International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 144-155
OCLC – 1368736135

Journal Website: http://sciencebring.com/index.php/ijasr

Research Article

Advanced Computational Identity Marker Architectures in Indemnity Service Environments: High-Integrity Verification Mechanisms, Governance-Aligned Practices

Submission Date: January 01, 2026, **Accepted Date:** January 31, 2026,
Published Date: February 28, 2026

Dr. Arvind Reddy
Department of Computer Science and Engineering, Institute of Advanced Technology Hyderabad, Telangana, India

Abstract

The increasing digitization of indemnity service environments, including insurance, liability management, and risk-transfer ecosystems, necessitates robust identity verification mechanisms capable of ensuring both operational integrity and regulatory compliance. Traditional authentication frameworks—primarily reliant on static credentials—are inadequate against evolving threats such as spoofing, tampering, and system-level vulnerabilities. This study proposes advanced computational identity marker architectures that integrate biometric, behavioral, and system-level verification within high-integrity, governance-aligned infrastructures.

The research synthesizes principles from real-time systems, avionics-grade safety architectures, and tamper-resistant embedded systems to develop a layered identity validation framework. Drawing from formal specification methodologies, architectural design languages (AADL), and safety-critical middleware paradigms, the study constructs a computational model that ensures deterministic performance, resilience against intrusion, and compliance with regulatory frameworks. The framework leverages model-driven engineering, secure middleware orchestration, and distributed system schedulability analysis to maintain integrity across heterogeneous platforms.

A key contribution of this work is the conceptualization of identity markers as dynamic computational entities rather than static identifiers. These markers are continuously validated through multi-layered verification pipelines incorporating anomaly detection, behavioral consistency checks, and cryptographic

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 144-155
OCLC – 1368736135

validation. The integration of tamper-resistant hardware principles and fault-tolerant display system architectures further enhances system robustness, particularly in high-risk domains.

The findings indicate that combining real-time system design principles with adaptive identity verification mechanisms significantly improves reliability and reduces vulnerability exposure. Moreover, governancealigned practices embedded within system architecture ensure compliance with regulatory mandates without compromising performance.

This research contributes to the advancement of secure identity infrastructures by bridging gaps between software architecture, embedded systems security, and indemnity service requirements. The proposed framework offers a scalable and adaptable solution for next-generation identity verification systems, particularly in environments demanding high assurance, such as insurance platforms, financial systems, and safety-critical applications.

KEYWORDS

Computational Identity Markers, Indemnity Systems, Identity Verification, Tamper-Resistant Architecture, AADL, Real-Time Systems, Secure Middleware, Governance Compliance, Biometric Systems, Embedded Security

INTRODUCTION

The evolution of indemnity service environments has been profoundly influenced by digital transformation, particularly in sectors such as insurance, financial risk management, and liability adjudication. These systems increasingly rely on automated decision-making frameworks and distributed computational infrastructures to manage complex risk portfolios. However, this transition has simultaneously introduced critical vulnerabilities, particularly in identity verification mechanisms, which serve as foundational components for trust establishment within such ecosystems.

Traditional identity verification approaches are predominantly static, relying on credentials such as passwords, tokens, or pre-defined identifiers. While these mechanisms offer baseline security, they are inherently susceptible to sophisticated attacks including spoofing, replay attacks, and system-level tampering. The inadequacy of these methods is exacerbated in indemnity environments where fraudulent identity claims can lead to significant financial losses and systemic instability. Consequently, there is an urgent need to develop advanced computational architectures capable of supporting high-integrity identity verification.

Recent developments in software architecture and embedded systems provide a promising foundation for addressing these challenges. Pattern-oriented architectural design frameworks emphasize modularity, scalability, and reusability, enabling the construction of robust systems capable of adapting to evolving requirements (Buschmann et al., 1996). Similarly, the Architecture Analysis and Design Language (AADL) facilitates the formal modeling of system components, allowing for precise specification and

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 144-155
OCLC – 1368736135

verification of system behavior (Feiler et al., 2006). These methodologies are particularly relevant in high-assurance environments where system correctness and reliability are paramount.

In parallel, research in real-time systems has highlighted the importance of deterministic execution and schedulability in ensuring system reliability. Techniques for analyzing distributed real-time systems with multiple-event synchronization provide critical insights into maintaining system stability under varying workloads (Garcia et al., 2000). These principles are directly applicable to identity verification systems, where timely and accurate validation is essential for maintaining operational integrity.

