitative impact on cost structure and MTTR, while detailed financial modelling and quantification of the 25% target are beyond its scope and recommended for further study. Future research should conduct post-implementation financial validation to calculate realized Return on Investment, actual Total Cost of Ownership reductions, and the specific impact on profit margins. The geographic scope was constrained to Jakarta-based SROC operations; future studies should extend the analysis to other regional branches, particularly remote mining and energy sites where infrastructure readiness and operational complexity differ. Finally, as the proposed solution envisions a transition toward a multisided digital ecosystem through API-based data monetization, future research should develop a comprehensive go-to-market strategy evaluating target segments, pricing models for data-as-a-service, and commercialization tactics for these tech-enabled value-added services.

REFERENCES

- Afreen, S., Hossain, M. S., Rahman, M. A., & Islam, M. T. (2023). IoT-based smart surveillance system for high-security areas. *Applied Sciences*, 13(15), 8936.
- Ashton, K. (2009). That 'Internet of Things' thing. *RFID Journal*.
- Benbow, D. W., & Kubiak, T. M. (2018). *The certified six sigma black belt handbook* (3rd ed.). ASQ Quality Press.
- Buer, S. V., Strandhagen, J. O., & Chan, F. T. S. (2018). The link between Industry 4.0 and lean manufacturing. *International Journal of Production Research*, 56(8), 2924–2940.
- Davenport, T. H., & Harris, J. G. (2017). *Competing on analytics: The new science of winning*. Harvard Business Review Press.
- Garcia, M. L. (2008). *The design and evaluation of physical protection systems* (2nd ed.). Butterworth-Heinemann.
- Horngren, C. T., Datar, S. M., Rajan, M., Wynder, M., Maguire, W., & Tan, R. (2021). *Cost accounting: A managerial emphasis* (8th Australasian ed.). Pearson.
- Maleyeff, J. (2006). Exploration of internal service systems using lean principles. *Management Decision*, 44(5), 674–689.
- McKinsey & Company. (2023). *The future of the security industry*.
- Slack, N., Brandon-Jones, A., & Burgess, N. (2022). *Operations management* (9th ed.). Pearson.
- Teixeira, T., et al. (2015). A survey on intelligent physical security. *ACM Computing Surveys*, 48(4), 1–36.
- Westerman, G., Bonnet, D., & McAfee, A. (2014). *Leading digital: Turning technology into business transformation*. Harvard Business Review Press.