

Oerlikon Skyshield Integration in Indonesia's Layered Architecture: The Politics of Interoperability, Defense Governance, and Deterrence

Suherfin Hardi Lubis*, Asep Setiawan, Usni

Universitas Muhammadiyah Jakarta, Indonesia

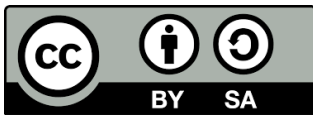
Email: yoffiekahn77@gmail.com*

Keywords:

defense politics; Oerlikon
Skyshield; interoperability;
defense governance; SHORAD;
C4ISR;

ABSTRACT

Indonesia's layered air defense architecture requires interoperable systems that integrate local sensors and weapon systems with national command-and-control networks. However, the acquisition of advanced defense platforms does not automatically translate into integrated operational capabilities. This study examined how technical interoperability, organizational capacity, and defense governance influenced the strategic role of the Oerlikon Skyshield air defense system within Indonesia's layered air defense architecture. A qualitative case study approach was employed, drawing on semistructured interviews with Indonesian Air Force personnel, documentary evidence, and relevant scholarly literature. Data were analyzed through data condensation, data display, and conclusion drawing and verification, supported by thematic coding. Source and methodological triangulation were applied to strengthen the credibility of the findings. The results identified three principal barriers: inadequate data communications infrastructure, limited personnel competencies in communications systems and cybersecurity, and insufficient middleware capabilities to standardize data exchange with the Indonesian National Air Operations Command (Komando Operasi Udara Nasional, Koopsudnas). These constraints limited shared air situational awareness and external target cueing, restricting Skyshield's operational role primarily to local point defense rather than enabling its full integration as a node within the national air defense network. The findings further indicated that these interoperability challenges were associated with fragmented institutional responsibilities for systems integration, procurement dependencies, and limitations in defense policy implementation capacity. The study concluded that air defense modernization should prioritize architecture-centered defense governance, clearly defined interoperability requirements throughout procurement and system life-cycle management, periodic integration testing, specialized personnel development, and technology transfer focused on systems integration capabilities. These measures could strengthen coordinated air defense operations, enhance deterrence by denial, and support Indonesia's strategic autonomy, although their operational effectiveness would require further technical validation.



This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.

Copyright © 2026 by Author. Published by
Pusat Publikasi Nusantara

INTRODUCTION

Modern air defense represents a strategic domain in which technology, organizational capacity, and political decision-making intersect. Radar systems, electro-optical sensors, command centers, communications networks, fighter aircraft, missiles, and antiaircraft artillery do not generate effective deterrence merely through their acquisition or deployment. Their strategic value depends on the state's ability to integrate these components into a coordinated

defense architecture that enables information to flow rapidly, securely, reliably, and effectively throughout the detection, identification, decision-making, and engagement processes. Consequently, air defense modernization cannot be understood solely as the accumulation of military platforms. Rather, it constitutes a political and institutional process through which technological capabilities distributed across different organizations, budgets, suppliers, and chains of command are integrated into a coherent operational system.

In Indonesia, these challenges are particularly significant because of the country's archipelagic geography, extensive airspace, geographically dispersed strategic assets, and diverse defense equipment acquired from different manufacturers and technological generations. These conditions require an integrated air defense architecture capable of facilitating interoperability among heterogeneous systems. Previous studies have emphasized the importance of radar systems, Air Defense Identification Zones (ADIZs), defense equipment modernization, and the management of the National Air Defense System (Sistem Pertahanan Udara Nasional, Sishanudnas) (Akib & Hariyono, 2019; Devi, 2022; Joesoef et al., 2022; Sudirin et al., 2022). However, existing research has predominantly focused on military capabilities and platform requirements, with comparatively limited attention to the political and institutional dimensions of interoperability. These dimensions include authority over technical standardization, the long-term dependencies created by procurement decisions, the distribution of institutional responsibilities for systems integration, and the state's capacity to transform acquired defense assets into effective operational capabilities.

Defense procurement constitutes a strategic and distributive policy decision rather than a purely technical acquisition process. Procurement contracts may be shaped by domestic political interests, bureaucratic incentives, defense industrial structures, and relationships between purchasing states and international suppliers (DeRouen & Heo, 2000; Kapstein & Oudot, 2009; Kim, 2000; Thorpe, 2010). Furthermore, defense procurement can function as an instrument of statecraft, establishing technological, institutional, and strategic dependencies that extend beyond the duration of individual contracts (Blankenship & Joyce, 2019; Marrone & Ungaro, 2014). This perspective is particularly relevant to Indonesia, where interoperability limitations may reflect the institutional consequences of fragmented procurement and modernization decisions rather than merely deficiencies in software or communications technology identified after systems enter operational service.

