FRAMEWORK FOR IDENTIFYING REQUIREMENTS IN THE DESIGN OF MULTI-DOMAIN COMMAND & CONTROL INFORMATION SYSTEM FOR TRI-SERVICE INTEGRATION

by **ME5 Chua Zhongwang**

Abstract:

This essay examines the challenges in designing a Command and Control Information System (CCIS) that shortens the Observe-Orientate-Decide-Act (OODA) cycle for an integrated Armed Force. This involves the co-ordination of air, land and sea assets of the Armed Forces, as well as cyber security necessary to ensure the robustness and resilience of the system. The mission-domains requirements of the CCIS and the impact of the environment and tactical operations at the different air-land-sea physical domains are examined in-depth. The essay also proposes a framework in the Requirement Analysis to achieve comprehensive requirements for CCIS system design across multi-domain operations.

Keywords: Command & Control; Communications; Information; Domain; Planning

INTRODUCTION

With the changing global landscape, the military's role has evolved from preparing and fighting the conventional war, to one that includes combating terrorism in counter-insurgencies operations, peace-keeping operations and Humanitarian Aid and Disaster Relief (HADR) operations. These operations often require the co-ordination of forces between different services in deploying air, land and sea assets in the Operational Theatre. To effectively command and control these forces, a common CCIS will be needed across the services to provide a Common Operating Picture (COP). In this essay, the author proposes a framework for identifying requirements in the design of such a CCIS system for different mission roles that spans across the air, land and sea domains, as well as in addressing the issue of cyber security to achieve a robust and resilient network with high capacity throughput.

IMPETUS

There is a rising trend of integrated operations where air, land and sea assets are employed in the same Operational Theatre to achieve mission success. Operation Desert Storm is an excellent example of this, where different assets from different services and nations are effectively deployed to achieve mission success in a short timeframe.[1] With this shift in operational focus, there is a strong impetus for the military to strengthen Command and Control of forces in different physical domains to enable a swift and decisive victory.

There is a rising trend of integrated operations where air, land and sea assets are employed in the same Operational Theatre to achieve mission success.

Achieving Information Superiority is another critical success factor in the modern battlefield. The military that is able to 'See First and See More' will gain significant advantages over the enemy and achieve mission success. This is best articulated in the article from Riscassi on the 4 key tenets to successful joint operations as stated below:[2]

1. Agility – Swift response and seize opportunities.
2. Initiative – Shorten OODA cycle and act first.
3. Depth – Pervasive awareness across entire spectrum of operations.
4. Synchronisation – Achieve common understanding and seamless operations outcome.

Another key aspect in the development of a robust and resilient CCIS system is in the area of cyber security.

An effective CCIS is identified as a key enabler to achieving the four tenets above. A well-designed CCIS will provide decision-makers with the COP for Pervasive Battlefield Awareness and decision-support algorithm for Superior Decision-Making.[3] When deployed to the frontline troops, the CCIS provides timely communications and effective task assignment to the different forces, preventing fratricide and enabling time-sensitive targeting.

LITERATURE RESEARCH

Timely, accurate and secured information form the basis for decision-making and is critical for the overall success of any military operations. In the article *'Air Force Aerial Layer Networking Transformation Initiatives'*, the authors highlighted the need for enhanced connectivity and collaboration as the top force multipliers.[4] In addition, the authors emphasised that multi-Service missions with dynamic operations will be more common resulting in an exponential rise in information nodes due to the increasingly complex and demanding operational environment. As a result, there is a greater need for higher bandwidth and automated decision support systems in the design of a CCIS.

These similar points are also articulated in the paper *'Army CCIS Requirements Definition'*.[5] Specifically, the author identified particular problems in the development of the land-based CCIS for the Army. These include constraints imposed by the environment and the large number of units in theatre (relative to other services) that the Army commands.

In the Navy, similar arguments can be found. In particular, the challenges for CCIS design in naval communications are expressed in the article, *'U.S. Navy Mass Communications Options.'*[6] Here, the authors focused on the uniqueness of naval operations far from land and without networking infrastructure. As a result, there is a particular need for the navy to invest in developing robust communications based on Beyond-Line-Of-Sight (BLOS) technologies.

