GLOBUS

Cosmos Journal of Engineering & Technology
A Refereed Research Journal
Vol 10 / No 1 / Jan-Jun 2020 ISSN: 2231-4210

A STUDY ON DEFENSE HIGH LEVEL ARCHITECTURE

*Varun Gupta

**Dr Sanjay Kumar

Paper Received: 06.07.2020 / **Paper Accepted**: 07.08.2020 / **Paper Published**: 08.08.2020
Corresponding Author: Varun Gupta; doi:10.46360/cosmos.et.620201013

Abstract

Défense-related robotics system integration has particular difficulties in terms of scale, coordination, and interoperability. The Department of Defence (DoD) has acknowledged the need for a standardised method to deal with these difficulties and make it easier for varied robotic platforms to cooperate and communicate in an efficient manner. The High-Level Architecture (HLA), a set of standards and recommendations for developing networked simulation systems, was created in response by the DoD. In order to improve interoperability and integration capabilities, the DoD HLA will be used to robotics software systems in this research.

Keywords: Defence, Architecture, DoD, DHLA.

Introduction

The Defence High-Level Architecture (DHLA) includes a number of essential elements that simplify the integration and interoperability of defence systems. These parts include the operational perspective, system view, and data view, which define, in that order, the operational concepts, the physical and logical parts, and the information flow within the architecture. For the purpose of assuring compatibility and seamless communication between various defence systems, technical standards and interoperability standards are essential. Data interchange is supported by a strong communication infrastructure, including networks and protocols. Information assurance protects the confidentiality and accuracy of data used in defence systems. The architecture is designed and evaluated with the use of modelling and simulation tools, and configuration management makes sure that modifications are properly controlled and tracked. Mechanisms for decision-making and compliance are established by governance and management procedures. Through the use of services, service-oriented architecture encourages modular and reusable design. Storage, retrieval, and sharing of data are handled through data management. Human-system integration maximises communication between people and defence systems, whereas mission assurance concentrates on dependability and performance.

Review of Literature

Jérémie (2016) [1] Modern robots that can communicate with people and carry out activities indoors, in healthcare facilities, or at business are about to become part of our daily lives. When certain systems behave dangerously due to malfunctions or harsh environmental circumstances, the results could be disastrous. Due to the unpredictable behaviour of those systems as they evolve in chaotic environments, well-known risk analysis techniques utilised in other important sectors (such as avionics, nuclear, medical, and transportation) must be extended or modified. Finding ways to identify risks brought on by robot duties and interactions with people from the very start of the creation process is thus a significant challenge.

(2012) Eleftheria [12]; There are several potential business uses for the expanding field of domestic robotics. Robotics systems have been effectively used in industrial production paths, but they must have greater reliability, robustness, and other specialised qualities to succeed in a dynamic residential context. When people live with and interact with robots, which is not too far off, safety will become the most important thing to keep an eye on. Regardless of potential failure, malfunction, or misuse, robot designers should create safe goods for humans. Therefore, household robots should also follow the appropriate safety procedures. The most difficult task is to maintain human safety without sacrificing even a small amount of the effectiveness needed to complete any work. Although the authors do not want to replace any existing robot security norms or guidelines, they discuss the necessity for safety rules in domestic robotics in this technical communication.

However, the work that is suggested may serve as an addition to the standards. Since there are no special safety standards for home robots, we

* *Research Scholar, Kalinga University, Naya Raipur, India.*
***Supervisor, Kalinga University, Naya Raipur, India.*

suggest that their safety be verified based on widely used standards that have been created in other fields and addressed here. A standard for household robots can be created based on the communication at hand. In order to attain an adequate degree of protection in domestic robots, it also suggests an integrated strategy that explicitly links the framework and user needs to an array of safety challenges. Asimov made reference to the need for security when using robotics technology as early as 1942. However, scientists have already determined that Asimov's three laws alone are insufficient to explain robot behaviour. Modern industrial robotics standards set clear guidelines for robots and the environment in which they operate.

Analysis

The Defence High-Level Architecture (DHLA) is a framework that gives the design and integration of simulation-based systems used in the defence industry a standard structure and set of rules. It is a technological standard created by the US Department of Defence (DoD) to support the reuse and interoperability of simulation systems across many military domains. Listed below are the Defence High-Level Architecture's (DHLA) main features:

Object-Oriented Modelling: To represent the elements and entities in a simulation environment, DHLA encourages the use of object-oriented modelling approaches. In order to specify the simulated entities and their interactions, it places a strong emphasis on the use of common object-oriented notions like classes, objects, properties, and behaviours.