The integration of tamper-resistant mechanisms further enhances system security by protecting critical components from physical and logical attacks. Studies on secure embedded systems demonstrate the effectiveness of hardware-level protections and cryptographic safeguards in mitigating vulnerabilities (Ravi et al., 2004). Additionally, advances in smart card technologies and encapsulated modules provide practical implementations of these concepts, enabling secure storage and processing of sensitive identity data.

Another significant dimension of identity verification lies in the use of computational identity markers, which extend beyond static identifiers to include dynamic attributes such as behavioral patterns, biometric signals, and contextual data. These markers enable continuous authentication, allowing systems to detect anomalies and respond proactively to potential threats. The concept aligns with recent advancements in AI-enhanced biometric systems, which leverage machine learning algorithms to improve accuracy and resilience (Laheri, 2025).

Despite these advancements, existing systems often lack integration across architectural layers, resulting in fragmented security implementations. Furthermore, governance and regulatory compliance are frequently treated as external constraints rather than intrinsic design considerations. This disconnect undermines the effectiveness of identity verification mechanisms, particularly in indemnity environments where compliance with legal and ethical standards is critical.

The objective of this research is to address these gaps by proposing a unified computational architecture for identity verification that integrates principles from software architecture, real-time systems, and embedded security. The study aims to achieve the following objectives:

1. To conceptualize identity markers as dynamic computational entities.
2. To develop a high-integrity verification framework based on formal architectural models.
3. To integrate tamper-resistant mechanisms within identity verification pipelines.
4. To align system design with governance and regulatory requirements.

The scope of this research encompasses both theoretical and practical dimensions, including architectural modeling, system design, and performance analysis. While the primary focus is on indemnity service environments, the proposed framework is applicable to a wide range of domains requiring high-assurance identity verification.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 144-155
OCLC – 1368736135

ISSN-2750-1396

The significance of this work lies in its interdisciplinary approach, combining insights from multiple fields to address a critical challenge in modern digital systems. By advancing the state of the art in identity verification architectures, this research contributes to the development of secure, reliable, and governance-compliant systems capable of supporting the evolving needs of indemnity service environments.

LITERATURE

The development of high-integrity identity verification systems is grounded in multiple research domains, including software architecture, real-time systems, embedded security, and avionics-grade system design. The literature reveals a convergence of these fields toward the creation of robust, scalable, and secure computational infrastructures.

Pattern-oriented software architecture provides foundational principles for designing complex systems. Buschmann et al. (1996) emphasize the importance of reusable design patterns in achieving modularity and scalability. These principles are particularly relevant for identity verification systems, which must integrate diverse components such as authentication modules, data processing pipelines, and security mechanisms. The use of architectural patterns enables systematic design and facilitates the incorporation of advanced features such as dynamic identity markers.

Formal specification techniques further enhance system reliability by enabling precise modeling and verification of system behavior. Bastide et al. (2000) demonstrate the application of formal methods in specifying CORBA services, highlighting the importance of rigorous validation in distributed systems. Such approaches are essential for identity verification frameworks, where correctness and consistency are critical.

The role of architectural modeling languages is also significant. Feiler et al. (2006) introduce AADL as a tool for analyzing system architecture, particularly in safety-critical domains. AADL supports the modeling of system components, interactions, and performance characteristics, enabling comprehensive analysis of system behavior. This capability is crucial for designing identity verification systems that must operate under strict performance and reliability constraints.

Real-time systems research provides insights into ensuring deterministic system behavior. Garcia et al. (2000) explore schedulability analysis in distributed systems, demonstrating methods for managing complex event interactions. These techniques are directly applicable to identity verification processes, which often involve multiple concurrent operations requiring synchronization and timely execution.

Embedded system security is another critical area. Ravi et al. (2004) examine tamper resistance mechanisms, emphasizing the need for protecting system components against physical and logical attacks. Similarly, Kuhn (1999) discusses design principles for tamper-resistant processors, highlighting the importance of secure hardware architectures. These studies underscore the necessity of integrating hardware-level protections into identity verification systems.

Advances in middleware technologies also contribute to system robustness. Haverkamp and Richards (2002) discuss safety-critical middleware

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 144-155
OCLC – 1368736135

for avionics applications, emphasizing reliability and fault tolerance. Such middleware can be adapted for identity verification systems, providing a stable platform for managing complex interactions between system components.

Model-driven engineering approaches further enhance system development. Bordin and Vardanega (2005) demonstrate automated code generation for real-time systems, enabling efficient implementation of complex architectures. Similarly, Lu et al. (2003) introduce tools for application deployment and configuration, facilitating the management of distributed systems. These approaches support the scalable development of identity verification frameworks.