The Oerlikon Skyshield air defense system provides a relevant case for examining these relationships. Designed for short-range air defense (SHORAD) and point defense of critical assets, Skyshield incorporates sensor systems, fire control components, command-and-control functions, and gun-based effectors. The central strategic issue identified in this study was not simply whether its local sensors could detect targets within their operational capabilities, but whether the resulting information could contribute to a recognized air picture shared across the national air defense network. Equally important was whether Skyshield's engagement units could receive external target cueing from other elements of the integrated defense architecture. The research findings indicated that detection information generated by Skyshield could not be optimally displayed within the air situation display operated by the Indonesian National Air Operations Command (Komando Operasi Udara Nasional, Koopsudnas). Conversely, air situational data from the Koopsudnas network were not fully accessible through the Skyshield

command post. These limitations suggested that the system's integration into the broader national air defense network remained incomplete.

The preliminary findings identified three interrelated obstacles: inadequate military data communications infrastructure, limited personnel competencies in communications systems and cybersecurity, and insufficient middleware capabilities for translating and standardizing data formats across heterogeneous systems. From a technical perspective, these challenges primarily concerned data connectivity and systems interoperability. However, from a political science perspective, they also raised broader questions about institutional responsibility, governance, and policy implementation. Specifically, the findings highlighted the need to examine why interoperability requirements were not adequately addressed during procurement and modernization, which institutions possessed authority to establish interface standards, how integration resources were prioritized, and whether defense organizations had sufficient policy capacity to manage complex technologies throughout their operational life cycles.

These questions connected the study to the literature on policy capacity. (Wu et al., 2015) conceptualized policy capacity in terms of the competencies and resources required to perform essential policy functions, (Peters, 2015) emphasized the bureaucracy's role in both implementing public policies and developing institutional capacity. Similarly, (Bajpai & Chong, 2019) demonstrated the relevance of policy capacity frameworks for examining institutional capabilities in strategic policy sectors. Within the defense sector, policy capacity encompasses the ability to formulate operational and technical requirements, coordinate institutional stakeholders, supervise procurement contracts, establish interoperability standards, conduct integration testing, and incorporate lessons learned into subsequent modernization programs. Accordingly, interoperability can be understood not merely as a technical characteristic of military equipment but also as an indicator of the state's institutional capacity to convert procurement investments into operationally effective defense capabilities.

The issue of interoperability is also closely related to civil–military governance. Contemporary scholarship on civil–military relations extends beyond traditional concerns regarding military intervention in politics and civilian control to examine institutional effectiveness, operational efficiency, jointness, and accountability in achieving national defense objectives (Bruneau & Tollefson, 2014; Croissant & Kuehn, 2009; Mukherjee, 2016). In this study, civil–military governance was not employed to evaluate the overall condition of civilian control over the Indonesian armed forces. Instead, the concept provided an analytical framework for understanding how decisions concerning defense budgets, operational doctrine, technical standardization, institutional authority, and systems integration influenced military effectiveness. This perspective positioned interoperability as a governance challenge involving coordination among political authorities, military organizations, procurement institutions, and defense technology suppliers.

Based on these considerations, this study addressed the following research questions: How do technical interoperability limitations, organizational capacity, and political-institutional governance influence the strategic value of Oerlikon Skyshield within Indonesia's layered air defense architecture? What development strategies are required to enable the system to function as an integrated sensor–effector node within the national air defense network? These questions reflected the study's original objective of examining strategies for developing

Skyshield's detection and integration capabilities to strengthen national air defense. However, the analytical focus was expanded beyond the technical characteristics of the platform to encompass the political, organizational, and institutional processes that determine whether acquired defense technologies can deliver coordinated operational capabilities.

This study offered four principal contributions. First, empirically, it identified interoperability constraints involving data integration, personnel competencies, and institutional coordination, demonstrating that the challenges associated with Skyshield extended beyond the availability of weapons and sensors. Second, theoretically, it proposed a political-institutional framework for defense interoperability that integrated technical interoperability, organizational capacity, defense governance, and strategic integration within the broader defense architecture. Third, it connected technical defense studies with political science perspectives by incorporating procurement politics, policy capacity, civil–military governance, and strategic autonomy into the analysis of air defense modernization. Fourth, from a policy perspective, it advocated a transition from platform-centric procurement toward architecture-centered defense governance, emphasizing interoperability requirements, institutional accountability, and mission-thread-based evaluation. Collectively, these contributions provided a framework for understanding how Indonesia could strengthen the integration of heterogeneous air defense systems while improving the effectiveness, sustainability, and strategic value of its defense modernization initiatives.

METHOD

This study employed a qualitative case study design to examine the integration of the Oerlikon Skyshield air defense system into Indonesia's layered air defense architecture. The case study approach was selected to investigate the contextual relationships among defense platforms, military organizations, procurement policies, technology suppliers, and institutional governance within the Indonesian Air Force (Tentara Nasional Indonesia Angkatan Udara, TNI AU) and the National Air Operations Command (Komando Operasi Udara Nasional, Koopsudnas) (Yin, 2018). Rather than experimentally evaluating the system's technical performance, the study focused on identifying the political, organizational, and institutional mechanisms influencing the transformation of acquired defense platforms into integrated operational capabilities.