Federated Architecture: DHLA uses a federated architecture strategy in which many simulation systems-referred to as federates-communicate and work together to build a bigger, more integrated simulation system. Platforms, sensors, entities, or environments are just a few examples of the various parts and pieces that each federate represents in the larger system. To achieve synchronised simulation, the federates communicate by exchanging data and messages.

Run-Time Infrastructure (RTI): In the DHLA framework, the Run-Time Infrastructure is a software element that permits data interchange and communication across federates. Message routing, time management, synchronisation, and data distribution are just a few of the administrative functions the RTI offers for the simulation federation. It guarantees that the federates can communicate and share information in an organised way.

The DHLA focuses on achieving data delivery and interoperability between federates. In order to ensure that the simulated entities can communicate successfully, it establishes standardised protocols and processes for sharing data and messages. The DHLA Data Distribution Management (DDM) specification offers recommendations for federate-to-federate data sharing and synchronisation.

Time Management: To maintain synchronisation and coordination among federates, time management is a crucial component of DHLA. Despite being dispersed across many computing platforms, the federates can still operate in unison because to DHLA, which defines a standard time reference known as the Logical Time. The RTI offers services for controlling logical time and dealing with interactions involving time.

The usage of standardised simulated Object Models (SOMs) to describe particular types of simulated entities, like as platforms, sensors, or weapon systems, is supported by DHLA. SOMs give definitions of the characteristics, actions, and interactions of simulation objects a common language and structure. They make it possible for simulation components to work together and be reused in various simulations.

Standards Compliance: To guarantee compatibility and interoperability with other simulation frameworks and tools, DHLA complies with a number of industry standards and specifications. To facilitate easy connection with other simulation systems and environments, it adheres to standards including the High-Level Architecture (HLA), Distributed Interactive Simulation (DIS), and IEEE Standard for Modelling and Simulation (M&S).

IDSs (intrusion detection systems) are security tools that keep an eye on system or network activity in order to spot and stop unauthorised access, intrusions, or other suspicious activity. They examine system logs or network packets and produce alerts or take steps to reduce potential security breaches.

Access Control: To limit and regulate user access to systems, networks, or physical locations, access control mechanisms are utilised. To ensure that only authorised people or entities can access sensitive information, this comprises authentication techniques (such as passwords and fingerprints), authorization processes, and privilege management.

Network security tools known as firewalls monitor and regulate incoming and outgoing network traffic in accordance with pre-established security standards. They provide as a barrier, prohibiting unauthorised access and defending against

network-based threats, between trusted internal networks and unreliable external networks.

Using information that is unreadable or incomprehensible to unauthorised users, cryptography is the practise of safeguarding communication and data. In order to guarantee the confidentiality, integrity, and validity of data, it also incorporates encryption methods, digital signatures, and secure key management systems.

SIEM systems gather, correlate, and analyse security event logs and data from numerous sources inside an organization's IT architecture. To improve the total security posture, they offer real-time monitoring, threat detection, incident response, and compliance reporting.

Systematic evaluation and identification of vulnerabilities in systems, networks, or applications is the goal of vulnerability assessment and penetration testing (VAPT). While vulnerability assessments look for flaws, penetration testing simulates actual attacks in order to evaluate the target system's security and resilience and to suggest countermeasures.

tangible Security Systems: Personnel, facilities, and tangible assets are all protected by physical security systems. To stop unauthorised access, theft, or damage, these technologies include surveillance cameras, access control systems, biometric systems, perimeter security measures, alarms, and physical barriers.

Threat intelligence is the process of obtaining and analysing data on prospective threats, such as malware, vulnerabilities, and newly developed attack methods. Organisations can use it to better understand the threat landscape, evaluate risks, and implement preventative security measures.

Detecting, analysing, and responding to security incidents, such as online assaults or data breaches, is the process of incident response. It entails the detection of incidents, their containment, elimination, and recovery. Digital data connected to security events is investigated and analysed using forensic techniques.

Security Policies and Compliance: Security policies outline the methods, standards, and laws that organisations must abide by in order to maintain security. To protect sensitive data, uphold privacy, and comply with legal and regulatory obligations, compliance requires complying to pertinent rules, industry standards, and best practises.

To increase the efficiency and efficacy of simulation-based systems used in defence applications, the Defence High-Level Architecture (DHLA) was created. It offers a standardised architecture for creating, incorporating, and running simulations, facilitating interoperability, reusability, and scalability across a variety of defence domains and applications. Security procedures and approaches used to protect the confidentiality and integrity of defence systems, networks, and infrastructure are referred to as defence architecture security. It entails the development, application, and maintenance of security policies and procedures to safeguard critical defence data, resources, and operations against unauthorised access, breaches, or halts. These are important defence architecture security points:

Threat Mitigation: The security of the defence architecture tries to find and address potential threats and holes in the defence systems. To analyse security risks and implement suitable countermeasures, this includes conducting risk assessments, vulnerability assessments, and threat modelling.