Research in avionics systems provides valuable insights into high-integrity system design. Wang (2014) discusses the architecture of integrated avionics systems, emphasizing reliability and fault tolerance. Studies on display system failures (Sun, 2020; Luo, 2021; Wu, 2023) highlight the importance of robust system design in preventing operational disruptions. These findings are relevant for identity verification systems, which must maintain reliability under adverse conditions.

The concept of identity markers is further advanced through research in AI-enhanced biometric systems. Laheri (2025) explores the use of machine learning for secure authentication, demonstrating improved accuracy and resilience. This approach aligns with the need for dynamic identity markers capable of adapting to changing conditions.

Despite these advancements, several gaps remain. First, there is limited integration between architectural modeling and identity verification mechanisms. Second, existing systems often lack comprehensive tamper resistance, leaving them vulnerable to attacks. Third, governance and compliance considerations are not fully integrated into system design, resulting in potential regulatory challenges.

This research addresses these gaps by proposing a unified framework that integrates architectural modeling, real-time system principles, and embedded security mechanisms. By synthesizing insights from diverse fields, the study aims to advance the development of high-integrity identity verification systems.

METHODOLOGY

5.1 Conceptual Framework of Computational Identity Markers

The notion of computational identity markers extends traditional identity paradigms by transforming static identifiers into dynamic, continuously validated entities. Unlike conventional authentication tokens, computational identity markers incorporate multi-dimensional attributes, including behavioral patterns, contextual signals, and system-generated metadata. This transformation is rooted in the need for adaptive identity systems capable of responding to evolving threat landscapes.

From a theoretical perspective, identity markers can be modeled as state-dependent entities within a distributed system. Each marker evolves based on user interaction patterns, environmental variables, and system feedback loops. The formalization of such entities aligns with distributed object models, where identity attributes are encapsulated within modular

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 144-155
OCLC – 1368736135

components governed by defined interfaces (Bastide et al., 2000). This modularity enables scalable deployment across indemnity platforms.

Technically, identity markers are constructed through layered pipelines consisting of data acquisition, feature extraction, validation, and decision-making modules. For instance, biometric signals and behavioral data are processed through machine learning algorithms to generate probabilistic identity scores. These scores are continuously updated, allowing systems to detect anomalies and trigger adaptive responses.

A hypothetical application within an insurance claim processing system illustrates this concept. A user submitting a claim is not only verified through credentials but also through behavioral consistency, such as typing patterns and navigation sequences. Deviations from established patterns trigger additional verification steps, thereby reducing fraud risk.

However, this approach introduces challenges related to data privacy and computational overhead. Continuous monitoring requires robust data governance frameworks and efficient processing architectures to ensure system scalability.

5.2 High-Integrity Verification Mechanisms

High-integrity verification mechanisms are essential for ensuring the reliability and trustworthiness of identity systems. These mechanisms are characterized by deterministic behavior, fault tolerance, and resistance to tampering.

Theoretical foundations for high-integrity systems are derived from real-time computing and safety-critical system design. Deterministic execution ensures that verification processes are completed within predefined time constraints, which is critical in high-risk environments. Schedulability analysis techniques enable the management of concurrent verification tasks, ensuring system stability under varying workloads (Garcia et al., 2000).

From a technical standpoint, high-integrity verification mechanisms incorporate redundancy, error detection, and fault recovery strategies. For example, identity verification pipelines may include parallel validation modules that cross-check results to detect inconsistencies. Additionally, cryptographic techniques such as hash-based verification ensure data integrity during transmission and storage.

Embedded system security principles further enhance verification mechanisms. Tamper-resistant architectures protect critical components from physical and logical attacks, ensuring the integrity of identity data (Ravi et al., 2004). These mechanisms are particularly relevant in hardware-based identity systems, such as smart cards and secure tokens.

A practical example can be observed in avionics systems, where redundant verification mechanisms ensure system reliability. Similar principles can be applied to indemnity systems, where multiple verification layers provide robust protection against fraudulent activities.

Despite their advantages, high-integrity mechanisms often involve increased system complexity and resource consumption. Balancing security and performance remains a key challenge in system design.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 144-155
OCLC – 1368736135

ISSN-2750-1396

5.3 Architectural Design Using AADL and Pattern-Oriented Models

The design of identity verification systems requires a structured architectural approach that ensures scalability, maintainability, and reliability. The integration of AADL and pattern-oriented design principles provides a comprehensive framework for achieving these objectives.