The unit of analysis was the process of integrating Skyshield into Indonesia's broader air defense architecture rather than the independent technical performance of the system. The analysis examined data link connectivity, middleware capabilities, personnel competencies, standard operating procedures (SOPs), institutional coordination with Koopsudnas, technology transfer, and capability development planning as interconnected components of defense policy implementation. This analytical perspective was consistent with the policy capacity framework, which examines institutional competencies in policy formulation, coordination, implementation, and evaluation (Peters, 2015; Wu et al., 2015). It also drew on military organizational change literature that distinguishes the formal adoption of defense technologies from their effective institutionalization within operational structures (Grauer, 2015; Nisser, 2021).

Primary data were obtained through semistructured interviews with Indonesian Air Force personnel representing operational, technical, and other relevant institutional functions. The source documentation identified three informant categories associated with operational support, data management, and legal functions. Secondary data were collected from relevant legislation, defense policy documents, operational materials available to the researchers, official defense institution publications, and scholarly literature. The literature review covered air defense systems, command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), technical interoperability, deterrence theory, defense procurement, civil–military governance, policy capacity, capability-based planning (CBP), and defense innovation.

Data were collected through semistructured interviews, document analysis, and indirect observation based on accessible defense-related publications and documented activities. The research documentation indicated that the formal study period extended from January to July 2026, although certain interview records were dated 2025. These records were retained as documented, without assuming an undocumented sequence of research activities. The analysis incorporated the available interview and documentary evidence to examine the institutional and operational factors influencing Skyshield's integration into the national air defense network.

Data were analyzed using the interactive qualitative analysis framework of (Miles & Huberman, 2014), comprising data condensation, data display, and conclusion drawing and verification. Mechanism-oriented thematic coding was applied to identify five principal analytical categories: Skyshield's operational role in point defense and layered air defense; technical interoperability barriers; organizational and personnel capabilities; institutional governance, integration authority, and standardization; and enabling conditions related to capability planning, procurement, financing, and technology transfer. These categories were subsequently examined within four interconnected dimensions of the analytical framework: technical interoperability, organizational capacity, political-institutional governance, and strategic integration.

The credibility and rigor of the analysis were supported by source and methodological triangulation, systematic comparison of interview findings with documentary evidence, and clear distinctions among empirical observations, institutional claims, and theoretical interpretations. The analysis followed qualitative research principles emphasizing credibility, transparency, contextual description, and auditability, as discussed by Tracy (2010), Nowell et al. (2017), and Braun and Clarke (2006). These procedures were intended to ensure that interpretations concerning defense governance and institutional capacity remained grounded in the available evidence rather than unsupported assumptions.

The study did not conduct independent technical testing of radar performance, network latency, detection probability, system survivability, weapon effectiveness, or cyber resilience. Classified operational data were also excluded from the analysis. Consequently, assessments of technical interoperability and operational effectiveness were limited to the available interview evidence, documentary materials, and publicly accessible literature. Unverified quantitative indicators, including national radar coverage, the number of vulnerable strategic sites, and defense budget benchmarks, were not treated as established empirical findings.

RESULTS AND DISCUSSION

Skyshield as a point defence that has not yet fully become a national network node

Oerlikon Skyshield serves as a SHORAD to protect vital objects, bases, and strategic points. At the firing unit level, sensors and command posts provide a local detection–tracking–engagement loop. The use of the system in exercises and security activities shows that Skyshield is not only in the acquisition stage, but has entered operations and training practices.

The research data shows the difference between the internal integration of firing units and the external integration into the national architecture. Inside the system, sensors can track and provide target data to command posts. Outside the system, data exchange with Koopsudnas has not been optimal. Skyshield is thus able to form a local tactical picture, but it has not consistently been part of the national/shared air picture and the local system has not always obtained a broader picture of the national network.

Interviews with Indonesian Air Force Officers confirmed this position. The interviewee stated that "Oerlikon Skyshield occupies a position as a short-range air defense or SHORAD" and functions to protect vital objects from threats such as drones and low-altitude vehicles (Interview with Indonesian Air Force Officers, 2026). The same interviewee emphasized the need for integration with national radars and other effectors so that layered defense and network-centric warfare can run comprehensively. These findings support the diagnosis that the value of Skyshield increases when the system functions as a node, not just an autonomous firing unit.

Technical barriers: communication infrastructure, data heterogeneity, and middleware

The most direct obstacle is the lack of data communication infrastructure that consistently connects the Skyshield Command Post with the Koopsudnas control center. The connectivity in question is not just voice communication, but datalink that allows for timely, secure, and machine-processed track exchange. Without this connectivity, local sensors cannot contribute full tracks to the common operating picture and firing units do not obtain optimal external cueing.