Defence architecture security uses a multi-layered defence strategy that incorporates various security controls at various levels. Intrusion detection and prevention systems, firewalls, access controls, encryption, network segmentation, and physical security measures are all included in this.

Secure Communication: Defence architecture security is concerned with protecting the lines of communication between persons, networks, and defence systems. To safeguard sensitive data and guarantee secure transmission and exchange of information, this entails the use of encryption, secure protocols, and virtual private networks (VPNs).

Access Control: To enforce authorised access and prevent unauthorised individuals or organisations from accessing sensitive defence systems and data, access control methods are crucial to the security of defence architecture. Strong authentication procedures, role-based access restrictions, and stringent user privilege administration are all part of this.

Defence architecture security requires strong incident response capabilities to identify, address, and resolve security lapses or occurrences. Establishing incident response plans, running drills, and putting systems in place for incident monitoring, analysis, and mitigation are all part of this.

Security Governance: A defence architecture's security depends on efficient security governance.

In addition to defining roles and duties for security management, this entails setting security policies, processes, and standards. Compliance with security standards and laws is guaranteed by routine security audits and compliance evaluations.

Defence architecture security also includes physical security measures in addition to digital security measures. To safeguard defence facilities, data centres, equipment, and key infrastructure from unauthorised entry or physical threats, this comprises access controls, surveillance systems, alarms, and physical barriers.

Secure Supply Chain: The security of the supply chain involved in acquiring and integrating defence systems is taken into account by defence architecture security. To avoid manipulation or intrusion, this includes screening vendors, ensuring the integrity of components, and putting secure configuration management procedures into place.

Defence architecture security places a strong emphasis on ongoing system, network, and data monitoring in order to quickly identify and address security incidents or anomalies. To be watchful against new attacks, this includes security information and event management (SIEM) systems, log monitoring, and threat intelligence.

Compliance and Regulation: Defence architecture security makes sure that all applicable security laws, standards, and best practises are followed. This involves adhering to export control laws, international security agreements, and security standards related to the defence industry.

Defence organisations may defend key assets, preserve operational readiness, and protect national security interests from attacks and dangers by putting in place strong defence architecture security measures.

Conclusion

Collaboration, growth, and adaptation are made possible by scalability, flexibility, and interagency interoperability. The architecture is tested and evaluated, modifications are managed through configuration control, and user comprehension is supported by training and documentation. Lifecycle management takes into account a defence system's whole lifespan. Together, these elements offer a thorough framework for planning, creating, and overseeing defence systems within the DHLA, facilitating interoperability, efficacy, and longevity. The Defence High-Level Architecture (DHLA) is a framework that makes it easier for different defence systems and parts to integrate and communicate with one another. The following are the main elements commonly present in a DHLA, though specific components may differ depending on implementation and context:

Operational View: The operational concepts, goals, and specifications of the defence system are defined by this component. It comprises identifying the missions, responsibilities, and duties that the architecture must serve.

System View: The defence system's logical and physical components are described in the system view. It covers the naming of subsystems, their interfaces, and the information passed back and forth. The network infrastructure, software, and other components necessary to support the defence system are also included in the system view.

Data View: The information flow within the defence system is the main topic of the data view. It describes the many kinds of data, their formats, and the ways that data is exchanged. Data standards and protocols for interoperability are also included in the data view.

Technical Standards: For easy integration and interoperability, DHLA contains technical standards that specify common protocols, interfaces, and data formats. These standards guarantee effective information exchange and communication between various defence systems.

Information Assurance: Information assurance plays a key role in DHLA by assuring the security, confidentiality, availability, and integrity of information related to defence systems. It contains safeguards against unapproved access, data breaches, and online dangers.

Interoperability Standards: Interoperability standards define the rules and requirements for information sharing and the fusion of various defence systems. Systems from many suppliers or organisations can cooperate smoothly thanks to these standards.

The DHLA needs a strong communications infrastructure to support the interchange of data and information between various systems and components. This covers networks, protocols for communication, routers, switches, and other networking hardware.

Designing, testing, and assessing the DHLA all need the use of modelling and simulation techniques. They make it possible for system developers to evaluate the performance of the architecture, spot potential problems, and improve system behaviour.

Configuration management: Configuration management makes ensuring that modifications made to the DHLA components are properly controlled and tracked. Version control, documentation management, and upholding uniformity across various system configurations are all part of it.

Governance and Management: The successful implementation and upkeep of the DHLA depend on efficient governance and management procedures. This includes developing decision-making procedures, defining roles and duties, and ensuring standards and rules are followed.