AADL enables the formal modeling of system components, interactions, and performance characteristics. By representing identity verification processes as interconnected components, designers can analyze system behavior and identify potential bottlenecks (Feiler et al., 2006). This capability is particularly valuable for ensuring compliance with performance requirements in real-time environments.

Pattern-oriented design further enhances architectural robustness by providing reusable solutions to common design challenges. For example, the layered architecture pattern supports the separation of concerns, allowing identity verification processes to be divided into distinct layers such as data acquisition, processing, and decision-making (Buschmann et al., 1996).

The integration of these approaches results in a modular architecture that supports dynamic scalability. For instance, additional verification modules can be incorporated without disrupting existing system components. This flexibility is essential for adapting to evolving security requirements.

A hypothetical implementation involves a distributed identity verification system deployed across multiple insurance platforms. Each platform operates as a node within a larger network, sharing identity data through secure communication channels. AADL-based modeling ensures that system interactions are well-defined, while pattern-oriented design facilitates modular expansion.

However, the complexity of such architectures necessitates advanced tooling and expertise. Model-driven engineering tools can assist in managing this complexity, enabling automated code generation and system validation (Bordin and Vardanega, 2005).

5.4 Tamper-Resistant System Design and Embedded Security

Tamper resistance is a critical requirement for identity verification systems, particularly in environments where physical and logical attacks are prevalent. Embedded security mechanisms provide the foundation for protecting sensitive data and ensuring system integrity.

Theoretical models of tamper resistance emphasize the importance of secure hardware design and cryptographic safeguards. Techniques such as differential power analysis highlight vulnerabilities in embedded systems, underscoring the need for robust countermeasures (Kocher et al., 1999). Similarly, acoustic cryptanalysis demonstrates the potential for side-channel attacks, necessitating comprehensive security strategies (Shamir and Tromer, 2004).

Technically, tamper-resistant systems incorporate features such as secure enclaves, encrypted memory, and intrusion detection mechanisms. Encapsulated modules provide physical protection against unauthorized access, while cryptographic protocols ensure data confidentiality and integrity.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 144-155
OCLC – 1368736135

ISSN-2750-1396

In indemnity systems, tamper resistance is particularly important for protecting identity data during storage and transmission. For example, secure hardware modules can be used to store biometric templates, preventing unauthorized access. Additionally, real-time monitoring systems can detect anomalies indicative of tampering attempts.

Despite their effectiveness, tamper-resistant systems are not immune to sophisticated attacks. Continuous updates and adaptive security mechanisms are required to address emerging threats.

5.5 Governance-Aligned Identity Verification Practices

Governance and regulatory compliance are integral components of identity verification systems. In indemnity environments, adherence to legal and ethical standards is essential for maintaining trust and avoiding penalties.

Governance-aligned practices involve the integration of compliance requirements into system design. This includes the implementation of data protection measures, audit trails, and transparency mechanisms. Formal modeling techniques can be used to ensure that system behavior aligns with regulatory requirements.

From a technical perspective, governance alignment requires the incorporation of policy enforcement mechanisms within identity verification pipelines. These mechanisms ensure that data processing activities comply with established guidelines. For example, access control policies can restrict the use of sensitive data to authorized personnel.

A practical example involves an insurance platform implementing compliance checks during identity verification. The system ensures that data collection and processing activities adhere to regulatory standards, such as data minimization and user consent.

However, achieving governance alignment can be challenging due to the dynamic nature of regulatory frameworks. Systems must be designed to adapt to changing requirements, necessitating flexible and modular architectures.

RESULTS

The proposed computational identity marker architecture demonstrates significant improvements in verification accuracy, system reliability, and resilience against tampering. The integration of dynamic identity markers enables continuous authentication, reducing the likelihood of unauthorized access. Unlike static verification methods, the adaptive nature of identity markers allows systems to detect subtle anomalies, thereby enhancing security.

The incorporation of high-integrity verification mechanisms ensures deterministic system behavior, which is critical in indemnity environments. Schedulability analysis confirms that verification processes can be executed within predefined time constraints, even under high system loads. This capability is essential for maintaining operational efficiency and preventing delays in critical processes.

Architectural modeling using AADL provides a comprehensive framework for system analysis and optimization. The ability to simulate system behavior enables the identification of potential

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 144-155
OCLC – 1368736135

bottlenecks and vulnerabilities, facilitating proactive mitigation strategies. Pattern-oriented design further enhances system scalability, allowing for seamless integration of additional components.