The TNI Air Operational Officer stated: "Radars of different types and generations often have different data formats. Integration into the command center requires conversion and synchronization that is not always seamless... there are still differences in protocols" (TNI AU Operational Officer Interview, 2026). The statement suggests that the problem is architectural: interface control, data mapping, semantic translation, timing rules, and cybersecurity controls must work simultaneously.

Operationally, heterogeneity results in at least three risks. First, the same track can be represented differently and complicate correlation. Second, conversion or transmission latency can reduce the value of information for high-speed threats. Third, operators can be forced to perform manual reconciliations that increase cognitive load and lengthen the decision cycle. Therefore, middleware is not just additional software; it is part of combat capability because it determines whether data can move from the local picture to shared situational awareness.

The public cyber security procurement literature also shows that the procurement of security information technology faces standard, competition, and vendor-specific requirements (Ruohonen, 2019). In the case of Skyshield, the research data does not allow for

the assessment of specific contracts or vendors. However, analytically, the need for middleware shows that the design of software-intensive system procurement should include interoperability and lifecycle integration requirements from the outset.

Organizational barriers: competence, learning, and doctrinal adaptation

Integration does not stop at software installation. Personnel need to understand radar, communication, networking, configuration, cybersecurity, and the relationship between technical data and operational decisions. Interviews show the need for certification and education in electronics, information technology, and communications. TNI AU Technical Officers emphasized the need for continuous training and knowledge transfer so that troubleshooting is not completely dependent on manufacturers (TNI AU Technical Officer Interview, 2026).

The findings are consistent with the military innovation literature that rejects technological determinism. Cheung (2021) places technology, organization, and doctrine as interlocking components; (Horowitz & Pindyck, 2022) distinguish technology ownership from innovations that truly change practices; and (Coticchia & Moro, 2016) point out the importance of learning and emulation for resource-constrained organizations. Thus, the capabilities of operators and technicians are organizational variables that mediate the benefits of technology.

The source manuscript shows that air defense procedures at the unit level already have a sequence of detection, identification, threat assessment, and quick reaction decisions and principles (Interview of Indonesian Air Force Operational Officers, 2026). However, readiness for a combination of UAVs, cruise missiles, cyberattacks, and electronic warfare is still in the process of adaptation. (Lehmann, 2023; Nisser, 2021) help explain the distance between formal doctrine and implementation: technological change is only effective if it is followed by training mechanisms, evaluation, revision of SOPs, and organizational learning.

Therefore, indicators of organizational interoperability need to include readiness and learning cycles: frequency of integration tests; documentation of communication failures; the ability of operators to read the quality of external data; fallback procedures when the network is disrupted; and the ability to retain knowledge after vendor support has diminished. Current research does not yet have longitudinal metrics to measure all of these indicators so the article limits them as an evaluation agenda rather than a quantitative finding.

Political-institutional barriers: ownership, standardization, and integrated governance

The findings on middleware have important political science implications. Data standardization is not a one-operator or one-unit decision because it concerns different radars, command systems, information classification, access authority, cyber assurance, and integration costs. This means that technical issues have political-institutional ownership. Without clear authority to set interface standards and control configurations, integration needs risk being addressed as local and fragmented projects.

The policy integration literature shows that fragmentation often arises when policies develop through layering without adequate coordination mechanisms (Rayner & Howlett, 2009). In bureaucracy, capacity does not only lie in individual expertise, but in organizations that are able to make decisions, mobilize resources, and maintain coordination across units (Peters, 2015; Wu et al., 2015). In the case of Skyshield, the data did not identify specific

actors as the cause of failure. Instead, the findings point to the need for institutional ownership of integration as an air defense architecture program.

The perspective of jointness clarifies this issue. Mukherjee (2016) shows that interoperability across organizations is influenced by the distribution of authority and civil–military arrangements. In air defense, these demands arise even in one domain because the functions of operations, communication, procurement, security, and training can be in different organizational chains. Therefore, integration governance needs to determine who defines standards, who conducts certification, how integration tests are received, and who is responsible for lifecycle configuration.

Procurement politics is also relevant. (Kapstein & Oudot, 2009; Murtazashvili et al., 2024) emphasize the importance of reforming the acquisition process in complex projects. The application of Skyshield is analytical: the procurement of the platform needs to be equipped with requirements that assess connectivity, permissible data rights, maintenance, test environment, and integration costs throughout the lifecycle. Without it, the cost that appears after procurement is actually a deferred governance cost.

Strategic embeddedness: from the local picture to deterrence by denial

A strategic consequence of these three barriers is the limited ability of Skyshield to contribute to shared situational awareness. Detection is a sensory event; situational awareness is the result of processing, correlation, identification, validation, and interpretation that is relevant to decisions. In slow threats, manual communication may be able to partially close the gap. In a saturation attack, drone swarm, cruise missile, or electronic interference, the tolerance for latency and ambiguity narrows.

Two-way connectivity with Koopsudnas has two potential benefits that can be directly derived from system logic. First, Skyshield can obtain early cueing from sensors that have a wider horizon so that operators have a longer orientation time. Second, local tracks can enrich the national picture for low targets in certain areas. These benefits remain conditional because they require data quality, security, authority, and time synchronization.