Another key aspect in the development of a robust and resilient CCIS system is in the area of cyber security. With the CCIS being a highly networked system-of-systems, any cyber attack on the CCIS will result in crippling effects on the overall sense-making and decision-making capabilities of the military. In his article 'Cyber Threat – A Global Security Threat', the author highlighted a possible cyber defence framework to protect, detect and respond to cyber threats.[7]

BROAD REQUIREMENTS FOR TRI-SERVICE CCIS IN DIFFERENT MISSION-DOMAINS

The CCIS fulfils three key missions during military operations — 1) Strategic Planning, 2) Operational Control, and 3) Tactical Communications. As such,

the functional Operational Requirements in the development of a joint CCIS must satisfy the operational needs that are unique to each of the three mission-domains. Here, a framework is proposed to elicit broad functional Operational Requirements that effectively and comprehensively defines the CCIS:

1. Strategic Planning. The CCIS is utilised by Senior Commanders to sense-make the current progress of the war-campaign. To fulfil this requirement, the CCIS must be able to maintain overall situation awareness of the friendly forces and potential enemy threats. The CCIS must have the flexibility to provide Senior Commanders with different Situation Pictures, from overall force deployment plans to logistics support plans and be equipped with Decision Support logic for large force employment planning. The CCIS will need to have the bandwidth and reach for the Senior Commanders to command and control the Operational Units in theatre, as well as information aggregation for effective decision-making. With up-to-date common situation pictures, the Senior Commanders will be better equipped to analyse and predict enemy's course of actions, and more effectively deploy own forces to achieve success in the overall campaign.

2. Operational Control. At the operational level, there is a need for Commanders to co-ordinate and control their forces in achieving each mission. Here, the CCIS will need to track positions of all friendly forces and enemy threats with a higher resolution and faster refresh rate, for effective control of the troops and assets in the theatre. In addition, the CCIS network will need to be pervasive and resilient to


Cyberpioneer

2WO Sathiaseelan operating the Software Defined Radio (SDR) mounted on an Operations Utility Vehicle.

enemy's actions, such as jamming or spoofing, which will render the system ineffective for operations. With information received from the tactical-level units through the CCIS systems, the Operational Headquarters (HQ) will able to achieve pervasive battlefield awareness and execute superior decision-making to deploy resources to maintain an edge over the enemy. This capability will provide a Commander with dynamic operational control of his unit, enabling real-time tasking and re-role. For example, a fighter on a Precision-strike mission can be effectively deployed to provide Close Air Support (CAS) for ground troops that are under enemy attacks.

3. Tactical Communication. The CCIS will be deployed to the troops and assets (such as aircraft, tanks and Navy vessels) on the frontline who will be executing the mission. Here, the CCIS is required to provide timely and accurate updates to the troops with information such as friendly forces' and enemy forces' locations. As the troops are executing the missions and maneuvers, the CCIS must have a high refresh rate for timely updates and high resolution to discern between friendly and enemy forces. With the integration of the CCIS and remote sensors (such as radar), the troops will have real time tracking for friendly and hostile forces, enabling effective tactical operations while preventing fratricides. For example, with CCIS connectivity, the ground forces will be able to call in air-support with detailed position marking.

BROAD REQUIREMENT OF CCIS IN DIFFERENT PHYSICAL-DOMAINS

In addition to the requirements arising from the different mission domains of CCIS, the CCIS design is also greatly influenced by environmental factors for tactical operations in the different air-land-sea domains and the requirement for interconnectivity between them. As the key information highway, the CCIS must also be strengthened in the area of cyber security. In this regard, the challenges and requirements in the 4 different domains are indicated in the following paragraphs.

Air Domain

In the air domain, the air assets, mainly aircraft, are moving at a much higher speed as compared to the land and sea forces. As such, for effective sense-making, there is a need for the system to maintain a high refresh rate, especially at the tactical level. In addition, air assets typically operate at a greater distance from the Operational HQ as compared to land forces and there is a need for airborne CCIS to achieve greater range to account for distance and altitude. This is further coupled by the fact that relays may not be readily set-up in the air if there are no airborne command and control assets available. As such, air-borne CCIS will need to achieve high bandwidth with strong signal transmission and reception.

In addition, the modern fighter aircrafts are designed to be sleek and compact and are capable of high altitude and high-G maneuvers. As a result of the aircraft design, there are often size constraints for airborne CCIS equipment. The equipment must also be designed to meet operational specifications at high altitude and high stress environment due to G-loading.

Land Domain

In the land domain, the troops may be equipped with man-portable size CCIS equipment for information-gathering. With the man-portable remote sensors, the troops can track the positions of friendly and enemy forces to effectively engage hostility and allow the troops to navigate accurately through the terrain and avoid known danger areas. In addition, as the land

Minister for Defence, Dr Ng Eng Hen (left,) and Mrs Ng being briefed by Lieutenant Colonel Chew Chun-Chau, Head of RSN's LMV Project Office, during a tour of the ship's Integrated Command Centre.

forces fight in different unit sizes, from a Squad of special forces, to company-size and battalion-size attack forces, as well as tanks and other armoured vehicles, there is a need for customisation in CCIS equipping for the different forces.[8] For example, a Company Commander will need access to more information as compared to the Squad Commander; and a tank can have larger equipment with larger range that can function as a relay, as compared to the man-portable set.