Service-Oriented Architecture (SOA): SOA is a design philosophy that encourages modularity and loose coupling. It enables the division of defence systems into smaller, independent parts known as services. These services are easily reusable and shareable, which improves the DHLA's interoperability and flexibility.

Data Management: In the DHLA, efficient data management is essential. It contains procedures for data storing, retrieving, and processing as well as data exchange and synchronisation between various systems. The availability of correct and timely information to assist defence activities is ensured by data management components.

Mission assurance is concerned with making sure that the defence systems in the DHLA can carry out their intended purposes consistently and successfully. It entails taking steps to recognise hazards, lessen their impact, keep systems available, and support continued operations even in difficult circumstances.

The integration of human operators, interfaces, and decision-support tools within the DHLA is the focus of the human-system integration component. It optimises the interaction between people and the defence systems by taking into account human variables like user interfaces, usability, and cognitive workload.

Scalability and Flexibility: The DHLA needs to be flexible enough to account for future expansion and changing needs. The architecture must be scalable in order to support growing system capabilities, higher data volumes, and increased workloads. New technologies can be incorporated and operating requirements can be changed with the help of flexibility.

Organisational and Coalition Interoperability: Cooperation with allies and other organisations is essential in multinational defence operations. The DHLA should have elements and controls that allow for easy data sharing, coordination, and communication with outside parties, fostering cooperation and collaborative operations.

Testing and Evaluation: To validate the DHLA and its components, sound testing and evaluation procedures are crucial. To make sure that the architecture satisfies the necessary goals and objectives, this includes carrying out functional testing, performance testing, security assessments, and other verification and validation activities.

Changes to the DHLA and its components must be managed in a controlled and methodical manner thanks to configuration control. To preserve the integrity and coherence of the architecture, it entails recording and tracking changes, doing impact analyses, and putting change management procedures into place.

Training and Documentation: The successful deployment and operation of the DHLA depend on adequate training and documentation support. To help users comprehend and effectively use the defence systems, this component also comprises training materials, user manuals, system documentation, and knowledge transfer procedures.

Lifecycle Management: The DHLA should take into account every stage of the development, deployment, operation, and eventual retirement or replacement of the defence equipment. The architecture is continuously improved, maintained, and sustained with the use of lifecycle management components.

These extra parts help the Defence High-Level Architecture assist defence operations and achieve interoperability among many systems and stakeholders while also enhancing its overall functionality, effectiveness, and durability. Together, these elements offer a thorough framework for planning, creating, and overseeing defence systems under the Defence High-Level Architecture.

Conflict of Interest

There is no conflict of interest between the authors in this manuscript.

References

1. Guiochet, Jérémie (2016). Hazard analysis of human-robot interactions with HAZOP-UML. Safety Science, 84, 225-237.
2. Portugal, D., Santos, M.A., Pereira, S., Couceiro, M.S. (2018). On the security of robotic applications using ROS. Artificial Intelligence Safety and Security, Chapman and Hall/CRC, 273-289.
3. Demir, Kadir Alpaslan (2009). Challenges of

Weapon Systems Software Development. Journal of Naval Science and Engineering, 5(3), 104-116.
4. Maguri, Dr. Ramesh (2015). A Quick Review on Cloud Computing and Related Security Issues. Cosmos An International Journal of Management, 4(2), 1-4.
5. Singh, Navdeep (2014). A Study on Cooperative Defense Against Network Attacks. Cosmos Journal of Engineering & Technology, 4(2), 1-4.
6. Kumar, Praveen (2014). A Study on Cloud Computing. Cosmos Journal of Engineering & Technology, 4(2), 1-3.
7. Anuradha (2015). Study in Technological Challenges in Digital Libraries. Cosmos An International Journal of Art & Higher Education, 4(2), 9-11.
8. Goel, Agarwal, Nidhi (2008). A Global Change in Education through Information Technology and Communication. Enterprises Information Systems & Technology, Mac Millan Advanced Research Series, ISBN: 13: 978-0230-63516-6, pp. 124-126.
9. Mishra, Dr. Pramod and Sharma, Pradeep Kumar (2018). Digital Literacy Competencies in The 21st Century. Globus Journal of Progressive Education, 8(2), 1-3.
10. Kumar, Puneet (2008). A Comparative Study of Information System's Security by using Graphs. Enterprise Information Systems & Technology, MacMillan India Ltd., 222-227, ISBN 0230-63516-4.
11. Vashishtha, Dr. Sangeet and Sharma, Pooja (2018). Big Data- New Trend of Change in Complex Corporate World. Globus An International Journal of Management & IT, 10(1), 4-6.
12. Mitka, Eleftheria, Gasteratos, Antonios, Kyriakoulis, Nikolaos & Mouroutsos, Spyridon G. (2012). Safety certification requirements for domestic robots. Safety Science, 50(9), 1888-1897.