At the strategic level, these conditions affect deterrence by denial. Simón (2020), Dall'Agnol and Duarte (2022), and Lupovici (2024) show that denial depends on the ability to make achieving opponents' goals more difficult and uncertain. This article does not state that the existence of Skyshield alone produces a chilling effect. Denial credibility increases when integration increases detection probability, cueing, resilience, and coordinated engagement; conversely, information blind spots and decision-cycle bottlenecks reduce the value of the system.

Strategic embeddedness is also related to autonomy. Smith (2018), Engelbrekt (2022), and Zhang (2023) place strategic autonomy as the ability to maintain decision space and capacity to act. In software-intensive defense, the decision space depends on legal and technical access to maintenance, interface, configuration, and integration. Therefore, technical interoperability can be understood as one of the micro-foundations of strategic autonomy.

From engineering issues to the politics of interoperability

The main finding of the article is that interoperability should be treated as a political-strategic capability. Technical diagnoses—datalinks, protocols, middleware—explain where systems are disconnected, but have not yet explained why those gaps persist. The political

perspective adds three mechanisms: path dependency of procurement decisions, governance fragmentation, and limited policy capacity. All three help explain why individually functioning systems can still result in less coherent architectures.

DeRouen and Heo (2000), Kim (2000), Thorpe (2010), and Kapstein and Oudot (2009) show that procurement is shaped by institutions and incentives. For Skyshield, the implication is not to allege a particular interest—the research data does not support such claims—but to change the evaluation question. A procurement is not completed when the platform is accepted; its success is only seen when the platform can be maintained, integrated, updated, and used alongside other systems. In other words, the interoperability debt that arises after an acquisition should be viewed as part of the political evaluation of defense policy.

This argument reinforces the capability-based planning approach. If the unit of analysis is a mission thread, then an additional firing unit should be compared to an investment in datalinks, radar gap-fillers, simulations, cyber hardening, operator training, or integration engineering based on its contribution to mission outcomes. This approach reduces visual and political bias towards large platforms that are easy to identify, but do not necessarily solve the system bottleneck.

Defense governance: control, effectiveness, and implementation capacity

The civil–military governance perspective extends the meaning of democratic control to questions of effectiveness and efficiency. Bruneau and Tollefson (2014) show that the quality of civil-military relations must also be judged by the ability of institutions to produce an effective and efficient military. Croissant and Kuehn (2009), Pion-Berlin (2011), Sarigil (2011), Salihu (2019), and Rokvić et al. (2013) show institutional variations in control and professionalism. For the Indonesian case, the article does not evaluate the whole of civil-military relations, but draws a more specific consequence: integration decisions require accountability, prioritization, and auditable division of responsibilities.

The governance needed is not micro-management of combat decisions, but the ability to set architecture, standards, resource envelopes, test regimes, and lifecycle responsibility. Wu et al. (2015) and Peters (2015) help explain that policy capacity is analytical, operational, and political. In the case of Skyshield, engineering capabilities without procurement and governance support are insufficient; conversely, policy decisions without operator and technician capacity also do not produce readiness.

Therefore, this study proposes the concept of architecture-centric defence governance. This concept means that platform decisions are assessed based on their compatibility with the architecture, not the other way around; standards are set as enterprise policies; integration tests become gates before the system is declared fully ready; and data on readiness are used to adjust investment priorities. The approach is consistent with literature policy integration (Rayner & Howlett, 2009) and jointness (Mukherjee, 2016).

"Strategic autonomy" and the paradox of supplier diversification

Indonesia, as a country that obtains defense equipment from various sources, faces a trade-off between political flexibility and architectural complexity. Diversification can magnify strategic choices, but each supplier can bring different protocols, licenses, software stacks, and sustainment models. Maye (2017) points out the autarky–interdependence dilemma, while Ploom et al. (2022) emphasize the challenges of countries with limited

industrial bases. At this point, diversification that is not accompanied by technical governance can turn single-vendor dependence into a multi-vendor integration dependence.

The literature on strategic autonomy shows that autonomy is not isolation. Smith (2018), Engelbrekt (2022), Zhang (2023), Gafarlı and Roknifard (2023), as well as Shlykov (2023) describe autonomy as the ability to maintain choices and act in interdependent relationships. Soubrier (2023) critically reminds that the autonomy narrative needs to be evidenced by material and institutional capacity. By this measure, the national ability to manage interfaces, software maintenance, configuration management, and integration engineering are substantive indicators of autonomy.

Technology transfer therefore needs to shift from local content to system-integration knowledge. The findings of technical speakers on training and troubleshooting lead to the need for absorptive capacity which is also emphasized by Balakrishnan and Lazar (2022) and Bezuidenhout and Bean (2022). This does not mean disclosing sensitive information or violating intellectual property rights, but negotiating the level of access, documentation, test environment, and knowledge transfer necessary for sustainment and integration throughout the lifecycle in accordance with law and licensing.