In addition to the requirements arising from the different mission domains of CCIS, the CCIS design is also greatly influenced by environmental factors for tactical operations in the different air-land-sea domains and the requirement for interconnectivity between them.

One key environmental factor in the development of land-based CCIS equipment is the issue of line-of-sight (LOS). For example, connectivity of CCIS can be easily degraded by the lack of LOS in the dense forests in the tropics, or by buildings and enclosed environment in an urban setting, and the CCIS equipment must have the transmission and reception capabilities under such environmental constraints.

Another important factor for front-line tactical CCIS is ruggedness. Land operations, unlike air or sea, can take place under very different environmental conditions, such as torrential rains, dry hot deserts or in ice-cold winter. The equipment may also be subjected to rough handling and hard-knocks due to the nature of land operations. As such, the equipment must be designed to operate under these conditions.

Sea Domain

In the sea domain, the naval vessels may be deployed to open oceans far away from the mainland. As a result, there is a lack of communication network infrastructure or relay nodes between the naval vessels and the Operational HQ. Here, the key environmental challenge in the sea domain is in achieving sustained BLOS communications and options such as High-Frequency Radio, Military or Commercial Satellite communications will need to be considered for implementation.[9]

In addition to BLOS, the naval equipment will need to be designed for operations in sea-water conditions with high humidity and high salinity, as well as motions induced by sea waves. The resulting CCIS equipment for shipborne operations needs to be qualified and environmentally-tested differently from airborne or land equipment.

Cyber Security

The CCIS is a system-of-systems comprising different sensors and information nodes. This is achieved through a network of wired and wireless connections, using network and communication protocols. As such, the system, if not designed against cyber attacks, will be vulnerable to enemy actions. Here, the CCIS network will need to be protected against different kind of attacks, namely, 1) Information Gathering, 2) Information Denial and 3) Information Spoofing.

To address the issue of cyber security, the CCIS will be required to be designed with, 1) Message Security whereby messages are encrypted and protected to prevent information loss when messages are intercepted, 2) Transmission Security such as the use of Electronic Counter-Counter Measures (ECCM) techniques in waveform generation to prevent Jamming, and 3) Physical Security such as the use of Firewalls and physical safeguards in CCIS equipment.

FRAMEWORK FOR REQUIREMENT IDENTIFICATION

The proposed framework takes into account the mission-domain and physical-domain in which the CCIS will be operating, and identify categories of requirements applicable in system design.

Operational Role	Range of Coverage	Resolution of Systems	Redundancy of System	Physical Ruggedness	Refresh Rate
Strategic Planning	Long-Range (All forces across different countries).	Lowest – Aggregated Information at Divisional level.	Highly Redundant with fixed installation and backup systems.	Least as the equip is setup in protected Command Post	Lowest –Aggregated information and long term planning.
Operational Control	Mid-Range (All forces In-theatre).	Mid-range – Aggregated information at Squadron, or Flight level.	Mobile Setup with relative redundancy and backup of critical systems.	Mid-range as the setup may not be well-protected	Mid-range – Decision planning for immediate operations.
Tactical Comms	Short-Range (Forces at current mission).	Highest – resolution at individual and asset level.	Low Redundancy with backup provided by nearby friendly unit.	Highest as the equipment is exposed to the environment.	Highest – Report real-time changes for immediate actions and preventing fratricide.

Table 1: Mission-domain Related Requirements

	Environmental Effects	Operational Effects
Air	Altitude: - Design for transmission and bandwidth. - Hermetically sealed.	High-G Manoeuvre: - Ruggedness requirement. - G-tolerance requirement. Aircraft Size and Weight & Balance: - Limits physical dimensions and weight.
Land	Geographical: - Affecting Line-Of-Sight transmission (urban setting, forests). - Wide range of environmental condition (desert heat, cold winter). - Wide temperature range, and water-proofing requirements.	Decentralised C2: - Customisation for different users (Division Comd vs Company Comd vs Squad Leader). - Possible rough handling in a rugged environment.
Sea	Sea Environment: - High humidity and salinity. - Lateral motions induced by waves - Water-proofing Requirements - Ruggedness Requirements.	Far from Land: - Deploy far from fixed infrastructure. - Require robust Beyond-Line-Of-Sight communications.
Cyber	Pervasive across all deployed system: - Protect Against Information Gathering, Information Denial and Information Spoofing. - Message Security, Transmission Security, Physical Security Requirements.	

Table 2: Physical-Domain Related Requirement for Tactical Operations

In addition to requirements arising from the CCIS mission roles and physical-domains specific requirements, the CCIS will need to be designed with the following considerations:

1. Survivability. The CCIS shall maintain system integrity with a robust network such that there is no single point of failure—i.e. loss of individual nodes will not result in loss of entire network.