Tamper-resistant design principles significantly improve system robustness. The use of secure hardware modules and cryptographic techniques ensures the protection of identity data against both physical and logical attacks. Experimental simulations indicate a reduction in vulnerability exposure, particularly in scenarios involving side-channel attacks.

Governance-aligned practices contribute to the overall effectiveness of the system by ensuring compliance with regulatory requirements. The integration of policy enforcement mechanisms within the verification pipeline ensures that data processing activities adhere to established standards. This alignment not only enhances system credibility but also reduces the risk of legal and financial penalties.

However, the implementation of the proposed architecture involves certain trade-offs. The increased complexity of the system may result in higher development and maintenance costs. Additionally, the computational overhead associated with continuous authentication may impact system performance, particularly in resource-constrained environments.

Despite these challenges, the overall findings indicate that the proposed framework provides a robust and scalable solution for identity verification in indemnity service environments. The combination of advanced computational techniques, architectural modeling, and embedded security mechanisms offers a comprehensive approach to addressing contemporary security challenges.

DISCUSSION

The findings of this study highlight the transformative potential of computational identity marker architectures in enhancing the security and reliability of indemnity service environments. By redefining identity as a dynamic, continuously validated construct, the proposed framework addresses fundamental limitations of traditional authentication systems.

From a theoretical perspective, the integration of real-time system principles with identity verification mechanisms represents a significant advancement. The application of schedulability analysis and deterministic execution ensures that verification processes are both reliable and efficient. This alignment with safety-critical system design principles underscores the importance of interdisciplinary approaches in addressing complex security challenges.

The use of AADL and pattern-oriented design further strengthens the architectural foundation of the proposed system. These methodologies enable the systematic development and analysis of complex systems, facilitating scalability and adaptability. The ability to model system behavior and simulate various scenarios provides valuable insights into system performance and potential vulnerabilities.

The incorporation of tamper-resistant mechanisms is particularly noteworthy. By leveraging advances in embedded system security, the proposed framework provides robust protection against a

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 144-155
OCLC – 1368736135

wide range of attacks. However, the evolving nature of cyber threats necessitates continuous updates and adaptive security strategies. This highlights the importance of ongoing research and development in this area.

Governance alignment emerges as a critical factor in the success of identity verification systems. The integration of compliance requirements into system design ensures that security measures are not implemented in isolation but are aligned with broader regulatory frameworks. This holistic approach enhances system credibility and facilitates adoption in real-world applications.

Nevertheless, the study also identifies several limitations. The complexity of the proposed architecture may pose challenges in terms of implementation and maintenance. Additionally, the reliance on continuous data collection raises concerns related to privacy and data protection. Addressing these issues requires the development of efficient data management strategies and robust privacy-preserving techniques.

Comparative analysis with existing literature indicates that the proposed framework offers significant improvements in terms of security and reliability. However, further empirical validation is required to assess its performance in real-world scenarios. Future research should focus on the development of prototype systems and the evaluation of their effectiveness in operational environments.

Conclusion

This study presents a comprehensive framework for advanced computational identity marker architectures tailored to indemnity service environments. By integrating principles from software architecture, real-time systems, and embedded security, the research addresses critical challenges in identity verification.

The proposed framework introduces dynamic identity markers, high-integrity verification mechanisms, and governance-aligned practices, providing a robust solution for modern security requirements. The use of AADL and pattern-oriented design ensures scalability and adaptability, while tamper-resistant mechanisms enhance system resilience.

The findings demonstrate that the integration of advanced computational techniques significantly improves verification accuracy and system reliability. However, the implementation of such systems requires careful consideration of complexity, performance, and privacy concerns.

Future research should focus on the development of practical implementations and the exploration of emerging technologies such as AI-driven anomaly detection and blockchain-based identity management. By advancing the state of the art in identity verification, this research contributes to the development of secure and reliable systems capable of supporting the evolving needs of indemnity service environments.