Military innovation as a political and organizational process

Skyshield also shows that military innovation is not a linear function of technology. Major (2009), te Kulve and Smit (2010), Horowitz and Pindyck (2022), Nisser (2021), Grauer (2015), Coticchia and Moro (2016), and Lehmann (2023) show from different angles that organization, bureaucracy, doctrine, and learning determine adoption. In this framework, the existence of modern systems can coexist with old practices if SOPs, authority structures, and learning mechanisms do not change.

This gives new meaning to integration exercises. The exercise is not just a demonstration of readiness, but a policy feedback mechanism: failure of track sharing, latency, ambiguity, or authority conflicts must be converted into subsequent configuration changes, SOPs, training requirements, and procurement requirements. This is where military learning meets public-policy evaluation.

Kinne (2019) shows that modern defense cooperation includes policy coordination, training, R&D, procurement, and information security. The findings show that interoperability can also be built through institutional mechanisms of cooperation, as long as national interests in security, data governance, and lifecycle independence are protected. The article does not propose specific suppliers or partners, but emphasizes that defense cooperation needs to be assessed based on its contribution to architectural knowledge and interoperability.

Policy implications: from platform-centric procurement to mission-thread governance

First, Skyshield integration needs to be positioned as part of an air defense architecture program, not a local software project. Institutional ownership is needed that can establish interface standards, configuration control, cyber assurance, data governance, and acceptance criteria across systems. The organizational form must be adjusted to the applicable legal and command structures; this research does not have enough data to determine a specific institutional design.

Second, procurement needs to use mission-thread-based requirements. Each new platform is evaluated based on its contribution to sensing, identification, dissemination,

decision, engagement, and assessment. Purchase prices need to be read along with integration costs, lifecycle support, training, software maintenance, and dependency risk. This approach expands on the logic of procurement reform discussed by Kapstein and Oudot (2009) and the political economy of procurement shown by Murtazashvili et al. (2024).

Third, strengthening human resources needs to combine operators, technicians, network engineers, cyber specialists, and policy/acquisition personnel. Interoperability is a cross-professional competence. Certification, simulation, recurrent joint integration exercise, and after-action review need to form a learning loop that connects operational experience with revision of doctrines and requirements.

Fourth, technology transfer needs to target diagnostics, configuration, software maintenance, interface management, and integration testing capabilities along security and licensing boundaries. The goal is not autarky, but to reduce vendor lock-ins and improve bargaining positions and strategic choices.

Fifth, modernization evaluation needs to use mission-capability indicators such as track continuity, latency, availability, resilience, cueing quality, operator readiness, and disruption recovery time. This study does not provide numerical values for these indicators; therefore, these recommendations are a measurement agenda for the next internal exercise or evaluation, not claims about actual performance.

Table 1. Policy implications

Dimensions	Empirical evidence	Political/strategic consequences	Development direction
Technical	Datalink is not optimal; format/protocol is heterogeneous; middleware is not adequate	Air picture fragmentation; latency; cross-cueing limitations	Standardization of architecture and interface; integration testing
Organizational	Communication/cyber and troubleshooting competencies need to be strengthened	human bottleneck; vendor dependency; non-automated learning	Certification; recurrent training; after-action learning
Political-institutional	Cross-functional standards and ownership needs	Deferred integration cost; fragmentation of priorities; vague accountability	Architecture governance; lifecycle responsibility; procurement requirement
Strategic	Skyshield is more powerful as a local defense point than a national node	Contribution to deterrence by denial and strategic autonomy has not been maximized	Embed to layered IADS/C4ISR; CBP based on mission thread

Source: Processed Author

CONCLUSION

This study demonstrated that strategies for developing the Oerlikon Skyshield air defense system to strengthen Indonesia's layered air defense architecture should prioritize interoperability governance rather than focusing exclusively on platform modernization. The findings identified three principal empirical challenges: inadequate data communications infrastructure, limited personnel competencies in communications systems and cybersecurity, and insufficient middleware capabilities to standardize data exchange with the Indonesian National Air Operations Command (Komando Operasi Udara Nasional, Koopsudnas). These challenges were interconnected with organizational capacity, institutional responsibilities for systems integration, defense procurement decisions, and the state's ability to manage complex technologies throughout their operational life cycles. The findings suggested that improving technical connectivity alone would be insufficient without corresponding improvements in institutional coordination, personnel development, and defense governance.

Theoretically, this study proposed a political-institutional framework for defense interoperability comprising four interconnected dimensions: technical interoperability, organizational capacity, political-institutional governance, and strategic integration. This framework explained how tactical defense capabilities could contribute to broader political and strategic objectives. Technical interoperability facilitated the exchange of operational information, while organizational capacity enabled personnel and institutions to interpret and utilize that information effectively. Political-institutional governance established the authority, standards, incentives, and resources necessary for coordinated implementation, whereas strategic integration connected local defense capabilities with layered air defense operations, mission threads, deterrence by denial, and national strategic autonomy. Together, these dimensions provided an analytical foundation for understanding the transformation of individual defense platforms into coordinated operational capabilities.