2. High Capacity. The CCIS shall be able to host and gather information from the respective units, using sub-networks as necessary to gather force-level information across different services and in different operational theatres.

3. Modularity. Due to the changing nature of today's operations, the CCIS shall be designed to be modular such that only necessary modules will be deployed in theatre. This is to enhance flexibility, while reducing deployment costs.

4. Decision Support. The CCIS provides an information rich environment for the decision-makers. However, this information glut may result in information overload, with delays in decision-making. To be effective, the CCIS shall be equipped with decision support algorithm to enable superior decision making.

5. Accuracy. Low Data Error Rate to ensure accuracy of transmitted information and tasking. In addition to effective communications, high accuracy will also strengthen the users' trust in the systems.

6. Reliability. The CCIS plays a critical role in today's military and a loss in CCIS capability may result in significant deterioration in the decision-making process. As such, the system shall be designed with a high reliability and availability. This, coupled with the redundancy in the system, shall provide the military with round-the-clock CCIS connectivity.

7. Maintainability. The CCIS equipment, especially equipment deployed to front line units, shall be highly maintainable to allow in-theatre repairs and servicing. For example, the systems shall be designed with low Mean-Time-To-Repair, and the maintenance tasks can be achieved using commonly-available tools.

8. Electro-Magnetic Interference/ Electro-Magnetic Compatibility (EMI/EMC). The tactical CCIS equipment will be deployed with the troops in operations. As a result, the equipment will be operating near explosives or ammunitions areas. As some of the CCIS equipment may have high power transmissions, CCIS equipment shall pass EMI/EMC testing prior to deployment for operational safety.[10]

9. Ease of Use. The CCIS must be user-friendly and allow users to operate the systems with minimal training. In addition, for tactical CCIS, the systems must be ergonomically-designed, especially in a high-tempo and high-stress operational environment.

10. Cost Effectiveness. Lastly, given the multitude of development and integration required in delivering the CCIS capability, Cost Effectiveness is a key consideration during the design process.

CONCLUSION

With a better understanding of the roles fulfilled by the CCIS and the environmental constraints affecting the tactical deployment of CCIS systems and equipment, the writer of this essay proposes a framework to identify requirements that are critical in the design of a tri-service CCIS. The writer feels that the framework will be useful during the Requirement Elicitation and Requirement Analysis phase of CCIS development to derive a baseline set of system requirements. It is important to recognise that the framework is not stagnant and will be enhanced as operational needs changes and new domains added. In this regard, further research can be conducted to include Space-Domain into the framework, and to expand scope in the Cyber domain.

ENDNOTES

1. P. Mason Carpenter, "Joint Operations in the Gulf War: An Allison Analysis". 1995.
2. Robert W. Riscassi, "Principles for Coalition Warfare," *Military Review*, v._ 73, n._ 6, 1993.
3. Singh, Ravinder; Tay, Andy; Ong, Melvyn; Lee, Jacqueline, "*IKC2 for the SAF: Organising around Knowledge*" POINTER, n._ 2, 12-18, 2007.
4. Schug, T.; Dee, C.; Harshman, N.; Merrell, R., "Air Force Aerial Layer Networking Transformation Initiatives," in Military Communications Conference, 2011, 1974-1978.
5. Kroening, Donald W., "Army Command and Control Information Systems Requirements Definition," *Systems, Man and Cybernetics, IEEE Transactions*, v._ 16, n._ 6, 974-979, 1986.
6. Breitler, A.L.; Nguyen, H.Q., "US Navy Mass Communications Options," Military Communications Conference, Conference Record, *IEEE*, v._ 3, 1093-1097, 1995.
7. Seah, S. T, "Cyber Threat – A Global Security Threat," *POINTER*, v._ 41, n._ 3, 51-63, 2015.
8. Ibid.

9. Ibid.

10. Eliardsson, P.; Axell, E.; Stenumgaard, P.; Wiklundh, K.; Johansson, B.; Asp, B., "Military HF communications considering unintentional platform-generated electromagnetic interference," in *Military Communications and Information Systems (ICMCIS), 2015 International Conference on*, 1-6, 2015.

ME5 Chua Zhongwang was awarded the Academic Training Award and graduated from National University of Singapore in Mechanical Engineering (1st Class Honours). He also completed his dual Masters' degree under the Master of Defence Technology and Systems Programme, where he was the top student for the course. ME5 Chua is an Air Force Engineer by vocation and is currently Branch Head in Air Engineering and Logistics Department. His previous appointments include OIC in Air Logistics Squadron, Changi Air Base, OC in 5th Air Engineering and Logistics Group, and Staff Officer in HQ, Air Power Generation Command.