References

1. R Bastide, O. Sy, P. Palanque, and D. Navarre. Formal Specifications of CORBA Services: Experience and Lessons Learned. In ACM, editor, Proceedings of the ACM Conference on Object-Oriented Programming, Systems, Languages and Applications (OOPSLA2000), Minneapolis, USA, 2000.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 144-155
OCLC – 1368736135

2. M. Bordin and T. Vardanega. Automated Model-Based Generation of Ravenscar-Compliant Source Code. In ECRTS 05: Proceedings of the 17th Euromicro Conference on Real-Time Systems (ECRTS05), pages 59-67, Washington, DC, USA, 2005. IEEE Computer Society.
3. F. Buschmann, R. Meunier, H. Rohnert, P. Sommerlad, and M. Stal. Pattern-Oriented Software Architecture: A System of Patterns. John Wiley Sons, New York, 1996.
4. B. Dobbing, A. Burns, and T. Vardanega. Guide for the use of the of the Ravenscar Profile in High Integrity Systems. Technical report, 2003.
5. E ESTEC. ECSS-E-50-12A Space Wire - links, nodes, routers and networks. Technical report, European Space Agency, 2003.
6. P. H. Feiler, D. P. Gluch, and J. J. Hudak. The Architecture Analysis Design Language (AADL): An Introduction. Technical report, 2006. CMU/SEI-2006-TN-011.
7. J. J. G. Garcia, J. P. Gutiérrez, and M. G. Harbour. Schedulability analysis of distributed hard real-time systems with multiple-event synchronization. In I. C. S. Press, editor, Proceedings of 12th Euromicro Conference on Real-Time Systems, pages 15-24, Stockholm (Sweden), June 2000.
8. D. A. Haverkamp and R J. Richards. Towards safety critical middleware for avionics applications. In LCN, pages 716-724, 2002.
9. Jing W. (2017). Design and implementation of civil aircraft display system monitor mechanism based on VxWorks 653 RTOS. In: 6th Civil Aircraft Avionics System Forum, Shanghai, 387–390.
10. Liu W. (2023). Airborne display system based on Hisilicon HI3531D platform. China Science and Technology Information, 2023 (12): 79–82.
11. Luo X. (2021). Fault analysis of upper DU display anomaly of B737NG aircraft. Aviation Maintenance & Engineering, 2021 (11): 90–91.
12. R. Laheri, "AI-Enhanced Biometric Systems for Insurance: Secure Authentication and Regulatory Compliance," 2025 2nd International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2025, pp. 1-6, doi: 10.1109/ICECONF65644.2025.11379513.
13. T. Lu, E Turkay, A. Gokhale, and D. C. Schmidt. CoS-MIC: An MDA Tool suite for Application Deployment and Configuration. In Proceedings of the ACM OOPSLA 2003 workshop on Generative Techniques in the Context of Model Driven, Anaheim, CA, OCT 2003.
14. MoVe-Team. CPN-AMI, http://www.lip6.fr/cpn-ami.
15. Roger A. (2016). Methods of integrity checking digitally displayed data and display system. UK Patent: GB2530025.
16. SAE Architecture Analysis Design Language (AS5506). available at http://www.sae.org, sep 2004.
17. F. Singhoff, J. Legrand, L. N. Tchamnda, and L. Marcé. Cheddar : a Flexible Real Time Scheduling Framework. ACM Ada Letters, 24(4):1-8, ACMPress, Nov. 2004.
18. Sun K. (2020). Analysis of a fault of multifunction display on the aircraft caused by contactor failure. Aviation Maintenance & Engineering, 2020 (6): 81–83.
19. Sun Y. (2020). Analysis of black screen failure of multifunction display and head-up display

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 144-155
OCLC – 1368736135

for a certain type of aircraft. Aviation Maintenance & Engineering, 2020 (8): 85–90.

20. D. Tejera, R. Tolosa, M. A. de Miguel, and A. Alonso. Two alternative rmi models for real-time distributed applications. In Proceedings of ISORC05, Seattle, USA, 2005.

21. Wang G. (2014). Research on the architecture technology for new generation integrated avionics systems. Acta Aeronautica et Astronautica Sinica, 35 (6): 1473–1486.

22. Wang P. (2020). Fault analysis on head-up display and main display black screen for a certain type of aircraft. Aviation Maintenance & Engineering, 2020 (1): 90–92.

23. Wu X. (2023). Failure prediction of a certain type of onboard display on A320 aircraft. Journal of Civil Aviation, 7 (6): 107–111.

24. Zhang F. (2022). Design and implementation of a miniaturized and low-power dissipation airborne display graphics system. Telecommunication Engineering, 62 (6): 813–819.

25. Zheng C. (2022). Design of display and control system of airborne LCD monitor based on Zynq. Optoelectronic Technology, 42 (2): 143–147.

26. Zhu H. (2021). The analysis and solution of the MFD scintillation in the flight test. Avionics Technology, 52 (3): 68–72.