The study's principal contribution to political science was its shift in analytical focus from individual defense platforms to the institutional processes governing their acquisition, integration, and operational utilization. Defense procurement was examined not merely as the acquisition of weapon systems but as a public policy process involving long-term resource allocation, technological dependencies, and institutional decision-making. From this perspective, accumulated interoperability deficiencies, conceptualized as interoperability debt, reflected the potential consequences of failing to incorporate systems integration requirements and associated costs into procurement planning and governance. Conversely, architecture-centered defense governance offered opportunities to improve operational effectiveness by strengthening coordination among existing capabilities without necessarily requiring additional defense platforms.

The findings highlighted several policy priorities, including establishing an architecture-based systems integration roadmap, incorporating interoperability requirements throughout acquisition and system life-cycle management, strengthening institutional policy capacity and technical integration expertise, conducting periodic integration testing, and prioritizing technology transfer related to systems integration. Defense investment evaluations should also adopt a mission-thread-based approach to assess how sensors, data links, middleware, cybersecurity measures, personnel training, and weapon effectors contribute to

the overall detection-to-engagement process. Such an approach could improve resource allocation, strengthen operational coordination, and enhance the effectiveness of Indonesia's layered air defense architecture.

Nevertheless, several limitations should be acknowledged. First, the single-case study design supported analytical rather than statistical generalization. Second, inconsistencies in informant documentation and interview dates spanning 2025–2026 required clarification to establish the precise chronology and scope of data collection. Third, the absence of independent technical performance testing prevented definitive conclusions regarding detection probability, actual network latency, system survivability, and engagement effectiveness. Fourth, certain quantitative indicators in the source materials required verification against authoritative primary sources before being treated as established findings. Finally, the political-institutional analysis relied primarily on interpretations of the available integration evidence rather than direct examination of all relevant policy-making processes. Consequently, further research involving defense policy officials, procurement authorities, budget planners, and systems architecture managers would be necessary to examine the mechanisms of bureaucratic politics, institutional coordination, and policy capacity more comprehensively.

Future research should employ comparative multiple-case study designs to examine interoperability across short-range air defense (SHORAD) systems, ground-controlled interception (GCI) radar systems, and surface-to-air missile systems. Process tracing could be used to investigate the relationship between procurement decisions and subsequent integration outcomes, while technical assessments using appropriately authorized and releasable exercise data could evaluate network latency, track quality, and information exchange performance. Social network analysis could further examine information flows and coordination among military units, whereas simulation-based wargaming could compare the marginal operational benefits of acquiring additional platforms with those of investing in systems integration. Comparative studies involving other archipelagic states and middle powers could also assess whether integration costs and governance gaps associated with heterogeneous, multivendor defense architectures produce similar institutional and operational challenges. These research directions could strengthen the empirical foundations of interoperability governance and support more effective, sustainable, and strategically coherent defense modernization policies.

FUNDING

The authors declare that no financial support was received for the conduct of this study and/or the publication of this article.

CONFLICT OF INTEREST

The authors declare that this study was conducted without any commercial or financial relationships that could be interpreted as a potential conflict of interest.

AUTHOR CONTRIBUTIONS

Suherfin Hardi Lubis: research conceptualization, methodology design, experiment execution, data collection, data analysis, manuscript drafting, and manuscript revision.

Asep Setiawan and Usni: research supervision, validation of research results, provision of scientific input, and manuscript review and revision. All authors have read and approved the final version of the manuscript.

GENERATIVE AI STATEMENT

The authors declare that generative artificial intelligence (AI) was used in the preparation of this manuscript to help improve linguistic clarity, correct grammar, and refine the writing structure. Generative AI was not used to generate, manipulate, or analyze research data. The entire content of the manuscript has been reviewed and verified by the author(s). The author(s) are fully responsible for the accuracy, integrity, and final content of the manuscript.

REFERENCES

- Akib, H., & Hariyono, U. S. (2019). The spread-out strategy of the main weapon system of the Indonesian Air Force in the territory of the Republic of Indonesia. *Austral: Brazilian Journal of Strategy & International Relations*, 8(15), 117–130. <https://doi.org/10.22456/2238-6912.83627>
- Bajpai, K., & Chong, B. W. (2019). India's foreign policy capacity. *Policy Design and Practice*, 2(2), 137–162. <https://doi.org/10.1080/25741292.2019.1615164>
- Blankenship, B., & Joyce, R. M. (2019). Purchasing power: US overseas defense spending and military statecraft. *Journal of Conflict Resolution*, 64(2–3), 545–573. <https://doi.org/10.1177/0022002719854786>
- Bruneau, T. C., & Tollefson, S. D. (2014). Civil–military relations in Brazil: A reassessment. *Journal of Politics in Latin America*, 6(2), 107–138. <https://doi.org/10.1177/1866802X1400600204>
- Coticchia, F., & Moro, F. N. (2016). Learning from others? Emulation and change in the Italian Armed Forces since 2001. *Armed Forces & Society*, 42(4), 696–718. <https://doi.org/10.1177/0095327X15626725>
- Croissant, A., & Kuehn, D. (2009). Patterns of civilian control of the military in East Asia's new democracies. *Journal of East Asian Studies*, 9(2), 187–217. <https://doi.org/10.1017/S1598240800002988>
- DeRouen, K., & Heo, U. (2000). Defense contracting and domestic politics. *Political Research Quarterly*, 53(4), 753–769. <https://doi.org/10.1177/106591290005300404>
- Devi, A. F. (2022). The air defense identification zone (ADIZ) Indonesia in order to ensure security in the air region jurisdiction of national jurisdiction. *Strategi Pertahanan Udara*, 8(1). <https://doi.org/10.33172/jspu.v8i1.1047>
- Grauer, R. (2015). Moderating diffusion: Military bureaucratic politics and the implementation of German doctrine in South America, 1885–1914. *World Politics*, 67(2), 268–312. <https://doi.org/10.1017/S0043887115000027>
- Horowitz, M. C., & Pindyck, S. (2022). What is a military innovation and why it matters. *Journal of Strategic Studies*, 46(1), 85–114. <https://doi.org/10.1080/01402390.2022.2038572>
- Joesoef, N., Risman, H., & Hadiano, M. (2022). Enhancing the Indonesia air defense system: The immediate and urgent application of GCI radar in safeguarding the airspace sovereignty of the Republic of Indonesia. *Technium Social Sciences Journal*, 38, 559–623. <https://doi.org/10.47577/tssj.v38i1.7862>
- Kapstein, E. B., & Oudot, J.-M. (2009). Reforming defense procurement: Lessons from France. *Business and Politics*, 11(2), 1–25. <https://doi.org/10.2202/1469-3569.1264>

- Kim, S. K. (2000). The political economy of defense procurement and acquisition: The case of South Korean ministry of defense. *Global Economic Review*, 29(2), 65–82. <https://doi.org/10.1080/12265080008449788>
- Lehmann, T. C. (2023). Adapting military doctrine in the shadow of the future. *The Journal of Defense Modeling and Simulation*, 22(3), 321–335. <https://doi.org/10.1177/15485129231189286>
- Marrone, A., & Ungaro, A. R. (2014). Relations between the United States of America and Italy in the post-Cold War period: A defense-industrial perspective. *Cahiers de La Méditerranée*, 88, 157–181. <https://doi.org/10.4000/cdlm.7542>
- Miles, M. B., & Huberman, A. M. (2014). *Qualitative Data Analysis: A Methods Sourcebook* (3rd ed., Ed.). SAGE Publications.
- Mukherjee, A. (2016). Fighting separately: Jointness and civil-military relations in India. *Journal of Strategic Studies*, 40(1–2), 6–34. <https://doi.org/10.1080/01402390.2016.1196357>
- Murtazashvili, J. B., Mylovanov, T., & Shapoval, N. (2024). The political economy of public procurement in Ukraine. *Journal of Public Finance and Public Choice*, 39(1), 118–138. <https://doi.org/10.1332/25156918Y2024D000000005>
- Nisser, J. (2021). Implementing military doctrine: A theoretical model. *Comparative Strategy*, 40(3), 305–314. <https://doi.org/10.1080/01495933.2021.1912514>
- Peters, B. G. (2015). Policy capacity in public administration. *Policy and Society*, 34(3–4), 219–228. <https://doi.org/10.1016/j.polsoc.2015.09.005>
- Rayner, J., & Howlett, M. (2009). Conclusion: Governance arrangements and policy capacity for policy integration. *Policy and Society*, 28(2), 165–172. <https://doi.org/10.1016/j.polsoc.2009.05.005>
- Ruohonen, J. (2019). An acid test for Europeanization: Public cyber security procurement in the European Union. *European Journal for Security Research*, 5(2), 349–377. <https://doi.org/10.1007/s41125-019-00053-w>
- Sudirin, S., Darmawan, W. B., & Hendra, H. (2022). Peran TNI AU dalam manajemen pertahanan udara (studi pada Kohanudnas dalam menggunakan Sishanudnas). *Aliansi Jurnal Politik Keamanan Dan Hubungan Internasional*, 1(1), 63. <https://doi.org/10.24198/aliansi.v1i1.38868>
- Thorpe, R. (2010). The role of economic reliance in defense procurement contracting. *American Politics Research*, 38(4), 636–675. <https://doi.org/10.1177/1532673X09337107>
- Wu, X., Ramesh, M., & Howlett, M. (2015). Policy capacity: A conceptual framework for understanding policy competences and capabilities. *Policy and Society*, 34(3–4), 165–171. <https://doi.org/10.1016/j.polsoc.2015.09.001>
- Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6th Edition, Ed.). Sage Publications Inc.